



DNSSEC Key Ceremony Script Friday, March 22, 2019

Sign In to Facility

Step	Activity	Time (UTC)	Initial
1	FO has all participants sign in on Facility Sign-In Sheet before entering the Key Management Facility.	16:19	MB
2	FO reviews emergency evacuation procedures and other relevant information with participants.	16:19	MB
3	FO collects and stores participants' 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.	16:19	MB
4	FO verifies the functioning of audio and video recording.	16:19	MB

Enter the Key Management Facility

Step	Activity	Time (UTC)	Initial
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>	16:26	MB

Ground Rules

Step	Activity	Time (UTC)	Initial
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. 	16:27	MB

Introduce New Participants

Step	Activity	Time (UTC)	Initial
7	<p>CA asks if anyone is not known to other attendees. Any unknown attendee is introduced.</p>	16:28	MB

Verify Time and Date

Step	Activity	Time (UTC)	Initial
8	<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>22 MAR. FRI</u></p> <p>Time: <u>16:28</u></p>	16:29	MB

Verify UPS

Step	Activity	Time (UTC)	Initial
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. 	16:32	MB

Remove Equipment from Safe

Step	Activity	Time (UTC)	Initial
10	<p>SC opens safe and records this action as an entry in the safe's log sheet.</p> <p>SC collects the following items from the safe:</p> <ul style="list-style-type: none"> - KSK-HSM-02-BRK HSM - boot-media - signing computer <p>SC indicates removal of each with any applicable TEB or serial number in the safe's log sheet. SC places equipment on work surface visible to all participants.</p> <p>[The laptop and boot-DVD are being retired and are placed aside.]</p>	16:36	MB
11	<p>CA reads out the HSM TEB number. W confirms that it matches that recorded in the script from the most recent key ceremony performed at this site.</p> <p>HSM TEB# BB69600249</p> <p>CA inspects the HSM TEB for evidence of tampering and removes the HSM from the TEB. CA discards the TEB.</p> <p>CA reads out the HSM serial number. W confirms that it matches that recorded in the script from the most recent key ceremony performed at this site.</p> <p>HSM Serial# H1411035</p>	16:38	MB

Collect OP Cards

Step	Activity	Time (UTC)	Initial
12	<p>CA collects card case from CO1, inspects outer TEB, and reads out and compares TEB number with that recorded in their last key 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 CO2 and CO7.</p> <p>[Smart Card Sign-Out Sheets from previous key ceremonies are reproduced in the appendices of this document. Different COs may appear on different pages.]</p>	16:44	MB

Set Up Signing Computer

Step	Activity	Time (UTC)	Initial
13	<p>CA shows the participants that the signing computer contains no boot devices.</p> <p>CA inserts the boot media.</p> <p>CA connects the display to the signing computer. CA ensures that the display is on, connecting it to power if necessary.</p> <p>CA connects the keyboard to the signing computer.</p> <p>CA connects the signing computer to power, using the UPS if available, and waits for the boot process to complete.</p>	16:51	MB
14	<p>CA initiates a login in tty1 using login pi and password raspberry.</p> <p>CA initiates a root login by executing:</p> <pre>sudo -i</pre>	16:53	MB
15	<p>CA sets time to match the wall clock:</p> <pre>date mmddHHMMYYYY</pre> <p>Verify:</p> <pre>date</pre> <p>Repeat as needed.</p>	16:54	MB

16	<p>CA calculates the SHA-256 checksum of the boot media by executing:</p> <pre>sha256sum /dev/mmcblk0</pre> <p>CA reads the hash of the checksum aloud.</p> <p>W records the sixty-four digit hash:</p> <p>A75B 7178 FA20 3BE9 9911 4163 B5EE 117A 9B7D A5BC 4A60 6469 4D64 E8CB 63EA 96B9</p> <p>W reads back the hash aloud.</p>	16:58	MB
17	<p>CA connects a blank flash drive labeled "HSMFD" to the signing computer.</p> <p>CA mounts the flash drive by executing:</p> <pre>mkdir /tmp/HSMFD</pre> <pre>mount -o noexec /dev/sda1 /tmp/HSMFD</pre>	17:00	MB

Start Logging Terminal Session

Step	Activity	Time (UTC)	Initial
18	<p>CA changes the default directory to the HSMFD and starts capture of terminal output to a file:</p> <pre>cd /tmp/HSMFD</pre> <pre>script -t script-20190322.log 2>script-20190322.timing</pre>	17:01	MB

Prepare Environment

Step	Activity	Time (UTC)	Initial
19	<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>	17:02	MB
20	<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-20180814.tar.gz . sha256sum HSMFD-20180814.tar.gz</pre> <p>Verify that the checksum is:</p> <p>A72A 7C25 9C29 FE24 ✓</p> <p>C556 BCD9 EFCA 0934 ✓</p> <p>8D19 1159 1E04 226F ✓</p> <p>FECE 1A56 0875 6542 ✓</p> <p>Un-tar the archive:</p> <pre>tar -xzvof HSMFD-20180814.tar.gz</pre>	17:05	MB
21	<p>CA copies the compressed input files from SCRIPTS into the current directory on the HSMFD.</p> <pre>cp -p /tmp/SCRIPTS/scripts-20190322.tar.gz . tar -xzvof scripts-20190322.tar.gz . bootstrap</pre>	17:07	MB

Start Logging HSM Output

Step	Activity	Time (UTC)	Initial
22	<p>CA connects the signing computer to the serial port of the HSM.</p> <p>CA switches to tty2 and initiates a login using login pi and password raspberry.</p> <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>[Do not unplug the USB-serial adaptor from the signing computer until instructed, as this would cause logging to stop.]</p>	17:09	MB

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

Step	Activity	Time (UTC)	Initial
23	<p>CA connects the HSM to power, using the UPS if one is available, and switches the HSM power to on, if required.</p> <p>[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.]</p>	17:16	MB

Activate HSM

Step	Activity	Time (UTC)	Initial
24	<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. CA repeats this process for OP cards 1, 2 and 7. When complete the HSM "Ready" LED illuminates.</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>	17:13	MB
25	<p>CA switches to tty1 and initiates communication with the HSM by connecting the HSM LAN port to the signing computer with an Ethernet cable and executing:</p> <pre>set-hsm-env KSK-HSM-02-BRK</pre>	17:15	MB

Start Generating Keys and Keybundles

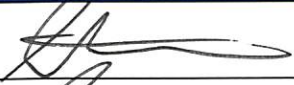

Step	Activity	Time (UTC)	Initial
26	<p>CA copies the encrypted backups of the KSKs and ZSKs by executing:</p> <pre>cd /tmp/kc makeallhsmfiles</pre>	17:16	MB
27	<p>CA initiates key and signature generation by executing:</p> <pre>key-and-sig-gen</pre> <p>[This will take a long time generating ZSKs and 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.]</p>	17:17	MB

Repackage and Redistribute OP Cards



Step	Activity	Time (UTC)	Initial
28	<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 CO2 and CO7.</p>	17:35	MPS

Smart Card Sign-Out Sheet



CO1 Steve FELDMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA 02670231	OP 1 of 7		3/22/19	17:26	MB
AE 26992156	Card Case		3/22/19	17:26	MB

CO2 Michael SINATRA

TEB#	Containing	Signature	Date	Time UTC	W
RA 02670233	OP 2 of 7		3/22/19	17:31	MB
AE 26992160	Card Case		3/22/19	17:31	MB

CO7 Gaurab UPADHAYA

TEB#	Containing	Signature	Date	Time UTC	W
RA 02670235	OP 7 of 7		3/22/19	17:35	MB
AE 26992152	Card Case		3/22/19	17:35	MB

Intermission

Step	Activity	Time (UTC)	Initial
29	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.]	17:39	MB
30	SC closes and seals the door.	17:41	MB

Reenter Facility

Step	Activity	Time (UTC)	Initial
31	SC and CA both inspect the door's seal for signs of tampering and open the door.	18:27	MB
32	Participants re-enter the room, noting their entry on the DNSSEC Key Ceremony Exit/Re-Entry Log.	18:28	MB

Pack and Store Keys and Keybundles

Step	Activity	Time (UTC)	Initial
33	CA confirms the completion of the key generation script.	18:29	MB
34	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>	18:30	MB

35	CA creates checksums of all files on the HSMFD by executing: <code>find . -type f -print0 xargs -0 -n 50 sha256sum</code>	18:31	MB
----	--	-------	----

Return HSM to a TEB

Step	Activity	Time (UTC)	Initial
36	CA switches to tty2. CA presses the HSM's RESTART button and waits for self-test to complete. CA disconnects HSM from power and signing computer (serial and Ethernet), places it into a new TEB, and seals. CA reads out TEB and HSM serial numbers and shows sealed TEB to participants. W records TEB and HSM serial numbers here: HSM TEB#: <u>BB69600251</u> HSM Serial#: <u>H1411035</u>	18:36	MB

Stop Recording Serial Port Activity

Step	Activity	Time (UTC)	Initial
37	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from the signing computer. CA then exits serial output terminal by executing: <code>exit</code> <code>exit</code> CA switches to tty1.	18:36	MB

Display HSMFD Contents

Step	Activity	Time (UTC)	Initial
38	CA displays contents of the HSMFD by executing: <code>ls -ltr</code>	18:37	MB

Stop Logging and Create Archive

Step	Activity	Time (UTC)	Initial
39	<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>	18:38	MB
40	<p>CA calculates the SHA-256 checksum of the archive by executing:</p> <pre>sha256sum HSMFD-20190322.tar.gz</pre> <p>CA reads the hash of the checksum aloud.</p> <p>W records the sixty-four digit hash:</p> <pre>C00F 20EF 7658 3961 689E 9697 F230 F6A2 B991 7525 1AF6 EB48 40BD 4F4C 54E7 1C50</pre> <p>W reads back the hash aloud.</p>	18:41	MB

Backup HSM Flash Drive Contents

Step	Activity	Time (UTC)	Initial
41	<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_ 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>	18:42	MB

42	<p>CA unmounts the new flash drive by executing:</p> <pre>umount /tmp/HSMFD_</pre> <p>CA removes the flash drive from the signing computer, places the flash drive in a new TEB and seals it, shows sealed TEB to participants, and reads out the TEB number. W records TEB number here:</p> <p>TEB#: <u>BB 69600245</u></p> <p>[This copy will be stored with the on-site audit bundle.]</p>	18:45	MB
43	<p>CA repeats the previous two steps to create a second backup.</p> <p>TEB#: <u>BB 69600244</u></p> <p>[This copy will be stored with the off-site audit bundle.]</p>	18:49	MB

Remove HSMFD

Step	Activity	Time (UTC)	Initial
44	<p>CA unmounts HSMFD by executing:</p> <pre>cd /tmp</pre> <pre>umount /tmp/HSMFD</pre> <p>CA removes the flash drive.</p> <p>[This copy is used for operations and the published archive.]</p>	18:50	MB

Return Boot Media to a TEB

Step	Activity	Time (UTC)	Initial
45	<p>CA executes:</p> <pre>halt -p -f</pre> <p>CA removes the boot media and places it in a new TEB and seals it, shows sealed TEB to participants, and reads out TEB number.</p> <p>W records TEB number here:</p> <p>Boot Media TEB#: <u>AE 26992150</u></p>	18:53	MB

Return Signing Computer to a TEB

Step	Activity	Time (UTC)	Initial
46	CA disconnects power and all other connections from the signing computer, puts it in new TEB and seals it, shows sealed TEB to participants, and reads out TEB number. W records TEB number here: Signing Computer TEB#: <u>BB71705487</u>	18:57	MB

Secure Equipment

Step	Activity	Time (UTC)	Initial
47	SC returns items to the safe. - KSK-HSM-02-BRK HSM - Signing Computer - Boot Media - HSMFD 1 above 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. [Power supplies and cables are not stored the safe and will be stored separately.]	19:01	MB
48	SC records a closing action in the safe's log sheet and returns the log sheet to the safe. SC closes the safe. W verifies it is locked.	19:02	MB

Sign-Out on Participant Signature Sheet

Step	Activity	Time (UTC)	Initial
49	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.	19:04	MB

Stop Audio-Visual Recording

Step	Activity	Time (UTC)	Initial
50	FO stops audio and video recording.	19:06	MB

Sign Out of Facility

Step	Activity	Time (UTC)	Initial
51	<p>FO returns computers and other items to participants. Participants return identification vests to FO.</p> <p>Participants are now free to depart. FO logs their exit times.</p>	19:07	MB

Attestations

Step	Activity	Time (UTC)	Initial
52	<p>SC completes Access Control System Attestation in Appendix A.</p> <p>CA completes Key Ceremony Script Attestation in Appendix B.</p> <p>W completes notary attestation.</p>		

Copy and Store the Script

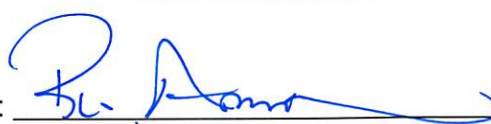
Step	Activity	Time (UTC)	Initial
53	<p>FO makes at least three colour copies of the W's script: one for the on-site audit bundle, one for off-site audit bundle, one for the W, and copies for other participants as requested. FO delivers the original to the SC.</p> <p>The two audit bundles each containing:</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 03/22/2019". 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: Bob Arasmith

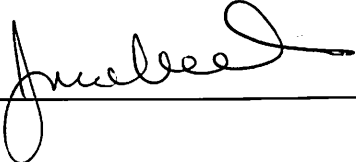
Signature:  _____

Date: 3/22/19

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 DNSSEC Key Ceremony Script Exception Forms.

Printed Name: JAMES MITCHELL

Signature: 

Date: 03/22/2019

Insert Notary Acknowledgement Here

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

CIVIL CODE § 1189

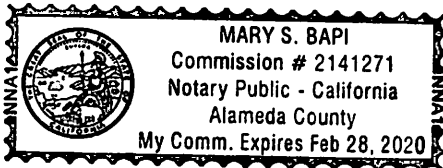
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of ALAMEDA
On MAR. 22, 2019 before me, MARY S. BAPI NOTARY PUBLIC,
Date Here Insert Name and Title of the Officer
personally appeared JAMES W. MITCHELL
Name(s) of Signer(s)

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

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

WITNESS my hand and official seal.



Signature [Handwritten Signature]
Signature of Notary Public

Place Notary Seal Above

OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: DNSSec Key Ceremony 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: _____

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

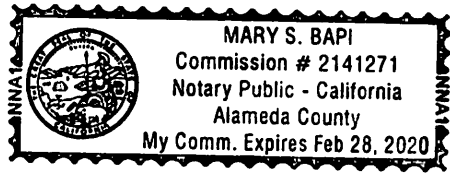
CIVIL CODE § 1189

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 MAR. 22, 2019 before me, MARY S. BAPI NOTARY PUBLIC,
Date Here Insert Name and Title of the Officer
personally appeared ROBERT E. ARASMITH
Name(s) of Signer(s)

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

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



WITNESS my hand and official seal.
Signature [Handwritten Signature]
Signature of Notary Public

Place Notary Seal Above

OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document
Title or Type of Document: DNISSEC KEY CEREMONY 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: _____

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
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 UTC	Exit Time UTC
FO	Mimi RAUSCHENDORF		3/22/19	15:45	19:08
CA1	James MITCHELL		3/22/19	15:45	19:08
W	Mary Shampa BAPI		3/22/19	15:45	19:08
CO1	Steve FELDMAN		3/22/19	15:46	19:08
CO2	Michael SINATRA		3/22/19	15:46	17:41
CO7	Gaurab UPADHAYA		3/22/19	15:47	17:41
SC2	Bob ARASMITH		3/22/19	15:30	19:08

Participant Signature Sheet

Role	Name	Citizen ship	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC	Signature upon Exit
CA1	James MITCHELL				3/22/19	16:24	19:03	
W	Mary Shampa BAPI				3/22/19	16:22	19:03	
CO1	Steve FELDMAN				3/22/19	16:23	19:03	
CO2	Michael SINATRA				3/22/19	16:22	17:31	
CO7	Gaurab UPADHAYA				3/22/19	16:25	18:26	
SC2	Bob ARASMITH				3/22/19	16:22	19:03	

DNSSEC Key Ceremony Script Exception Form

Step	Activity	Time	Initial
1	W describes exception and action here:		

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

Appendix: E





Smart Card Sign Out Sheet from Key Ceremony 18

DNSSEC Key Ceremony Script


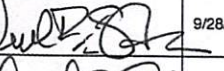
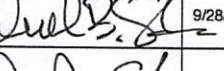
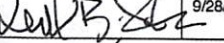
Thursday, September 28, 2017

Key Ceremony 18
Smart Card Sign Out Sheet

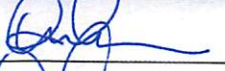



CO1 Steve FELDMAN

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
AE20992100	Card Case 2		9/28/17	18:17	MAB

CO3 Kim DAVIES

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


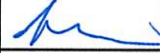


Appendix: F





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	AE20992006	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	RA02070389	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

Appendix: G

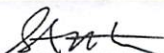
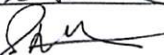
Smart Card Sign Out Sheet from Key Ceremony 20

DNSSEC Key Ceremony Script

Tuesday, August 14, 2018

Smart Card Sign-Out Sheet



CO1 Steve FELDMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA02670378	OP 1 of 7		8/14/18	18:14	MB
AE 26992002	Card Case		8/14/18	18:14	MB

CO3 Kim DAVIES

TEB#	Containing	Signature	Date	Time UTC	W
RA02670241	OP 3 of 7		8/14/18	18:18	MB
AE 26991998	Card Case		8/14/18	18:18	MB

CO4 Eric ALLMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA02670239	OP 4 of 7		8/14/18	18:22	MB
AE 26992000	Card Case		8/14/18	18:22	MB