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				
SO				
SC				
IW				
EW1				
EW2				
EW3				

Participants Arrive

Step	Activity	Initial	Time
1	SA escorts SC, SO, 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 sign-in 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.		

- Safe Bootstrap -

Setting Combination

Step	Activity	Initial	Time
5	SC opens already unlocked safe.		
6	SC sets the new safe combination.		

Test Combination

Step	Activity	Initial	Time
7	SC closes and locks the safe.		
8	SC dials in the new combination (shielded from the camera)		
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 _____ Signature _____ IW initials safe log and this entry. SC must privately relay the new combination to his/her backup.		
10	SC places log back in safe and closes and locks safe. SO and SA verify safe is		

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.		
12	SA repeats above for a second O/S DVD.		

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.		
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.		
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# Serial # _____		
16	SA places both O/S DVDs in TEB labeled with description, date, SA and IW initials. IW records TEB# here: TEB#		

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.		
18	SO places smartcards in a new TEB; labels and seals TEB with description, date, SO and IW initials. IW records TEB# here: TEB#		

Smartcard Reader – Verify Chain of Custody

Step	Activity	Initial	Time
19	SA unpacks card reader while inspecting for tampered packaging and matching		

Step	Activity	Initial	Time
	any documentation with contents.		
20	SA places reader in a new TEB; labels and seals TEB with description, date, SA and IW initials. IW records TEB# here: TEB#		

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.		
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#		

Placing Equipment in Safe

Step	Activity	Initial	Time
23	SC opens Safe shielding combination from camera.		
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.		
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.		
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.		
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.		
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.		
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.		
30	SA places remaining cables, adapters, power supplies inside safe. No log entry needed.		

Closing Safe

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.		
32	SC places log back in safe and locks Safe.		
33	SA and SO verify safe is locked.		

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.		
35	SA, SO, SC review IW’s script and sign it.		

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.		

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.		

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

ri.co.cr/#schsm

PKCS11 Smart Card and TPM DNSSEC Demo Training Material

Richard Lamb 20120927 SMARTCARD HSM UPDATE Richard Lamb 20130819

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=c5045720002064a838d8597011c81c7fb9a01a1e11525d4a1201d163f3fea0f4)
- 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.

Back to order details

Payment Summary

Date printed: Mar-30-12

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

aventra

Simply Secure

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	1

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

Y-tunnus: 1894068-2

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

DO NOT CUT HERE TO OPEN DIEBOLD DO NOT CUT HERE TO OPEN DIEBOLD DO NOT CUT HERE TO OPEN DIEBOLD

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: Kathie Wilson

Store Location/Number:

DEPOSIT SAID TO CONTAIN:

Date: 16 JUNE 2010

Cash: KK20120612

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

ITEM # 0003199100XX

TEAR OFF RECEIPT

DATE: 16 JUNE 2010 PREPARED BY: KW

TOTAL DEPOSIT $ KSK 2 of 3 VERIFIED BY:

AA 138807 TEAR OFF RECEIPT 3