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# BB 21880442		
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 and (if used) printer and boots laptop from DVD. [NOTE: The following steps may be skipped depending on facility configuration]		
19	SA logs in as root / dnssec.		
20	SA enters the command startx and ensures that external display works.		
21	SA configures printer as default and prints test page.		
22	SA opens a terminal window and maximizes its size for visibility. (CTRL++)		
23	SA opens a second window (e.g., using ALT-F2) 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 as created by the software development department should be: 27cbaeb7f0aef5b7c82360ae8a410bb0d74af2231c0462d751ee11cf8f3daa79		
24	SA verifies the time zone, date, and time on the laptop and synchronizes it if necessary. Display the current time and timezone: **date**		

Step	Activity	Initial	Time
	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 (mm=month dd=day): **date mmddHHMMYYYY** Verify: date		
25	SA inspects the HSMFD TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB# BB 501472		
26	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
27	SA executes script /media/HSMFD/script–20140424.log to start a capture of terminal output.		

Connecting Card Reader

Step	Activity	Initial	Time
28	SA inspects the card reader TEB for tamper evidence; reads out TEB # while participants match it with the prior script entry. TEB# BB 21880443		
29	SA removes reader from TEB; discards TEB; and connects smartcard reader to free USB slot on laptop or expander.		

Initializing Smartcards

Step	Activity	Initial	Time
30	SO inspects the TEB of smartcards for tamper evidence; reads out TEB # while SA matches it with a prior script entry. TEB# BB 501475 and removes smartcards from TEB and discards TEB.		
31	SO takes a new smartcard and plugs it into card reader. Light on reader should flash.		
32	SO initializes the smartcard by running hcarderase SO enters new PIN (say 123456) 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.		
33	SO begins process of making 2 of 2 keys or "shares" needed to clone the smartcard HSM to other smartcards and thus make backups. SO executes: hmakeshares When asked for a password for share 1, the SO enters a password (say password1). When asked for a password for the second share, have the SA (not SO) enter a password (say password2).		
34	SO now imports their share into the card by executing: himportshare dkek-share-1.pbe and entering their password from above.		
35	SA now imports their share into the card by executing: himportshare dkek-share-2.pbe and entering their password from above.		
36	SA now sets the domain name by typing: export DOMAIN=cr (and optionally "export TEST=yes" to generate short term signatures)		

Generate a New KSK and put on Smartcards

Step	Activity	Initial	Time
37	To generate KSK inside the card, SO runs hgenksk SO notes CKA_LABEL of the form ksk.cr.2014…		
38	SO then executes hcardshow To verify contents of card to see private key label ksk.cr.2014…. Note that for these smartcards, the public key will be stored in a file of the form ksk.cr.2014…pub		
39	The SO now exports an encrypted backup of the KSK by executing: hwrapkey and entering CKA_LABEL ksk.cr.2014… from above. This will generate a file of the form ksk.cr.2014…wrap SO may display directory contents using ls –lt		
40	SA copies permanent information to HSMFD by executing:		

Step	Activity	Initial	Time
	cp –p * /media/HSMFD/		
41	SO removes card physically labeling it with CKA_LABEL (e.g., ksk.cr.2014…) and "KSK 1 of 2". 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 2 TEB# _____ CKA_LABEL ksk.cr.2014… IW initials TEB and leaves on table.		
42	SO makes backup smartcards by inserting a new smartcard and executing: hcarderase and entering the same PIN as before (123456). SO executes: himportshare dkek-share-1.pbe entering the password entered above (e.g., password1) when prompted. The SA then executes himportshare dkek-share-2.pbe entering the password entered above (e.g., password2) when prompted. The SO executes: hunwrapkey and responds with the encrypted backup of the key (e.g., ksk.cr.201…wrap). The SO executes hcardshow to display and verify the smartcard contents. (The above steps may be repeated for additional backup cards)		

- KSK Generation Complete –

Start Hardware Random Number Generator (RNG)

Step	Activity	Initial	Time
43	SA starts RNG by opening a new terminal window and executing hcardrng SO enters PIN when requested.		
44	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
45	To generate ZSKs using the smartcard RNG, SA runs hgenzsk Note that cardrng window should show "…" indicating activity. SA may display directory contents using ls –lt		
46	SA stops RNG by going to RNG terminal window and hitting CTRL-C then entering "exit".		

- DNSKEY RRset Signing -

Signing DNSKEY RRsets with KSK

Step	Activity	Initial	Time
47	Leaving the smartcard in the reader the SA executes hcardsign and the SA enters a passphrase (say "abc") when prompted to do so. This will be used to encrypt the private ZSK material during transport to online signer. The SA enters the CKA_LABEL that resulted from KSK generation above of the form ksk.cr.2014… The SA may do a directory listing to see this again. When prompted to do so, the SO enters their PIN (e.g., 123456). This will generate KSK signed DNSKEY RRsets and corresponding ZSKs in passphrase encrypted files.		
48	Once complete SO removes card physically labeling it with CKA_LABEL (e.g., ksk.cr.2014…) and "KSK 2 of 2". 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 2 TEB# _____ CKA_LABEL ksk.cr.2014… IW initials TEB and leaves on table.		
49	SA puts stationery into printer and runs /opt/dccom/bind/bin/dnssec/dnssec-dsfromkey *.key | tee dsset-cr. and then enscript --copies=N [-p out.ps] dsset-cr. and hands printouts to participants. "N" is the number of copies.		
50	SA reads out the displayed DS record 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 that will be deployed in the DNS.		
51	SA asks "does anyone object"?		

Step	Activity	Initial	Time
	IW attached a printout to his/her script.		
52	SA runs tar --no-recursion -zcf /media/HSMFD/kc20140424.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 hsignzone and enters passphrase used to encrypt ZSKs from above (e.g., "abc") 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 cr @127.0.0.1 SA may query other RRsets as well. The SA may also run "monitor" as an example of a script monitoring time to signature expiration.		

Stop Logging Terminal Output

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

Backup HSM FD Contents

Step	Activity	Initial	Time
54	SA displays contents of HSMFD by executing **ls –lt /media/HSMFD**		
55	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		
56	SA displays contents of HSMFD_ by executing **ls –lt /media/HSMFD_**		
57	SA unmounts new HSMFD using **umount /media/HSMFD_**		
58	SA removes HSMFD_ and places on table.		
59	SA repeats steps above and creates 4 more copies.		

Returning HSMFD to a TEB

Step	Activity	Initial	Time
60	SA unmounts HSMFD by executing **`umount /media/HSMFD`**		
61	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
62	After all print jobs are complete, SA executes **`shutdown -hP now`** removes DVD and turns off laptop.		
63	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
64	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
65	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
66	SC opens safe shielding combination from camera.		
67	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.		
68	SO records return of KSK 1 of 2 in next entry field of safe log with TEB #, printed name, date, time, and signature. Places item in safe. IW initials the entry.		
69	SO records return of KSK 2 of 2 in next entry field of safe log with TEB #, printed name, date, time, and signature. Places item in safe. IW initials the entry.		

Step	Activity	Initial	Time
70	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.		
71	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.		
72	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.		
73	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.		
74	SA returns remaining power supplies, adaptors, and cables to safe. No entry in log is necessary.		

Closing KMF Safe

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

Participant Signing of IW's Script

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

Signing out of Ceremony Room

Step	Activity	Initial	Time
80	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
81	SA stops filming.		

Copying and Storing the Script

Step	Activity	Initial	Time
82	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		

Step	Activity	Initial	Time
	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)

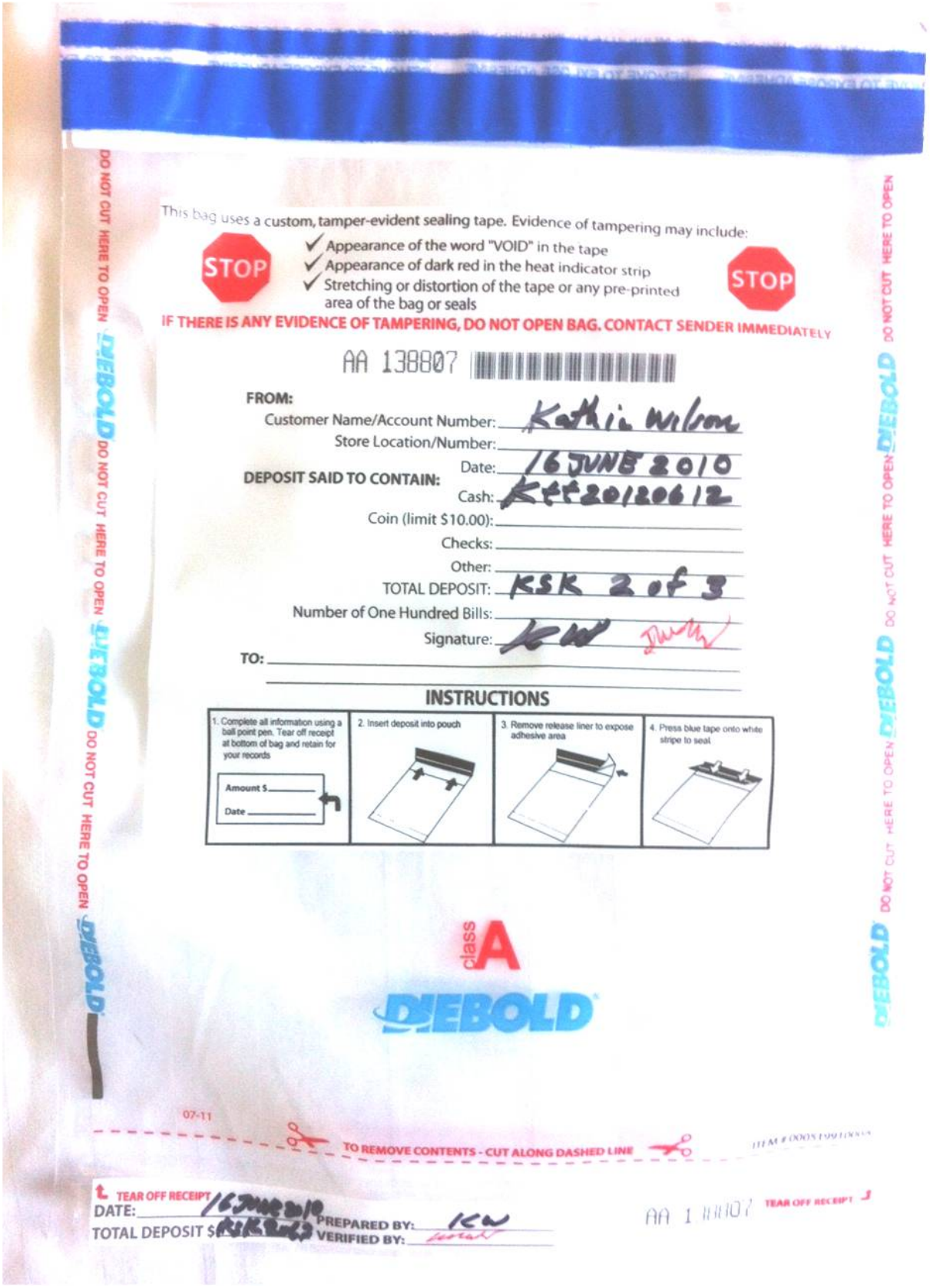
I have reviewed the physical access control system and not found any discrepancies or anything else out of the ordinary.

Enclosed is the audited physical access log.

Printed Name: _____

Signature: _____

Date: _____



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: KSK20120612

Coin (limit $10.00):

Checks:

Other:

TOTAL DEPOSIT: KSK 2 of 3

Number of One Hundred Bills:

Signature: KW

TO:

INSTRUCTIONS

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

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 –