






Packet Clearing House
572B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
9 4 1 2 9 - 0 9 2 0 U S A
+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.		13:28
2	FO collects cell phones, laptops, etc. Management Facility, and the SA may retain a laptop.		13:29


Emergency Evacuation Procedures

Step	Activity	Initial	Time (SST)
3	FO reviews emergency evacuation procedures and other relevant information with participants.		13:30


Enter the Key Management Facility

Step	Activity	Initial	Time (SST)
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>Note that participants do not sign the sheet until the end of the ceremony.</p> <p>As the participants are identified, the EW distributes their role identification placards.</p>		13:37




Ground Rules

Step	Activity	Initial	Time (SST)
5	CA reviews ground rules and break procedures with participants.		13:42


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: <u>20.06.2011</u> Time: <u>05.44.</u> This and all subsequent entries into this script and any associated logs should follow this common source of time.		05.44.

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.		05:48
8	CA reads out HSM TEB and serial number while EW matches them with those from previous key ceremony. TEB# A3112528 Serial# K1011055		05.49
9	CA reads out HSMFD TEB numbers while EW matches it with one from previous key ceremony. HSMFD TEB# A21094973 or A21094974		05:51

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.		06:06

C03 outside TEB no A21094984

OP3 TEB

A21095007

Packet Clearing House

C06 A21094982


A21094998

C07 A21094981



A21094995

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.	<i>[Signature]</i>	06:18 06:24
12	CA logs in as root.	<i>[Signature]</i>	06:29/18
13	CA opens a terminal window.	<i>[Signature]</i>	06:30
14	<p>CA verifies the time zone, 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>	<i>[Signature]</i>	06:37 21
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	<p>EW records the sixty-four digit boot-DVD checksum</p> <p><u>7DE4</u> <u>31FN</u> <u>C330</u> <u>DFEF</u></p> <p><u>9089</u> <u>AB56</u> <u>13A7</u> <u>8126</u></p> <p><u>708A</u> <u>3AC1</u> <u>A784</u> <u>38A7</u></p> <p><u>B9C9</u> <u>2A4F</u> <u>52A1</u> <u>F87C</u></p> <p>Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in Appendix F of this document.</p>	<i>[Signature]</i>	06:15
17	CA connects USB hub to laptop.	<i>[Signature]</i>	06:22

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.		06:25



Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
19	CA changes the default directory to the HSMFD: <code>cd /media/HSMFD</code>		06:25
20	CA starts capture of terminal output: <code>script script-20110620.log</code>		06:27



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.		06:28
22	CA opens a second terminal screen and ensures its default directory is also /media/HSMFD and executes <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port output. Note: DO NOT unplug USB serial port adaptor from laptop as this causes logging to stop.		06:29





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.		06:30
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.		06:32

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.		06:34
26	CA connects Ethernet cable between laptop and HSM and tests network connectivity between laptop and HSM by entering <code>ping 192.168.0.2</code> on the laptop terminal window and looking for responses. Ctrl-C to exit program.		06:35

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: <code>cp -p /media/SCRIPTS/* .</code> <code>cp -p /media/SCRIPTS/* /opt/dccom</code> and executing: <code>bulkgen_3</code>		06:51
28	CA creates a snapshot of the updated DB files by executing: <code>tar zcf 20110620.KSK-HSM-01-SIN.db.tar.gz *.db</code>		06:51
29	CA creates encrypted backups of the ZSKs by executing <code>zskbackup</code> (The resultant .hsm file will be imported into the other on-line signer HSM)		06:52
30	CA similarly does this for the KSKs by executing <code>kskbackup</code> (The resultant .hsm file will be imported into the other off-line KSK HSM.)		06:53

Step	Activity	Initial	Time (UTC)
31	<p>CA generates KSK signed DNSKEY RRsets (keybundles) by executing the script for a pre-determined set of domains as follows:</p> <pre> 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 </pre> <p>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.</p>		06.58

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
32	<p>CA places the HSM offline by using "Set Offline" menu item and three (3) OP cards. The "Ready" LED should go off.</p> <p>Use cards 6, 7 and 1.</p>		06.59.
33	<p>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.</p>		
34	<p>CA reads out TEB # and HSM serial #, shows item to participants while EW records TEB # and HSM serial # here.</p> <p>TEB # <u>A3112531</u></p> <p>HSM serial # <u>K1011055</u></p>		07.06.

Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
35	<p>CA terminates HSM serial output capture by disconnecting USB serial adaptors from laptop. CA then exits out of serial output terminal window.</p>		07.06

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
36	CA displays contents of HSMFD by executing <code>ls -lt</code>		07.08
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 <code>cp -Rp * /media/HSMFD_</code>		07.09
38	CA displays contents of HSMFD_ by executing <code>ls -lt /media/HSMFD_</code>		07:09
39	CA unmounts new FD using <code>umount /media/HSMFD_</code>		07.09
40	CA removes HSMFD_ and places on table		07.09
41	CA repeats the first five steps of this activity a second time, to create a second backup.		07.11
42	CA repeats the first five steps of this activity a third time, to create a third backup.		07.12
43	CA repeats the first five steps of this activity a fourth time, to create a fourth backup.		07.13




Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
44	CA stops logging terminal output by entering "exit" in remaining terminal window		07.13



Return HSM FD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
45	CA unmounts HSMFD by executing <code>cd /tmp</code> then <code>umount /media/HSMFD</code>		07.14.
46	CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants.		07.15
47	EW records TEB # here. TEB # <u>A19204865</u>		07.18



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.		07.20
49	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.		07.20
50	EW records TEB # here. TEB # <u>A 19204866</u>		07.21.


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.		07.26
52	EW records TEB # here. TEB # <u>A3112532</u>		07.27


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.		07.29.
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.		07.34





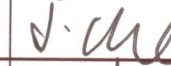





Re-Package OP Cards

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.		07:45

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.		07:52

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	07:51	
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:

CO 1: A 19204875




CO 3: A 19204873

CO 4: A 19204871

CO 6: A 19204869

CO 7: A 19204867

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.		07.58
58	CA reviews EW's script and signs it. CA Signature: 		07.58.

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

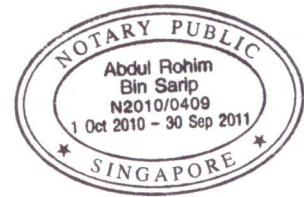
(by EW)

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: Abdul Rohim Sarip

Signature: 

Date: 20. 6. 2011.



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: Bill Woodcock

Signature: 

Date: JUNE 20, 2011

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

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
A19204943	CO1 OP 1 of 7	A19204935	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<input checked="" type="checkbox"/>
	CO1 SO 1 of 7	A19204934	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<input checked="" type="checkbox"/>
	CO1 SMK 1 of 7		Steve FELDMAN		5/30/11		
A19204942	CO2 OP 2 of 7	A19204933	Michael SINATRA	<i>[Signature]</i>	5/30/11	0049	<input checked="" type="checkbox"/>
	CO2 SO 2 of 7	A19204931	Michael SINATRA	<i>[Signature]</i>	5/30/11	0049	<input checked="" type="checkbox"/>
	CO2 SMK 2 of 7		Michael SINATRA		5/30/11		
A19204944	CO4 OP 4 of 7	A19204932	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<input checked="" type="checkbox"/>
	CO4 SO 4 of 7	A19204930	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<input checked="" type="checkbox"/>
	CO4 SMK 4 of 7		Jonny MARTIN		5/30/11		
A19204941	CO5 OP 5 of 7	A19204929	Stefan SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<input checked="" type="checkbox"/>
	CO5 SO 5 of 7	A19204928	Stefan SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<input checked="" type="checkbox"/>
	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 - C04
 A19204943 - C01
 A19204942 - C02
 A19204941 - C05

Packet Clearing House Page 25 of 32

Appendix F:

Boot-DVD Checksum from Key Ceremony 1

DNSSEC Key Ceremony Script		Tuesday, April 26, 2011	
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.	Jf	4:48 PM UTC
9	CA logs in as root.	Jf	4:49 PM
10	CA opens a terminal window.	Jf	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: <code>date</code> If the timezone is not set to UTC: <code>cd /etc/</code> <code>rm localtime</code> <code>ln -s /usr/share/zoneinfo/UTC localtime</code> Set time to match the wall clock: <code>date mmddHHMMYYYY</code> Verify: <code>date</code>	Jf	4:50 PM
12	CA calculates sha256 checksum of the boot-DVD and reads it aloud, four digits at a time.	Jf	5:01 PM
13	EW records the sixty-four digit boot-DVD checksum 7DE4 31F9 C33D DFEF 9089 AB56 13A3 8126 708A 3AC1 A784 38A7 B9C9 2A4F 52A1 F87C	Jf	5:04 PM
14	CA connects USB hub to laptop.	Jf	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.	Jf	4:55 PM

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




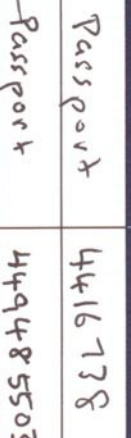







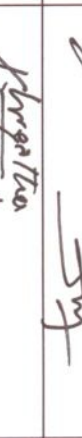



Packet Clearing House
572 B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
9 4 1 2 9 - 0 9 2 0 U S A
+ 1 4 1 5 8 3 1 3 1 0 0 main
+ 1 4 1 5 8 3 1 3 1 0 1 fax

Singapore Interim Key Signing Facility InterContinental Bugis Vault Facility Sign-In Sheet

SST SST











Name	Signature	Date	Entry Time PDT	Exit Time PDT
Vicky SHRESTHA		6/20/11	13:27	16:04
Rick LAMB		6/20/11	13:26	16:04
Abdul Rohim Bin SARIP		6/20/11	13:26	16:04
Steve FELDMAN		6/20/11	13:24	16:04
Kim DAVIES		6/20/11	13:25	16:04
Jonny MARTIN		6/20/11	13:26	16:04
LIM Choon Sai		6/20/11	13:52	16:04
Gaurab UPADHAYA		6/20/11	13:24	16:04
Bill WOODCOCK		6/20/11	17:25	16:04
LEE Han Chuan		6/20/11	13:26	16:04
James KILABA		6/20/11	13:25	16:04
Kabindra SHRESTHA		6/20/11	13:24	16:04
Robert MARTIN-LEGÈNE		6/20/11	13:25	16:04

Participant Signature Sheet

Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
CA1	Vicky SHRESTHA	NP		Passport	4416178	6/20/11	05:37	07:58
CA2	Rick LAMB	US		Passport	449485503 E0036754L E36039911	6/20/11	05:31	07:53
EW	Abdul Rohim Bin SARIP	SG		Passport	E0036754L	6/20/11	05:36	07:57
CO1	Steve FELDMAN	US		Passport	214647366	6/20/11	05:32	07:55
CO3	Kim DAVIES	AU		Passport	E7602871	6/20/11	05:31	07:55
CO4	Jonny MARTIN	NZ		Passport	LA720703	6/20/11	05:35	07:54
CO6	LIM Choon Sai	SG		Identity card	S0098628C	6/20/11	05:55	07:56
CO7	Gaurab UPADHAYA	NP		Emigration Pass	G5020133W	6/20/11	05:34	7:55
SC1 SA	Bill WOODCOCK	US		Passport	464466862	6/20/11	05:36	07:53
SC2 FO	LEE Han Chuan	SG		Driver License	S76178415	6/20/11	05:33	07:59
W	James KILABA	TZ		Passport	AG8240412	6/20/11	05:35	07:55
W	Kabindra SHRESTHA	NP		Passport	4768872	6/20/11	05:34	7:59
W	Robert MARTIN-LEGÈNE	DK		Passport	200138770	6/20/11	05:36	07:56

Notes: Michael SINATRA and Stephan SOMOGYI will not be present for this ceremony, so the necessary five of seven sets of keys present are: 1, 3, 4, 6 and 7.

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here:		
1.	C04 hands C07 smart key bundle, A21094981.		05:47
2.	Don't have the HSM FD generated during the last ceremony, we are using a new HSM FD generated from a backup.		05:51.
3.	Performing DVD checks on external laptop		06:09
4.	did not have USB hub. not required.		06:22
5.	tar - ext 20110530.kSK-Hsm-01-SIN.db.tar.gz (step 20)		06:26.
6.	James Kilaba left the room.		06:47
7.	James Kilaba is back		06:49.
8.	step 34 - returning HSM to secure container.		07:04
9.	step 51. - Remove Hard Drive and battery from laptop.		
2	EW notes date and time of key ceremony exception and signs here: Signature: 		08:00.

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