Packet Clearing House
572 B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
94129-0920 USA
+1 415 831 3100 main
+1 415 831 3101 fax

DNSSEC Key Ceremony Script
Monday, June 20, 2011

Sign In to Facility

Step	Activity	Initial	Time (SST)
1	FO has all participants sign in before entering the Key Management Facility.		
2	FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility, and the SA may retain a laptop.		

Emergency Evacuation Procedures

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

Enter the Key Management Facility

Step	Activity	Initial	Time (SST)
4	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. Note that participants do not sign the sheet until the end of the ceremony. As the participants are identified, the EW distributes their role identification placards.		

Ground Rules

Step	Activity	Initial	Time (SST)
5	CA reviews ground rules and break procedures with participants.		

Verify Time and Date

Step	Activity	Initial	Time (UTC)
6	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. Date: ________________________________ Time: ________________________________ This and all subsequent entries into this script and any associated logs should follow this common source of time.		

Assemble Equipment

Step	Activity	Initial	Time (UTC)
7	CA collects HSM, corresponding HSMFD, boot-DVD, laptop, power supplies, cables, etc. Equipment is placed on table visible to all participants.		
8	CA reads out HSM TEB and serial number while EW matches them with those from previous key ceremony. TEB# A3112528 Serial# K1011055		
9	CA reads out HSMFD TEB numbers while EW matches it with one from previous key ceremony. HSMFD TEB# A21094973 or A21094974		

Collect OP Cards

Step	Activity	Initial	Time (SST)
10	CA collects OP cards from COs, comparing TEB numbers with those recorded in the prior ceremony, reproduced for convenience in Appendix E of this document. Note any discrepancies. CA places the OP cards in plain view on the table.		

Set Up Laptop

Step	Activity	Initial	Time (UTC)
11	CA places the boot-DVD and laptop on the table; connects laptop power and boots laptop from DVD.		
12	CA logs in as root.		
13	CA opens a terminal window.		

14	CA verifies the time zone, date, and time on the laptop and synchronizes it if necessary.
	Display the current time and timezone:
	`date`
	If the timezone is not set to UTC:
	`cd /etc/`
	`rm localtime`
	`ln -s /usr/share/zoneinfo/UTC localtime`
	Set time to match the wall clock:
	`date mmddHHMMYYYY`
	Verify:
	`date`		

15	CA calculates sha256 checksum of the boot-DVD. CA may proceed with additional steps while this process completes. When the checksum is complete, CA reads it aloud, four digits at a time.		
16	EW records the sixty-four digit boot-DVD checksum __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ __________ Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in Appendix F of this document.		
17	CA connects USB hub to laptop.		

Step	Activity	Initial	Time (UTC)
18	CA removes HSMFD from TEB and plugs into a free USB slot on the laptop (NOT on expander); waits for operating system to recognize the FD. CA lets participants view contents of HSMFD, then closes FD window.		

Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
19	CA changes the default directory to the HSMFD: `cd /media/HSMFD`		
20	CA starts capture of terminal output: `script script-20110620.log`		

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
21	CA connects a serial to USB null modem cable to laptop USB expander. Please note that the first USB cable connected will be “ttyUSB0”, the second will be “ttyUSB1” and so on.		
22	CA opens a second terminal screen and ensures its default directory is also /media/HSMFD and executes `ttyaudit /dev/ttyUSB0` to start logging HSM serial port output. Note: DO NOT unplug USB serial port adaptor from laptop as this causes logging to stop.		

Connect HSM (KSK-HSM-01-SIN)

Step	Activity	Initial	Time (UTC)
23	CA inspects the HSM TEB for tamper evidence and removes it from TEB; discards TEB and plugs ttyUSB0 null modem serial adaptor and cable to the back.		
24	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 operational state.		

Activate HSM (KSK-HSM-01-SIN)

Step	Activity	Initial	Time (UTC)
25	CA sets HSM online (“Set Online” menu item) using three (3) OP cards. The “Ready” LED should go on. Use OP cards 1, 3, and 4.		
26	CA connects Ethernet cable between laptop and HSM and tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` on the laptop terminal window and looking for responses. Ctrl-C to exit program.		

New Key Generation and Key Signing

Step	Activity	Initial	Time (UTC)

27	CA generates new keys by copying scripts pre-generated by CA specific for this ceremony from external FD by plugging in FD and copying scripts:
	`cp -p /media/SCRIPTS/* .`
	`cp -p /media/SCRIPTS/* /opt/dccom`
	and executing:
	`bulkgen_3`		

28	CA creates a snapshot of the updated DB files by executing: `tar zcf 20110620.KSK-HSM-01-SIN.db.tar.gz *.db`		
29	CA creates encrypted backups of the ZSKs by executing `zskbackup` (The resultant .hsm file will be imported into the other on-line signer HSM)		
30	CA similarly does this for the KSKs by executing `kskbackup` (The resultant .hsm file will be imported into the other off-line KSK HSM.)		

Step	Activity	Initial	Time (UTC)

31	CA generates KSK signed DNSKEY RRsets (keybundles) by executing the script for a pre-determined set of domains as follows:
	`cd /tmp`
	`mkdir kb`
	`cd kb`
	`cp /opt/dnssec/aep.hmsconfig .`
	`cp /media/HSMFD/nextzsk .`
	`keybundle-generate`
	`tar zcf /media/HSMFD/20110620.kb.tar.gz .`
	`cd /media/HSMFD`
	This will create time dependant archive files of the form date.domain.keybundle.tar.gz that must be copied to the on-line signer in a timely manner after completion of the key ceremony.		

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
32	CA places the HSM offline by using “Set Offline” menu item and three (3) OP cards. The “Ready” LED should go off. Use cards 6, 7 and 1.		
33	CA presses RESTART button and waits for self test to complete. CA then disconnects HSM from power and laptop (serial and Ethernet), placing HSM into a new TEB and seals.		
34	CA reads out TEB # and HSM serial #, shows item to participants while EW records TEB # and HSM serial # here. TEB # ______________________________ HSM serial # ________________________		

Stop Recording Serial Port Activity

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

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
36	CA displays contents of HSMFD by executing `ls -lt`		
37	CA plugs a blank FD labeled HSMFD 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 `cp -Rp * /media/HSMFD_`		
38	CA displays contents of HSMFD_ by executing `ls -lt /media/HSMFD_`		
39	CA unmounts new FD using `umount /media/HSMFD_`		
40	CA removes HSMFD_ and places on table		
41	CA repeats the first five steps of this activity a second time, to create a second backup.		
42	CA repeats the first five steps of this activity a third time, to create a third backup.		
43	CA repeats the first five steps of this activity a fourth time, to create a fourth backup.		

Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
44	CA stops logging terminal output by entering “exit” in remaining terminal window		

Return HSM FD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)

45	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`		

46	CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants.		
47	EW records TEB # here. TEB # ______________________________		

Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
48	After all print jobs are complete, CA executes `shutdown -hP now` removes DVD and turns off laptop.		
49	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.		
50	EW records TEB # here. TEB # ___________________________		

Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
51	CA disconnects power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants.		
52	EW records TEB # here. TEB # ___________________________		

Return Power Supplies, USB Hub, and Cables

Step	Activity	Initial	Time (UTC)
53	CA places HSM and laptop power supplies, 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.		
54	CA hands KSK-HSM-01-SIN, HSMFD, laptop, and boot-DVD to the SCs to transfer to the IPS in the permanent Singapore KSK facility. CA and SC record each item on a log with TEB #, printed name, date, time, signature, and a witness initialing each entry. CA keeps any remaining materials for later analysis.		

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
55	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.		

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
56	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.		

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7		Steve FELDMAN		6/20/11		
CO3	OP 3 of 7		Kim DAVIES		6/20/11		
CO4	OP 4 of 7		Jonny MARTIN		6/20/11		
CO6	OP 6 of 7		LIM Choon Sai		6/20/11		
CO7	OP 7 of 7		Gaurab UPADHAYA		6/20/11		

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
57	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.		
58	CA reviews EW's script and signs it. CA Signature: ________________________________		

Sign Out of Facility

Step	Activity	Initial	Time (UTC)
59	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 (UTC)
60	SA stops audio and video recording.		

Copy and Store the Script

Step	Activity	Initial	Time (UTC)
61	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 EW, and copies for other participants, as requested. Audit bundles each contain 1) output of signer system - HSMFD; 2) copy of EW's key ceremony script; 3) audio-visual recording; 4) logs from the Facility Physical Access Control; 5) SA attestation (A.2 below); and 6) the EW attestation (A.1 below) - all in a TEB labeled "Key Ceremony 3". One bundle will be stored by the SC along with HSM above and other equipment. The second bundle will be kept securely at PCH's office.		

* End of Key Ceremony Script *

Appendix A:

Key Ceremony Script Attestation

(by EW)

I hereby attest that the Key Ceremony was conducted in accordance with this script and that any exceptions which may have occurred were accurately and properly documented on the attached Script Exception Forms.

Printed Name: ____

Signature: ____

Date: ____

Attach notarization to this page.

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: ____

Appendix C:

Abbreviations Used in This Document

Roles

CA	Ceremony Administrator
EW	External Witness
SA	System Administrator
SC	Security Controller
FO	Facility Operator
W	Witness

Other Abbreviations

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

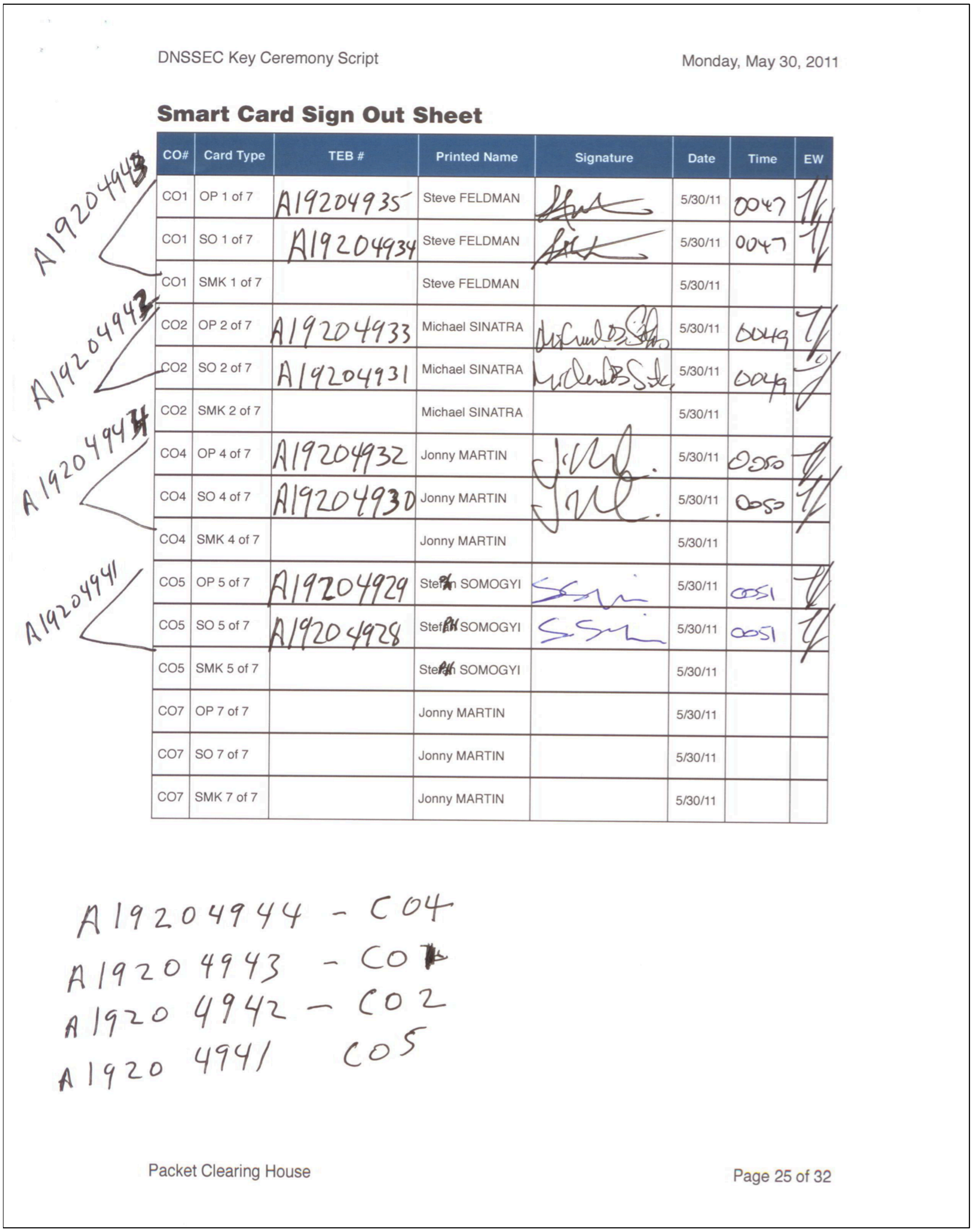
Appendix D:

Letter and Number Pronunciations

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	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:

Smart Card Sign Out Sheet from Key Ceremony 2



DNSSEC Key Ceremony Script

Monday, May 30, 2011

Smart Card Sign Out Sheet

A19204943

A19204942

A19204944

A19204941

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A19204935	Steve FELDMAN		5/30/11	0047	
CO1	SO 1 of 7	A19204934	Steve FELDMAN		5/30/11	0047	
CO1	SMK 1 of 7		Steve FELDMAN		5/30/11		
CO2	OP 2 of 7	A19204933	Michael SINATRA		5/30/11	0049	
CO2	SO 2 of 7	A19204931	Michael SINATRA		5/30/11	0049	
CO2	SMK 2 of 7		Michael SINATRA		5/30/11		
CO4	OP 4 of 7	A19204932	Jonny MARTIN		5/30/11	0050	
CO4	SO 4 of 7	A19204930	Jonny MARTIN		5/30/11	0050	
CO4	SMK 4 of 7		Jonny MARTIN		5/30/11		
CO5	OP 5 of 7	A19204929	Stefan SOMOGYI		5/30/11	0051	
CO5	SO 5 of 7	A19204928	Stefan SOMOGYI		5/30/11	0051	
CO5	SMK 5 of 7		Stefan SOMOGYI		5/30/11		
CO7	OP 7 of 7		Jonny MARTIN		5/30/11		
CO7	SO 7 of 7		Jonny MARTIN		5/30/11		
CO7	SMK 7 of 7		Jonny MARTIN		5/30/11		

A19204944 - CO4

A19204943 - CO1

A19204942 - CO2

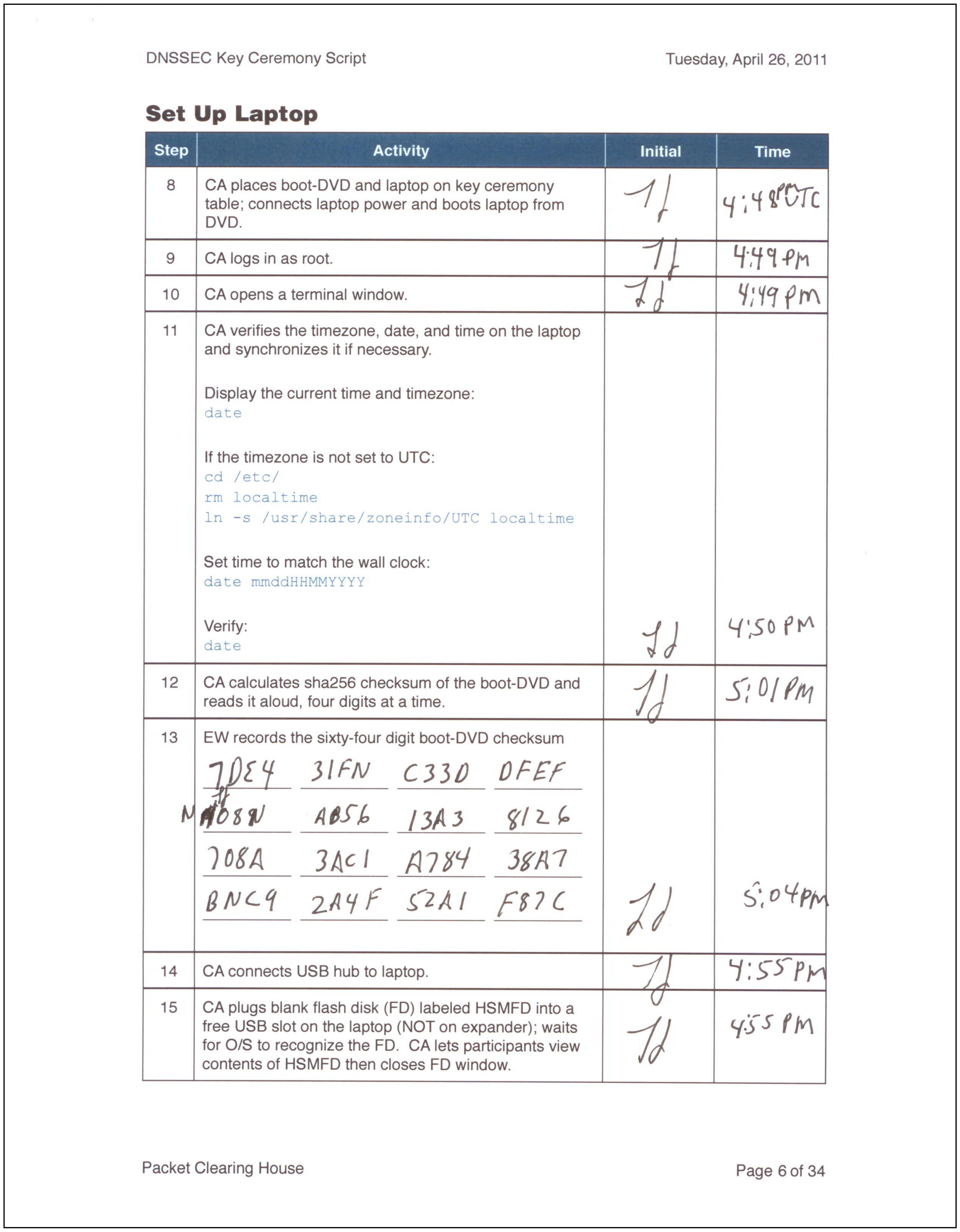
A19204941 CO5

Packet Clearing House

Page 25 of 32

Appendix F:

Boot-DVD Checksum from Key Ceremony 1



Set Up Laptop

Step	Activity	Initial	Time
8	CA places boot-DVD and laptop on key ceremony table; connects laptop power and boots laptop from DVD.	Jd	4:48PM UTC
9	CA logs in as root.	Jd	4:49 PM
10	CA opens a terminal window.	Jd	4:49 pm

11	CA verifies the timezone, date, and time on the laptop and synchronizes it if necessary.
	Display the current time and timezone:
	`date`
	If the timezone is not set to UTC:
	`cd /etc/`
	`rm localtime`
	`ln -s /usr/share/zoneinfo/UTC localtime`
	Set time to match the wall clock:
	`date mmddHHMMYYYY`
	Verify:
	`date`
		Jd	4:50 PM

12	CA calculates sha256 checksum of the boot-DVD and reads it aloud, four digits at a time.	Jd	5:01 PM
13	EW records the sixty-four digit boot-DVD checksum 7DE4 31FN C33D DFEF N A08N AB56 13A3 8126 708A 3AC1 A784 38A7 BNC9 2A4F 52A1 F87C	Jd	5:04PM
14	CA connects USB hub to laptop.	Jd	4:55PM
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.	Jd	4:55 PM

```
7de4 31f9 c33d dfef
9089 ab56 13a3 8126
708a 3ac1 a784 38a7
b9c9 2a4f 52a1 f87c
```