PCH
Packet Clearing House
572B 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
Friday, January 20, 2012

Sign In to Facility

Step	Activity	Initial	Time (SST)
1	FO has all participants sign in before entering the Key Management Facility.		17:31
2	FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility, and the SA may retain a laptop.		17:31

Emergency Evacuation Procedures

Step	Activity	Initial	Time (SST)
3	FO reviews emergency evacuation procedures and other relevant information with participants.		17:31

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.		18:00

Ground Rules

Step	Activity	Initial	Time (SST)
5	CA reviews ground rules and break procedures with participants.		18:04

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: 1/20/12 Time: 18:04 This and all subsequent entries into this script and any associated logs should follow this common source of time.		18:04

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
7	SC opens safe and makes entry in log sheet indicating opening of safe		1806
8	CA collects KSK-HSM-01B-SJC HSM, boot-DVD, laptop, KSK-HSM-01B-SJC HSMFD, power supplies, cables, etc. and any other items that me be scheduled for removal indicating removal of each with corresponding TEB number on safe log. Equipment is placed on table visible to all participants.		18:11
9	CA reads out KSK-HSM-01B-SJC HSM TEB and serial number while EW matches this with previous key ceremony recorded entry. TEB# A3112627 Serial # K1011066		18:12
10	CA similarly reads out boot-DVD, laptop, and HSMFD TEB numbers while EW matches them with prior script entries. DVD TEB# A21094977 Laptop TEB# A3112622 HSMFD KSK-HSM-01B-SJC TEB# A19204936 37		18:13

Step	Activity	Initial	Time (UTC)
11	SC makes entry in log sheet indicating closing of safe then closes safe. EW verifies safe is locked.		18:14

Collect OP Cards

Step	Activity	Initial	Time (SST)
12	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.		18:21

Set Up Laptop

Step	Activity	Initial	Time (UTC)
13	CA places the boot-DVD and laptop on the table; connects laptop power and boots laptop from DVD.		18:23
14	CA logs in as root.		18:28
15	CA opens a terminal window.		18:28

16	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`
			18:29

17	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.		18:47

Step	Activity	Initial	Time (UTC)
18	EW records the sixty-four digit boot-DVD checksum 7DF4 31F9 C33D DFEF 9089 AB56 1383 8106 7088 3AC1 A784 3887 3BA7 B9C9 2A4F S2A1 B9C9 2A4F S2A1 F87C Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in Appendix F of this document.		18:47
19	CA connects USB hub to laptop.		18:30
20	CA removes HSMFD KSK-HSM-01B-SJC from TEB and plugs 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.		18:33

Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
21	CA changes the default directory to the HSMFD: `cd /media/HSMFD`		18:33
22	CA starts capture of terminal output: `script script-20120120.log`		18:33

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
23	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.		18:35
24	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.		18:35

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

Step	Activity	Initial	Time (UTC)
25	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.		18:36
26	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.		18:41

Activate HSM

Step	Activity	Initial	Time (UTC)
27	CA sets HSM online ("Set Online" menu item) using three (3) OP cards. The "Ready" LED should go on. Use OP cards 2, 4, and 5.		18:50
28	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.		18:50

Generate Keys and Keybundles

Step	Activity	Initial	Time (UTC)

29	CA copies shell scripts that will be used to generate new keys and bundles by plugging in SCRIPTS FD and executing:
	`ls /media/SCRIPTS`
	`cp -p /media/SCRIPTS/* .`
	`cp -p /media/SCRIPTS/* /opt/dccom`
	`mkdir /tmp/pch`
	`cp -p *.hsm 20120120.data /tmp/pch`
			18:53

30	Begin the key+keybundle generation by first: `tar zcf 20110620.KSK-HSM-01-SIN.db.tar.gz *.db`		

Step	Activity	Initial	Time (UTC)

31	CA creates encrypted backups of the ZSKs by executing
	`cd /tmp/pch`
	then executing:
	`keybundle-generate.20120120 < 20120120.data`
	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.
			19:38

32	CA now archives the results onto the HSMFD by executing:
	`tar zcf /media/HSMFD/ 20120120.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256`
	to generate the archive destined for the signer and
	`tar zcf /media/HSMFD/ 20120120.session.tar.gz .`
	to archive all results including encrypted ksks for future use.
			19:40

33	CA executes:
	`cd /media/HSMFD`
	`ls`
	to return to HSMFD and list contents.
			19:41

34	CA creates a snapshot of any changes to DB files by executing: `tar zcf 20120120.KSK-HSM-01B-SJC.db.tar.gz *.db`		19:42

35	CA zeroizes SCRIPTS FD and unmounts by executing:
	`rm -rf /media/SCRIPTS/*`
	`unmount /media/SCRIPTS`
	and removes the SCRIPTS FD for reuse.
			19:42

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
36	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.		19:48

Step	Activity	Initial	Time (UTC)
37	CA reads out TEB # and HSM serial #, shows item to participants while EW records TEB # and HSM serial # here. TEB # A3112557 HSM serial # K1011066		19:53

Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
38	CA terminates HSM serial output capture by disconnecting USB serial adaptors from laptop. CA then exits out of serial output terminal window.		19:53

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
39	CA displays contents of HSMFD by executing `ls -lt`		19:54
40	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 `cp -Rp * /media/HSMFD_`		20:06
41	CA displays contents of HSMFD_ by executing `ls -lt /media/HSMFD_`		20:06
42	CA unmounts new FD using `umount /media/HSMFD_`		20:06
43	CA removes HSMFD_ and places it in new TEB and seals; reads out TEB # and shows item to participants while EW records TEB # here. TEB # A19204963		20:10
44	CA repeats this activity a second time, to create a second backup. EW records TEB # here. TEB # A19204964		20:12

Step	Activity	Initial	Time (UTC)
45	CA repeats this activity a third time, to create a third backup. EW records TEB # here. TEB # A19204945	//	20:15
46	CA repeats this activity a fourth time, to create a fourth backup. EW records TEB # here. TEB # A19204946	//	20:18

Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
47	CA stops logging terminal output by entering "exit" in remaining terminal window	//	20:19

Return HSM FD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)

48	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
		//	20:19

49	CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants.	//	20:19
50	EW records TEB # here. TEB # A19204947	//	20:21 //

Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
51	After all print jobs are complete, CA executes `shutdown -hP now` removes DVD and turns off laptop.	//	20:22
52	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.	//	20:23

Step	Activity	Initial	Time (UTC)
53	EW records TEB # here. TEB # A1920 4948	JJ	20:24

Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
54	CA disconnects power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants.	JJ	20:26
55	EW records TEB # here. TEB # A 3112599	JJ	20:27

Return Power Supplies, USB Hub, and Cables

Step	Activity	Initial	Time (UTC)
56	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.	JJ	20:29
57	SC opens safe indicating this on safe log sheet.	JJ	20:29
58	CA returns KSK-HSM-01B-SJC HSM, laptop, original HSMFD above and fourth HSNFD backup, DVD, and other items to safe. CA will record return of each item on the safe log with TEB #, printed name, date, time, and signature with a second participant initialing each entry.	JJ	20:35
59	SC closes safe. EW verifies it is locked. Two of the remaining HSMFDs will be packaged with the two audit bundles below. CA keeps any remaining materials (e.g. extra HSMFD) for next key ceremony preparation and analysis.	JJ	20:35

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.	1/	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.	1/	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		1/20/12	2051	
CO2	SO 2 of 7	A19204952	Michael SINATRA		1/20/12	2051	
CO4	OP 4 of 7	A19204949	Jonny MARTIN		1/20/12	2049	
CO4	SO 4 of 7	A19204953	Jonny MARTIN		1/20/12	2049	
CO5	OP 5 of 7	A19204951	Stephan SOMOGYI		1/20/12	2046	
CO5	OUTSIDE BAG SO 5 of 7	A19204954	Stephan SOMOGYI		1/20/12	2046	

~~OUTSIDE BAG~~

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
62	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.		20:55
63	CA reviews EW's script and signs it. CA Signature: _____		20:55

Sign Out of Facility

Step	Activity	Initial	Time (UTC)
64	FO returns phones, laptops, and other items to participants and logs their exit times. Participants are now free to depart.		20:55

Stop Audio-Visual Recording

Step	Activity	Initial	Time (UTC)
65	SA stops audio and video recording.		20:55

Copy and Store the Script

Step	Activity	Initial	Time (UTC)
66	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. The two 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. The second bundle will be kept securely offsite.		

* 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: Larry W. Jordan

Signature: Larry W. Jordan

Date: 1/20/12

Attach notarization to this page.

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California
County of San Mateo }

On 1/20/12 (Date) before me, Larry W. Jordan (Here Insert Name and Title of the Officer),

personally appeared William Edward Woodcock (Name(s) of Signer(s))

,

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

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

WITNESS my hand and official seal.

Signature: _____ (Signature of Notary Public)

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

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: _____

☐ Corporate Officer — Title(s): _____
☐ Individual
☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact
☐ Trustee
☐ Guardian or Conservator
☐ Other: _____

Signer Is Representing: _____

RIGHT THUMBPRINT OF SIGNER
Top of thumb here

Signer's Name: _____

☐ Corporate Officer — Title(s): _____
☐ Individual
☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact
☐ Trustee
☐ Guardian or Conservator
☐ Other: _____

Signer Is Representing: _____

RIGHT THUMBPRINT OF SIGNER
Top of thumb 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: Bill Woodcock

Signature: 

Date: Jan 20, 2012

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

Role	Name	Signature	Date	Entry Time PDT	Exit Time PDT
FO	Peter ROWLAND		1/20/12	9:32	1:00 PM.
CA1	Vicky SHRESTHA		1/20/12	9:25	1:00PM
CA2	Rick LAMB		1/20/12	9:25	1:00
EW	Larry JORDAN		1/20/12	9:25	1:00
CO2	Michael SINATRA		1/20/12	9:25	1254
CO4	Jonny MARTIN		1/20/12	9:30	1254
CO5	Stephan SOMOGYI		1/20/12	09:25	1257
SC1 SA	Bill WOODCOCK		1/20/12	9:25 AM	12:55 PM
SC2	Bob ARASMITH		1/20/12	9:25	12:56
W	Mark DOYLE		1/20/12	9:25	12:55
W	Gian-Carlo BAVA		1/20/12	10:30	12:56

Appendix C:

Abbreviations Used in This Document

Roles

CA	Ceremony Administrator
EW	External Witness
SA	System Administrator
CO	Crypto Officer
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:

Card Distribution from Key Ceremony 1

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

Appendix F:

Smart Card Sign Out Sheet from Key Ceremony 1

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	

Appendix G:

Smart Card Sign Out Sheet from Key Ceremony 2

Smart Card Sign Out Sheet

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 - C04
A19204943 - CO7
A19204942 - CO2
A19204941 CO5

Appendix H:

Smart Card Sign Out Sheet from Key Ceremony 3

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A 1920487[illegible]	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	A19204872	Jonny MARTIN		6/20/11	07:49	
CO6	OP 6 of 7	A19204870	LIM Choon Sai		6/20/11	07.50	
CO7	OP 7 of 7	A192048 68	Gaurab UPADHAYA		6/20/11	07.49	

ENCLOSING BAGS:

CO1: A 19204875

CO3: A 19204873

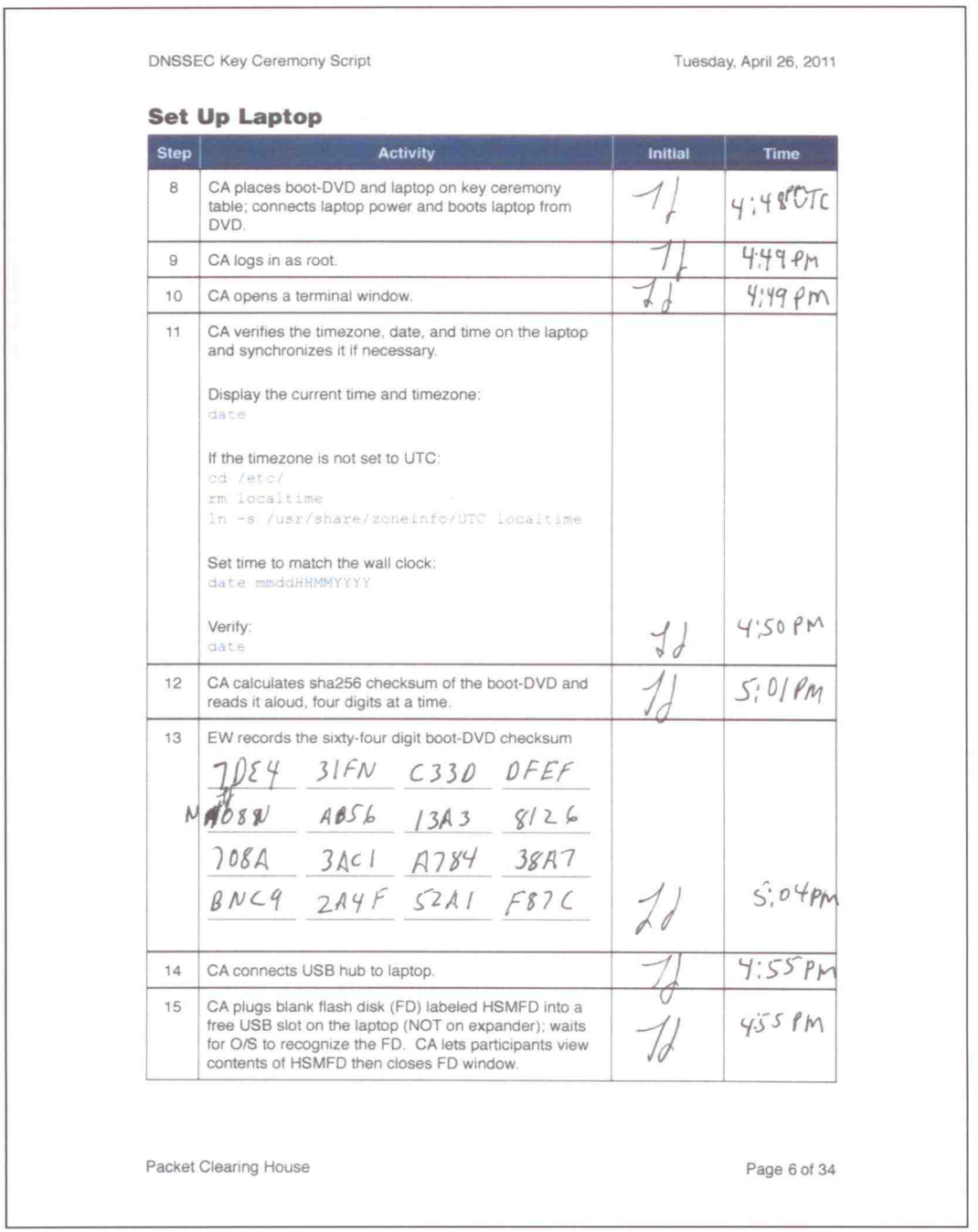
CO 4: A19204871

CO 6: A19204869

CO7: A19204867

Appendix I:

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.		4:48 UTC
9	CA logs in as root.		4:49 PM
10	CA opens a terminal window.		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`
			4:50 PM

12	CA calculates sha256 checksum of the boot-DVD and reads it aloud, four digits at a time.		5:01 PM
13	EW records the sixty-four digit boot-DVD checksum 7DE4 31FN C330 DFEF N9089 AB56 13A3 8126 708A 3AC1 A784 38A7 BNC9 2A4F 52A1 F87C		5:04 PM
14	CA connects USB hub to laptop.		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.		4:55 PM

Packet Clearing House Page 6 of 34

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

Participant Signature Sheet

Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
CA1	Vicky SHRESTHA	NP		CDL	F1092677	1/20/12	17:59	20:54
CA2	Rick LAMB	US		CDL	E1123160	1/20/12	17:39	
EW	Larry JORDAN	US		LDL	N4675802	1/20/12	17:37	
CO2	Michael SINATRA	US		CDL	B3410470	1/20/12	17:39	2052
CO4	Jonny MARTIN	NZ		CDL	F1781184	1/20/12	17:39	2052
CO5	Stephan SOMOGYI	CA		CDL	A6289747	1/20/12	17:38	2052
SC1 SA	Bill WOODCOCK	US		CDL	A1005023	1/20/12	17:37	20:53
~~SC2~~	~~Bob ARASMITH~~	~~US~~				~~1/20/12~~		
W	Mark DOYLE	US		CDL	N9709398	1/20/12	17:40	20:54
W	Gian-Carlo BAVA	US		CDL	N0293824	1/20/12	18:38	20:53

DO NOT ENTER FACILITY

Notes: Steve FELDMAN, Kim DAVIES, LIM Choon Sai, and Gaurab UPADHAYA will not be present for this ceremony, so the necessary three of seven sets of keys present are: 2, 4 and 5.

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here: Step 1-5 & 12 SST 1-5 should have said PST Step 12 should be UTC	JJ	1800
2	EW notes date and time of key ceremony exception and signs here: Signature: JJ	JJ	18:00

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here: Instead of the Important Read Manual / it said set online	JJ	18:42
2	EW notes date and time of key ceremony exception and signs here: Signature:	JJ	18:42

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

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here: Step 30 not needed cross out R Left over from a prior Script	TJ	1854
2	EW notes date and time of key ceremony exception and signs here: Signature:	TJ	18:54

* End of DNSSEC Key Ceremony Script Exception *

```
#
# ** fo. refresh/retry/expire: 600 300 2592000 **
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
fo 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** nic.fo. refresh/retry/expire: 10800 3600 2419000 **
#Estimated DNSSEC Parameters
# RRSIG validity 37(days)
# New keybundle every 10(days)
# ZSK roll every 113(days)
# SOAexp=27(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
nic.fo 20120121000000 47304000 none none RSASHA256 86400 3283000 864000 9849000
#
# ** com.ar. refresh/retry/expire: 21600 3600 1728000 **
#Estimated DNSSEC Parameters
# RRSIG validity 30(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=20(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
com.ar 20120121000000 47304000 none none RSASHA256 86400 2592000 864000 7884000
#
# ** net.ar. refresh/retry/expire: 86400 3600 1728000 **
#Estimated DNSSEC Parameters
# RRSIG validity 30(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=20(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
net.ar 20120121000000 47304000 none none RSASHA256 86400 2592000 864000 7884000
#
# ** org.ar. refresh/retry/expire: 43200 3600 1728000 **
#Estimated DNSSEC Parameters
# RRSIG validity 30(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=20(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
org.ar 20120121000000 47304000 none none RSASHA256 86400 2592000 864000 7884000
#
# ** int.ar. refresh/retry/expire: 86400 3600 1728000 **
#Estimated DNSSEC Parameters
# RRSIG validity 30(days)
```

co.na 20120121000000 47304000 none none RSASHA256 86400 3283200 864000 9849600
#
** org.na. refresh/retry/expire: 7200 3600 2419200 **
#Estimated DNSSEC Parameters
RRSIG validity 38(days)
New keybundle every 10(days)
ZSK roll every 114(days)
SOAexp=28(days) maxttl=86400
DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
org.na 20120121000000 47304000 none none RSASHA256 86400 3283200 864000 9849600
#
** alt.na. refresh/retry/expire: 7200 3600 2419200 **
#Estimated DNSSEC Parameters
RRSIG validity 38(days)
New keybundle every 10(days)
ZSK roll every 114(days)
SOAexp=28(days) maxttl=86400
DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
alt.na 20120121000000 47304000 none none RSASHA256 86400 3283200 864000 9849600
#
** edu.na. refresh/retry/expire: 7200 3600 2419200 **
#Estimated DNSSEC Parameters
RRSIG validity 38(days)
New keybundle every 10(days)
ZSK roll every 114(days)
SOAexp=28(days) maxttl=86400
DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
edu.na 20120121000000 47304000 none none RSASHA256 86400 3283200 864000 9849600
#
** net.na. refresh/retry/expire: 7200 3600 2419200 **
#Estimated DNSSEC Parameters
RRSIG validity 38(days)
New keybundle every 10(days)
ZSK roll every 114(days)
SOAexp=28(days) maxttl=86400
DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
net.na 20120121000000 47304000 none none RSASHA256 86400 3283200 864000 9849600
#
** lisse.na. refresh/retry/expire: 7200 3600 2419200 **
#Estimated DNSSEC Parameters
RRSIG validity 38(days)
New keybundle every 10(days)
ZSK roll every 114(days)
SOAexp=28(days) maxttl=3600
DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
lisse.na 20120121000000 47304000 none none RSASHA256 86400 3283200 864000 9849600
#
** co.ug. refresh/retry/expire: **
Zone does not exist. Picking SOA numbers

```
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
ne.ug 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** com.ug. refresh/retry/expire:    **
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
com.ug 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** org.ug. refresh/retry/expire:    **
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
org.ug 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** eahd.or.ug. refresh/retry/expire: 10800 3600 604800 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=7(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
eahd.or.ug 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
# ** registry.co.ug. refresh/retry/expire: 10800 3600 604800 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=7(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
registry.co.ug 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
# ** whois.co.ug. refresh/retry/expire: 10800 3600 604800 **
#Estimated DNSSEC Parameters
```

```
# SOAexp=7(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
woodynet.net 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
# ** uy. refresh/retry/expire: 10800 3600 432000 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=5(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
uy 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
# ** seciu.uy. refresh/retry/expire:    **
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
seciu.uy 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** com.uy. refresh/retry/expire: 10800 1800 604800 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=7(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
com.uy 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
# ** edu.uy. refresh/retry/expire: 10800 3600 432000 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=5(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
edu.uy 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
# ** gub.uy. refresh/retry/expire: 10800 3600 432000 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=5(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
gub.uy 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
```

```
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
edu.sv 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** gob.sv. refresh/retry/expire:    **
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
gob.sv 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** org.sv. refresh/retry/expire:    **
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
org.sv 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** red.sv. refresh/retry/expire:    **
# Zone does not exist.  Picking SOA numbers
#Estimated DNSSEC Parameters
# RRSIG validity 40(days)
# New keybundle every 10(days)
# ZSK roll every 120(days)
# SOAexp=30(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
red.sv 20120121000000 47304000 none none RSASHA256 86400 3456000 864000 10368000
#
# ** bnonline.fi.cr. refresh/retry/expire: 900 600 86400 **
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
# New keybundle every 10(days)
# ZSK roll every 91(days)
# SOAexp=1(days) maxttl=86400
# DN START PERIOD KSK STARTING-ZSK ALG DNSKEY-TTL VALIDITY STEP ZSK-ROLL-PERIOD
bnonline.fi.cr 20120121000000 47304000 none none RSASHA256 86400 1468800 864000 7884000
#
#Estimated DNSSEC Parameters
# RRSIG validity 17(days)
```

```
#
#
export PATH=/opt/dccom:$PATH
cp -p /opt/dnssec/aep.hsmconfig .
#TEST export PATH=opt/dccom:$PATH
#TEST cp -p ~/dnssec/msigner/bill/km/makeksr/aep.hsmconfig .
khsmconfigfile="aep.hsmconfig"
kslot="1"
zhsmconfigfile="aep.hsmconfig"
zslot="0"
#
now=`date -u +%Y%m%d%H%M%S`
#
# Gather ALL .hsm files ever created onto HSMFD
#
# Determine next free sequential ZSK cka_label
lastzsklabel=`cat zsk*.hsm | grep ^label:Z | sort -u | tail -1`
zcnt=`echo $lastzsklabel | cut -f2 -dZ`
zcnt=$(( $zcnt + 1 ))
echo "$zcnt" > nextzcnt
# for km_one_dn_zsk_roll
echo "Z$zcnt:aep.hsmconfig:0" > nextzsk
echo "Next free ZSK CKA_LABEL Z$zcnt"
#
# Determine next free sequential KSK cka_label
lastksklabel=`cat ksk*.hsm | grep ^label:K | sort -u | tail -1`
kcnt=`echo $lastksklabel | cut -f2 -dK`
kcnt=$(( $kcnt + 1 ))
echo "$kcnt" > nextkcnt
echo "Next free KSK CKA_LABEL K$kcnt"
#
################################################################
#
#
# Pre-determine parameters and starting ksk and zsk if existing domain
dn="hn"
tstart="20120131000000"
tperiod="47304000"
ksk="K200025"
zsk="Z200097"
algorithm="RSASHA256"
ttl=86400
validity=2160000
step=864000
zroll=7884000
#
while [ "1" ]; do
  read dn tstart tperiod kskhsmslot zskhsmslot algorithm ttl validity step zroll
  if [ $? -ne 0 ]; then exit 0; fi
  rs=`echo $dn | grep ^#`
  if [ "$rs" ]; then continue; fi
  #
  echo "Doing $dn ************************************************"
#  khsmconfigfile="aep.hsmconfig"
#  kslot="1"
  if [ "$kskhsmslot" = "none" ]; then
    ksk=""
  else
    ksk=`echo "$kskhsmslot" | cut -f1 -d':'`
    kskhsmslot="$ksk:$khsmconfigfile:$kslot"
  fi
  kpin="123456"
  kskhsmfile="ksk.$dn.$now.hsm"
```

```
      fi
      exkey $zsk < $frs | pkcs11-backup -P $zpin -h $zhsmconfigfile -S $zslot
      echo ""
    fi
  fi
  #
  # Pre-generate the ZSKs that km_one_dn_zsk_roll will need using same steps
  #  Note: will go away with new km_one_dn_zsk_roll which will itself gen ZSKs
  echo "Generate new ZSKs for $dn"
  tinc="$tstart"
  tend=`addsecs2date $tstart $tperiod`
  rm -f delzsks
  if [ "$zsk" ]; then
    echo "$zsk " > delzsks
    oldzsk="true"
  fi
  while [ $tinc -lt $tend ]; do
    troll="$zroll"
    zcnt=`cat nextzcnt`
    tzsk="Z$zcnt"
    pkcs11-backup -P $zpin -h $zhsmconfigfile -S $zslot -grsa:1024:$tzsk
    pkcs11-backup -P $zpin -h $zhsmconfigfile -S $zslot -p$tzsk >> $zskhsmfile
    echo ""
    echo "$tzsk " >> delzsks
    zcnt=$(( $zcnt + 1 ))
    echo "$zcnt" > nextzcnt
    if [ "$oldzsk" ]; then
      ttperiod="$validity"
      tinc=`addsecs2date $tinc $ttperiod`
      troll=$(( $troll - $ttperiod ))
      tinc=`addsecs2date $tinc $ttperiod`
      troll=$(( $troll - $ttperiod ))
    fi
    tinc=`addsecs2date $tinc $troll`
    oldzsk="true"
  done
  #
  # Generate KSK signed DNSKEY RRsets
  echo "Generating KSK signed DNSKEY RRsets"
  km_one_dn_zsk_roll $dn $tstart $tperiod $kskhsmslot $zskhsmslot $algorithm $ttl
$validity $step $zroll
  #TEST ./km_one_dn_zsk_roll_x $dn $tstart $tperiod $kskhsmslot $zskhsmslot
$algorithm $ttl $validity $step $zroll
  echo ""
  #
  echo "Deleting ZSKs from HSM"
  lst=`cat delzsks`
  for i in $lst; do
    pkcs11-backup -P $zpin -h $zhsmconfigfile -S $zslot -d$i
    echo ""
  done
  echo "Deleting KSK from HSM"
  pkcs11-backup -P $kpin -h $khsmconfigfile -S $kslot -d$ksk
  echo ""
  #
  #
done
#
# End
#
```

```
kl="label:$1"
while [ "1" ]; do
  read line
  if [ $? -ne 0 ]; then exit 0; fi
  if [ "$gg" ]; then
    echo $line
    if [ -z "$line" ]; then
      echo ""
      gg=""
    fi
  else
    if [ "$line" = "$kl" ]; then
      echo "$line"
      gg="true"
    fi
  fi
done
```