



DNSSEC Key Ceremony Script Friday, July 8, 2016



Sign In to Facility

Step	Activity	Initial	Time (PDT)
1	FO has all participants sign in on Facility Sign-In Sheet before entering the Key Management Facility.	dch	9:22am
2	FO reviews emergency evacuation procedures and other relevant information with participants.	dch	9:22am
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.	dch	9:22am
4	FO verifies the functioning of audio and video recording.	dch	9:22am

Enter the Key Management Facility

Step	Activity	Initial	Time (PDT)
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.	dch	9:35 a.m.

Ground Rules

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

Verify Time and Date

Step	Activity	Initial	Time (PDT)
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>July 8, 2016</u></p> <p>Time: <u>16:38 UTC</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>	<i>ACH</i>	9:39

Verify UPS

Step	Activity	Initial	Time (UTC)
8	<p>If there is a UPS (uninterruptible power supply), then</p> <ul style="list-style-type: none"> - CA verifies that the UPS is connected to and receiving power from the electric grid and that it is charged. - CA verifies that the audio recorder is receiving power from the UPS. 	<i>ACH</i>	16:39

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
9	<p>SC opens the safe and records this action as an entry in the safe's log sheet.</p>	<i>ACH</i>	16:40

<p>10</p>	<p>SC collects the following items from the safe:</p> <ul style="list-style-type: none"> - KSK-HSM-01B-SJC HSM - boot-DVD - laptop <p>...and any other items that may be required, indicating removal of each with any applicable TEB or serial numbers in the safe's log sheet. SC also provides any necessary power supplies and cables. Equipment is placed on the work surface visible to all participants.</p> <p>If the immediately preceding key ceremony was also held in this same facility, the HSMFD is also collected from the safe. If the preceding key ceremony was performed in a different facility, any HSMFD from the preceding key ceremony may be used, provided it's still in its TEB and the TEB number and integrity are verified.</p>	<p><i>ACK</i></p>	<p>16:44</p>
<p>11</p>	<p>CA reads out KSK-HSM-01B-SJC HSM TEB and serial numbers while EW checks that they match those recorded in the script from the most recent key ceremony performed at this site.</p> <p>TEB# A4128460</p> <p>Serial# K1011066</p>	<p><i>ACK</i></p>	<p>16:45</p>
<p>12</p>	<p>CA reads out boot-DVD, laptop, and HSMFD TEB numbers while EW checks that they match those recorded in the script from the most recent key ceremony performed at this site.</p> <p>DVD TEB# A28410758</p> <p>Laptop TEB# A4128461</p> <p>HSMFD TEB# should be one of:</p> <ul style="list-style-type: none"> - A28410757 - A28410738 - A28410739 - A28410740 - A28410754 - A28410755 - A28410756 - A28410757 <p>EW Denotes which TEB# was removed from the safe: HSMFD TEB#: <u>A28410757</u></p>	<p><i>ACK</i></p>	<p>16:47</p>

Collect OP, SO, SMK and APP Cards

Step	Activity	Initial	Time (UTC)
13	CA collects OP, SO and SMK cards from COs, reading out and comparing TEB numbers with those recorded in the most recent ceremony each participated in, reproduced for convenience in the appendices of this document. Different COs may appear on different pages. Note any discrepancies. CA places the cards in plain view on the work surface, removing cards from TEBs, discarding used TEBs but saving warning slips for reuse.	<i>ACL</i>	17:02
14	CA reads out and the TEB number from APP Card for COs so they can compare the TEB number with those recorded in the KC1, reproduced for convenience in the appendix of this document. CA places the APP card in plain view on the work surface, removing card from TEBs, discarding used TEBs but saving warning slips for reuse.	<i>ACL</i>	17:04

Set Up Laptop



Step	Activity	Initial	Time (UTC)
15	CA removes the boot-DVD and laptop from their TEBs, showing participants that the laptop contains no boot devices. CA places the boot-DVD and the laptop on the work surface, connects laptop power to the UPS. Any external monitor or projector may be powered from either the grid (or the UPS if it's large enough). Power the laptop on, booting it from the DVD. CA makes sure the output on the laptop screen is visible on any external monitor or projector. Use the function + F8 keys to cycle through until the display shows only on the external monitor or projector. Boot warnings may be ignored if it continues to boot.	<i>ACL</i>	17:09
16	CA logs in as root.	<i>ACL</i>	17:12
17	CA opens a terminal window via the Menu: applications -> accessories -> terminal	<i>ACL</i>	17:14

18	<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>def</i>	17:16
19	<p>CA opens a terminal window, which we will refer to as the "checksum window". In this window the CA starts the calculation of the sha256 checksum of the boot-DVD. This calculation takes about 9 minutes to complete and the results will be verified in a later step; this step is considered complete as soon as the command is issued.</p> <pre>sha256sum /dev/cdrom</pre>	<i>def</i>	17:16
20	<p>CA connects USB hub to laptop.</p> <p>CA removes HSMFD from its TEB, connects it to the laptop, and waits for operating system to recognize the FD. CA ensures this HSMFD is from the prior KC, regardless of location. CA lets participants view contents of HSMFD then closes FD window</p>	<i>def</i>	17:19

Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
21	<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 script-20160708.log</pre>	<i>def</i>	17:20

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
22	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.		17:23
23	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</pre> <pre>ttyaudit /dev/ttyUSB0</pre> Note: Do not unplug USB serial port adaptor from the laptop until instructed, as this would cause logging to stop.		17:24

Verify DVD checksum

Step	Activity	Initial	Time (UTC)
24	<p>CA will paste the checksum into the "hexread" program at the appropriate prompt.</p> <p>CA will read the checksum aloud, four digits at a time.</p> <p>EW verifies that the checksum of the boot-DVD is:</p> <p>7DE4 31F9 C33D DFEF</p> <p>9089 AB56 13A3 8126</p> <p>708A 3AC1 A784 38A7</p> <p>B9C9 2A4F 52A1 F87C</p> <p>Participants may compare this with the boot-DVD checksum calculated during Key Ceremony 6, reproduced for convenience in the appendices of this document.</p> <p>CA closes the terminal window by typing</p> <p>exit</p>	<i>[Handwritten Signature]</i>	17:26

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

Step	Activity	Initial	Time (UTC)
25	<p>CA connects UPS power to the HSM. Status information will appear in the "ttyaudit window" and the "Ready" LED on the will HSM blink. After its self-test the HSM will display the text "Set Online" indicating that the HSM is in the initialized state and the "Ready" LED will be off.</p>	<i>[Handwritten Signature]</i>	17:27

Make Crypto Officer (CO) Cards from HSM (KSK-HSM-01B-SJC)

Step	Activity	Initial	Time (UTC)
26	CA presses ">" to select "4.HSM Mgmt" and then "ENT". Confirm "HSM Mgmt ?" by pressing "ENT".	<i>CAF</i>	17:28
27	Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card. Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.	<i>CAF</i>	17:29
28	Press ">" to select "6.Issue Cards" and then "ENT". Confirm "Issue Cards ?" by pressing "ENT". For "Num Cards ?" enter "2" and then "ENT". Confirm "Num Req Cards ?" enter "2" and then "ENT". Using cards labeled "CO Card 1 of 2" and "CO Card 2 of 2", insert them when prompted, enter PIN 11223344 and then "ENT" after inserting each card. Confirm "Cards Issued" by pressing "ENT".	<i>CAF</i>	17:32
29	Press "CLR" until you are back in main menu where the display will show "1.Set Online"	<i>CAF</i>	17:32

18:33

18:35

Make Authorization Key (AAK) Cards from HSM (KSK-HSM-01B-SJC)

Step	Activity	Initial	Time (UTC)
30	CA Presses ">" to select "5. Key Mgmt" and then "ENT". Confirm "Key Mgmt ?" by pressing "ENT". Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card. Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.	<i>CAF</i>	17:34
31	Press ">" to select "3.AAK" and then "ENT". Press "ENT" to choose "1.Backup AAK" and confirm "Backup AAK ?" by pressing "ENT". For "Num Cards ?" enter "2" and then "ENT". Using cards labeled "AAK Card 1 of 2" and "AAK Card 2 of 2", insert them when prompted. Confirm "AAK Exported" by pressing "ENT".	<i>CAF</i>	17:36

32	CA presses the RESTART button on the HSM, waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet). CA places this HSM aside on the table.	<i>del</i>	17:37
----	--	------------	-------

18:36

Unpacking new HSMs

Step	Activity	Initial	Time (UTC)
33	Before unpacking HSMs, CA inspects the HSM TEB for evidence and reads aloud the TEB numbers for COs to verify against shipping label in appendix.	<i>del</i>	17:40
34	<p>CA unpacks HSMs confirming Serial number on TEB matches the one on the HSM and offers to the COs to do the same:</p> <ul style="list-style-type: none"> - Serial H1411035 is in TEB PS417133. - Serial H1411033 is in TEB PS417132. - Serial H1412044 is in TEB PS417131. - Serial H1411034 is in TEB PS417129. <p>CA labels each HSM:</p> <ul style="list-style-type: none"> - Serial H1411035 apply label "KSK-HSM-02-SJC" - Serial H1411033 apply label "KSK-HSM-02-SIN" - Serial H1412044 apply label "ZSK-HSM-02-SJC" - Serial H1411034 apply label "ZSK-HSM-02-ZRH" <p>CA places the 4 HSMs aside on the table.</p>	<i>del</i>	17:57

Bringing ZSK-HSM-02-SJC HSM into the family

Step	Activity	Initial	Time (UTC)
35	<p>CA connects the ttyUSB0 null modem serial adaptor and cable already connected to the laptop to ZSK-HSM-02-SJC HSM.</p> <p>In the ttyaudit window, the CA restarts logging HSM serial output by executing</p> <pre>ctl + c</pre> <pre>stty -F /dev/ttyUSB0 115200</pre> <pre>ttyaudit /dev/ttyUSB0</pre> <p>CA connects UPS power to 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 "Important Read Manual". Press "ENT" to confirm. .</p>	<i>AKH</i>	17:59
36	<p>Press ">" to select "2. Restore AAK" and then "ENT" and confirm "Restore AAK ?" by pressing "ENT".</p> <p>Using cards labeled "AAK Card 1 of 2" and "AAK Card 2 of 2", insert them when prompted.</p> <p>Confirm "AAK Imported" by pressing "ENT".</p>	<i>AKH</i>	18:00
37	<p>Press ">" to select "3. Secure" and then "ENT" and confirm "Secure ?" by pressing "ENT".</p>	<i>AKH</i>	18:00
38	<p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>	<i>AKH</i>	18:01
39	<p>When prompted with "SMK AES", press "CLR" to accept default and press ">" to continue.</p>	<i>AKH</i>	18:02
40	<p>When prompted with "Set HSM Port ?", press "CLR" to accept default .</p>	<i>AKH</i>	18:02

18:38

<p>41</p>	<p>When prompted with "Enable IPv4/IPv6 ?", press "ENT" to change values.</p> <p>Press ">" to get to "2.IPv4 only", then "ENT"</p> <p>When prompted with "IPv4 Only?", press "ENT"</p> <p>When prompted with "Set IPv4 Address ?", press "ENT" to change values.</p> <p>When prompted with "192.168.0.2", press "ENT"</p> <p>When prompted with "192. ?" / "xxx. ?", enter "192"</p> <p>When prompted with "168. ?" / "xxx. ?", enter "168"</p> <p>When prompted with "000. ?" / "xxx. ?", enter "013"</p> <p>When prompted with "002. ?" / "xxx. ?", enter "002"</p> <p>When prompted with "192.168.13.2 ?", press "ENT"</p> <p>When prompted with "Set IPv4 NetMask?", press "CLR" to accept default.</p> <p>When prompted with "Set IPv4 Gateway?", press "CLR" to accept default.</p>	<p><i>OK</i></p>	<p>18:03</p>
<p>42</p>	<p>When prompted with "Change Clock?", press "CLR" to accept default.</p> <p>When prompted with "Import Config?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On Disable?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On?", press "ENT" to accept default.</p> <p>When prompted with "Global Key Export Enabled?", press "CLR" to accept default.</p> <p>At this point the HSM will reboot.</p>	<p><i>OK</i></p>	<p>18:04</p>
<p>43</p>	<p>When the HSM is done booting, Press ">" to get to "5.Key Mgmt", then "ENT"</p> <p>Insert CO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		





44	<p>Press ">" to get to "4.SMK", then "ENT"</p> <p>Press ">" to select "3. Restore SMK" and then "ENT" and confirm "Restore SMK ?" by pressing "ENT".</p> <p>Insert SMK cards as prompted.</p> <p>Acknowledge "SMK Restored" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>	<i>OK</i>	18:58
45	<p>Press ">" to get to "3.APP Keys", then "ENT"</p> <p>Press ">" to select "2.Restore" and then "ENT" and confirm "Restore ?" by pressing "ENT".</p> <p>Press ">" to get to "3.From Card", then "ENT"</p> <p>Insert APP cards as prompted.</p> <p>Acknowledge "Restore Complete" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>	<i>OK</i>	19:00
46	<p>Press ">" to get to "5.API Settings", then "ENT"</p> <p>Press ">" to get to "2.Key Export", then "ENT"</p> <p>When prompted with "Key Export On" "Disable?", press "ENT" to change values.</p> <p>Press ">" to get to "5.Sym Key Der", then "ENT"</p> <p>When prompted with "Sym Key Der On" "Disable?", press "ENT".</p> <p>Press "CLR" until you are back in main menu where the display will show "1.Set Online"</p>	<i>OK</i>	19:01
47	<p>CA Presses ">" to select "6.HSM Mgmt" and then "ENT".</p> <p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>	<i>OK</i>	19:03







48	<p>Press ">" to select "2.Change Clock" and then "ENT" and confirm "Change Clock ?" by pressing "ENT".</p> <p>When prompted with "ddmmyyyyhhmmss ?", type full date and time in UTC with 30 seconds added into the future and then "ENT"</p> <p>Press "ENT" when the time you entered in the HSM appears on the official clock.</p> <p>If you are not satisfied with the accuracy, you may set clock again using the instructions in this step.</p>	<i>df</i>	19:06
49	<p>Press ">" to select "2.Auto Online" and then "ENT" and confirm "Auto Online ?" by pressing "ENT".</p> <p>When prompted with "Auto Online Off" .. "Enable?", press "ENT".</p> <p>Press "CLR" until you are back in main menu where the display will show "1.Set Online"</p>	<i>df</i>	19:07
50	<p>CA sets the HSM online using the "Set Online" menu item by pressing "1" and then "ENT". The "Ready" LED should illuminate.</p> <p>When prompted, insert OP cards, and PIN 11223344 and then "Enter" after inserting each card.</p>	<i>df</i>	19:08
51	<p>CA presses the RESTART button on the HSM, waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet). CA places this HSM aside on the table.</p>	<i>df</i>	19:10

Bringing ZSK-HSM-02-ZRH HSM into the family

Step	Activity	Initial	Time (UTC)
52	<p>CA connects the ttyUSB0 null modem serial adaptor and cable already connected to the laptop to ZSK-HSM-02-ZRH HSM.</p> <p>In the ttyaudit window, the CA restarts logging HSM serial output by executing</p> <pre>ctl + c stty -F /dev/ttyUSB0 115200 ttyaudit /dev/ttyUSB0</pre> <p>CA connects UPS power to 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 "Important Read Manual". Press "ENT" to confirm. .</p>	<i>df</i>	19:24




53	<p>Press ">" to select "2. Restore AAK" and then "ENT" and confirm "Restore AAK ?" by pressing "ENT".</p> <p>Using cards labeled "AAK Card 1 of 2" and "AAK Card 2 of 2", insert them when prompted.</p> <p>Confirm "AAK Imported" by pressing "ENT".</p>	<i>ALH</i>	19:25
54	<p>Press ">" to select "3. Secure" and then "ENT" and confirm "Secure ?" by pressing "ENT".</p>	<i>ALH</i>	19:25
55	<p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>	<i>ALH</i>	19:26
56	<p>When prompted with "SMK AES", press "CLR" to accept default and press ">" to continue.</p>	<i>ALH</i>	19:27
57	<p>When prompted with "Set HSM Port ?", press "CLR" to accept default .</p>	<i>ALH</i>	19:27
58	<p>When prompted with "Enable IPv4/IPv6 ?", press "ENT" to change values.</p> <p>Press ">" to get to "2.IPv4 only", then "ENT"</p> <p>When prompted with "IPv4 Only?", press "ENT"</p> <p>When prompted with "Set IPv4 Address ?", press "ENT" to change values.</p> <p>When prompted with "192.168.0.2", press "ENT"</p> <p>When prompted with "192. ?" / "xxx. ?", enter "192"</p> <p>When prompted with "168. ?" / "xxx. ?", enter "168"</p> <p>When prompted with "000. ?" / "xxx. ?", enter "014"</p> <p>When prompted with "002. ?" / "xxx. ?", enter "002"</p> <p>When prompted with "192.168.14.2 ?", press "ENT"</p> <p>When prompted with "Set IPv4 NetMask?", press "CLR" to accept default.</p> <p>When prompted with "Set IPv4 Gateway?", press "CLR" to accept default.</p>	<i>ALH</i>	19:28






59	<p>When prompted with "Change Clock?", press "CLR" to accept default.</p> <p>When prompted with "Import Config?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On Disable?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On?", press "ENT" to accept default.</p> <p>When prompted with "Global Key Export Enabled?", press "CLR" to accept default.</p> <p>At this point the HSM will reboot.</p>		19:29
60	<p>When the HSM is done booting, Press ">" to get to "5.Key Mgmt", then "ENT"</p> <p>Insert CO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		19:30
61	<p>Press ">" to get to "4.SMK", then "ENT"</p> <p>Press ">" to select "3. Restore SMK" and then "ENT" and confirm "Restore SMK ?" by pressing "ENT".</p> <p>Insert SMK cards as prompted.</p> <p>Acknowledge "SMK Restored" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>		19:31
62	<p>Press ">" to get to "3.APP Keys", then "ENT"</p> <p>Press ">" to select "2.Restore" and then "ENT" and confirm "Restore ?" by pressing "ENT".</p> <p>Press ">" to get to "3.From Card", then "ENT"</p> <p>Insert APP cards as prompted.</p> <p>Acknowledge "Restore Complete" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>		19:32

63	<p>Press ">" to get to "5.API Settings", then "ENT"</p> <p>Press ">" to get to "2.Key Export", then "ENT"</p> <p>When prompted with "Key Export On" "Disable?", press "ENT" to change values.</p> <p>Press ">" to get to "5.Sym Key Der", then "ENT"</p> <p>When prompted with "Sym Key Der On" "Disable?", press "ENT".</p> <p>Press "CLR" until you are back in main menu where the display will show "1.Set Online"</p>		19:33
64	<p>CA Presses ">" to select "6.HSM Mgmt" and then "ENT".</p> <p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		19:34
65	<p>Press ">" to select "2.Change Clock" and then "ENT" and confirm "Change Clock ?" by pressing "ENT".</p> <p>When prompted with "ddmmyyyyhhmmss ?", type full date and time in UTC with 30 seconds added into the future and then "ENT"</p> <p>Press "ENT" when the time you entered in the HSM appears on the official clock.</p> <p>If you are not satisfied with the accuracy, you may set clock again using the instructions in this step.</p>		19:36
66	<p>Press ">" to select "2.Auto Online" and then "ENT" and confirm "Auto Online ?" by pressing "ENT".</p> <p>When prompted with "Auto Online Off" .. "Enable?", press "ENT".</p> <p>Press "CLR" until you are back in main menu where the display will show "1.Set Online"</p>		19:36
67	<p>CA sets the HSM online using the "Set Online" menu item by pressing "1" and then "ENT". The "Ready" LED should illuminate.</p> <p>When prompted, insert OP cards, and PIN 11223344 and then "Enter" after inserting each card.</p>		19:38
68	<p>CA presses the RESTART button on the HSM, waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet). CA places this HSM aside on the table.</p>		19:38

Bringing KSK-HSM-02-SIN HSM into the family

Step	Activity	Initial	Time (UTC)
69	<p>CA connects the ttyUSB0 null modem serial adaptor and cable already connected to the laptop to KSK-HSM-02-SIN HSM.</p> <p>In the ttyaudit window, the CA restarts logging HSM serial output by executing</p> <pre>ctl + c</pre> <pre>stty -F /dev/ttyUSB0 115200</pre> <pre>ttyaudit /dev/ttyUSB0</pre> <p>CA connects UPS power to 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 "Important Read Manual". Press "ENT" to confirm. .</p>	<i>CAF</i>	19:39
70	<p>Press ">" to select "2. Restore AAK" and then "ENT" and confirm "Restore AAK ?" by pressing "ENT".</p> <p>Using cards labeled "AAK Card 1 of 2" and "AAK Card 2 of 2", insert them when prompted.</p> <p>Confirm "AAK Imported" by pressing "ENT".</p>	<i>CAF</i>	19:40
71	<p>Press ">" to select "3. Secure" and then "ENT" and confirm "Secure ?" by pressing "ENT".</p>	<i>CAF</i>	19:40
72	<p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>	<i>CAF</i>	19:41
73	<p>When prompted with "SMK AES", press "CLR" to accept default and press ">" to continue.</p>	<i>CAF</i>	19:42
74	<p>When prompted with "Set HSM Port ?", press "CLR" to accept default .</p>	<i>CAF</i>	19:42





<p>75</p>	<p>When prompted with "Enable IPv4/IPv6 ?", press "ENT" to change values.</p> <p>Press ">" to get to "2.IPv4 only", then "ENT"</p> <p>When prompted with "IPv4 Only?", press "ENT"</p> <p>When prompted with "Set IPv4 Address ?", press "ENT" to change values.</p> <p>When prompted with "192.168.0.2", press "ENT"</p> <p>When prompted with "192. ?" / "xxx. ?", enter "192"</p> <p>When prompted with "168. ?" / "xxx. ?", enter "168"</p> <p>When prompted with "000. ?" / "xxx. ?", enter "012"</p> <p>When prompted with "002. ?" / "xxx. ?", enter "002"</p> <p>When prompted with "192.168.12.2 ?", press "ENT"</p> <p>When prompted with "Set IPv4 NetMask?", press "CLR" to accept default.</p> <p>When prompted with "Set IPv4 Gateway?", press "CLR" to accept default.</p>		<p>19:43</p>
<p>76</p>	<p>When prompted with "Change Clock?", press "CLR" to accept default.</p> <p>When prompted with "Import Config?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On Disable?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On?", press "ENT" to accept default.</p> <p>When prompted with "Global Key Export Enabled?", press "CLR" to accept default.</p> <p>At this point the HSM will reboot.</p>		<p>19:44</p>
<p>77</p>	<p>When the HSM is done booting, Press ">" to get to "5.Key Mgmt", then "ENT"</p> <p>Insert CO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		<p>19:45</p>

78	<p>Press ">" to get to "4.SMK", then "ENT"</p> <p>Press ">" to select "3. Restore SMK" and then "ENT" and confirm "Restore SMK ?" by pressing "ENT".</p> <p>Insert SMK cards as prompted.</p> <p>Acknowledge "SMK Restored" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>		19:46
79	<p>Press ">" to get to "3.APP Keys", then "ENT"</p> <p>Press ">" to select "2.Restore" and then "ENT" and confirm "Restore ?" by pressing "ENT".</p> <p>Press ">" to get to "3.From Card", then "ENT"</p> <p>Insert APP cards as prompted.</p> <p>Acknowledge "Restore Complete" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>		19:47
80	<p>CA Presses ">" to select "6.HSM Mgmt" and then "ENT".</p> <p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		19:49
81	<p>Press ">" to select "2.Change Clock" and then "ENT" and confirm "Change Clock ?" by pressing "ENT".</p> <p>When prompted with "ddmmyyyyhhmmss ?", type full date and time in UTC with 30 seconds added into the future and then "ENT"</p> <p>Press "ENT" when the time you entered in the HSM appears on the official clock.</p> <p>If you are not satisfied with the accuracy, you may set clock again using the instructions in this step.</p>		19:50
82	<p>CA presses the RESTART button on the HSM, waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet). CA places this HSM aside on the table.</p>		19:50

Bringing KSK-HSM-02-BRK HSM into the family

Step	Activity	Initial	Time (UTC)
83	<p>CA connects the ttyUSB0 null modem serial adaptor and cable already connected to the laptop to KSK-HSM-02-BRK HSM.</p> <p>In the ttyaudit window, the CA restarts logging HSM serial output by executing</p> <pre>ctl + c</pre> <pre>stty -F /dev/ttyUSB0 115200</pre> <pre>ttyaudit /dev/ttyUSB0</pre> <p>CA connects UPS power to 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 "Important Read Manual". Press "ENT" to confirm. .</p>	<i>ABF</i>	19:51
84	<p>Press ">" to select "2. Restore AAK" and then "ENT" and confirm "Restore AAK ?" by pressing "ENT".</p> <p>Using cards labeled "AAK Card 1 of 2" and "AAK Card 2 of 2", insert them when prompted.</p> <p>Confirm "AAK Imported" by pressing "ENT".</p>	<i>ABF</i>	19:52
85	<p>Press ">" to select "3. Secure" and then "ENT" and confirm "Secure ?" by pressing "ENT".</p>	<i>ABF</i>	19:52
86	<p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>	<i>ABF</i>	19:53
87	<p>When prompted with "SMK AES", press "CLR" to accept default and press ">" to continue.</p>	<i>ABF</i>	19:53
88	<p>When prompted with "Set HSM Port ?", press "CLR" to accept default .</p>	<i>ABF</i>	19:54

<p>89</p>	<p>When prompted with "Enable IPv4/IPv6 ?", press "ENT" to change values.</p> <p>Press ">" to get to "2.IPv4 only", then "ENT"</p> <p>When prompted with "IPv4 Only?", press "ENT"</p> <p>When prompted with "Set IPv4 Address ?", press "ENT" to change values.</p> <p>When prompted with "192.168.0.2", press "ENT"</p> <p>When prompted with "192. ?" / "xxx. ?", enter "192"</p> <p>When prompted with "168. ?" / "xxx. ?", enter "168"</p> <p>When prompted with "000. ?" / "xxx. ?", enter "011"</p> <p>When prompted with "002. ?" / "xxx. ?", enter "002"</p> <p>When prompted with "192.168.11.2 ?", press "ENT"</p> <p>When prompted with "Set IPv4 NetMask?", press "CLR" to accept default.</p> <p>When prompted with "Set IPv4 Gateway?", press "CLR" to accept default.</p>		<p>19:55</p>
<p>90</p>	<p>When prompted with "Change Clock?", press "CLR" to accept default.</p> <p>When prompted with "Import Config?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On Disable?", press "CLR" to accept default.</p> <p>When prompted with "FIPS Mode On?", press "ENT" to accept default.</p> <p>When prompted with "Global Key Export Enabled?", press "CLR" to accept default.</p> <p>At this point the HSM will reboot.</p>		<p>19:55</p>
<p>91</p>	<p>When the HSM is done booting, Press ">" to get to "5.Key Mgmt", then "ENT"</p> <p>Insert CO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		<p>19:57</p>

92	<p>Press ">" to get to "4.SMK", then "ENT"</p> <p>Press ">" to select "3. Restore SMK" and then "ENT" and confirm "Restore SMK ?" by pressing "ENT".</p> <p>Insert SMK cards as prompted.</p> <p>Acknowledge "SMK Restored" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>		19:59
93	<p>Press ">" to get to "3.APP Keys", then "ENT"</p> <p>Press ">" to select "2.Restore" and then "ENT" and confirm "Restore ?" by pressing "ENT".</p> <p>Press ">" to get to "3.From Card", then "ENT"</p> <p>Insert APP cards as prompted.</p> <p>Acknowledge "Restore Complete" by pressing "ENT"</p> <p>Press "CLR" to back in "Key Mgmt" menu. Be careful to not press "ENT" too many times or CA will have to re-authenticate with the CO Cards.</p>		19:59
94	<p>CA Presses ">" to select "6.HSM Mgmt" and then "ENT".</p> <p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		20:01
95	<p>Press ">" to select "2.Change Clock" and then "ENT" and confirm "Change Clock ?" by pressing "ENT".</p> <p>When prompted with "ddmmyyyyhhmmss ?", type full date and time in UTC with 30 seconds added into the future and then "ENT"</p> <p>Press "ENT" when the time you entered in the HSM appears on the official clock.</p> <p>If you are not satisfied with the accuracy, you may set clock again using the instructions in this step.</p> <p>Press "CLR" until you are back in main menu where the display will show "1.Set Online"</p>		20:02



Wiping AAK and CO Cards with KSK-HSM-02-BRK HSM

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





96	<p>CA Presses ">" to select "7. Role Mgmt" and then "ENT".</p> <p>Insert SO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Note that the HSM will always refer to cards 1 and 2, regardless of our numbering.</p>	<i>AKJ</i>	20:03
97	<p>CA Presses ">" to select "5. Clear AAK Card" and then "ENT". Confirm "Clear AAK Card ?" by pressing "ENT".</p> <p>For "Num Cards ?" enter "2" and then "ENT".</p> <p>Using cards labeled "AAK Card 1 of 2" and "AAK Card 2 of 2", insert them when prompted.</p> <p>Press "CLR" until you are back in Role Mgmt menu.</p>	<i>AKJ</i>	20:05
98	<p>CA Presses ">" to select "4. Clear RoleCard" and then "ENT".</p> <p>When prompted with "Clear Card?", press "ENT".</p> <p>For "Num Cards ?" enter "2" and then "ENT".</p> <p>Insert CO cards as prompted, PIN 11223344 and then "ENT" after inserting each card.</p> <p>Press "CLR" until you are back in main menu where the display will show "1.Set Online"</p>	<i>AKJ</i>	20:06

Bringing KSK-HSM-02-BRK HSM online

Step	Activity	Initial	Time (UTC)
99	<p>CA sets the HSM online using the "Set Online" menu item by pressing "1" and then "ENT".</p> <p>When prompted, insert OP cards, and PIN 11223344 and then "Enter" after inserting each card.</p> <p>The "Ready" LED should illuminate.</p>	<i>AKJ</i>	20:08
100	<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>	<i>AKJ</i>	20:09

101	<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-20160708.tar.gz . sha256sum scripts-20160708.tar.gz tar -xzvof scripts-20160708.tar.gz</pre>		20:11
102	<p>CA connects Ethernet cable between laptop and HSM and sets the HSM IP in the config by entering</p> <pre>./ipadd ./set-hsm-env</pre>		20:14

Start generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)
103	CA copies the shell scripts that will generate new keys and bundles by executing: ./copystuff		20:16
104	CA disables screen saver by typing ./disable-screensaver Now, using the GUI menu, in "System" -> "Preferences" -> "Screensaver" uncheck "activate screen saver when computer is idle" Click "Close". In "System" -> "Preferences" -> "More Preferences" -> "Power Management" Ensure both sliders in "Running on AC" are set to "never". Click "Close".		20:17
105	CA copies the encrypted ZSKs by executing: cd /tmp/pch makeallhsmfiles		20:18
106	CA starts key and signature generation by executing: keybundle-generate.20160708 < 20160708.kc_script_gen.out 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. this step is considered complete as soon as the command is issued.		20:19

Re-Package OP Cards and APP Card

Step	Activity	Initial	Time (UTC)
107	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.	<i>[Signature]</i>	00:27
108	CA places the APP card with HS MDB #3 in its own new TEB and reads the TEB number aloud. The EW records TEB number for reference in future KCs: <u>A28410743</u>	<i>[Signature]</i>	20:48

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
109	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>[Signature]</i>	00:33

Smart Card Sign Out Sheet





See Script exception Form

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7		Steve FELDMAN		7/8/16		
CO2	OP 2 of 7		Michael SINATRA		7/8/16		
CO3	OP 3 of 7		Kim DAVIES		7/8/16		
CO4	OP 4 of 7		Eric ALLMAN		7/8/16		
CO7	OP 7 of 7		Gaurab UPADHAYA		7/8/16		

Optionally leave facility

Step	Activity	Initial	Time (UTC)
110	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.	<i>[Signature]</i>	20:51

Pack and store Keys and Keybundles

Step	Activity	Initial	Time (UTC)
111	<p>When the key generation script is complete, CA generates the archive destined for the signing HSMs by executing:</p> <pre>tar -cvzf /media/HSMFD/20160708.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256 2> errors</pre> <p>The redirection of stderr to the "errors" file is to capture any error messages which may result. This file should be empty, and if so, should be deleted:</p> <pre>cat errors rm errors</pre>		02:57
112	<p>CA archives all results including encrypted KSKs for future use by executing:</p> <pre>tar -cvzf /media/HSMFD/20160708.session.tar.gz . 2> errors</pre> <pre>cat errors rm errors</pre>		02:58
113	<p>CA creates a snapshot of any changes to DB files by executing:</p> <pre>cd /media/HSMFD tar -czf 20160708.KSK-HSM-01B- SJC.db.tar.gz *.db</pre>		03:00
114	<p>CA calculates checksums of all files on the HSMFD:</p> <pre>find . -type f -print0 xargs -0 -n 50 sha256sum</pre> <p>If that command fails, the following will suffice instead:</p> <pre>sha256sum *</pre> <p>Finally, to keep an eye on available space on the HSMFD, execute:</p> <pre>df -h</pre>		03:00

115	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.		
		<i>AKS</i>	03:01


Return KSK-HSM-02-BRK HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
116	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.		
		<i>AKS</i>	03:05
117	CA reads out TEB number and HSM serial number and allows participants to verify them while the EW records the TEB and HSM serial numbers here: TEB# <u>A4128467</u> HSM Serial#: <u>H1411035</u>		
		<i>AKS</i>	03:07


Return Other HSMs to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
118	CA reads out the 3 TEB numbers and 3 HSM serial numbers and allows participants to verify them while the EW records the TEBs and HSM serial numbers here: KSK-HSM-02-SIN TEB# <u>A4128466</u> KSK-HSM-02-SIN HSM Serial#: <u>H1411033</u> ZSK-HSM-02-SJC TEB# <u>A4128464</u> ZSK-HSM-02-SJC HSM Serial#: <u>H1412044</u> ZSK-HSM-02-ZRH TEB# <u>A4128465</u> ZSK-HSM-02-ZRH HSM Serial#: <u>H1411034</u> CA ensures these 3 HSMs leave the CA to be delivered to their appropriate destinations.		
		<i>AKS</i>	03:12

Hard reset of HSM (KSK-HSM-01B-SJC)

Step	Activity	Initial	Time (UTC)
119	CA physically resets HSM by inserting a pin into the tiny hole in the back, above the text saying "config". Power on to verify it has detected the tampering. Do not put this back in the safe CA ensures this HSM leaves the CA to be returned to the manufacturer.		03:17

Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
120	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from the laptop. CA then exits out of the "ttyaudit window". exit		03:17

Display HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
121	CA displays contents of HSMFD by executing: ls -ltr		03:18

Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
122	CA stops logging terminal output by typing "exit" in the "command window": exit		
		<i>CAF</i>	<i>03:18</i>
123	CA calculates sha256 checksum of the logfile by executing: sha256sum script-20160708.log CA reads the hash of the checksum aloud. EW records the sixty-four digit hash: <u>6395 2F6F AC0F 3876</u> <u>EFES CA47 73CE DD7A</u> <u>0E83 CEE0 B9AC 4D2F</u> <u>E6D3 5D4B 2A95 6A3A</u>		
		<i>CAF</i>	<i>03:21</i>


Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
124	CA plugs a blank FD labeled "HSMFD" into the laptop waits for it to be recognized by the operating system as HSMFD_ and copies the contents of the HSMFD to the blank drive by executing: cp -Rp * /media/HSMFD_ CA then unmounts new FD using umount /media/HSMFD_ CA then removes HSMFD_ from the laptop and places it a new TEB and seals; reads out TEB number and shows item to participants while the EW records the TEB number here: TEB# <u>A28410687</u> This copy will later be stored in the on-site audit bundle.		
		<i>CAF</i>	<i>03:27</i>

125	CA performs this activity a second time to create a second copy. TEB# <u>A28410690</u> This copy will later be stored in the off-site audit bundle.	<i>CAF</i>	03:29
126	CA performs this activity a third time to create a third copy. TEB# <u>A28410691</u> This copy will later be stored in the EW audit bundle.	<i>CAF</i>	03:31
127	CA performs this activity a fourth time to create a fourth copy. TEB# <u>A28410688</u> This copy will later be placed in the safe.	<i>CAF</i>	03:33
128	CA performs this activity a fifth time to create a fifth copy. TEB# <u>A28410689</u> This copy will later be sent to the other KSK generating country.	<i>CAF</i>	03:35
129	CA performs this activity a sixth time to create a sixth copy. TEB# <u>A28410716</u> This copy will later be CA's copy. CA will later upload the contents to the published archive.	<i>CAF</i>	03:36

Return HSMFD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
130	CA unmounts HSMFD by executing: cd /tmp then umount /media/HSMFD	<i>CAF</i>	03:38

131	CA removes HSMFD and places it in a new TEB and seals; reads out TEB number and shows item to participants. EW records TEB # here. TEB# <u>A28410715</u>		63:39
-----	--	--	-------

Return Boot-DVD to a Tamper Evident Bag


Step	Activity	Initial	Time (UTC)
132	CA executes: shutdown -h now removes DVD and turns off laptop. To remove DVD, CA may need to briefly power on laptop, press eject button, and power off.	<i>AKS</i>	03:40
133	CA places boot-DVD in new TEB and seals; reads out TEB number and shows item to participants. EW records TEB number here: TEB# <u>A28410714</u>	<i>AKS</i>	03:41

Return Laptop to a Tamper Evident Bag


Step	Activity	Initial	Time (UTC)
134	CA disconnects power and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB number and shows item to participants. EW records TEB number here: TEB# <u>A4128463</u>	<i>AKS</i>	03:43

Return Power Supplies, USB Hub, and Cables


Step	Activity	Initial	Time (UTC)
135	CA places HSM power supply and laptop power supply, USB hub, serial cable, USB serial adapter, power and networking cables in a bag. This need not be a TEB as it is only used for convenience.	<i>AKS</i>	03:43

136	<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"> - KSK-HSM-01B-SJC HSM - laptop - original HSMFD above - fourth HSMFD backup - DVD <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>03:54</p>
-----	---	--	--------------



Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
137	All participants leave the Key Management Facility, and on the Participant Signature Sheet note their exit time and sign.		03:58

Stop Audio-Visual Recording

Step	Activity	Initial	Time (PDT)
138	FO stops audio and video recording.		9:00 pm


Script review

Step	Activity	Initial	Time (UTC)
139	<p>CA reviews EWs script and signs it:</p> <p>CA Signature </p>		<p>9:00 pm</p>

PDT

Sign Out of Facility

Step	Activity	Initial	Time (PDT)
------	----------	---------	------------

140	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.		9:01 pm
-----	---	--	---------

Copy and Store the Script

Step	Activity	Initial	Time (PDT)
141	<p>FO makes at least three color copies of his script: one for the off-site audit bundle, one for the on-site audit bundle, one for himself, copies for other participants as requested, and delivers the original to the SC.</p> <p>The two audit bundles each contain hard copies and soft copies on an SD card:</p> <ul style="list-style-type: none"> - output of signer system - HSMFD - copy of EWs key ceremony script - audio-visual recording - logs from the Facility Physical Access Control - SC attestation (A.2 below) - the EW attestation (A.1 below) <p>all in a TEB labeled "Key Ceremony 07/08/2016", 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> <p>The fifth copy of the HSMFD will be sent to the other key signing facility.</p> <p>CA retains any remaining materials (e.g. extra HSMFD) for next key ceremony preparation and analysis.</p> <p>CA ensures 3 HSMs newly entered into the family are delivered to their respective locations.</p> <p>CA ensures APP Card TEB is put in storage with other KC material.</p>		

*WILL BE COMPLETED
POST-KC*

**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: Aimee Leonetti

Signature: 

Date: July 8, 2016

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 July 8, 2016 before me, Aimee Leonetti, Notary Public
Date Here Insert Name and Title of the Officer

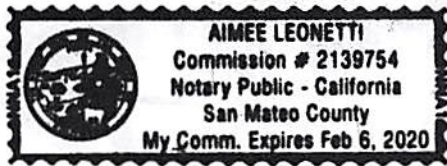
personally appeared William Edward Woodcock IV
Name(s) of Signer(s)

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 [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: DNISSEC Key Ceremony Script Document Date: 7/8/16

Number of Pages: 62 Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____

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

Signer Is Representing: _____

Signer's Name: _____

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

Signer Is Representing: _____

ALBERT ROBERT
Commissioner of
State Public Health
San Mateo County
San Francisco, California



Appendix B:
Access Control System Attestation
(by SC)

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

Attached is the audited physical access log.

Printed Name: Bill Woodcock

Signature: 

Date: July 8, 2016



1600 Shattuck Avenue Facilities Sign-In Sheet

Role	Name	Signature	Date	Entry Time PDT	Exit Time PDT
FO3	Mimi RAUSCHENDORF	Personally identifiable information redacted	7/8/16	9:24	
CA	Robert MARTIN-LEGENE		7/8/16	9:23	
CA2	Ashley JONES		7/8/16	9:23	
EW3	Aimee LOENETTI		7/8/16	9:24	
CO1	Steve FELDMAN		7/8/16	9:22	
CO2	Michael SINATRA		7/8/16	9:22	
CO3	Kim DAVIES		7/8/16	9:22	
CO4	Eric ALLMAN		7/8/16	9:22	
CO7	Gaurab UPADHAYA		7/8/16	9:23	
SC1	Bill WOODCOCK		7/8/16	9:23	
R	Kabindra SHRESTHA		7/8/16	9:25	

Appendix C:

Abbreviations Used in This Document

Roles

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

Other Abbreviation

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

Appendix D: Letter and Number Pronunciation

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

Appendix: E**Card Distribution from Key Ceremony 1**

DNSSEC Key Ceremony Script

Tuesday, April 26, 2011

Distribute Cards

Step	Activity	Initial	Time
103	Due to limited number of personnel at this key ceremony, cards will be distributed in groups that maintain multi-person control requirements. A subsequent key ceremony will redistribute cards to their final holders. Each group of cards shall be placed in another TEB whose numbers are recorded below on the EW's script.	<i>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

Packet Clearing House

Page 29 of 34

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	CO1	SO 1 of 7	A21095012	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	✓
1	CO1	SMK 1 of 7	A21095011	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	✓
1	CO2	OP 2 of 7	A21095010	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	✓
1	CO2	SO 2 of 7	A21095009	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	✓
1	CO2	SMK 2 of 7	A21095008	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	✓
1	CO3	OP 3 of 7	A21095007	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	✓
1	CO3	SO 3 of 7	A21095006	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	✓
1	CO3	SMK 3 of 7	A21095004	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	✓
1	CO4	OP 4 of 7	A21095005	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	✓
1	CO4	SO 4 of 7	A21095003	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	✓
1	CO4	SMK 4 of 7	A21095002	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	✓
1	CO5	OP 5 of 7	A21095001	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:50	✓
1	CO5	SO 5 of 7	A21095000	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	✓
1	CO5	SMK 5 of 7	A21094999	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:50	✓
1	CO6	OP 6 of 7	A21094998	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	✓
1	CO6	SO 6 of 7	A21094997	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	✓
1	CO6	SMK 6 of 7	A21094996	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	✓
1	CO7	OP 7 of 7	A21094995	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	✓
1	CO7	SO 7 of 7	A21094994	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	✓
1	CO7	SMK 7 of 7	A21094993	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	✓

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	CO1 OP 1 of 7	A19204935	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<i>[Initials]</i>
	CO1 SO 1 of 7	A19204934	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<i>[Initials]</i>
	CO1 SMK 1 of 7		Steve FELDMAN		5/30/11		
A19204942	CO2 OP 2 of 7	A19204933	Michael SMATRA	<i>[Signature]</i>	5/30/11	0049	<i>[Initials]</i>
	CO2 SO 2 of 7	A19204931	Michael SMATRA	<i>[Signature]</i>	5/30/11	0049	<i>[Initials]</i>
	CO2 SMK 2 of 7		Michael SMATRA		5/30/11		
A19204944	CO4 OP 4 of 7	A19204932	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<i>[Initials]</i>
	CO4 SO 4 of 7	A19204930	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<i>[Initials]</i>
	CO4 SMK 4 of 7		Jonny MARTIN		5/30/11		
A19204941	CO5 OP 5 of 7	A19204929	Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<i>[Initials]</i>
	CO5 SO 5 of 7	A19204928	Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<i>[Initials]</i>
	CO5 SMK 5 of 7		Steve SOMOGYI		5/30/11		
	CO7 OP 7 of 7		Jonny MARTIN		5/30/11		
	CO7 SO 7 of 7		Jonny MARTIN		5/30/11		
	CO7 SMK 7 of 7		Jonny MARTIN		5/30/11		

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

Packet Clearing House Page 25 of 32





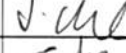





Appendix: H

Smart Card Sign Out Sheet from Key Ceremony 3

DNSSEC Key Ceremony Script

Monday, June 20, 2011

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	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	Gaurab UPADHAYA		6/20/11	07:49	

ENCLOSING BAGS:

CO1: A19204875

CO3: A19204873

CO4: A19204871

CO6: A19204869

CO7: A19204867

Appendix: I

Smart Card Sign Out Sheet from Key Ceremony 4

DNSSEC Key Ceremony Script

Friday, January 20, 2012

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
60	CA places each OP card with instruction slip in its own new TEB and records the number in the smart card sign out sheet below.	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.	TF	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	2046	TF
CO5	<i>outside bag</i> SO 5 of 7	A19204954	Stephan SOMOGYI	<i>Stephan</i>	1/20/12	2046	TF

OUTSIDE BAG

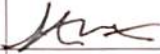









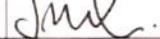

Appendix: J

Smart Card Sign Out Sheet from Key Ceremony 5


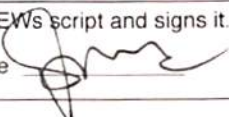

DNSSEC Key Ceremony Script

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	Outer 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	Outer SO 3 of 7 Bag	A3112572	Kim DAVIES		4/27/12	18:46	
CO4	OP 4 of 7	A3112565	Jonny MARTIN		4/27/12	18:47	
CO4	Outer SO 4 of 7 bag	A3112593	Jonny MARTIN		4/27/12	18:47	

Sign-Out on Participant Signature Sheet

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

Sign Out of Facility

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

Stop Audio-Visual Recording

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

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>JS</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.	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	1
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.	TF	20:44

Re-Distribution of Cards


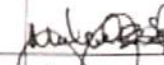
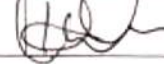
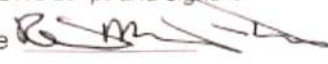
Step	Activity	Initial	Time (UTC)
66	The CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and the EW initials their entry.	TF	20:46

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

Appendix: N

Smart Card Sign Out Sheet from Key Ceremony 8

DNSSEC Key Ceremony Script		Thursday, September 12, 2013					
Re-Distribution of Cards							
Step	Activity	Initial	Time (UTC)				
63	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.	JJ	18:20				
Smart Card Sign Out Sheet							
CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410802	Steve FELDMAN		9/12/13	1812	JJ
CO2	OP 2 of 7	A28410801	Michael SINATRA		9/12/13	1816	JJ
CO3	OP 3 of 7	A28410800	Kim DAVIES		9/12/13	1819	JJ
Sign-Out on Participant Signature Sheet							
Step	Activity	Initial	Time (UTC)				
64	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.	JJ	22:53				
65	CA reviews EWs script and signs it. CA Signature 	JJ	22:55				
Sign Out of Facility							
Step	Activity	Initial	Time (PDT)				
66	FO returns phones, laptops, and other items to participants and logs their exit times. Participants return identification vests to the FO. Participants are now free to depart.	JJ	3:58 PM				
Stop Audio-Visual Recording							
Step	Activity	Initial	Time (PDT)				
67	SA stops audio and video recording.	JJ	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

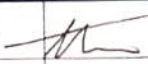


Re-Package OP Cards

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

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.	tf	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>[Handwritten Initials]</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>[Handwritten Initials]</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>[Handwritten Signature]</i>	3/26/14	0846	<i>[Handwritten Initials]</i>
CO6	OP 6 of 7	LIM Choon Sar	A28410777	<i>[Handwritten Signature]</i>	3/26/14	0846	<i>[Handwritten Initials]</i>
CO7	OP 7 of 7	Gaurab UPADHAYA	A28410779	<i>[Handwritten Signature]</i>	3/26/14	0846	<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.		

Appendix: Q

Smart Card Sign Out Sheet from Key Ceremony 11

DNSSEC Key Ceremony Script

Friday, December 12, 2014


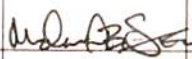

Re-Package OP Cards

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		12/12/14	19:17	11
CO2	OP 2 of 7	A28410735	Michael SINATRA		12/12/14	19:18	11
CO4	OP 4 of 7	A28410736	Eric ALLMAN		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>[Signature]</i>	0746

Re-Distribution of Cards

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

Smart Card Sign Out Sheet


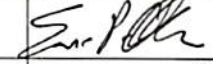

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO3	OP 3 of 7	A28410768	Kim DAVIES	<i>[Signature]</i>	2/9/15	0747	<i>[Initials]</i>
CO6	OP 6 of 7	A28410767	LEE Han-Chuan	<i>[Signature]</i>	2/9/15	0747	<i>[Initials]</i>
CO7	OP 7 of 7	A28460766	Gaurab UPADHAYA	<i>[Signature]</i>	2/9/15	0748	<i>[Initials]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

Optionally leave facility

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

Appendix: S

Smart Card Sign Out Sheet from Key Ceremony 13

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


Appendix: T

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

Packing Slip For 4 New HSMs For KC15

From: Peter Clements <Peter.Clements@ultra-cis.com>
Subject: FW: Payment Request from ULTRA ELECTRONICS LIMITED t/as Ultra electronics CIS
Date: June 6, 2016 at 7:50:20 AM PDT
To: "'peter@pch.net" <peter@pch.net>
Cc: Daryl Hyett <Daryl.Hyett@ULTRA-AEP.COM>, Ges Muir <Ges.Muir@ultra-cis.com>

Dear Peter,
 As requested please find details of your order listed below, if you have any questions please don't hesitate to contact me;

Your order has been dispatched please see details below:

Date	27/05/16
Customer PO#	PCH_AEP_2016_1
AEP Ref#	850671
Courier Used	Fedex
AWB/Tracking #	776388441230
Product Type	KEY-PLUS
Serial Number	Tamper Bag Ref
H1406001	PS417130
H1411033	PS417132
H1411034	PS417129
H1411035	PS417133
H1412044	PS417131

Upon receipt please check that the serial number and tamper evident bag number match the details above. If they do not it could indicate the goods have tampered with. If you believe the goods have been tampered with during transit please contact AEP Immediately at customerorders@ultra-aep.com

Best Regards,

Peter Clements

Head of Compliance

Ultra Electronics

COMMUNICATION & INTEGRATED SYSTEMS

419 Bridport Road, Greenford

Middlesex, UB6 8UA, United Kingdom

peter.clements@ultra-cis.com

Tel: +44 (0) 208 813 4701

Mob: +44 (0) 7799 894462

www.ultra-cis.com

www.ultra-electronics.com

Appendix: V

APP TEB Packaging from Key Ceremony 1

DNSSEC Key Ceremony Script		Tuesday, April 26, 2011	
Package APP Cards and HSMDB Flash Drives			
Step	Activity	Initial	Time
68	CA places one of the backup HSMDB FDs and APP 1 card in a TEB and seals.	<i>J</i>	7:35 PM
69	CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # <u>A 21094991</u>	<i>J</i>	7:35 PM
70	CA places one of the backup HSMDB FDs and APP 2 card in a TEB and seals.	<i>J</i>	7:36 PM
71	CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # <u>A 21094990</u>	<i>J</i>	7:36 PM
72	CA places one of the backup HSMDB FDs and APP 3 card in a TEB and seals.	<i>J</i>	7:37 PM
73	CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # <u>A 21094989</u>	<i>J</i>	7:38 PM
Package SMK Cards			
Step	Activity	Initial	Time
74	CA places each SMK card with an instruction slip indicating the ownership and disposition of the card in its own new TEB and records the number in the Smart Card Sign Out Sheet.	<i>J</i>	7:51 PM
Package SO Cards			
Step	Activity	Initial	Time
75	CA places each SO card with instruction slip in its own new TEB and records the number in the smart card sign out sheet below.	<i>J</i>	8:29 PM

Appendix: W

Boot-DVD Checksum from Key Ceremony 6

DNSSEC Key Ceremony Script		Friday, July 27, 2012	
16	CA opens a terminal window.	/	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 mmddHHMMYYYY</code> Verify: <code>date</code>	/	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>	/	17:34
19	EW records the sixty-four digit boot-DVD checksum <u>7DE4 31F9 C33D 0FEF</u> <u>9089 ABS6 13A3 8126</u> <u>708A 3AC1 A784 38A7</u> <u>B9C9 2A4F 52A1 F87C</u> Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in the appendices of this document.	/	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

REPHRASE SCRIPTS FOR FBI-AT DUBS


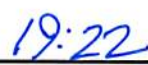
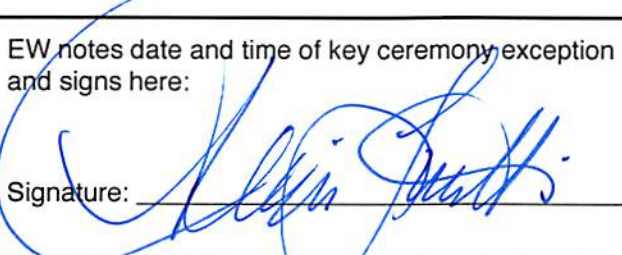
PCH DNSSEC Key Ceremony Script Exception Form

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	

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>At Step 43 the new HSM informed us that the cards generated in Step 28 were invalid. Discussion of reasons ensued. Most likely cause thought to be that smart cards used were of an old version, not fully compatible with the new model of HSM.</p> <p>TTYAudit window was halted, baud rate was changed back to 9600 bps, TTYAudit window logging was verified. Between 18:32 and 18:38, Steps 23, 25-28, 32, and 35 were repeated, using the newer model of smart card received with the new HSMs. Step 43 was then repeated, but failed with the same error.</p> <p>As a diagnostic measure, we then used the "6 - View Cards" feature of the new HSM, and determined that the cards generated in Step 28 were actually OP cards, rather than the CO cards that were needed.</p> <p>We used the "7 - Role Management" feature of the new HSM to generate CO cards, and then used them to repeat Step 43, completing successfully at 18:56.</p> <p>We then resumed the normal script sequence by proceeding to Step 44.</p>		
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>		

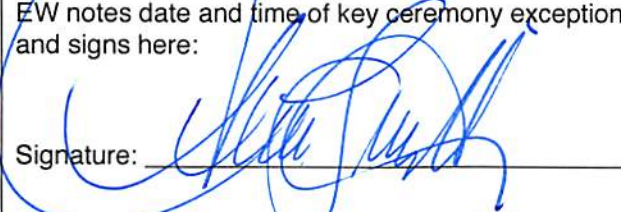

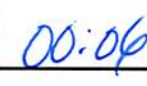
*** End of DNSSEC Key Ceremony Script Exception ***

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>EW Describes exception and action here:</p> <p>In step 34 the text reads apply label "KSK-HSM-02-SJC"</p> <p>Instead we labeled the HSM correctly as "KSK-HSM-02-BRK"</p>		
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>		<p>17:53</p>



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

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>At Step 106 we encountered a large number of errors in key generation, as a result of the dirty state of the immediately preceding key ceremonies.</p> <p>Step 108 was completed in its entirety, and Steps 107 and 109 were partially completed (with respect to COs 3 and 7, Kim DAVIES and Gaurab UPADHAYA, who had planes to catch), and the remainder of the party stepped out temporarily in accordance with Step 110, while CA1 Robert MARTIN-LEGENE and CA2 Ashley JONES created a file called 20160708.kc_script_gen.outmore to replace the previous 20160708.kc_script_gen.out.</p> <p>Files resulting from the dirty state in /tmp/pch have been tarred into an archive on the HSM-FD entitled 20160708-exception.tmp-pch.tar-gz before they were deleted.</p> <p>We ran Step 103 again, completed 0:04. We ran Step 105 again, completed 0:04 We ran Step 106 again using the outmore file, begun 0:06, and expected to complete at approximately 2:40am UTC.</p> <p>We then resumed the normal script sequence by completing Steps 107 and 109, and then sealing the room again in accordance with Step 110.</p>		
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>		

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

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>EW Describes exception and action here:</p> <p>STEP 113 SPECIFIES KSK-HSM-01B-SJC WHICH SHOULD BE KSK-HSM-02-BRM</p> <p>Step 136 specifies KSK-HSM-01B-SJC HSM Should be KSK-HSM-02-BRM</p>		
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>	<p></p>	<p>03:00</p>

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

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>EW Describes exception and action here:</p> <p>During course of key ceremony 15 we passed midnight UTC passed from July 8th to July 9th most dates hand recorded after midnight were erroneously recorded as July 8th.</p>	<p><i>EW</i></p>	<p>03:47</p>
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: <i>[Handwritten Signature]</i></p>		

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

Participant Signature Sheet

Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
FO	Mimi RAUSCHENDORF	US	Personally identifiable information redacted			7/8/16		
CA1	Robert MARTIN-LEGÈNE					7/8/16	16:31	7/9/2016 03:56
CA2	Ashley JONES					7/8/16	16:30	00:14
EW	Aimee <u>Loenetti</u> LOENETTI					7/8/16	16:32	7/9/2016 03:57
CO1	Steve FELDMAN					7/8/16	16:29	0037
CO2	Michael SINATRA					7/8/16	16:30	0038
CO3	Kim DAVIES					7/8/16	16:30	2049
CO4	Eric ALLMAN					7/8/16	16:29	7/9/16 03:56
CO7	Gaurab UPADHAYA					7/8/16	16:30	2050
SC1	Bill WOODCOCK					7/8/16 9	16:28	03:55
R	Kabindra SHRESTHA					7/8/16		

UTC

PCH DNSSEC Key Ceremony Entry/Exit Log

	Name	Enter	Exit	Initial	Time
	Ashley Jones	19:00	19:44	AKJ	19:00
	Robert	19:21	19:12	AKJ	19:23
	Steve Feldman	19:20	19:13	AKJ	19:23
	Eric Allman	19:20	19:13	AKJ	19:23
	Kim Davies	19:21	19:13	AKJ	19:23
	Ursula B. Syta	19:19	19:13	AKJ	19:23
	Stacey Smith	19:21	19:14	AKJ	19:23
	Casey Ashley Jones	19:19	19:15	AKJ	19:23
	Robert Martini-Leejme	22:32	20:45	AKJ	22:38
	Bill Woodcock	22:37	20:50	AKJ	22:37
	Ashley Jones	22:37	20:51	AKJ	22:38
	Steve Feldman	22:39	20:51	AKJ	22:39
	Eric Allman	22:38	20:52	AKJ	22:39
	Michael Sinatra	22:36	20:52	AKJ	22:38
	Stacey Leonetti	22:37	20:52	AKJ	22:37
	Eric Allman	02:54	00:38	AKJ	02:54

PCH DNSSEC Key Ceremony Entry/Exit Log

UTC

	Name	Enter	Exit	Initial	Time
	Aimee Leonetti		00:39	ALH	02:55
	Bill Woodcock	2:54	00:39	ALH	02:54
	Robert Martin-Legone	02:55	00:39	ALH	02:54