



DNSSEC Key Ceremony Script Tuesday, August 14, 2018

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.		
2	FO reviews emergency evacuation procedures and other relevant information with participants.		
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.		
4	FO verifies the functioning of audio and video recording.		

Enter the Key Management Facility

Step	Activity	Initial	Time (PDT)
5	<p>As the participants enter the Key Management Facility, W verifies the identity of each by examining a government-issued photo identification. As the participants are identified, W issues each an identification vest.</p> <p>W notes the type and number of each piece of identification and the participant's entry time on the Participant Signature Sheet.</p> <p>Participants do not sign the sheet until the end of the ceremony.</p>		

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"> - Ceremony participants follow the script step by step. - CA reads each step aloud prior to its performance. Text in [square brackets] 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. 		

Introduce New Participants

Step	Activity	Initial	Time (PDT)
7	<p>CA asks if anyone is not known to other attendees. Any unknown attendee is introduced.</p>		

Verify Time and Date

Step	Activity	Initial	Time (PDT)
8	<p>W 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: _____</p> <p>Time: _____</p> <p>[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>		

Verify UPS

Step	Activity	Initial	Time (UTC)
9	<p>If there is a UPS,</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. 		

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
10	<p>SC opens safe and records this action as an entry in the safe's log sheet.</p>		
11	<p>SC collects the following items from the safe:</p> <ul style="list-style-type: none"> - KSK-HSM-02-BRK HSM - boot-DVD - laptop - any other items that may be required <p>SC indicates removal of each with any applicable TEB or serial number in the safe's log sheet. SC also provides any necessary power supplies and cables. SC places equipment on work surface visible to all participants.</p>		

12	<p>CA reads out KSK-HSM-02-BRK HSM TEB and serial numbers. W confirms that they match those recorded in the script from the most recent key ceremony performed at this site.</p> <p>HSM TEB# BB69600253</p> <p>HSM Serial# H1411035</p>		
13	<p>CA reads out boot-DVD and laptop TEB numbers. W confirms that they match those recorded in the script from the most recent ceremony performed at this site.</p> <p>DVD TEB# BB71705227</p> <p>Laptop TEB# BB69600254</p>		

Collect OP Cards

Step	Activity	Initial	Time (UTC)
14	<p>CA collects card case from CO1, inspects outer TEB, and reads out and compares TEB number with that recorded in the last ceremony. CA retrieves OP1 from the card case, reads out and compares TEB number with that recorded in the last ceremony, then opens the TEB, placing the card in plain view on the work surface.</p> <p>CA repeats the step above for CO3 and CO4.</p> <p>[Smart Card Sign-Out Sheets from previous key ceremonies are reproduced for convenience in the appendices of this document. Different COs may appear on different pages.]</p>		

Set Up Laptop

Step	Activity	Initial	Time (UTC)
15	<p>CA removes the boot-DVD and laptop from their TEBs and places them on the work surface. CA shows the participants that the laptop contains no boot devices.</p> <p>CA connects the laptop to power, using the UPS if available. Any external monitor or projector is powered from either utility power or the UPS, if it has sufficient capacity.</p> <p>CA powers the laptop on, booting it from the DVD.</p> <p>CA makes sure the output on the laptop screen is visible on any external monitor or projector.</p> <p>[Use the function + F8 keys to cycle through until the display shows only on the external monitor or projector. This must be done before Linux gets past the boot loader, or you may have to reboot again until you succeed. Boot warnings may be ignored if it continues to boot.]</p>		
16	CA initiates a root login.		
17	<p>CA opens a terminal window.</p> <p>[Applications > Accessories > Terminal]</p>		
18	<p>CA sets the time zone on the laptop to UTC:</p> <pre>cd /etc/ rm localtime ln -s /usr/share/zoneinfo/UTC localtime</pre> <p>CA sets time to match the wall clock:</p> <pre>date mmddHHMMYYYY</pre> <p>Verify:</p> <pre>date</pre> <p>Repeat as needed. When pleased, close the window:</p> <pre>exit</pre>		
19	CA connects a blank flash drive labeled "HSMFD" to the laptop, then closes the window when the operating system recognizes the flash drive.		

Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
20	<p>CA opens new terminal window. In this window, the CA changes the default directory to the HSMFD and starts capture of terminal output to a file:</p> <pre>cd /media/HSMFD script -t script-20180814.log 2>script-20180814.timing</pre> <p>CA connects the flash drive labeled "SCRIPTS" to the laptop, then closes the window when the operating system recognizes the flash drive.</p> <p>CA copies the compressed archive of the previous key ceremony from SCRIPTS into the current directory on the HSMFD.</p> <pre>ls /media/SCRIPTS/ cp -p /media/SCRIPTS/HSMFD-20180202.tar.gz . sha256sum HSMFD-20180202.tar.gz</pre> <p>Verify that the checksum is:</p> <pre>6C3A 8D60 26AD E9A9 97BD 74DA CFA2 F9AF 24EE E13A AFB9 62A4 C642 17A1 703E D1FA</pre> <p>Un-tar the archive:</p> <pre>tar -xzvof HSMFD-20180202.tar.gz</pre> <p>CA copies the compressed input files from SCRIPTS into the current directory on the HSMFD.</p> <pre>cp -p /media/SCRIPTS/scripts-20180814.tar.gz . tar -xzvof scripts-20180814.tar.gz sh bootstrap</pre>		

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
21	<p>CA inspects the HSM TEB for evidence of tampering and removes the HSM from the TEB. CA discards the TEB and uses a USB-serial adaptor to connect the laptop to the serial port of the HSM.</p>		

22	<p>CA opens a second terminal window, which we will refer to as the "ttyaudit window". In this window the CA starts logging HSM serial output by executing:</p> <pre>cd /media/HSMFD stty -F /dev/ttyUSB0 115200 ttyaudit /dev/ttyUSB0</pre> <p>[Do not unplug the USB-serial adaptor from the laptop until instructed, as this would cause logging to stop.]</p>		
----	---	--	--

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

Step	Activity	Initial	Time (UTC)
23	<p>CA connects the HSM to power, using the UPS if one is available.</p> <p>[Status information appears in the "ttyaudit window," 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.</p>		

Activate HSM

Step	Activity	Initial	Time (UTC)
24	<p>CA sets HSM online using the "Set Online" menu item and OP cards 1, 3, and 4. The "Ready" LED illuminates.</p> <p>Use OP cards 1, 3 and 4.</p> <p>[All cards have PIN 11223344]</p> <p>[The HSM always refers to cards 1, 2, and 3, regardless of our numbering (possibly) being different.]</p>		
25	<p>CA initiates communication with the HSM by connecting it to the laptop with an Ethernet cable and executing:</p> <pre>ipadd set-hsm-env</pre>		

Ensure HSM Data Synchronization

Step	Activity	Initial	Time (UTC)
26	CA ensures the local database is synchronized with the HSM by executing: <code>reset-local-slot-db</code> [This step recovers from a data synchronization issue that occurred in KC18 and KC19.]		

Start Generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)
27	CA disables laptop screen saver and power management features by executing: <code>disable-screensaver</code>		
28	CA copies the encrypted backups of the ZSKs by executing: <code>cd /tmp/pch</code> <code>makeallhsmfiles</code>		
29	CA initiates key and signature generation by executing: <code>key-and-sig-gen</code> [This will take a long time generating ZSKs and KSKs as necessary and creating keybundles (KSK signed DNSKEY RRsets). KSKs and ZSKs will automatically be backed up in encrypted form and deleted from HSM as each zone is completed.]		

Repackage and Redistribute OP Cards

Step	Activity	Initial	Time (UTC)
30	<p>CA places the OP1 card in its own new TEB reading the TEB number aloud. W records the TEB number in the Smart Card Sign-Out Sheet below, repeating it aloud for verification.</p> <p>CA places the sealed OP1, SO1 and SMK1 cards in CO1's card case.</p> <p>CA places the card case in its own new TEB reading the TEB number aloud. W records the TEB number in the Smart Card Sign-Out Sheet below, repeating it aloud for verification.</p> <p>CA calls CO1 to retrieve their sealed card case. CO1 verifies, dates, and signs W's copy of the Smart Card Sign-Out Sheet. W initials their entries on the Smart Card Sign-Out Sheet.</p> <p>CA repeats the steps above for CO3 and CO4.</p>		

Smart Card Sign-Out Sheet

CO1 Steve FELDMAN

TEB#	Containing	Signature	Date	Time UTC	W
	OP 1 of 7		8/14/18		
	SO 1 of 7		8/14/18		
	SMK 1 of 7		8/14/18		
	Card Case		8/14/18		

CO3 Kim DAVIES

TEB#	Containing	Signature	Date	Time UTC	W
	OP 3 of 7		8/14/18		
	SO 3 of 7		8/14/18		
	SMK 3 of 7		8/14/18		
	Card Case		8/14/18		

CO4 Eric ALLMAN

TEB#	Containing	Signature	Date	Time UTC	W
	OP 4 of 7		8/14/18		
	SO 4 of 7		8/14/18		
	SMK 4 of 7		8/14/18		
	Card Case		8/14/18		

Intermission

Step	Activity	Initial	Time (UTC)
31	All participants leave the room and record an entry in the DNSSEC Key Ceremony Exit/Re-Entry Log. Participants who do not intend to return to the Key Ceremony must complete the Participant Signature Sheet and note their exit time on the Facility Sign-In Sheet. [This break is to accommodate the long-running script.]		
32	SC closes and seals the door.		

Reenter Facility

Step	Activity	Initial	Time (UTC)
33	SC and CA both inspect the door's seal for signs of tampering and open the door.		
34	Participants re-enter the room, noting their entry on the DNSSEC Key Ceremony Exit/Re-Entry Log.		

Pack and Store Keys and Keybundles

Step	Activity	Initial	Time (UTC)
35	CA confirms the completion of the key generation script.		
36	CA generates the archive destined for the signers by executing: <code>pack-today-kb</code>		
37	CA archives all results including encrypted KSKs for future use by executing: <code>pack-today-session</code>		
38	CA creates a snapshot of any changes to database files by executing: <code>cd /media/HSMFD</code> <code>pack-snapshot-db KSK-HSM-02-BRK</code>		

39	CA creates checksums of all files on the HSMFD by executing: <code>find . -type f -print0 xargs -0 -n 50 sha256sum</code>		
----	--	--	--

Return HSM to a TEB

Step	Activity	Initial	Time (UTC)
40	CA presses the HSM's RESTART button and waits for self-test to complete. CA then disconnects HSM from power and laptop (serial and Ethernet), places it into a new TEB, and seals.		
41	CA reads out TEB and HSM serial numbers and shows sealed TEB to participants. W records TEB and HSM serial numbers here: TEB#: _____ HSM Serial#: _____		

Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
42	CA terminates HSM serial output capture by disconnecting USB serial adaptors from laptop. CA then exits serial output terminal window. <code>exit</code>		

Display HSM FD Contents

Step	Activity	Initial	Time (UTC)
43	CA displays contents of the HSMFD by executing: <code>ls -ltr</code>		

Stop Logging and Create Archive

Step	Activity	Initial	Time (UTC)
44	CA stops logging terminal output by executing: <code>exit</code>		

45	Pack all into a single archive by executing: <pre>pack-hsmfd</pre>		
46	CA calculates checksum of the archive by executing: <pre>sha256sum HSMFD-20180814.tar.gz</pre> CA reads the hash of the checksum aloud. W records the sixty-four digit hash: _____ _____ _____ _____		

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
47	CA plugs a blank flash drive labeled "HSMFD" into the laptop. When the FD is recognized as HSMFD_, CA copies the contents of the HSMFD to the blank drive for backup by executing: <pre>cp -Rp * /media/HSMFD_</pre>		
48	CA unmounts the new flash drive by executing: <pre>umount /media/HSMFD_</pre> CA removes the flash drive from the laptop, places the flash drive in a new TEB and seals it, reads out TEB number, and shows sealed TEB to participants. W records TEB number here: TEB#: _____ [This copy will be stored with the on-site audit bundle.]		
49	CA repeats the previous two steps to create a second backup. TEB#: _____ [This copy will be stored with the off-site audit bundle.]		

Remove HSM FD

Step	Activity	Initial	Time (UTC)
50	CA unmounts HSMFD by executing: <pre>cd /tmp umount /media/HSMFD</pre>		
51	CA removes the flash drive. [This copy is used for operations and the published archive.]		

Return Boot-DVD to a TEB

Step	Activity	Initial	Time (UTC)
52	CA executes: <pre>halt -p -f</pre> removes DVD and turns off laptop. [CA may need to power on the laptop for the eject button to function.]		
53	CA places boot-DVD in new TEB and seals it, reads out TEB number, and shows sealed TEB to participants. W records TEB number here: DVD TEB#: _____		

Return Laptop to a TEB

Step	Activity	Initial	Time (UTC)
54	CA disconnects power and any other connections from laptop, puts laptop in new TEB and seals it, reads out TEB number, and shows sealed TEB to participants. W records TEB number here: Laptop TEB#: _____		

Return Power Supplies and Cables

Step	Activity	Initial	Time (UTC)
55	<p>CA places the following in a box or bag.</p> <ul style="list-style-type: none"> - HSM power supply - Laptop power supply - Serial cable - USB serial adapter - Networking cables <p>[The bag is used for convenience and need not be a TEB.]</p>		
56	<p>SC returns items to the safe. 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> <ul style="list-style-type: none"> - KSK-HSM-02-BRK HSM - laptop - HSMFD 1 above - boot-DVD <p>[Power supplies and cables need not go in the safe and can be stored separately.]</p>		
57	<p>SC records a closing action in the safe's log sheet and returns the log sheet to the sage. SC closes the safe. W verifies it is locked.</p>		

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
58	<p>All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.</p>		

Stop Audio-Visual Recording

Step	Activity	Initial	Time (PDT)
59	<p>FO stops audio and video recording.</p>		

Script Review

Step	Activity	Initial	Time (PDT)
60	CA reviews W's script and signs it. CA Signature: _____		

Sign Out of Facility

Step	Activity	Initial	Time (PDT)
61	FO returns personal phones, laptops, and other items to participants. Participants return identification vests to FO. Participants are now free to depart. FO logs their exit times.		

Attestations

Step	Activity	Initial	Time (PDT)
62	SC completes Access Control System Attestation in Appendix A. CA completes Key Ceremony Script Attestation in Appendix B. W completes notary attestation.		

Copy and Store the Script

Step	Activity	Initial	Time (PDT)
63	<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 08/14/2018". CA dates and signs each bundle.</p> <p>[One bundle will be stored by the SC. The second bundle will be kept securely offsite.]</p>		

Appendix A:
Access Control System Attestation
(by SC)

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

Attached is the audited physical access log.

Printed Name: _____

Signature: _____

Date: _____

Appendix B:
Key Ceremony Script Attestation
(by CA)

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: _____

Signature: _____

Date: _____

Insert Notary Acknowledgement Here

Appendix C:

Abbreviations Used in This Document

Roles

CA	Ceremony Administrator
CO	Crypto Officer
FO	Facilities Officer
O	Observer
SC	Security Controller
W	Witness

Other Abbreviations

AAK	Adapter Authorization Key
FD	Flash Drive
HSM	Hardware Security Module
KSK	Key Signing Key
OP	Operator
SMK	Storage Master Key
SO	Security Operator
TEB	Tamper Evident Bag
UPS	Uninterruptible Power Supply
ZSK	Zone Signing Key

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	November	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	X-ray	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



1600 Shattuck Avenue Facility Sign-In Sheet

Role	Name	Signature	Date	Entry Time PDT	Exit Time PDT
FO	Mimi RAUSCHENDORF		8/14/18		
CA1	James MITCHELL		8/14/18		
W	Mary Shampa BAPI		8/14/18		
CO1	Steve FELDMAN		8/14/18		
CO3	Kim DAVIES		8/14/18		
CO4	Eric ALLMAN		8/14/18		
SC1	Bill WOODCOCK		8/14/18		
O	Ashley JONES		8/14/18		

Participant Signature Sheet

Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
FO	Mimi RAUSCHENDORF					8/14/18		
CA1	James MITCHELL					8/14/18		
W	Mary Shampa BAPI					8/14/18		
CO1	Steve FELDMAN					8/14/18		
CO3	Kim DAVIES					8/14/18		
CO4	Eric ALLMAN					8/14/18		
SC1	Bill WOODCOCK					8/14/18		
O	Ashley JONES					8/14/18		

DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	W describes exception and action here:		
2	W notes date and time of key ceremony exception and signs here: Signature: _____		

End of DNSSEC Key Ceremony Script Exception Form

Appendix: E

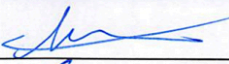

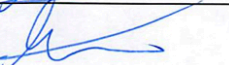
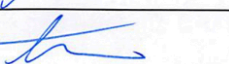
Smart Card Sign Out Sheet from Key Ceremony 18

DNSSEC Key Ceremony Script

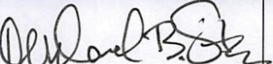
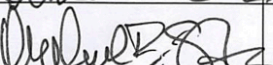
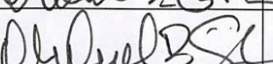
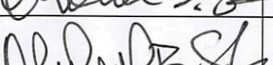
Thursday, September 28, 2017

Key Ceremony 18
Smart Card Sign Out Sheet

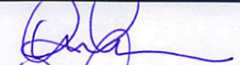
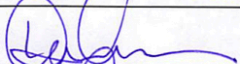


CO1 Steve FELDMAN

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

CO2 Michael SINATRA

TEB #	Containing	Signature	Date	Time	EW
RA02070179	OP2 of 7		9/28/17	18:15	MAB
RA02070187	SO2 of 7		9/28/17	18:15	MAB
RA02070171	SMK2 of 7		9/28/17	18:10	MAB
AE20992106	Card Case 2		9/28/17	18:17	MAB

CO3 Kim DAVIES

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





Appendix: F



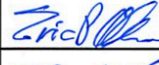

Smart Card Sign Out Sheet from Key Ceremony 19





DNSSEC Key Ceremony Script

Friday, February 2, 2018

Smart Card Sign Out Sheet

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

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

CO 7	OP 7 of 7	RA02070382	Gaurab UPADHAYA		2/2/18	20:22	MB
CO 7	SO 7 of 7	RA02070384	Gaurab UPADHAYA		2/2/18	20:22	MB
CO 7	SMK 7 of 7	RA02070147	Gaurab UPADHAYA		2/2/18	20:22	MB
CO 7	Card Case	AE20992008	Gaurab UPADHAYA		2/2/18	20:22	MB