ABC DNSSEC Key Ceremony Scripts

Abbreviations

KMF= Key Management Facility
TEB = Tamper Evident Bag (large AMPAC stock #GCS1216 large, #GCS1013 small)
HSM = Hardware Security Module
FD = Flash Drive
SO = Security Officer
SA = System Administrator
SC = Safe Controller
IW= Internal Witness
EW= External Witness
MC= Master of Ceremonies

Participants

Instructions: At the end of the ceremony, participants print name, citizenship, signature, date, time, and time zone on SO's copy.

Title	Printed Name	Signature	Date	Time
Sample	Bert Smith	*Bert Smith*	12 Jul 2010	18:00 UTC
SA				
SO				
SC				
IW				
MC				
EW1				
EW2				
EW3				

Participants Arrive

Step	Activity	Initial	Time
1	SA escorts SO, SC, IW and other authorized personnel into the KMF after starting cameras.		

Sign into KMF

Step	Activity	Initial	Time
2	SA has all participants sign into the KMF log.		

Emergency Evacuation Procedures

Step	Activity	Initial	Time
3	SA reviews emergency evacuation procedures with participants.		

Verify Time and Date

Step	Activity	Initial	Time
4	IW enters date (month/day/year), UTC time using a reasonably accurate wall clock visible to all here: Date (UTC): _____Time (UTC): _____ All entries into this script or any logs should follow this common source of time.		

Open KMF Safe

Step	Activity	Initial	Time
5	SC, while shielding combination from camera, opens KMF Safe.		
6	SC takes out safe log and prints name, date, time, signature, and reason (i.e. “open safe”) in safe log. IW initials this entry.		

Remove Equipment from KMF Safe

Step	Activity	Initial	Time
7	SO removes blank smartcards (in TEB) from the safe and completes the next entry in the safe log indicating removal with “Blank Smartcard Removal,” TEB #, printed name, date, time, and signature. IW initials this entry.		
8	SA removes card reader (in TEB) from the safe and completes the next entry in the safe log indicating removal with “Card Reader Removal,” TEB #, printed name, date, time, and signature. SA places the item on KMF table. IW initials this entry.		
9	SA takes out the TEB with the O/S DVD from the safe and completes the next entry in the safe log indicating its removal with “DVD Removal,” TEB #, printed name, date, time, and signature. SA places the item on KMF table. IW initials this entry.		

Step	Activity	Initial	Time
10	SA takes out the TEB with blank, labeled (HSMFD), flash drives from the safe and completes the next entry in the safe log indicating its removal with "HSMFD Removal." TEB #, printed name, date, time, and signature. SA places the item on KMF table. IW initials this entry.		
11	SA takes out the TEB with laptop from the safe and completes the next entry in the safe log indicating its removal with "Laptop Removal," TEB #, printed name, date, time, and signature. SA places item on KMF table. IW initials this entry.		
12	SA removes any power supply units, cables and other equipment necessary from safe and places them on KMF table.		

Close KMF Safe

Step	Activity	Initial	Time
13	SC makes an entry including printed name, date, time and signature into the safe log indicating closing of the safe. IW initials this entry.		
14	SC places safe log back in safe and closes and locks safe.		
15	SO and SA verify that the safe is locked.		

Set Up Laptop

Step	Activity	Initial	Time
16	SA inspects the O/S DVD TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB# BB21876861		
17	SA inspects the laptop TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB# BB24708206		
18	SA takes O/S DVD and laptop out of TEBs placing them on KMF table; discards TEBs; connects laptop power, external display and (if used) printer and boots laptop from DVD.		
19	SA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.		
20	SA enters the commands **`system-config-display --noui`** and **`killall Xorg`** SA ensures that external display works.		
21	SA logs in as root / dnssec		
22	SA configures printer as default and prints test page.		
23	SA opens a terminal window and maximizes its size for visibility. (CTRL++)		
24	SA opens a second window and executes **`sha256sum /dev/cdrom`** To verify the authenticity of the DVD. The SA may continue with other elements while this computation is taking place by returning to the first window. The sha256 hash for caribnog.iso should be: 4bfc9b62688743dced5797d6dfea91bf6acbc765d2e0f2977b21a17cf025aeb5		
25	SA verifies the time zone, date, and time on the laptop and synchronizes it if		

Step	Activity	Initial	Time
	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		
26	SA inspects the HSMFD TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB# BB21876859		
27	SA takes HSMFDs out of TEB; discards TEB; and plugs it into free USB slot. Note:If only unprepared FDs are available, the SA may follow the following steps to format and label: a) Plug FD in b) Unmount FD if auto mounted by O/S c) determine device name using dmesg (should be /dev/sdb1) d) execute mkfs.vfat –n HSMFD /dev/sdb1 e) remove FD f) re-insert FD and wait for O/S to recognize as above The O/S should recognize the FD as /media/HSMFD If the FD is not recognized, SA mounts the HSMFD using: **`mkdir /media/HSMFD`** **`mount /dev/sda1 /media/HSMFD`** Where /dev/sda1 should be the FD in dmesg output. Then displays contents to participants using ls –lt /media/HSMFD		

Start Logging Terminal Session

Step	Activity	Initial	Time
28	SA executes **`script /media/HSMFD/script-20130321.log`** to start a capture of terminal output.		

Connecting Card Reader

Step	Activity	Initial	Time
29	SA inspects the card reader TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB# BB21876858		
30	SA removes reader from TEB; discards TEB; and connects smartcard reader to free USB slot on laptop.		

Initializing Smartcards

Step	Activity	Initial	Time

Step	Activity	Initial	Time
31	SO inspects the TEB of smartcards for tamper evidence; reads out TEB # while SA matches it with a prior script entry. TEB# BB21876860 and removes smartcards from TEB and discards TEB.		
32	SO takes a new smartcard and plugs it into card reader. Light on reader should flash.		
33	SO initializes the smartcard by running carderase SO enters new 8 digit long PIN (say 12345678) while shielding from camera. If reusing a previously initialized card, you may be asked for "Security Officer PIN". Respond with PIN used previously for this card. Note: For our configuration, PIN, PUK, and SO PIN are made equal.		
34	SO executes cardshow to display contents of card. There should be entries for "Security Officer PIN" and "Card Auth"		

Start Hardware Random Number Generator (RNG)

Step	Activity	Initial	Time
35	SA starts RNG by opening a new terminal window and executing cardrng SO enters PIN when requested.		
36	SA tests RNG by returning to the script window and executing rngtest < /dev/random waiting at least 10 seconds; then hitting CTRL-C. The number of successful tests should greatly exceed any failures, if any. During the test, the RNG window should be displaying dots indicating the feeding of random numbers into the kernel.		

Generate New ZSKs

Step	Activity	Initial	Time
37	To generate ZSK in ram disk, SA runs **export DOMAIN=tn** **genzsk** and enters password to protect private half of ZSKs. Note that cardrng window should show "…" indicating activity. The list of generated key file names can be found in genzsk.out. The public ZSKs end in .key. The corresponding encrypted private halves end in .private.aes256. SA may display directory contents using ls -lt		

Generate a New KSK and put on Smartcards

Step	Activity	Initial	Time
38	To generate KSK in ram disk, SA runs **genksk**		

Step	Activity	Initial	Time
	and enters "temp" as filename.		
39	SA puts stationery into printer and runs **`enscript --copies=N [-p out.ps] temp.out`** and hands printouts to participants. "N" is the number of copies.		
40	SA reads out the displayed public key hash from terminal while participants match this to the printouts to ensure what is displayed is properly captured in the printouts that participants will take with them to verify and attest that the KSK generated in this ceremony is the one deployed in the DNS.		
41	SA asks "does anyone object"?		
42	IW attached a printout to his/her script.		
43	SA stops RNG by going to RNG terminal window and hitting CTRL-C then entering "exit".		
44	SO runs **`cardwrite`** and enters "temp" for KSK file, Ktn20130422 for CKA_LABEL followed by PIN when prompted to write the new KSK to smartcard.		
45	SO then executes cardshow To verify contents of card to see private and public keys labeled Ktn20130422. SO removes card labeling it with Ktn20130422, date, and "KSK 1 of 3". SO then writes same information along with printed name and signature on a new TEB and places card in TEB and seals it. Finally, the SO writes TEB#, and CKA_LABEL here: Description: KSK 1 of 3 TEB# _____ CKA_LABEL Ktn20130422 IW initials TEB.		
46	SO takes a new smartcard and plugs it into card reader. Light on reader should flash.		
47	SO initializes the smartcard by running carderase SO enters same PIN above while shielding from camera.		
48	SO runs **`cardwrite`** and enters "temp" for KSK file, Ktn20130422 for CKA_LABEL followed by PIN when prompted to write the new KSK to smartcard.		
49	SO then executes cardshow To verify contents of card to see private and public keys labeled Ktn20130422. SO removes card labeling it with Ktn20130422, date, and "KSK 2 of 3". SO then writes same information along with printed name and signature on a new TEB and places card in TEB and seals it. Finally, the SO writes TEB#, and CKA_LABEL here: Description: KSK 2 of 3		

Step	Activity	Initial	Time
	TEB# _____ CKA_LABEL Ktn20130422 IW initials TEB.		
50	SO takes a new smartcard and plugs it into card reader. Light on reader should flash.		
51	SO initializes the smartcard by running carderase SO enters same PIN above while shielding from camera.		
52	SO runs **cardwrite** and enters "temp" for KSK file, Ktn20130422 for CKA_LABEL followed by PIN when prompted to write the new KSK to smartcard.		
53	SO then executes cardshow To verify contents of card to see private and public keys labeled Ktn20130422. SO removes card labeling it with Ktn20130422, date, and "KSK 3 of 3". SO then writes same information along with printed name and signature on a new TEB and leaves it on the table for later use. Finally, the SO writes TEB#, and CKA_LABEL here: Description: KSK 3 of 3 TEB# _____ CKA_LABEL Ktn20130422		

Delete Private Key File

Step	Activity	Initial	Time
54	SA deletes private key file from ram disk* by running **shred -u temp** *Note: due to the underlying automated management techniques, deletion cannot be guaranteed if on flash media		

- KSK Generation Complete -

- DNSKEY RRset Signing -

Signing DNSKEY RRsets with KSK

Step	Activity	Initial	Time
55	SO inserts smartcard KSK 3 of 3 from above in reader and runs **cardsign** Enter a passphrasewhen prompted to do so. CKA_LABEL is the value used above or Ktn20130422 When asked for PIN, SO enters it while hiding it from cameras.		

Step	Activity	Initial	Time
	This will generate KSK signed DNSKEY RRsets an corresponding ZSKs in passphrase encrypted files.		
58	SO removes smartcard from reader and places card in "KSK 3 of 3" TEB created for it above and seals it. IW initials TEB.		
59	SA runs **`tar zcf /media/HSMFD/kc20130321.tar.gz .`** to archive all results and ZSK+DNSKEY RRsets destined for signer and DS records for parent zone.		

- DNSKEY RRset Signing Complete -

For Demonstration Only

Step	Activity	Initial	Time
XX	SA executes signzone Enter passphrase used to encrypt ZSKs from above when asked. This will create a test zone, add DNSKEY RRset, decrypt ZSKs above; start a local DNSSEC enabled nameserver; and show output from "dig +dnssec –t DNSKEY tn @127.0.0.1" asking for DNSKEY RRset. SA may qury other RRset as well.		

Stop Logging Terminal Output

Step	Activity	Initial	Time
60	SA stops logging terminal output by entering "exit" in terminal window		

Backup HSM FD Contents

Step	Activity	Initial	Time
61	SA displays contents of HSMFD by executing **`ls –lt /media/HSMFD`**		
62	SA plugs a blank HSMFD into the laptop, then waits for it to be recognized by the O/S as /media/HSMFD_ and copies the contents of the original HSMFD to the blank drive for backup by executing **`cp -Rp /media/HSMFD/* /media/HSMFD_`** Note:If only unprepared FDs are available, the SA may follow the following steps to format and label: g) Plug FD in h) Unmount FD if auto mounted by O/S i) determine device name using dmesg (should be /dev/sdb1) j) execute mkfs.vfat –n HSMFD /dev/sdb1 k) remove FD l) re-insert FD and wait for O/S to recognize as above		
63	SA displays contents of HSMFD_ by executing **`ls –lt /media/HSMFD_`**		

Step	Activity	Initial	Time
64	SA unmounts new HSMFD using **`umount /media/HSMFD_`**		
65	SA removes HSMFD_ and places on table.		
66	SA repeats steps above and creates 4 more copies.		

Returning HSMFD to a TEB

Step	Activity	Initial	Time
67	SA unmounts HSMFD by executing **`umount /media/HSMFD`**		
68	SA removes HSMFD and places it in new TEB and seals; reads out TEB #; shows item to participants and IW records TEB # here TEB # _____ and places it on KMF table.		

Returning O/S DVD to a TEB

Step	Activity	Initial	Time
69	After all print jobs are complete, SA executes **`shutdown –hP now`** removes DVD and turns off laptop.		
70	SA places DVDs in new TEB and seals; reads out TEB #; shows item to participants and IW records TEB # here. TEB# _____ and places it on KMF table.		

Returning Laptop to a TEB

Step	Activity	Initial	Time
71	SA disconnects card reader, printer, display, power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants and IW records TEB # here. TEB# _____ and places it on KMF table.		

Returning Card Reader to a TEB

Step	Activity	Initial	Time
72	SA places card reader in new TEB and seals; reads out TEB #; shows item to participants and IW records TEB # here. TEB# _____ and places it on KMF table.		

Returning Equipment in TEBs to KMF Safe

Step	Activity	Initial	Time
73	SC opens safe shielding combination from camera.		

Step	Activity	Initial	Time
74	SC removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW initials the entry.		
75	SO records return of KSK 3 of 3 in next entry field of safe log with TEB #, printed name, date, time, and signature. Places item in safe. IW initials the entry.		
76	SO records return of KSK 2 of 3 in next entry field of safe log with TEB #, printed name, date, time, and signature. Places item in safe. IW initials the entry.		
77	SO records return of KSK 1 of 3 in next entry field of safe log with TEB #, printed name, date, time, and signature. Places item in safe. IW initials the entry.		
78	SA records return of card reader in next entry field of safe log with TEB #, printed name, date, time, and signature; places the card reader into safe and IW initials the entry.		
79	SA records return of laptop in next entry field of safe log with TEB #, printed name, date, time, and signature; places the laptop into safe and IW initials the entry.		
80	SA records return of HSMFD in next entry field of safe log with TEB #, printed name, date, time, and signature; places the HSMFD into safe and IW initials the entry.		
81	SA records return of O/S DVD in next entry field of safe log with TEB #, printed name, date, time, and signature; places the O/S DVD into safe and IW initials the entry.		
82	SA returns remaining power supplies, adaptors, and cables to safe. No entry in log is necessary.		

Closing KMF Safe

Step	Activity	Initial	Time
83	SC makes an entry including printed name, date, time, signature and notes closing safe into the safe log. IW initials the entry.		
84	SC places log back in safe and locks safe.		
85	SO and SA verify safe is locked.		

Participant Signing of IW's Script

Step	Activity	Initial	Time
86	All EWs enter printed name, date, time, and signature on IW's script coversheet.		
87	SA, SC, SO review IW's script and signs it.		

Signing out of Ceremony Room

Step	Activity	Initial	Time
88	SA ensures that all participants sign out of KMF (except IW who must remain) sign-in log and are escorted out of the KMF.		

Filming Stops

Step	Activity	Initial	Time
89	SA stops filming.		

Copying and Storing the Script

Step	Activity	Initial	Time
90	IW makes at least 5 copies of his or her script: one for off-site audit bundle, one for on-site audit bundle, one for IW, and copies for other participants, as requested. Audit bundles each contain 1) output of signer system - HSMFD; 2) copy of IW's key ceremony script; 3) audio-visual recording; 4) SA attestation (A.2 below); and 5) the IW attestation (A.1 below) - all in a TEB labeled "Key Ceremony", dated and signed by IW and SA. One bundle will be stored by the SA at the KMF – typically in the same area as the safe. The second bundle will be kept securely by the IW at a bank safe deposit box.		

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

Appendix A.1:

Key Ceremony Script

(by IW)

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: _____

Signature: _____

Date: _____

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: _____

Signature: _____

Date: _____

This bag uses a custom, tamper-evident sealing tape. Evidence of tampering may include:

STOP

- ✓ Appearance of the word "VOID" in the tape
- ✓ Appearance of dark red in the heat indicator strip
- ✓ Stretching or distortion of the tape or any pre-printed area of the bag or seals

STOP

IF THERE IS ANY EVIDENCE OF TAMPERING, DO NOT OPEN BAG. CONTACT SENDER IMMEDIATELY

AA 138807

FROM:

Customer Name/Account Number: Kathi Wilson

Store Location/Number:

Date: 16 JUNE 2010

DEPOSIT SAID TO CONTAIN:

Cash: KSK20120612

Coin (limit $10.00):

Checks:

Other:

TOTAL DEPOSIT: KSK 2 of 3

Number of One Hundred Bills:

Signature: KW

TO:

INSTRUCTIONS

1. Complete all information using a ball point pen. Tear off receipt at bottom of bag and retain for your records

Amount $

Date

2. Insert deposit into pouch

3. Remove release liner to expose adhesive area

4. Press blue tape onto white stripe to seal

class A

DIEBOLD

07-11

TO REMOVE CONTENTS - CUT ALONG DASHED LINE

TEAR OFF RECEIPT

DATE: 16 JUNE 2010

TOTAL DEPOSIT $ KSK 2 of 3

PREPARED BY: KW

VERIFIED BY:

AA 138807 TEAR OFF RECEIPT

DO NOT CUT HERE TO OPEN DIEBOLD

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

ABC DNSSEC Script Exception

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
SO = Security Officer
IW = Internal Witness
EW= External Witness
SA = System Administrator
SC = Safe Controller

Instructions: Initial each step that has been completed below, e.g., *BTS*. Note time.

Note Exception Time

Step	Activity	Initial	Time
1	IW notes date and time of key ceremony exception and signs here: _____		
2	IW Describes exception and action below		

– End of DNSSEC Script Exception –

ABC DNSSEC Script Exception

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
SO = Security Officer
IW = Internal Witness
EW= External Witness
SA = System Administrator
SC = Safe Controller

Instructions: Initial each step that has been completed below, e.g., *BTS*. Note time.

Note Exception Time

Step	Activity	Initial	Time
1	IW notes date and time of key ceremony exception and signs here: _____		
2	IW Describes exception and action below		

– End of DNSSEC Script Exception –

ABC DNSSEC Script Exception

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
SO = Security Officer
IW = Internal Witness
EW= External Witness
SA = System Administrator
SC = Safe Controller

Instructions: Initial each step that has been completed below, e.g., *BTS*. Note time.

Note Exception Time

Step	Activity	Initial	Time
1	IW notes date and time of key ceremony exception and signs here: _____		
2	IW Describes exception and action below		

– End of DNSSEC Script Exception –

ABC DNSSEC Acceptance Ceremony Scripts

Abbreviations

KMF= Key Management Facility
TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
SO = Security Officer
IW = Internal Witness
SA = System Administrator
SC = Safe Security Controller
EW= External Witness

Participants

Title	Printed Name	Signature	Date	Time
Sample	Bert Smith /US	Bert Smith	16 Jun 2010	18:00 UTC
SA	Rick Jones	[illegible]	13 Mar 2013	9:20 UTC
SO	SARA Security	SARA Security	13 MAR 2013	9:21
SC	Bill Crocker	Bill Crocker	13 Mar 2013	9:25
IW	Frank T. Worthy	Frank Worthy	13 Mar	9:28
EW1	Zed Mang	Zed Mang	13 Mar	9:30
EW2				
EW3				

FWO

Participants Arrive

Step	Activity	Initial	Time
1	SA escorts SC, SO, IW and other authorized personnel into the KMF after starting cameras.	Stw	7:55

Sign into KMF

Step	Activity	Initial	Time
2	SA has all participants sign into the KMF sign-in log.	Stw	8:02

Emergency Evacuation Procedures

Step	Activity	Initial	Time
3	SA reviews emergency evacuation procedures with participants.	Stw	8:04

Verify Time and Date

Step	Activity	Initial	Time
4	IW enters date (month/day/year), UTC time using a reasonably accurate wall clock visible to all here: Date (UTC): 13MAR2013 Time (UTC): 8:06 All entries into this script or any logs should follow this common source of time.	Stw	8:06

- Safe Bootstrap -

Setting Combination

Step	Activity	Initial	Time
5	SC opens already unlocked safe.	Stw	8:07
6	SC sets the new safe combination.	Stw	8:12

Test Combination

Step	Activity	Initial	Time
7	SC closes and locks the safe.	Stw	8:16
8	SC dials in the new combination (shielded from the camera)	Stw	8:17
9	SC updates the safe log with description, e.g., "Safe Combination Changed", printed name, date, time, and signature and repeats on IW's script here: Description: Safe Combination Changed Name Bill Cracker Signature Bill Cracker IW initials safe log and this entry. SC must privately relay the new combination to his/her backup.	Stw	8:20
10	SC places log back in safe and closes and locks safe. SO and SA verify safe is	Stw	8:22

ftw (B)

Step	Activity	Initial	Time
	locked.		

DVD - Verify Chain of Custody

Step	Activity	Initial	Time
11	SA asks another participant to compute the SHA256 hash for the O/S DVD using their laptop and compares to that provided and published by ABC for the O/S DVD. The following command may be used: **`openssl dgst -sha256 /dev/sdc0`** where /dev/scd0 refers to the raw DVD drive. If they do not match, terminate ceremony. Otherwise remove DVD from laptop and place on table.	ftw	8:25
12	SA repeats above for a second O/S DVD.	ftw	8:28

Laptop - Verify Chain of Custody

Step	Activity	Initial	Time
13	SA unpacks laptop while inspecting for tampered packaging and matching any packing slips with contents. Note: these laptops should not have internal disk drive storage or battery. Remove such storage or battery if they do.	ftw	8:30
14	SA boots up laptop with one of the O/S DVDs; plugs in displays and printer to check that all work. SA labels laptop with marker as **laptop #1**.	ftw	8:39
15	SA powers down and removes DVD. SA then places only laptop in TEB labeled with description, date, and SA and IW initials. IW records TEB# and clearly identifiable serial number if available here. Power supplies and other cables may remain outside: TEB# BB24708206 Serial # 425844 9621	ftw	8:43
16	SA places both O/S DVDs in TEB labeled with description, date, SA and IW initials. IW records TEB# here: TEB# BB 21876861	ftw	8:45

Smartcards - Verify Chain of Custody

Step	Activity	Initial	Time
17	SO unpacks blank smartcards while inspecting for tampered packaging and matching any documentation with contents.	ftw	8:49
18	SO places smartcards in a new TEB; labels and seals TEB with description, date, SO and IW initials. IW records TEB# here: TEB# BB21876860	ftw	8:50

Smartcard Reader - Verify Chain of Custody

Step	Activity	Initial	Time
19	SA unpacks card reader while inspecting for tampered packaging and matching any documentation with contents.	ftw	8:52

Attach (4)

Step	Activity	Initial	Time
20	SA places reader in a new TEB; labels and seals TEB with description, date, SA and IW initials. IW records TEB# here: TEB# BB21876858	Atw	8:53

Flash Drives

Step	Activity	Initial	Time
21	SA unpacks blank flash drives to be used for HSMFDs while inspecting for tampered packaging and matching any documentation with contents.	Atw	8:57
22	SA places HSMFDs in a new TEB; labels and seals TEB with description, date, initials. TEB is initialed by IW. IW records TEB# here: TEB# BB21876859	Atw	9:00

Placing Equipment in Safe

Step	Activity	Initial	Time
23	SC opens Safe shielding combination from camera.	Atw	9:08
24	SC removes the safe log and fills the next entry with printed date, time, name, and signature indicating the opening of the safe. IW initials the entry.	Atw	9:08
25	SA records placement of laptop #1 in next entry field of safe log with TEB #, printed date, time, name, and signature; places laptop #1 into Safe and IW initials the entry.	Atw	9:10
26	SA records placement of O/S DVDs in next entry field of safe log with TEB #, printed date, time, name, and signature; places O/S DVDs into Safe and IW initials the entry.	Atw	9:10
27	SA records placement of HSMFDs in next entry field of safe log with TEB #, printed date, time, name, and signature; places HSMFDs into Safe and IW initials the entry.	Atw	9:12
28	SO records placement of smartcards in next entry field of safe log with TEB #, printed date, time, name, and signature; places smartcards into Safe and IW initials the entry.	Atw	9:14
29	SA records placement of card reader in next entry field of safe log with TEB #, printed date, time, name, and signature; places card reader into Safe and IW initials the entry.	Atw	9:15
30	SA places remaining cables, adapters, power supplies inside safe. No log entry needed.	Atw	9:15

Closing Safe

ftw (5)

Step	Activity	Initial	Time
31	SC makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW initials the entry.	ftw	9:18
32	SC places log back in safe and locks Safe.	ftw	9:18
33	SA and SO verify safe is locked.	ftw	9:20

Participant Signing of IW's Script

Step	Activity	Initial	Time
34	All EWs enter printed name, date, time, and signature on IW's script coversheet.	ftw	9:23
35	SA, SO, SC review IW's script and sign it.	ftw	9:33

Filming Stops

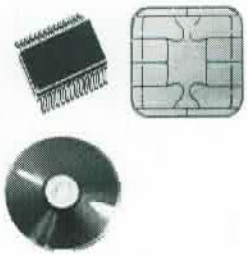
Step	Activity	Initial	Time
36	SA stops filming and makes 2 copies of film, one for on-site and one for off-site storage along with IW script copies made below.	ftw	9:58

Copying and Storing the Script

Step	Activity	Initial	Time
37	IW makes at least 5 copies of his or her script: one for off-site audit bundle, one for on-site audit bundle, one for IW, and copies for other participants, as requested. Audit bundles each contain 1) copy of IW's acceptance script; 2) audio-visual recording; 3) SA attestation (A.2 below); and 4) the IW attestation (A.1 below) - all in a TEB labeled "Acceptance Ceremony", dated and signed by IW and SA. One bundle will be stored by the SA at the KMF – typically in the same area as the safe. The second bundle will be kept securely by the IW at a bank safe deposit box.	ftw	10:10

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

PKCS11 Smart Card and TPM DNSSEC Demo Training Material



Richard Lamb 20120927

We have 5 demo examples:

- Offline Smart Card KSK + Online software ZSKs
- Offline HSM KSK + Online software ZSKs using fake HSM
- Offline Smart Card KSK + Online Smart Card ZSKs
- Online Smart Card KSK + ZSKs + BIND 9.9 in-line signing
- Online TPM KSK + ZSKs + BIND 9.9 in-line signing

Note: The PKCS11 standard allows for a simplified upgrade path to HSMs. Smartcards and TPMs do on the order of 1 1024 RSA signature per second while an HSM can do greater than 1000/s. Although key backup and inialization strategies vary across devices, the C_Sign function call to generate RSA signatures is consistent across all. The examples on the demo DVD use BIND 9.9 tools with the modification of one file - bind/lib/dns/opensslrsa_link.c - to natively support PKCS11. The modified single bind-9.9.1-P2 file and the rest of the source is on the DVD.

For smart cards:

- get a USB smartcard reader (SCR331 $15)
- get a smartcard (Aventra $11)
- boot DVD and login as root password dnssec (900M ISO file for complete bootable Smartcard and TPM DVD here sha256=4bfc9b62688743dced5797d6dfea91bf6acbc765d2e0f2977b21a17cf025aeb5)
- plug in reader and insert smartcard. (card reader light, if it has one, should blink indicating pcscd daemon has recognized the card)

Note: If not using the Aventra MyEID PKI smart card 2012, replace PKCS11_LIBRARY_PATH="/opt/dccom/lib/opensc-pkcs11.so" with different pkcs11 library in various scripts such as the ones below. I have tried Athena SCS IDProtect LASER, Feitian PKI, and a few other cards and unfortunately each card vendor have very different techniques for initializing and formatting cards so all the routines will have to be customized for each vendor. The Aventra cards are easy to purchase in small quantities. However, the smallest vendor change (e.g., ATR,..) can render the OpenSC PKCS11 driver useless (this is a case in favor of proprietary driver+card like Athena SCS). So there is no guarentee that this setup will work if any element is changed.

- carderase
- cardrng
- cardsign
- genksk-sc
- genzsk-sc
- signem-sc

Pfw
(7)

Back to order details

Date printed: Mar-30-12

Payment Summary

Status: Paid with PayPal on Mar 29, 2012.
Seller: shopmmc
Buyer: naticklamb

Shipping

Seller should ship to: **richard lamb**
88 S. Broadway
Ste 3209
millbrae CA 94030
United States

Payment

Item Name	Shipping	Qty	Price
Lot of 20 USB SCM SCR331 Common Access CAC DoD Military ID Smart Card Reader 390393507540 - Price: US $199.00	Expedited Shipping FREE USPS Priority Mail® Estimated delivery: April 2 - April 3	1	US $199.00

Subtotal:	US $199.00
Shipping & handling:	FREE
Total:	**US $199.00**

Payment details: PayPal

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

Ftr
(9)

This bag uses a custom, tamper-evident sealing tape. Evidence of tampering may include:

STOP

- ✓ Appearance of the word "VOID" in the tape
- ✓ Appearance of dark red in the heat indicator strip
- ✓ Stretching or distortion of the tape or any pre-printed area of the bag or seals

STOP

IF THERE IS ANY EVIDENCE OF TAMPERING, DO NOT OPEN BAG. CONTACT SENDER IMMEDIATELY

AA 138807

FROM:

Customer Name/Account Number: Kathi Wilson

Store Location/Number:

Date: 16 JUNE 2010

DEPOSIT SAID TO CONTAIN:

Cash: KK 20/20/12

Coin (limit $10.00):

Checks:

Other:

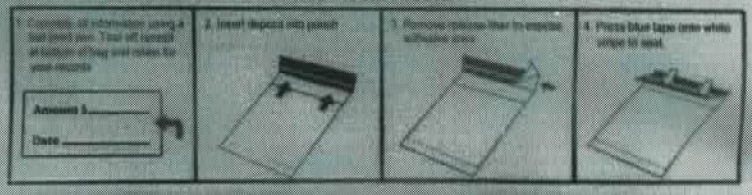
TOTAL DEPOSIT: KSK 2 of 3

Number of One Hundred Bills:

Signature: KW

TO:

INSTRUCTIONS



class A

DIEBOLD

DO NOT CUT HERE TO OPEN DIEBOLD

TO REMOVE CONTENTS - CUT ALONG DASHED LINE

TEAR OFF RECEIPT

DATE: 16 JUNE 2010

TOTAL DEPOSIT $ KSK 2 of 3

PREPARED BY: KW

VERIFIED BY:

AA 138807 TEAR OFF RECEIPT

aventra

Simply Secur

Recipient	Webshop packing list	
richard lamb 88 S BROADWAY UNIT 3209 88 S. Broadway Suite 3209 94030 millbrae United States	Packing list number	Delivery date 30.03.2012
	Order nbr 826	Order date 30.03.2012
	Customer number	Delivery method Mail
Contact person	Customer reference	
Additional information		

Product code	Description	Pcs
MYEID-25	MyEID 80k PKI card, 25 pcs	

Aventra Oy
Lanttikatu 2, 02770 ESPOO, Finland
09-4251 1251
www.aventra.fi, sales@aventra.fi

Y-tunnus: 1894068-2

ABC

ABC DNSSEC Sign in/Sign out Log

Entry #	Signature	Printed Name	Date In	Time In	Date Out	Time Out
1	Bert Smith	Bert Smith	08 Sep 2011	13:00 UTC	08 Sep 2011	18:00 UTC
2	Rick Jones	Rick Jones	13 MAR 2013	7:56	13 MAR 2013	10:20 UTC
3	[illegible]	[illegible] Secret	13 Mar	7:58	13 Mar	9:35
4	Bill Crooke	Bill Crooke	13 Mar	8:00	13 Mar	9:35
5	Frank Worthy	Frank Worthy	13 MAR	8:01	13 Mar	10:20
6	[illegible]	[illegible]	13 MAR	8:02	13 Mar	9:35
7						
8						
9						
10						
11						

ABC DNSSEC Safe Log

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
IW= Internal Witness

Entry #	Printed Name	Reason or Description	TEB # (and serial #, if applicable)	Date	Time	Signature	IW Initials
1	Bert Smith	DVD removal	A13004346	16 Jun 2010	18:00 UTC	Bert Smith	ESP
2	Bill Crocker	Safe Combo Changed	—	13 MAR 2013	8:21	[illegible]	FTW
3	Bill Crocker	open safe	—	13 Mar	9:08	[illegible]	FTW
4	Rick Powe	laptop	BB 21708206	13 Mar	9:10	[illegible]	FTW
5		OS/DVD	BB 21876861		9:11	Rick Powe	ftw
6		smart card	BB 21876860		9:14	Rick Powe	ftw
7		reader	BB 21876858		9:15	Rick Powe	ftw
8		HSM FDs IN	BB 21876859		9:12	Rick Powe	ftw
9	Bill Crocker	closing	—	13 Mar 2013	9:18	Bill Crocker	ftw