ABC DNSSEC Key Ceremony Scripts

Abbreviations

KMF= Key Management Facility
TEB = Tamper Evident Bag (large DIEBOLD item #00051991000C small #00051991000A)
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. 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.		
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.		

Step	Activity	Initial	Time
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#		
17	SA inspects the laptop TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB#		
18	SA takes O/S DVD and laptop out of TEBs placing them on KMF table; discards TEBs; connects laptop power, external display, printer and boots laptop from DVD.		
20	SA configures external display for participants to see.		
21	SA logs in as root		
22	SA configures printer as default and prints test page.		
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: 3c1f7-PUT-your-DVD-HASH-HERE-4324234		
25	SA 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		

Step	Activity	Initial	Time
26	SA inspects the HSMFD TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB#		
27	SA takes HSMFDs out of TEB; discards TEB; and plugs it into free USB slot. 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-20121001.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#		
30	SA removes reader from TEB; discards TEB; and connects smartcard reader to free USB slot on laptop.		

Initializing Smartcards

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# 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 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.		

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=py** **export TEST=yes** **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** 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, Kpy20121001 for CKA_LABEL, and 2 for CKA_ID followed by PIN when prompted to write the new KSK to smartcard.		
45	SO then executes		

Step	Activity	Initial	Time
	cardshow To verify contents of card to see private and public keys labeled Kpy20121001. SO removes card labeling it with Kpy20121001, 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 Kpy20121001 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, Kpy20121001 for CKA_LABEL, and 2 for CKA_ID 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 Kpy20121001. SO removes card labeling it with Kpy20121001, 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 TEB# _____ CKA_LABEL Kpy20121001 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, Kpy20121001 for CKA_LABEL, and 2 for CKA_ID 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 Kpy20121001. SO removes card labeling it with Kpy20121001, date, and "KSK 3 of 3".		

Step	Activity	Initial	Time
	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 Kpy20121001		

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 on flash media		

- KSK Generation Complete -

- DNSKEY RRset Signing -

Signing DNSKEY RRsets

Step	Activity	Initial	Time
55	SO inserts smartcard KSK 3 of 3 from above in reader and runs **`cardsign`** CKA_LABEL is the value used above or Kpy20121001 When asked for PIN, SO enters it while hiding it from cameras. This will generate KSK signed DNSKEY RRsets and ZSKs in encrypted files of the form 20121001hhmmss.py.keybundle.tar.gz.aes256 at least one ZSK rollover.		
56	SA runs **`enscript --copies=N tt.dnskeyrrset.9`** and hands printouts to participants for them to verify and attest that the ZSKs generated in this ceremony are the ones that get deployed in the DNS. DNSKEY RRset 9 will have the public keys from both what will be the current ZSK and what it will roll to at the next rollover cycle.		
57	IW attaches a printout to his/her script.		
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/kc20121001.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 This will create a test zone, add DNSKEY RRset, decrypt ZSKs above. SA may display live output from signer process using **tail –f /tmp/namedb/signemd.out** (for this demo) or **monitor** to simply view ZSK and KSK key tags using "dig".		

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: 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		
63	SA displays contents of HSMFD_ by executing **ls –lt /media/HSMFD_**		
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 #;		

Step	Activity	Initial	Time
	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.		
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		

Step	Activity	Initial	Time
	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 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		

Step	Activity	Initial	Time
	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)

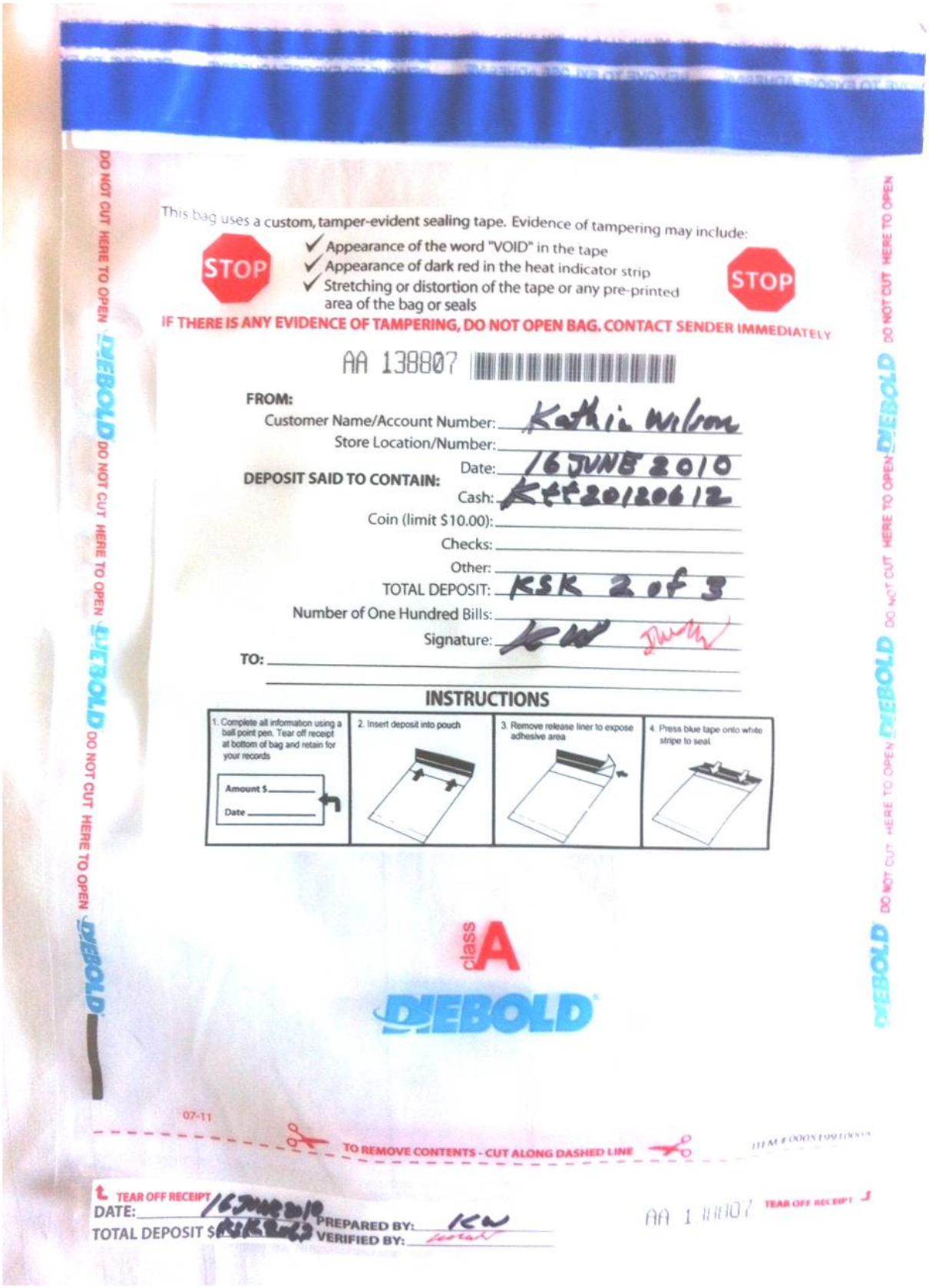
I have reviewed the physical access control system and not found any discrepancies or anything else out of the ordinary.

Enclosed is the audited physical access log.

Printed Name: _____

Signature: _____

Date: _____



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: Kathi Wilson
Store Location/Number:
Date: 16 JUNE 2010

DEPOSIT SAID TO CONTAIN:
Cash: KK 20120612
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 DO NOT CUT HERE TO OPEN DIEBOLD 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 –