PCH
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
Tuesday, April 26, 2011

Roles

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

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

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

Participants

Role	Name	Citizenship	Signature	Date	Entry Time UTC	Exit Time UTC
CA	Vicky SHRESTHA	NP		26 4/25/11	4:32	9:10 pm
EW	Larry JORDAN	US		26 4/25/11	4:33	9:10 pm
CO1	Steve FELDMAN	US		26 4/25/11	4:34	20:57
CO2	Michael SINATRA	US		26 4/25/11	4:34	20:56
CO3	Kim DAVIES	AU		26 4/25/11	4:35	8:53
CO4	Jonny MARTIN	NZ		26 4/25/11	4:35	9:09
CO5	Stephan SOMOGYI	CA		26 4/25/11	4:36	5:31 UTC
CO6	LEONG Keng Thai	SG				
CO7	Gaurab UPADHAYA	NP				
SA FO	Peter ROWLAND	US		26 4/25/11	4:36	9:10 PM
SC	Bill WOODCOCK	US		4/25/11	4:36	9:09 PM UTC
CA	Rick LAMB	US		26 4/25/11	4:37	9:09 pm

CA 1092677
CAN4675802
CA N6019042
CA B3400470
CA D5002436
CA F1781184
CA A6289747
CA D1874950
CA A1005023
CA E1123160

Note: Stephan SOMOGYI will be present for only the first portion of this ceremony, while LEONG Keng Thai and Gaurab UPADHAYA will not be present for any of this ceremony. Cryptographic components will be conveyed to these Crypto Officers after the ceremony.

Sign In to Key Management Facility

Step	Activity	Initial	Time
1	FO logs identification of all participants before entering the Key Management Facility.	JL	4:26PM
2	FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility.	JL	4:27PM
3	EW verifies the identity of all participants by examining a government-issued photo identification, and distributes role identification placards.	JL	4:38PM

Emergency Evacuation Procedures

Step	Activity	Initial	Time
4	FO reviews emergency evacuation procedures and other relevant information with participants.	JL	4:25PM

Ground Rules

Step	Activity	Initial	Time
5	CA reviews ground rules and break procedures with participants.	JL	4:39 PM

Verify Time and Date

Step	Activity	Initial	Time
6	EW reads aloud and records the date (month/day/year) and time (UTC) using an NTP-synchronized wall clock visible to all. Participants verify that the time is correct. Date: 4/26/11 Time: 4:40 PM UTC All entries into this script or any logs should follow this common source of time.	TJ	4:40PM

Collect Equipment

Step	Activity	Initial	Time
7	CA collects HSM, boot-DVD, laptop, power supplies, cables, cards, etc. on table visible to all participants.	TJ	4:42 UTC

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.	JJ	4:48 PM UTC
9	CA logs in as root.	JJ	4:49 PM
10	CA opens a terminal window.	JJ	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`
		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	EW records the sixty-four digit boot-DVD checksum 7DE4 31FN C330 DFEF M#08N AB56 13A3 8126 708A 3AC1 A784 38A7 BNC9 2A4F 52A1 F87C	JJ	5:04 PM
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

Start Logging Terminal Session

Step	Activity	Initial	Time
16	CA changes the default directory to the HSMFD: `cd /media/HSMFD`	JL	4:56 PM
17	CA starts capture of terminal output: `script script-20110426.log`	JL	4:56 PM

Start Logging HSM Output

Step	Activity	Initial	Time
18	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.	JL	4:57 PM
19	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.	JL	4:57 PM

Initialize HSM1: ZSK-HSM-01-SJC

Step	Activity	Initial	Time
20	CA inspects the HSM1 TEB for tamper evidence; reads out TEB # and serial # while EW matches it with the prior script entry: TEB# A3379433 Serial # K0705020	JJ	4:59 PM
21	CA removes HSM1 from TEB; discards TEB, labels HSM1 "ZSK-HSM-01-SJC" and plugs ttyUSB0 null modem serial cable to the back.	JJ	5:01 PM
22	CA connects power to HSM. Status information should appear on the serial logging screen and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state.	JJ	5:06 PM

Make Security Officer (SO) Cards

~~A2109496~~ 6/A2109496 5

Step	Activity	Initial	Time
23	CA makes one set of the seven (7) Security Officer (SO) cards via "Issue Cards" from main menu (use '>' key to navigate menu) with "num req cards" equal 3 and total number "num cards" equal 7 using pre-labeled cards. Note: Default PIN="11223344". As each card is created the CA shows it to the participants and places it on table visible to the camera.	JJ	5:15 PM

Go Operational and Setup

Step	Activity	Initial	Time
24	CA sets the HSM operational ("Go Operational" on menu) using any three (3) SO cards. When presented with "Import config" press CLR button repeatedly until the "Set Online" menu item is reached. HSM date and time are not used in the ceremony. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 4 of 7 5 of 7 6 of 7	JJ	5:18PM
25	CA then dumps the status of the HSM using the "Output Status" menu item (using '>' key).	JJ	5:20PM
26	CA verifies settings below. If not set, CA may fix the settings with any three (3) SO cards using "API Setting" via "Key Mgmt" (eg, if LCD display shows "key import disable" this means key import is enabled. Click ENT to disable.). For auto online enable, use HSM Mgmt menu. Global Key Export Enabled App Key Import Enabled **App Key Export Disabled** Asymmetric Key Gen Enabled Symmetric Key Gen Enabled **Symmetric Key Derive Disabled** Signing Enabled Signature Verification Enabled MAC Gen Enabled MAC Ver Enabled Enc/Dec Enabled Delete Asym Key Enabled Delete Sym Key Enabled Output Key Details Enabled Output Key Summary Enabled Suite B Algorithms Enabled Non Suite B Algorithms Enabled AES SMK **Auto Online Enabled** FIPS Mode	JJ	5:30PM

USE cards 2, 3, 7

USE 1, 3, 6

Make Adapter Authorization Key (AAK) Backup Cards

Step	Activity	Initial	Time
27	CA makes one set of two (2) AAK backup cards while labeling them with "AAK", HSM serial number, and card number using any three (3) SO cards via the "Key Mgmt", "AAK", "Backup AAK", "num cards" = 2 menu items. CA presses CLR when done. As each card is created the CA shows it to the participants and places it on table visible to the camera. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 3 of 7 4 of 7 5 of 7		5:39PM

Make Storage Master Key (SMK) Backup Cards

Step	Activity	Initial	Time
28	CA makes one set of SMK backup cards on to pre-labeled smartcards. 5 (num req cards) of 7 (num cards) using any three (3) SO cards via the "Key Mgmt", "SMK", "Backup SMK" menu items. As each card is created the CA shows it to the participants and places it in on table visible to the camera. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 3 of 7 5 of 7 _____ of 7 (Note: SO cards may not be needed if this step is performed shortly after prior key management operation)		5:42PM

Make Operator (OP) Cards

Step	Activity	Initial	Time
29	CA makes one set of the seven (7) Operator (OP) cards using pre-labeled smartcards with number needed (num req cards) equal 3 and total number (num cards) equal 7 using any three (3) SO cards via the "HSM Mgmt" menu and "Issue Cards". CA presses CLR key to return to main menu. Note: Default PIN="11223344". As each card is created the CA shows it to the participants and places it on table visible to the camera. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 1 of 7 2 of 7 3 of 7 (Note: SO cards may not be needed if this step is performed shortly after prior key management operation)	JJ	5:49 PM

Activate HSM1

Step	Activity	Initial	Time
30	CA sets HSM1 online ("Set Online" menu item) using any three (3) OP cards. The "Ready" LED should go on. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) _____ of 7 _____ of 7 _____ of 7 (Note: Alternatively CA may just press RESTART which should put HSM online after self test.)	JJ	5:50 PM

Check Network Connectivity Between Laptop and HSM1

Step	Activity	Initial	Time
31	CA connects HSM to laptop using Ethernet cable.		5:51PM
32	CA 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.		5:51 PM

Initialize HSM1 Configuration and Files

Step	Activity	Initial	Time

33	CA executes
	`. /opt/dnssec/fixenv`
	to set environment variables for HSM then runs
	`inittoken`
	entering
	`0`
	for Slot
	`ZSK-HSM-01`
	for PKCS11 Token name
	`123456`
	for SO PIN and
	`123456`
	for USER PIN. This should return
	`Token initialized OK.`
			5:54PM

34	CA executes
	`inittoken`
	entering
	`1`
	for Slot
	`KSK-HSM-01`
	for PKCS11 Token name
	`123456`
	for SO PIN and
	`123456`
	for USER PIN. This should return
	`Token initialized OK.`
			5:54PM

Step	Activity	Initial	Time

35	CA executes
	`inittoken`
	entering
	`2`
	for Slot
	`RZSK-HSM-01`
	for PKCS11 Token name
	`123456`
	for SO PIN and
	`123456`
	for USER PIN. This should return
	`Token initialized OK.`
			5:55PM

36	CA executes
	`inittoken`
	entering
	`3`
	for Slot
	`RKSK-HSM-01`
	for PKCS11 Token name
	`123456`
	for SO PIN and
	`123456`
	for USER PIN. This should return
	`Token initialized OK.`
			5:56PM

Create Wrapping Keys for Key Backup

Step	Activity	Initial	Time
37	CA executes `makewrapkeys` ✓ Which should result in the creation of wrapping keys in each slot. CA verifies contents of HSM1 by executing `Showallkeys` ✓	TJ	5:57PM
38	CA places HSM offline using any 3 OP cards via the "set offline" menu item. List OP cards used and order here (e.g., 2 of 7, 5 of 7...) 2 of 7 4 of 7 6 of 7	TJ	5:59PM
39	CA makes a backup of the wrapping keys via the Key Mgmt, App Key, Backup App Key, "all keys", "backup keys" menu items using any 3 SO cards and inserting an APP smartcard (labeled APP 1) when requested. If asked to override, affirm by pressing "ENT" key. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 1 of 7 2 of 7 3 of 7	TJ	6:02PM
40	CA repeats the above step a second time, making a backup of the wrapping keys using the same 3 SO cards and inserting an APP smartcard (**labeled APP 2**) when requested. If asked to override, affirm by pressing "ENT" key.	TJ	6:06PM
41	CA repeats the above step a ~~second~~ Third time, making a backup of the wrapping keys using the same 3 SO cards and inserting an APP smartcard (**labeled APP 3**) when requested. If asked to override, affirm by pressing "ENT" key.	TJ	6:07PM
42	CA makes a backup of the HSM config files linked to these APP cards by executing: `tar zcf hsmbaseconfig20110426.tar.gz *.db`	TJ	6:08PM

Step	Activity	Initial	Time

43	CA plugs a blank FD labeled HSMDB into a spare USB slot and waits for O/S to recognize drive.
	Once recognized, CA copies *.db files linked with the APP cards just created to the new blank FD by executing:
	`cp -p *.db /opt/dnssec/machine /media/HSMDB`
	`ls -lt /media/HSMDB`
	CA then un-mounts HSMDB by executing
	`umount /media/HSMDB`
	and remove FD
			6:11PM

44	CA repeats above step a second time, placing the completed backup flash drive alongside the APP cards. These will later be packaged together for safekeeping.		6:12PM
45	CA repeats above step a third time, placing the completed backup flash drive alongside the APP cards. These will later be packaged together for safekeeping.		6:13PM
46	CA presses RESTART button on HSM. After self test completes, Ready LED should be lit indicating HSM is configured for auto-online mode.		6:19PM
47	CA executes `showallkeys` to do a final check on the HSM before transport to San Jose.		6:29PM
48	Via the HSM Mgmt, "Set Network", "IP Address" menu items the CA changes the HSM network configuration to IP address 192.168.100.2 to correspond with the signer configuration using any 3 SO cards. Each byte of the IP address is entered as 3 digits, i.e., 2 = 002, and must be entered even if already displaying correct value. Once this is complete, press "ENT". List SO cards used and order here (e.g., 2 of 7, 5 of 7...) _____ of 7 _____ of 7 _____ of 7 CA verifies IP address settings by pressing RESTART and reviewing network settings via the View Network and IP address menu items.		6:31PM

Step	Activity	Initial	Time
49	CA disconnects Ethernet and serial connection from HSM and unplugs power from unit and places it inside a new TEB. A337N431/K0705020		6:38PM
50	CA reads out TEB # and HSM serial #, shows item to participants.		6:38PM
51	EW records TEB # and HSM serial # here. TEB # A337N431 HSM serial # K075020		6:38PM
52	The HSM will be transported by at least two trusted persons to the signer facility for installation.		6:38PM

Initialize HSM2 : KSK-HSM-01-SJC

Step	Activity	Initial	Time
53	CA inspects the HSM2 TEB for tamper evidence; reads out TEB # and serial # while EW matches it with the prior script entry: TEB # A3379385 ✓ Serial # K0911004 ✓		6:39PM
54	CA removes HSM2 from TEB; discards TEB, labels HSM2 "KSK-HSM-01-SJC" and plugs the null modem serial cable to the back.		6:42PM
55	CA connects power to HSM. Status information should appear on the serial logging screen and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state.		6:43PM

Import Adapter Authorization Key (AAK)

Step	Activity	Initial	Time
56	CA imports AAK using the HSM main menu "Restore AAK" and AAK cards. Once imported, press CLR.		6:44PM

Go Operational and Setup

Step	Activity	Initial	Time
57	CA sets the HSM operational ("Go Operational" on menu) using any three (3) SO cards. When presented with "Import config" press CLR button repeatedly until you reach the "Set Online" menu item. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 5 of 7 6 of 7 7 of 7		6:46PM
58	CA dumps the status of the HSM via the "Output Status" menu item (using '>' key).		6:47PM

Step	Activity	Initial	Time
59	CA verifies settings below. If not set, CA may fix the settings using "API Setting" via "Key Mgmt" (eg, if LCD display shows "key import, disable" this means key import is enabled. Click ENT to disable). For auto online disable, use HSM Mgmt menu. Global Key Export Enabled App Key Import Enabled **App Key Export Enabled** Asymmetric Key Gen Enabled Symmetric Key Gen Enabled **Symmetric Key Derive Enabled** Signing Enabled Signature Verification Enabled MAC Gen Enabled MAC Ver Enabled Enc/Dec Enabled Delete Asym Key Enabled Delete Sym Key Enabled Output Key Details Enabled Output Key Summary Enabled Suite B Algorithms Enabled Non Suite B Algorithms Enabled AES SMK **Auto Online Disabled** FIPS Mode		6:48 PM

Erasing the Adapter Authorization Key (AAK) Cards

Step	Activity	Initial	Time
60	CA erases the two AAK cards using any three (3) of a set of SO cards via "Key Mgmt", "AAK", "Clear Card", "# Cards" menu items. CA then puts cards into a new TEB and seals placing TEB on table. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 3 of 7 4 of 7 5 of 7 CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # _____		7:00 PM

Note

Import Storage Master Key (SMK)

Step	Activity	Initial	Time
61	CA imports SMK from HSM1 using any 5 of the 7 SMK cards and any three (3) SO cards via the "Key Mgmt", "SMK", "Restore" menu item. . List SO cards used and order here (e.g., 2 of 7, 5 of 7...) 1 of 7 2 of 7 7 of 7 List SMK cards used and order here. 1 of 7 2 of 7 3 of 7 4 of 7 5 of 7	JF	7:03PM

Import the Wrapping Keys

Step	Activity	Initial	Time
62	CA imports the wrapping keys from HSM1 using any APP card and any three (3) SO cards via the "Key Mgmt", "APP", "Restore" menu item. If a second card is requested hit "CLR". List SO cards used and order here (e.g., 2 of 7, 5 of 7...) of 7 of 7 of 7 APP card number 2	JF	7:04PM

Testing HSM2

Step	Activity	Initial	Time
63	CA sets HSM online ("Set Online" menu item) using any three (3) OP cards. The "Ready" LED should go on. List OP cards used and order here (e.g., 2 of 7, 5 of 7...) 1 of 7 2 of 7 3 of 7	JJ	7:06PM
64	CA connects HSM to laptop using Ethernet cable that was previously connected to HSM1.	JJ	7:06PM
65	CA tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` on the laptop terminal window. Control-C to exit program.	JJ	7:06PM
66	CA executes `showallkeys` to check.	JJ	7:19PM

Generate KSKs and ZSKs

Step	Activity	Initial	Time
67	CA starts generation of RSA 2048bit and 1024bit keys inside the HSM by executing `bulkgen` This will take approximately 15sec/2048bit key and 3sec/1024bit key. (Note: Crypto Officers, Security Controllers, and System Administrators are not necessary during this step.)	JJ	7:33PM

Package APP Cards and HSMDB Flash Drives

Step	Activity	Initial	Time
68	CA places one of the backup HSMDB FDs and APP 1 card in a TEB and seals.		7:35PM
69	CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # A21094991		7:35PM
70	CA places one of the backup HSMDB FDs and APP 2 card in a TEB and seals.		7:36PM
71	CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # A21094990		7:36PM
72	CA places one of the backup HSMDB FDs and APP 3 card in a TEB and seals.		7:37PM
73	CA reads out TEB #; shows item to participants and EW records TEB # here. TEB # A21094989		7:38PM

Package SMK Cards

Step	Activity	Initial	Time
74	CA places each SMK card with an instruction slip indicating the ownership and disposition of the card in its own new TEB and records the number in the Smart Card Sign Out Sheet.		7:51PM

Package SO Cards

Step	Activity	Initial	Time
75	CA places each SO card with instruction slip in its own new TEB and records the number in the smart card sign out sheet below.		8:29PM

Backup of KSKs and ZSKs

Step	Activity	Initial	Time
76	CA creates encrypted backups of the ZSKs by executing `zskbackup` After the key ceremony, this file will be transferred to the signer where it will be imported into the HSM.		7:53PM
77	CA similarly does this for the KSKs by executing `kskbackup` This file will not be imported by the signer HSM and is kept for backup purposes only.		7:54PM

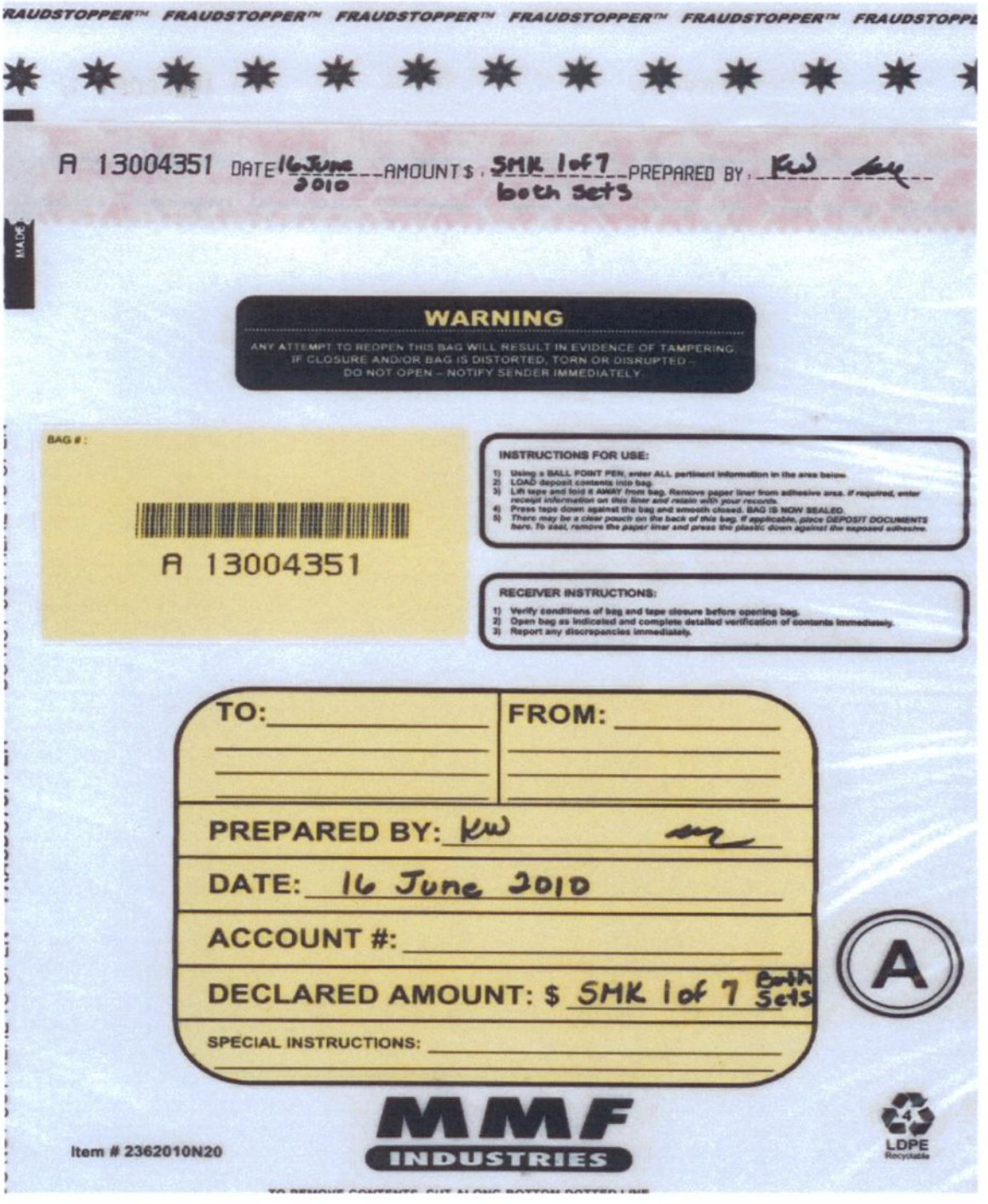
Generate Signed DNSKEY RRsets

Step	Activity	Initial	Time

78	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 -p /opt/dnssec/aep.hsmconfig .`
	`keybundle-generate`
	`tar zcf /media/HSMFD/20110426.kb.tar.gz .`
	`cd /media/HSMFD`
	This will create time sensitive 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.
			7:59PM

Package OP Cards

Step	Activity	Initial	Time
79	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.		8:35PM


FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™
A 13004351 DATE 16 June 2010 AMOUNT $ SMK 1 of 7 both sets PREPARED BY: KW
WARNING
ANY ATTEMPT TO REOPEN THIS BAG WILL RESULT IN EVIDENCE OF TAMPERING.
IF CLOSURE AND/OR BAG IS DISTORTED, TORN OR DISRUPTED –
DO NOT OPEN – NOTIFY SENDER IMMEDIATELY.
BAG #:
A 13004351
INSTRUCTIONS FOR USE:
1) Using a BALL POINT PEN, enter ALL pertinent information in the area below.
2) LOAD deposit contents into bag.
3) Lift tape and fold it AWAY from bag. Remove paper liner from adhesive area. If required, enter receipt information on this liner and retain with your records.
4) Press tape down against the bag and smooth closed. BAG IS NOW SEALED.
5) There may be a clear pouch on the back of this bag. If applicable, place DEPOSIT DOCUMENTS here. To seal, remove the paper liner and press the plastic down against the exposed adhesive.
RECEIVER INSTRUCTIONS:
1) Verify conditions of bag and tape closure before opening bag.
2) Open bag as indicated and complete detailed verification of contents immediately.
3) Report any discrepancies immediately.
TO:
FROM:
PREPARED BY: KW
DATE: 16 June 2010
ACCOUNT #:
DECLARED AMOUNT: $ SMK 1 of 7 both Sets
SPECIAL INSTRUCTIONS:
A
Item # 2362010N20
MMF INDUSTRIES
4 LDPE Recyclable

Return HSM2 to a Tamper Evident Bag

Step	Activity	Initial	Time
80	CA presses RESTART button and waits for self test to complete.		8:03PM
81	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.		8:06PM
82	CA reads out TEB # and HSM serial #, shows item to participants.		8:06 PM
83	EW records TEB # and HSM serial # here. TEB # A3379430 HSM serial # K0911004		8:07PM

Stop Recording Serial Port Activity

Step	Activity	Initial	Time
84	CA terminates HSM serial output capture by disconnecting USB serial adaptors from laptop. CA then exits out of serial output terminal window.		8:09PM

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time
85	CA displays contents of HSMFD by executing `ls -lt`		8:11 PM
86	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_`		8:12 PM
87	CA displays contents of HSMFD_ by executing `ls -lt /media/HSMFD_`		8:12 PM
88	CA unmounts new FD using `umount /media/HSMFD_`		8:12 PM
89	CA removes HSMFD_ and places on table		8:12 PM
90	CA repeats the first four steps of this activity a second time, to create a second backup.		8:12 PM
91	CA repeats the first four steps of this activity a third time, to create a third backup.		8:13 PM
92	CA repeats the first four steps of this activity a fourth time, to create a fourth backup.		8:14 PM

Stop Logging Terminal Output

Step	Activity	Initial	Time
93	CA stops logging terminal output by entering "exit" in remaining terminal window		8:15 PM

Return HSM FD to a Tamper Evident Bag

Step	Activity	Initial	Time

94	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
			8:15 PM

95	CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants.		8:16 PM
96	EW records TEB # and HSM serial # here. TEB # A21094988 HSM serial # N/A		8:17pm

Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time
97	After all print jobs are complete, CA executes `shutdown -hP now` removes DVD and turns off laptop.		8:19PM
98	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.		8:20
99	EW records TEB # and HSM serial # here. TEB # A21094987 HSM serial #		8:20

Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time
100	CA disconnects power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants.	[signature]	9:00PM
101	EW records TEB # and HSM serial # here. TEB # A 3379432 HSM serial # _____	[signature]	9:02PM

Return Power Supplies, USB Hub, and Cables to Cart

Step	Activity	Initial	Time
102	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. This, APP 1 card TEB, erased AAK card TEB, and the above items will be stored in the bank safe deposit box controlled by the SSC. There the SSC will record return of each item on the safe log with TEB #, printed name, date, time, and signature with a second party initialing each entry. The remaining APP 2 and APP 3 TEBs will be kept in a secure container in the PCH office.	[signature]	9:07PM

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.		8:37PM
104	SMK1, SO1, OP1 TEB# A21094986 go to CO1, Steve FELDMAN.		8:39PM
105	SMK5, SO5, OP5 TEB# A21094983 are entrusted to CO1, Steve FELDMAN, for conveyance to CO5, Stephan SOMOGYI.		8:43PM
106	SMK2, SO2, OP2 TEB# A21094985 go to CO2, Michael SINATRA.		8:45PM
107	SMK3, SO3, OP3 TEB# A21094984 go to CO3, Kim DAVIES.		8:46PM
108	SMK6, SO6, OP6 TEB# A21094982 are entrusted to CO3, Kim DAVIES, for conveyance to CO6, LEONG Keng Thai.		8:48PM
109	SMK 4, SO4, OP4 TEB# A21094980 go to CO4, Jonny MARTIN.		8:49PM
110	SMK7, SO7, OP7 TEB# A21094981 are entrusted to CO4, Jonny MARTIN, for conveyance to CO7, Gaurab UPADHAYA.		8:50PM

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A21095013	Steve FELDMAN		4/25/11	20:56	
CO1	SO 1 of 7	A21095012	Steve FELDMAN		4/25/11	20:56	
CO1	SMK 1 of 7	A21095011	Steve FELDMAN		4/25/11	20:56	
CO2	OP 2 of 7	A21095010	Michael SINATRA		4/25/11	20:55	
CO2	SO 2 of 7	A21095009	Michael SINATRA		4/25/11	20:55	
CO2	SMK 2 of 7	A21095008	Michael SINATRA		4/25/11	20:55	
CO3	OP 3 of 7	A21095007	Kim DAVIES		4/25/11	8:52	
CO3	SO 3 of 7	A21095006	Kim DAVIES		4/25/11	8:52	
CO3	SMK 3 of 7	A21095004	Kim DAVIES		4/25/11	8:52	
CO4	OP 4 of 7	A21095005	Jonny MARTIN		4/25/11	8:58	
CO4	SO 4 of 7	A21095003	Jonny MARTIN		4/25/11	8:58	
CO4	SMK 4 of 7	A21095002	Jonny MARTIN		4/25/11	8:58	
CO5	OP 5 of 7	A21095001	Steve FELDMAN		4/25/11	20:56	
CO5	SO 5 of 7	A21095000	Steve FELDMAN		4/25/11	20:56	
CO5	SMK 5 of 7	A21094999	Steve FELDMAN		4/25/11	20:56	
CO6	OP 6 of 7	A21094998	Kim DAVIES		4/25/11	8:53	
CO6	SO 6 of 7	A21094997	Kim DAVIES		4/25/11	8:53	
CO6	SMK 6 of 7	A21094996	Kim DAVIES		4/25/11	8:53	
CO7	OP 7 of 7	A21094995	Jonny MARTIN		4/25/11	8:58	
CO7	SO 7 of 7	A21094994	Jonny MARTIN		4/25/11	8:58	
CO7	SMK 7 of 7	A21094993	Jonny MARTIN		4/25/11	8:58	

Participant Sign-Out on External Witness' Script

Step	Activity	Initial	Time
111	All participants sign EW's script coversheet, and note their exit time.		9:25pm
112	CA reviews EW's script and signs it. CA Signature: _____		9:25pm

Sign Out of Key Management Facility

Step	Activity	Initial	Time
113	FO returns phones, laptops, and other items to participants and logs their exit.		9:16pm

Stop Audio-Visual Recording

Step	Activity	Initial	Time
114	SA stops audio and video recording.		9:16pm

Copy and Store the Script

Step	Activity	Initial	Time
115	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 4", dated and signed by EW and CA. One bundle will be stored by the SC along with equipment in bank safe deposit box. The second bundle will be kept securely at PCH's office.		

All remaining participants sign out of ceremony room log and leave.

Notes

From the Audit Bundle Checklist Document:

1. Output of Signer System (CA)

One electronic copy (physical flash drive) of the HSMFD in each audit bundle, each placed within a tamper-evident bag, labeled, dated and signed by the CA and the EW

2. Key Ceremony Scripts (EW)

Hard copies of the EW's key ceremony scripts, including the EW's notes and the EW's attestation. See Appendix A.1.

3. Audio-visual recordings from the key ceremony (SA)

4. Logs from the Physical Access Control and Intrusion Detection System (SA)

One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC-IDS configuration review, the list of the enrolled users, the event log file and the configuration audit log file in each audit bundle, each placed in a tamper-evident bag, labeled, dated and signed by the SA and the EW

5. Configuration review of the Physical Access Control and Intrusion Detection System (SA)

SA's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix A.2.

6. Configuration review of the Firewall System (SA)

SA's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3.

Appendix A.1:

Key Ceremony Script

(by EW)

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

Printed Name: Larry W. [illegible]

Signature: [illegible]

Date: 4/26/11

Appendix A.2:

Access Control System Configuration Review

(by SA)

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

Enclosed is the audited physical access log.

Printed Name: PETER ROWLAND

Signature: P. Rowland

Date: APRIL 26, 2011

SEE ATTACHED FACILITY SIGN-IN SHEET.
PERIMETER ACCESS CONTROL WAS NOT BREACHED
DURING THE CEREMONY.

PCH
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

1600 Shattuck Avenue
Facility Sign-In Sheet

Name	Signature	Date	Entry Time PDT	Exit Time PDT
Vicky SHRESTHA		4/25/11	8:05 AM	2:29 pm
Larry JORDAN		4/25/11	8:16AM	2:24pm
Steve FELDMAN		4/25/11	8:47 AM	14:27
Michael SINATRA		4/25/11	8:45AM	1:57 PM
Kim DAVIES		4/25/11	9:18am	1:56pm
Jonny MARTIN		4/25/11	8:45am	2:30PM
Stephan SOMOGYI		4/25/11	8:16 PDT	10:31AM
Peter ROWLAND		4/25/11	8:17 PDT	2:26PM
Bill WOODCOCK		4/25/11	7:55AM	2:19 PM
Rick LAMB		4/25/11	7:55AM	2:26PM

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature: Ty W Jones		6:56PM
2	EW Describes exception and action below		6:56PM

Steve Feldmon Left the room temp 6:56PM
steve Feldman Return at 7:20pm

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature: E W. J	//	6:58 PM
2	EW Describes exception and action below	//	6:58 PM

Step #60 ~~Destroy~~ // Destroyed AAK Cards & Bad OP card with scissors // In addition to Clearing

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature: Larry W. Jr	LJ	7:23pm
2	EW Describes exception and action below	LJ	7:23pm

Rick Lamb is leaving the room 7:23 PM
Rick Lamb back in the room 7:27 PM

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature:		7:38 PM
2	EW Describes exception and action below		7:38 PM

Bill Woodcock left the room & came back at 7:38 PM

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature:		7:51pm
2	EW Describes exception and action below		

Skipping step 75 postponed & 79 going to step 80.

After Step 99 returning to step 95 8:21pm

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature: Z W. Jan	1/	6:16PM
2	EW Describes exception and action below		

Step 46. required CA to reset HSM to Auto online mode using SO cards.
OP card /3 displayed failuer on HSM.
We will regenarate OP cards at end.
we will regenarate OP cards 6:22PM
redo step 29.
we use SO cards 4, 5, 6
using Operator cards 1-7

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

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW notes date and time of key ceremony exception and signs here: Signature: Ray W. Jr	RH	5:32PM
2	EW Describes exception and action below	RH	5:33PM

Peter Rowland left the room temp.
Peter Rowland return at 5:53 PM
Peter Rowland left the room at 7:19 PM
Peter Rowland return 8:50 pm

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

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California
County of San Mateo

On 4/26/11 (Date) before me, Larry W. Jordan (Here Insert Name and Title of the Officer),

personally appeared Vicky Shrestha (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.

LARRY W. JORDAN
Commission # 1852953
Notary Public - California
San Mateo County
My Comm. Expires Jun 7, 2013

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: Larry W. Jordan (Signature of Notary Public)

Place Notary Seal and/or Stamp Above

OPTIONAL

Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another document.

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____	Signer's Name: _____
☐ Corporate Officer — Title(s): _____	☐ Corporate Officer — Title(s): _____
☐ Individual	☐ Individual
☐ Partner — ☐ Limited ☐ General	☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact	☐ Attorney in Fact
☐ Trustee	☐ Trustee
☐ Guardian or Conservator	☐ Guardian or Conservator
☐ Other: _____	☐ Other: _____
Signer Is Representing: _____	Signer Is Representing: _____
RIGHT THUMBPRINT OF SIGNER — Top of thumb here	RIGHT THUMBPRINT OF SIGNER — Top of thumb here

LARRY W. JORDAN
Commission # 1852953
Notary Public - California
San Mateo County
My Comm. Expires Jun 7, 2013