



DNSSEC Key Ceremony #24 Friday, November 20, 2020

Start Audio and Video Recording

Step	Activity	Time (UTC)	Initial
1	FO starts the continuous recording of the video cameras. FO starts the Youtube live stream of the security video cameras. FO starts the Youtube live stream of the signing device. FO starts the tape recorder.	17:39	MB

Sign In to Facility

Step	Activity	Time (UTC)	Initial
2	FO verifies the functioning of audio and video recording. FO confirms all participants are familiar with site procedures.	17:39	MB

Enter the Key Management Facility

Step	Activity	Time (UTC)	Initial
3	Each participant is issued an identification vest. W verifies the identity of each participant by examining a government-issued photo identification. W records the type and number of each piece of identification on the Participant Sheet. Participant signs their record.	17:39	MB

Ground Rules

Step	Activity	Time (UTC)	Initial
4	<p>CA previews ground rules and break procedures with participants.</p> <ul style="list-style-type: none"> - Ceremony participants follow the script step by step. - CA reads each step aloud prior to its performance. Italicized text is informational only and is not read aloud. - Upon completion of each step, CA announces the time of completion. W records the completion time and initials their copy of the script. - Any participant who notices a problem or believes that an error has occurred should interrupt the ceremony immediately. Participants agree upon a resolution before proceeding. - W records any significant discrepancies or deviations from the script on the provided DNSSEC Key Ceremony Script Exception Form. - CA and anyone else handling items removed from a TEB or items on the work surface should have rolled-up sleeves or, preferably, short sleeves. - Questions and suggestions for improvement are welcome at any time, are incorporated into the record, and contribute to the quality of this and future key ceremonies. 	17:42	MB

Introduce New Participants

Step	Activity	Time (UTC)	Initial
5	<p>CA asks if anyone is not known to other attendees. Any unknown attendee is introduced.</p>	17:43	MB

Verify Time and Date

Step	Activity	Time (UTC)	Initial
6	<p>W reads aloud and records the date (month/day/year) and time using the clock visible to all. Participants verify that the time is correct.</p> <p>Date: <u>Nov-20, FR</u></p> <p>Time: <u>17:43</u></p>	17:43	MB

Verify Power

Step	Activity	Time (UTC)	Initial
7	<p>CA verifies that the UPS is connected to and receiving power from the electric grid and that it is charged.</p> <p>CA verifies that both the HSM and signing computer power cables are connected to the UPS.</p>	17:44	MB

Remove Equipment from Safe

Step	Activity	Time (UTC)	Initial
8	<p>SC opens safe and records this action as an entry on the safe's log sheet.</p> <p>SC collects the following items from the safe:</p> <ul style="list-style-type: none"> - HSM - Signing Computer <p>SC reads out the HSM TEB number. W confirms that it matches that last used to seal this HSM.</p> <p>HSM TEB# BB69600212</p> <p>SC reads out the signing computer TEB number. W confirms that it matches that last used to seal this Signing Computer.</p> <p>Signing Computer TEB# BB71705481</p> <p>SC provides sealed HSM and signing computer to the CA.</p> <p>SC records the removal of the HSM and Signing Computer in the safe's log sheet.</p>	17:48	MB
9	<p>CA inspects the TEBs for evidence of tampering, removes and discards the TEBs.</p> <p>CA reads out the HSM serial number. W confirms that it matches that recorded below.</p> <p>HSM Serial# H1411035</p>	17:50	MB

Collect OP Cards

Step	Activity	Time (UTC)	Initial
10	<p>For each of the COs listed in the following table:</p> <p>CA collects the CO's Card Case, shows the card case to the camera, reads out and compares TEB number with that recorded below, and inspects for evidence of tampering.</p> <p>CA retrieves the OP card from the Card Case, reads out and compares TEB number with that recorded below, and inspects for evidence of tampering.</p> <p>CA retrieves the OP card and places it in plain view on the work surface.</p> <p><i>Reproductions of the key ceremony script are available at https://www.pch.net.</i></p>	17:56	MB

Smart Card Reference

CO1 Steve FELDMAN

Item	TEB#	Reference
Card Case	AE26992022	KC23
OP 1 of 7	RA02670368	KC23

CO4 Eric ALLMAN

Item	TEB#	Reference
Card Case	AE26992026	KC23
OP 4 of 7	RA02670366	KC23

CO7 Gaurab UPADHAYA

Item	TEB#	Reference
Card Case	AE26992186	KC22
OP 7 of 7	RA02670219	KC22

Set Up Signing Computer

Step	Activity	Time (UTC)	Initial
11	CA connects the display to the signing computer. CA connects the keyboard to the signing computer. CA connects the signing computer to power and waits for the boot process to complete.	17:59	MB
12	CA initiates a login in tty1 using login pi and password raspberry. CA sets the font size for easy readability by executing: <code>setfont /usr/share/consolefonts/Uni3-Terminus32x16.psf.gz</code> CA initiates a root login by executing: <code>sudo -i</code>	18:00	MB
13	CA sets time to match the wall clock: <code>date mmddHHMMYYYY</code> 20 Nov Fri Verify: <i>Repeat as needed.</i>	18:02	MB
14	CA connects a blank flash drive labeled "HSMFD" to the signing computer. CA mounts the flash drive by executing: <code>mkdir /tmp/HSMFD</code> <code>mount -o noexec /dev/sda1 /tmp/HSMFD</code>	18:03	MB

Start Logging Terminal Session

Step	Activity	Time (UTC)	Initial
15	CA changes directory to the HSMFD and starts capture of terminal output to a file: <code>cd /tmp/HSMFD</code> <code>script -t script-20201120.log 2>script-20201120.timing</code>	18:04	MB

Prepare Environment

Step	Activity	Time (UTC)	Initial
16	<p>CA connects the flash drive labeled "SCRIPTS" to the signing computer.</p> <p>CA mounts the flash drive by executing:</p> <pre>mkdir /tmp/SCRIPTS mount -o ro,noexec /dev/sdb1 /tmp/SCRIPTS</pre> <p>CA lists the contents of the SCRIPTS flash drive for the record.</p> <pre>ls /tmp/SCRIPTS</pre>	18:06	MB
17	<p>CA copies the compressed archive of the previous key ceremony from SCRIPTS into the current directory on the HSMFD.</p> <pre>cp -p /tmp/SCRIPTS/HSMFD-20200619.tar.gz . sha256sum HSMFD-20200619.tar.gz</pre> <p>Verify that the checksum is:</p> <pre>E25C 3469 7C8C 641E D6E6 1E7A 3F57 9157 E65D C42D CAB6 243D F08E 0894 7B33 FA69</pre> <p>Un-tar the archive:</p> <pre>tar -xzvof HSMFD-20200619.tar.gz</pre>	18:09	MB
18	<p>CA copies the compressed input files from SCRIPTS into the current directory on the HSMFD.</p> <pre>cp -p /tmp/SCRIPTS/scripts-20201120.tar.gz . tar -xzvof scripts-20201120.tar.gz . bootstrap</pre>	18:10	MB

Start Logging HSM Output

Step	Activity	Time (UTC)	Initial
19	<p>CA connects the signing computer to the serial port of the HSM.</p> <p>CA switches to tty2 by pressing Ctrl+Alt+F2 and initiates a login using login pi and password raspberry.</p> <p>CA sets the font size for easy readability by executing:</p> <pre>setfont /usr/share/consolefonts/Uni3-Terminus32x16.psf.gz</pre> <p>CA initiates a root login by executing:</p> <pre>sudo -i</pre> <p>CA starts logging HSM serial output by executing:</p> <pre>cd /tmp/HSMFD stty -F /dev/ttyUSB0 115200 /tmp/kc/bin/ttyaudit /dev/ttyUSB0</pre> <p><i>Do not unplug the USB-serial adaptor from the signing computer until instructed, as this would cause logging to stop.</i></p>	18:13	MB

Connect Offline HSM (KSK-HSM-02-BRK)

Step	Activity	Time (UTC)	Initial
20	<p>CA connects the HSM to power and toggles HSM power switch, if required.</p> <p><i>Status information appears on the display and the "Ready" LED on the HSM blinks. After completing its self-test the HSM displays the text "Set Online," indicating that the HSM is in the initialized state, and the "Ready" LED is off.</i></p>	18:14	MB

Activate HSM

Step	Activity	Time (UTC)	Initial
21	<p>CA brings HSM online using the "Set Online" menu item. When prompted, CA inserts one of the OP cards and enters the corresponding card PIN.</p> <p><i>All cards have PIN 11223344.</i></p> <p>CA repeats this process using two open OP cards. When complete the HSM "Ready" LED illuminates.</p> <p><i>The HSM always refers to cards 1, 2, and 3.</i></p>	18:16	MB
22	<p>CA switches to tty1 by pressing Ctrl+Alt+F1.</p> <p>CA connects the signing computer to the HSM's LAN port using an Ethernet cable.</p> <p>CA initiates communication by executing:</p> <pre>set-hsm-env KSK-HSM-02-BRK</pre> <p>CA truncates the ZSKSlotDB and KSKSlotDB files:</p> <pre>cd /tmp/kc reset-token-store KSK-HSM-02-BRK</pre>	18:18	MB

Start Generating Keys and Keybundles

Step	Activity	Time (UTC)	Initial
23	<p>CA copies the encrypted backups of the KSKs and ZSKs by executing:</p> <pre>makeallhsmfiles</pre> <p>CA initiates key and signature generation by executing:</p> <pre>key-and-sig-gen</pre> <p><i>This will take a long time generating new keys and keybundles (KSK signed DNSKEY RRsets). KSKs and ZSKs will automatically be backed up in encrypted form and deleted from HSM as each zone is completed.</i></p>	18:19	MB

Repackage and Redistribute OP Cards

Step	Activity	Time (UTC)	Initial
24	<p>For each of the COs listed in the following table:</p> <p>CA places the respective OP card in its own new TEB reading the TEB number aloud. W confirms the TEB matches that recorded in the Smart Card Sign-Out Sheet below.</p> <p>CA holds the TEB to one of the cameras for the visual record.</p> <p>CA places the sealed cards into the respective Card Case, and places the Card Case in its own new TEB reading the TEB number aloud. W confirms the TEB matches that recorded on the Smart Card Sign-Out Sheet below.</p> <p>CA calls the CO to retrieve their sealed Card Case. The CO verifies and signs W's copy of the Smart Card Sign-Out Sheet. W records the time and initials the CO's entries on the Smart Card Sign-Out Sheet.</p>	18:29	W

Smart Card Sign-Out Sheet

CO1 Steve FELDMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA02670346	OP 1 of 7		11/20/20		
AE26992042	Card Case		11/20/20		

CO4 Eric ALLMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA02670356	OP 4 of 7		11/20/20		
AE26992036	Card Case		11/20/20		

CO7 Gaurab UPADHAYA

TEB#	Containing	Signature	Date	Time UTC	W
RA02670358	OP 7 of 7		11/20/20		
AE26992038	Card Case		11/20/20		

Intermission

Step	Activity	Time (UTC)	Initial
25	All participants leave the vault and record an entry on the DNSSEC Key Ceremony Entry/Exit Log. <i>This break is to accommodate the long-running script.</i>	18:31	MB

Reenter Facility

Step	Activity	Time (UTC)	Initial
26	Participants re-enter the vault and record an entry on the DNSSEC Key Ceremony Entry/Exit Log.	20:36	MB

Pack and Store Keys and Keybundles

Step	Activity	Time (UTC)	Initial
27	CA confirms the completion of the key generation script.	20:38	MB
28	CA generates the archive destined for the signers by executing: <code>pack-today-kb</code> CA archives all results including wrapped KSKs for future use by executing: <code>pack-today-session</code> CA creates a snapshot of any changes to database files by executing: <code>cd /tmp/HSMFD</code> <code>pack-snapshot-db KSK-HSM-02-BRK</code>	20:41	MB
29	CA creates checksums of all files on the HSMFD by executing: <code>find . -type f -print0 xargs -0 -n 50 sha256sum</code>	20:42	MB

Return HSM to a TEB

Step	Activity	Time (UTC)	Initial
30	<p>CA switches to tty2 by pressing Ctrl+Alt+F2.</p> <p>CA presses the HSM's RESTART button and waits for self-test to complete.</p> <p>CA confirms the HSM is offline by checking the Ready LED is off.</p> <p>CA disconnects HSM from power and signing computer (serial and Ethernet), places it into a new TEB, and seals.</p> <p>CA shows sealed TEB to participants.</p> <p>CA reads out the HSM serial number. W confirms that it matches that recorded below:</p> <p>HSM Serial#: H1411035</p> <p>CA reads out the TEB number. W confirms that it matches that recorded below:</p> <p>HSM TEB#: BB69600206</p>	<p>20:46</p>	<p>MB</p>

Stop Recording Serial Port Activity

Step	Activity	Time (UTC)	Initial
31	<p>CA terminates HSM serial output capture by disconnecting the USB serial adaptor from the signing computer.</p> <p>CA then exits serial output terminal by executing:</p> <pre>exit exit</pre> <p>CA switches to tty1 by pressing Ctrl+Alt+F1.</p>	<p>20:47</p>	<p>MB</p>

Stop Logging and Create Archive

Step	Activity	Time (UTC)	Initial
32	<p>CA displays contents of the HSMFD by executing:</p> <pre>ls -ltr</pre> <p>CA stops logging terminal output by executing:</p> <pre>exit</pre> <p>CA creates a single archive by executing:</p> <pre>/tmp/kc/bin/pack-hsmfd</pre>	20:50	MB
33	<p>CA calculates the SHA-256 checksum of the archive by executing:</p> <pre>sha256sum HSMFD-20201120.tar.gz</pre> <p>CA reads the hash of the checksum aloud.</p> <p>W records the sixty-four digit hash:</p> <p><u>5AAF A673 0340 F5BF</u> <u>0193 D205 2DB2 B604</u> <u>BC F01B 8F67 9273</u> <u>DD88 2F25 5F45 10565C</u></p> <p>W reads back the hash aloud.</p>	21:00	MB

Backup HSM Flash Drive Contents

Step	Activity	Time (UTC)	Initial
34	<p>CA plugs a blank flash drive labeled "HSMFD" into the signing computer.</p> <p>CA mounts the flash drive by executing:</p> <pre>mkdir /tmp/HSMFD_</pre> <pre>mount -o noexec /dev/sdc1 /tmp/HSMFD_</pre> <p>CA copies the contents of the HSMFD to the blank drive for backup by executing:</p> <pre>cp -a * /tmp/HSMFD_</pre>	21:04	MB

35	<p>CA unmounts the new flash drive by executing: <code>umount /tmp/HSMFD_</code></p> <p>CA removes the flash drive from the signing computer, places the flash drive in a new TEB and seals it.</p> <p>CA shows sealed TEB to participants.</p> <p>CA reads out the TEB number. W confirms that it matches that recorded below:</p> <p>TEB#: RA02670340</p> <p><i>This copy will be stored with the on-site audit bundle.</i></p>	21:07	MB
36	<p>CA repeats the previous two steps to create a second backup.</p> <p>CA reads out the TEB number. W confirms that it matches that recorded below:</p> <p>TEB#: RA02670330</p> <p><i>This copy will be stored with the off-site audit bundle.</i></p>	21:11	MB

Remove Flash Drives

Step	Activity	Time (UTC)	Initial
37	<p>CA unmounts SCRIPTS by executing: <code>umount /tmp/SCRIPTS</code></p> <p>CA removes the flash drive labelled SCRIPTS.</p> <p><i>This flash drive is retained by the CA.</i></p> <p>CA unmounts HSMFD by executing: <code>cd /tmp</code> <code>umount /tmp/HSMFD</code></p> <p>CA removes the flash drive labelled HSMFD.</p> <p><i>This copy is used for operations and the published archive.</i></p>	21:13	MB

Return Signing Computer to a TEB

Step	Activity	Time (UTC)	Initial
38	<p>CA disconnects power, keyboard, and display cables from the signing computer. CA and W take note of anything else that needs to be removed from the signing computer.</p> <p>CA places the signing computer in new TEB and seals it.</p> <p>CA shows sealed TEB to participants.</p> <p>CA reads out the TEB number. W confirms that it matches that recorded below:</p> <p>Signing Computer TEB#: BB71705480</p>	21:14	MB

Secure Equipment

Step	Activity	Time (UTC)	Initial
39	<p>SC returns items to the safe.</p> <ul style="list-style-type: none"> - KSK-HSM-02-BRK HSM - Signing Computer - HSMFD 1 above <p>SC records return of each item on the safe log with TEB number, name of item, date, time, and signature. A second participant initials each entry.</p> <p><i>Power supplies and cables are not stored the safe and will be stored separately.</i></p> <p>SC records a closing action on the safe's log sheet and returns the log sheet to the safe. SC closes the safe. W verifies it is locked.</p>	21:19	MB

Sign-Out

Step	Activity	Time (UTC)	Initial
40	<p>All participants leave the Key Management Facility and record an entry on the DNSSEC Key Ceremony Entry/Exit Log.</p>	21:20	MB

Stop Audio-Visual Recording

Step	Activity	Time (UTC)	Initial
41	FO stops audio and video recording.	21:21	MB

Sign Out of Facility

Step	Activity	Time (UTC)	Initial
42	FO returns computers and other items to participants. Participants return identification vests to FO. Participants are now free to depart. FO logs their exit times.	21:24	MB

Attestations

Step	Activity	Time (UTC)	Initial
43	SC completes Access Control System Attestation. CA completes Key Ceremony Script Attestation.		

Copy and Store the Script

Step	Activity	Time (UTC)	Initial
44	<p>FO makes at least three colour copies of the W's script: one for the on-site audit bundle, one for off-site audit bundle, one for the W, and copies for other participants as requested. FO delivers the original to the SC.</p> <p>The two audit bundles each containing:</p> <ul style="list-style-type: none"> - output of signer system - HSMFD - copy of W's key ceremony script - audio-visual recording - logs from the Facility Physical Access Control - SC attestation (Appendix A) - CA attestation (Appendix B) <p>FO places each bundle in a TEB labeled "Key Ceremony 2020-11-20". CA dates and signs each bundle.</p> <p><i>One bundle will be stored by the SC. The second bundle will be kept securely offsite.</i></p>		

Stop Audio and Video Recording

Step	Activity	Time (UTC)	Initial
45	<p>FO stops the tape recorder.</p> <p>FO stops the Youtube live stream of the signing device.</p> <p>FO stops the Youtube live stream of the security video cameras.</p> <p>FO stops the continuous recording of the video cameras.</p>		

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 Nov. 20, 2020 before me, MARY SHAMPA BAPI, Notary Public,
Date Here Insert Name and Title of the Officer
personally appeared ROBERT ARSMITH
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 Mary Shampa Bapi
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 SERIA ATTESTATION Document Date: _____
Number of Pages: _____ Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____
 Corporate Officer — Title(s): _____
 Partner — Limited General
 Individual Attorney in Fact
 Trustee Guardian or Conservator
 Other: _____
Signer Is Representing: _____

Signer's Name: _____
 Corporate Officer — Title(s): _____
 Partner — Limited General
 Individual Attorney in Fact
 Trustee Guardian or Conservator
 Other: _____
Signer Is Representing: _____

Access Control System Attestation

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








Printed Name: ROBERT ANASMITA

Signature: 

Date: 11/20/2020

SEE NOTARY'S CERTIFICATE

Participant Sheet

Role	Name	Citizenship	Form of Identification	Identification Number	Signature
CA2	Bob ARASMITH	US	CADL	CA2	
W	Mary Shampa BAPI	US	CADL	A	
CO1	Steve FELDMAN				
CO4	Eric ALLMAN	US	CADL	N	
CO7	Gaurab UPADHAYA				
SC2	Bob ARASMITH	US	CADL		
O	Mimi RAUSCHENDORF	US	CADL	C	
R	Jorge CANO				REMOTE

DNSSEC Key Ceremony Entry/Exit Log

Name	Time UTC	In/Out	Initial	Witness
Mimi Rauschendorf	17:35	In/Out	MR	
Eric Allman	17:36	In/Out	EA	
Robert Arasmita	17:37	In/Out	RA	
MARY BAPI	17:37	In/Out	MB	
Robert Arasmita	18:32	In/Out		
Eric Allman	18:32	In/Out		
Mimi Rauschendorf	18:32	In/Out	MR	
MARY BAPI	18:30	In/Out	MB	
Eric Allman	20:13	In/Out		
Mimi Rauschendorf	20:13	In/Out	MR	
Robert Arasmita	20:19	In/Out		
MARY BAPI	20:50	In/Out	MB	
Robert Arasmita	21:19	In/Out		
Eric Allman	21:20	In/Out		
Mimi Rauschendorf	21:20	In/Out	MR	
MARY BAPI	21:20	In/Out	MB	
		In/Out		
		In/Out		
		In/Out		
		In/Out		

Notary Acknowledgment

The Notary Acknowledgment is provided on the following page(s).

Facility Sign In Sheet

Facility supplied entry and exit records are provided on the following page(s).