

DNSSEC Key Ceremony Script Friday, December 14, 2012

Sign In to Facility

Step	Activity	Initial	Time (PDT)
1	The FO has all participants sign in before entering the Key Management Facility.		
2	The FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility.		

Emergency Evacuation Procedure

Step	Activity	Initial	Time (PDT)
3	The FO reviews emergency evacuation procedures and other relevant information with participants.		

Enter the Key Management Facility

Step	Activity	Initial	Time (PDT)
4	<p>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.</p> <p>As the participants are identified, the EW distributes their role identification placards.</p> <p>Note: The participants do not sign the sheet until the end of the ceremony.</p>		

Ground Rules

Step	Activity	Initial	Time (PDT)
5	The CA previews ground rules and break procedures with participants.		

Verify Time and Date

Step	Activity	Initial	Time (UTC)
6	<p>The 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: _____</p> <p>Time: _____</p> <p>This and all subsequent entries into this script and any associated logs should follow this common source of time.</p>		

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
7	The SC opens safe and makes entry in log sheet indicating opening of safe.		
8	<p>The CA collects the following items from the safe:</p> <ul style="list-style-type: none"> - KSK-HSM-01B-SJC HSM - boot-DVD - laptop - KSK-HSM-01B-SJC HSMFD - power supplies - cables <p>and any other items that may be scheduled for removal indicating removal of each with corresponding TEB number of safe log. Equipment is placed on table visible to all participants.</p>		

9	The CA reads out KSK-HSM-01B-SJC HSM TEB and serial number while the EW checks that it matches the TEB serial number recorded in the script from the previous key ceremony. TEB# A3112570 Serial# K1011066		
10	The CA similarly reads out boot-DVD, laptop, and HSMFD TEB numbers while the EW checks that they match the TEB serial numbers in the script from the previous key ceremony. DVD TEB# A28410818 Laptop TEB# A3112569 HSMFD KSK-HSM-01B-SJC TEB# A28410819		
11	The SC makes entry in log sheet indicating closing of safe then closes safe. The EW verifies safe is locked.		

Collect OP Cards

Step	Activity	Initial	Time (UTC)
12	The CA collects OP cards from COs, reading out and comparing TEB numbers with those recorded in the prior ceremony, reproduced for convenience in the appendices of this document. Note any discrepancies. The CA places the OP cards in plain view on the table.		

Inspect New Laptop

Step	Activity	Initial	Time (UTC)
13	The CA takes new laptop that will replace the laptop from the safe and shows participants that its internal storage has been removed.		

Set Up Laptop

Step	Activity	Initial	Time (UTC)
14	The CA places the boot-DVD and laptop on the table; connects laptop power and external monitor and boots laptop from DVD.		

15	The CA logs in as root.		
16	The CA opens a terminal window.		
17	<p>The 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>		
18	<p>The CA calculates sha256 checksum of the boot-DVD. The CA may proceed with additional steps while this process completes. When the checksum is complete, the CA reads it aloud, four digits at a time.</p> <pre>sha256sum /dev/cdrom</pre>		
19	<p>The EW records the sixty-four digit boot-DVD checksum.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in the appendices of this document.</p>		
20	The CA connects USB hub to laptop.		
21	The 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. The CA lets participants view contents of HSMFD then closes FD window.		

Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
22	The CA closes the terminal window and opens a new one. The CA changes the default directory to the HSMFD by executing: <code>cd /media/HSMFD</code>		
23	The CA starts capture of terminal output by executing: <code>script script-20121214.log</code>		

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
24	The CA connects a serial to USB null modem cable to laptop USB hub. Please note that the first USB cable connected will be "ttyUSB0", the second will be "ttyUSB1" and so on.		
25	The CA opens a second terminal screen and changes the default directory to the HSMFD by executing: <code>cd /media/HSMFD</code> The CA starts logging HSM serial port output by executing: <code>ttyscript /dev/ttyUSB0</code> Note: DO NOT unplug USB serial port adaptor from laptop as this causes logging to stop.		

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

Step	Activity	Initial	Time (UTC)
26	The CA inspects the HSM TEB for evidence of tampering and removes it from TEB; discards TEB and plugs ttyUSB0 null modem serial adaptor and cable to the back.		
27	The CA connects power to HSM. Status information should appear on the serial logging screen and after self test the HSM display should say: "Set Online" indicating the HSM is in the initialized state.		

Activate HSM

Step	Activity	Initial	Time (UTC)
28	<p>The CA sets HSM online (“Set Online” menu item) using three (3) OP cards. The “Ready” LED should go on.</p> <p>Use 3 OP cards 1, 2 and 4.</p> <p>Enter PIN: 11223344</p>		
29	<p>The CA connects Ethernet cable between laptop and HSM and tests network connectivity between laptop and HSM by executing:</p> <pre data-bbox="313 674 570 705">ping 192.168.0.2</pre> <p>on the laptop terminal window and looking for responses. Ctrl-C to exit program.</p>		
30	<p>The CA inserts flash drive labeled "SCRIPTS" into a free USB slot on the laptop (NOT on USB hub); waits for O/S to recognize the FD.</p>		
31	<p>The CA calculates sha256 checksum of the compressed scripts on the drive labeled "SCRIPTS" by executing:</p> <pre data-bbox="313 1073 854 1125">sha256sum /media/SCRIPTS/scripts-20121214.tar.gz</pre> <p>The CA may proceed with additional steps while this process completes. When the checksum is complete, the CA reads it aloud, four digits at a time.</p>		
32	<p>The EW records the sixty-four digit checksum of the file "scripts-20121214.tar.gz".</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>		

Generate Keys and Keybundles

Step	Activity	Initial	Time (UTC)
33	<p>The CA copies shell scripts that will be used to generate new keys and bundles by executing:</p> <pre>ls /media/SCRIPTS tar -xzvof /media/SCRIPTS/scripts-20121214.tar.gz cp -p makeallhsmfiles exkey keybundle-generate.20120530 /opt/dccom mkdir /tmp/pch cp -p 20121214.kc_script_gen.out /tmp/pch cp -p /opt/dnssec/aep.hsmconfig /tmp/pch</pre>		
34	<p>The CA creates encrypted backups of the ZSKs by executing:</p> <pre>cd /tmp/pch makeallhsmfiles keybundle-generate.20120530 < 20121214.kc_script_gen.out</pre> <p>The data file contains a line for each zone for which ZSKs will be rolled or a new zone will be generated. 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>		
35	<p>The CA generates the archive destined for the signer by executing:</p> <pre>tar zcfv /media/HSMFD/20121214.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256</pre>		
36	<p>The CA archives all results including encrypted ksks for future use by executing:</p> <pre>tar zcfv /media/HSMFD/20121214.session.tar.gz .</pre>		
37	<p>The CA returns to HSMFD and lists the contents by executing:</p> <pre>cd /media/HSMFD ls</pre>		

38	The CA creates a snapshot of any changes to DB files by executing: <code>tar zcf 20121214.KSK-HSM-01B-SJC.db.tar.gz *.db</code>		
39	The CA zeroizes SCRIPTS FD and unmounts by executing: <code>rm -rf /media/SCRIPTS/*</code> <code>umount /media/SCRIPTS</code> and removes the SCRIPTS FD for reuse.		

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
40	The CA presses RESTART button and waits for self test to complete. The CA then disconnects HSM from power and laptop (serial and Ethernet), placing HSM into a new TEB and seals.		
41	The CA reads out TEB # and HSM serial #, shows item to participants while the EW records TEB # and HSM serial # here. TEB# _____ HSM Serial#: _____		

Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
42	The CA terminates HSM serial output capture by disconnecting USB serial adaptors from laptop. The CA then exits out of serial output terminal window.		

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
43	The CA displays contents of HSMFD by executing: <code>ls -lt</code>		
44	The CA plugs a blank FD labeled "HSMFD KSK-HSM-01B-SJC" into the laptop waits for it to be recognized by the O/S as HSMFD_ and copies the contents of the HSMFD to the blank drive for backup by executing: <code>cp -Rp * /media/HSMFD_</code>		
45	The CA unmounts new FD by executing: <code>umount /media/HSMFD_</code> The CA removes HSMFD_ from the laptop.		
46	The CA repeats this activity a second time to create a second backup.		
47	The CA repeats this activity a third time to create a third backup.		
48	The CA repeats this activity a fourth time to create a fourth backup.		
49	The CA places first backup HSMFD_ in a new TEB and seals; reads out TEB # and shows item to participants while the EW records TEB # here. TEB# _____		
50	The CA places second backup HSMFD_ in a new TEB and seals; reads out TEB # and shows item to participants while the EW records TEB # here. TEB# _____		
51	The CA places third backup HSMFD_ in a new TEB and seals; reads out TEB # and shows item to participants while the EW records TEB # here. TEB# _____		
52	The CA places fourth backup HSMFD_ in a new TEB and seals; reads out TEB # and shows item to participants while the EW records TEB # here. TEB# _____		

Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
53	The CA stops logging terminal output by entering "exit" in remaining terminal window.		

Return HSMFD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
54	The CA unmounts HSMFD by executing: <pre>cd /tmp umount /media/HSMFD</pre>		
55	The CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants. The EW records TEB # here. TEB# _____		

Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
56	The CA executes: <pre>shutdown -h now</pre> The CA removes DVD and turns off laptop.		
57	The CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.		
58	The EW records TEB # here. TEB# _____		

Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
59	<p>The CA disconnects power, external video, USB hub, and any other connections from the laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants.</p> <p>The EW records TEB # here.</p> <p>TEB# _____</p>		

Return Power Supplies, USB Hub, and Cables

Step	Activity	Initial	Time (UTC)
60	The CA places HSM power supply, laptop power supply, USB hub, USB serial adapter, power and networking cables in a bag. This need not be a TEB as it is only used for convenient packaging.		
61	The SC opens safe indicating this on safe log sheet.		
62	<p>The SC returns items to the safe. The SC records return of each item on the safe log with TEB #, printed name, 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 		
63	The SC closes safe. The EW verifies it is locked.		
64	Two of the remaining HSMFDs will be packaged with the two audit bundles below. The CA keeps any remaining materials (e.g. the extra HSMFD) for next key ceremony preparation and analysis.		

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.		

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.		

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7		Steve FELDMAN		12/14/12		
CO2	OP 2 of 7		Michael SINATRA		12/14/12		
CO4	OP 4 of 7		Jonny MARTIN		12/14/12		

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
67	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.		
68	The CA reviews the EWs script and signs it. The CA Signature _____		

Sign Out of Facility

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

Stop Audio-Visual Recording

Step	Activity	Initial	Time (PDT)
70	The SA stops audio and video recording.		

Copy and Store the Script

Step	Activity	Initial	Time (PDT)
71	<p>The EW makes at least 5 copies of his or her script: one for off-site audit bundle, one for on-site audit bundle, one for the EW, and copies for other participants, as requested. The two audit bundles each contain 1) output of signer system - HSMFD; 2) copy of the EWs key ceremony script; 3) audio-visual recording; 4) logs from the Facility Physical Access Control; 5) The SA attestation (A.2 below); and 6) the EW attestation (A.1 below) - all in a TEB labeled "Key Ceremony null", dated and signed by the EW and the CA. One bundle will be stored by the SC along with equipment. The second bundle will be kept securely offsite.</p>		

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 excpetions which may have occurred were accurately and properly documented on the attached Script Exception Forms.

Printed Name: _____

Signature: _____

Date: _____

Insert Notary Acknowledgement Here

Appendix B:
Access Control System Attestation
(by SA)

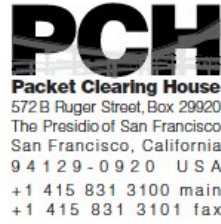
I have reviewed the physical access control system and not found any discrepancies or anything else out of the ordinary.

Attached is the audited physical access log.

Printed Name: _____

Signature: _____

Date: _____



1600 Shattuck Avenue Facilities Sign-In Sheet

Role	Name	Signature	Date	Entry Time PST	Exit Time PST
FO	Peter ROWLAND		12/14/12		
CA	Robert MARTIN- LEGENE		12/14/12		
EW	Larry JORDAN		12/14/12		
CO1	Steve FELDMAN		12/14/12		
CO2	Michael SINATRA		12/14/12		
CO4	Jonny MARTIN		12/14/12		
SA/SC1	Bill WOODCOCK		12/14/12		
R	Daniel GRIGGS		12/14/12		

Appendix C: Abbreviations Used in This Document

Roles

CA	Ceremony Administrator
EW	External Witness
SA	System Administrator
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	SMK4, SO4, OP4 TEB# <u>A21094980</u> go to CO4, Jonny MARTIN.	<i>JF</i>	8:49PM
110	SMK7, SO7, OP7 TEB# <u>A21094981</u> are entrusted to CO4, Jonny MARTIN, for conveyance to CO7, Gaurab UPADHAYA.	<i>JF</i>	8:50PM

Appendix: F

Smart Card Sign Out Sheet from Key Ceremony 1

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

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	TED #	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		
A19204944	CO5 OP 5 of 7	A19204929	Steve SOMODYI	<i>[Signature]</i>	5/30/11	0051	<i>[Initials]</i>
	CO5 SO 5 of 7	A19204928	Steve SOMODYI	<i>[Signature]</i>	5/30/11	0051	<i>[Initials]</i>
	CO5 SMK 5 of 7		Steve SOMODYI		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	A 19204876	Steve FELDMAN		6/20/11	07:51	
CO3	OP 3 of 7	A 19204874	Kim DAVIES		6/20/11	0751	
CO4	OP 4 of 7	A 19204872	Jonny MARTIN		6/20/11	07:49	
CO6	OP 6 of 7	A 19204870	LIM Choon Sai		6/20/11	07:50	
CO7	OP 7 of 7	A 19204869	Gaurab UPADHAYA		6/20/11	07:49	

ENCLOSING BAGS:

CO1: A 19204875

CO3: A 19204873

CO4: A 19204871

CO6: A 19204869

CO7: A 19204867

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	OP SO 5 of 7 BAG	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.	1/	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	1/
CO1	Outer SO 1 of 7	A28410826	Steve FELDMAN	<i>[Signature]</i>	5/30/12	19:11	1/
CO2	OP 2 of 7	A28410828	Michael SINATRA	<i>[Signature]</i>	5/30/12	19:12	1/
CO2	Outer SO 2 of 7	A28410825	Michael SINATRA	<i>[Signature]</i>	5/30/12	19:12	1/
CO4	OP 4 of 7	A28410827	Jonny MARTIN	<i>[Signature]</i>	5/30/12	19:14	1/
CO4	Outer SO 4 of 7	A28410823	Jonny MARTIN	<i>[Signature]</i>	5/30/12	19:14	1/

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	A284/0816	Steve FELDMAN	<i>[Signature]</i>	7/27/12	2019	11
CO1	Outer 1 of 7		Steve FELDMAN		7/27/12		
CO4	OP 4 of 7	A284/0814	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	A284/0817	Stephan SOMOGYI	<i>[Signature]</i>	7/27/12	2019	11
CO5	Outer 5 of 7		Stephan SOMOGYI		7/27/12		

Appendix: M

Boot-DVD Checksum from Key Ceremony 1

Step	Activity	Initial	Time																
8	CA places boot-DVD and laptop on key ceremony table; connects laptop power and boots laptop from DVD.	JJ	4:48 ⁰⁰ PM																
9	CA logs in as root.	JJ	4:49 PM																
10	CA opens a terminal window.	JJ	4:49 PM																
11	<p>CA verifies the timezone, date, and time on the laptop and synchronizes it if necessary.</p> <p>Display the current time and timezone: date</p> <p>If the timezone is not set to UTC: cd /etc/ rm localtime ln -s /usr/share/zoneinfo/UTC localtime</p> <p>Set time to match the wall clock: date mmddHHMMYYYY</p> <p>Verify: date</p>	JJ	4:50 PM																
12	CA calculates sha256 checksum of the boot-DVD and reads it aloud, four digits at a time.	JJ	5:01 PM																
13	<p>EW records the sixty-four digit boot-DVD checksum</p> <table border="0"> <tr> <td>7DE4</td> <td>31FN</td> <td>C33D</td> <td>DFEF</td> </tr> <tr> <td>M#08N</td> <td>A056</td> <td>13A3</td> <td>8126</td> </tr> <tr> <td>708A</td> <td>3AC1</td> <td>A784</td> <td>38A7</td> </tr> <tr> <td>BNC9</td> <td>2A4F</td> <td>52A1</td> <td>F87C</td> </tr> </table>	7DE4	31FN	C33D	DFEF	M#08N	A056	13A3	8126	708A	3AC1	A784	38A7	BNC9	2A4F	52A1	F87C	JJ	5:04 PM
7DE4	31FN	C33D	DFEF																
M#08N	A056	13A3	8126																
708A	3AC1	A784	38A7																
BNC9	2A4F	52A1	F87C																
14	CA connects USB hub to laptop.	JJ	4:55 PM																
15	CA plugs blank flash disk (FD) labeled HSMFD into a free USB slot on the laptop (NOT on expander); waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes FD window.	JJ	4:55 PM																