ICANN DNSSEC Key Ceremony 7 Script

AbbreviationsDraft

TEB = Tamper Evident Bag (MMF Industries, item #2362010N20 small or #2362011N20 large)
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller
MC = Master of Ceremony
IKOS = ICANN KSK Operations Security

Participants

Instructions: At the end of the ceremony, participants print name, citizenship, signature, date, time, and time zone on IW1's copy.

Title	Printed Name/Citizenship	Signature	Date	Time
Sample	Bert Smith	*Bert Smith*	07 Feb 2011	18:00 UTC
CA	Mehmet Akcin		30 Sep 2011	
IW1	Francisco Arias		30 Sep 2011	
SA2	Alexander Kulik		30 Sep 2011	
SSC1	Julie Hedlund		30 Sep 2011	
SSC2	Patrick Jones		30 Sep 2011	
CO1	Frederico Neves /BR		30 Sep 2011	
CO2	Anne-Marie Eklund Lowinder /SE		30 Sep 2011	
CO4	Robert Seastrom /US		30 Sep 2011	
EW1	Alejandro Bolivar		30 Sep 2011	
EW2	James Adair		30 Sep 2011	
EW3	Spencer Roessner		30 Sep 2011	
EW4	Exavier Chabata		30 Sep 2011	
CA2	Joe Abley		30 Sep 2011	
IKOS/IW2	Tomofumi Okubo		30 Sep 2011	

Note: Dual Occupancy enforced. CA leads ceremony. Only CAs, IWs, or SAs can enter ceremony room and/or escort other participants. Only CA+IW can enter safe room. CAs, SAs or IWs may let individuals out of the ceremony room but only when CA+IW remain in the ceremony room. No one may leave when CA+IW are in safe room. Participants must sign in and out of ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before completion of the ceremony. The SA starts filming before the participants enter the room.

Some steps during the ceremony require the participants to tell and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the phonetic alphabet shown below will be used:

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

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initial	Time
1	SAs or IWs escort participants into the Ceremony Room and all participants sign into the Ceremony Room log.		

Emergency Evacuation Procedures

Step	Activity	Initial	Time
2	CA or IW reviews emergency evacuation procedures with participants.		

Verify Time and Date

Step	Activity	Initial	Time
3	IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room**:** Date and time: _____ All entries into this script or any logs should follow this common source of time.		

Open Credential Safe #2

Step	Activity	Initial	Time
4	CA and IW1 escort SSC2 and COs into the safe room together.		
5	SSC2, while shielding combination from camera, opens Safe #2.		
6	SSC2 takes out safe log and prints name, date, time, signature, and reason (i.e. “open safe”) in safe log. IW1 initials this entry.		

COs extract OP Cards from safe deposit boxes

Step	Activity	Initial	Time
7	One by one, the selected COs checks the SO cards and retrieves the OP cards following the steps shown below. a) With the assistance of CA (and his/her common key), opens her/his safe deposit box. b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below. c) Returns SO cards, retains OP TEB and locks box. d) Makes an entry in safe log indicating verification of integrity of contents and OP TEB removal with box #, printed name, date, time and signature. Example entry in the "reason" field: verified SO, removed OP TEBs. Repeat these steps until all cards are removed. IW1 initials this entry when all CO have finished. **CO1: Frederico Neves** **Box 1238** **OP TEB # A15473417** **SO TEB # A14377117** **CO2: Anne-Marie Eklund Lowinder** **Box 1259** **OP TEB # A14365375** **SO TEB # A14377119** **CO4: Robert Seastrom** **Box 1260** **OP TEB # A15473415** **SO TEB # A14377123**		

Close Credential Safe #2

Step	Activity	Initial	Time
8	Once all safe deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry.		
9	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions).		
10	CA and IW1 verify that the safe is locked and card reader indicator is green.		
11	IW1, CA, SSC2, and COs leave safe room, with OP cards in TEBs, closing the door behind them.		

OS/DVD Acceptance Test

Step	Activity	Initial	Time
12	CA uses general purpose laptop to compute the SHA256 hash for the O/S DVD and compares to that published by ICANN for the O/S DVD. The following command may be used: **`sudo umount /dev/scd0 (or /dev/disk2..etc)`** **`openssl dgst -sha256 /dev/scd0 (or /dev/disk2..etc)`** where /dev/scd0 refers to the raw DVD drive. If hash does not match, terminate ceremony. Otherwise remove DVD from laptop and place on table where visible from camera and participants. **SHA256 HASH for Release 600:** **7da0d1c5eecb822d7bbd47b31d25e4f0f37bb8a46cfbe288d2b07b32f5e38146**		
13	CA repeats above for a second new O/S DVD.		
14	IW records date, time and signature here upon successful completion: Date _____ Time _____ Signature _____		

Open Equipment Safe #1

Step	Activity	Initial	Time
15	CA, IW1 and SSC1 enter the safe room with an empty equipment cart.		
16	SSC1, while shielding combination from camera, opens Safe #1.		
17	SSC1 takes out safe log and prints name, date, time, signature and reason (i.e., "opened safe") in safe log. IW1 initials this entry.		

Remove Equipment from Safe #1

Step	Activity	Initial	Time
18	CA **CAREFULLY** removes HSM1 (in TEB) from the safe and completes the entry in the safe log indicating "HSM1 Removal," TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry. **HSM1: TEB# A2751142 / serial # K6002016** Verify the integrity of the other HSM that will not be in used this time. **HSM2: TEB# A2826709 / serial # K6002013 (last used)**		

Step	Activity	Initial	Time
19	CA takes out the items listed below from the safe and completes the entry in the safe log indicating each item, TEB#, serial number if available. Printed name, date, time and signature. CA places the item on the equipment cart. IW1 initials this entry. **Laptop #2: TEB# A2751140 / serial# 35063364997** **O/S DVDs (Rev 575): TEB# A14365371** **HSMFD: TEB # A14365372** Verify the integrity of the other Laptop that will not be in used this time. **Laptop #1: TEB A2826708 / serial # 41593712005 (last used)**		

Close Equipment Safe #1 and exit safe room

Step	Activity	Initial	Time
20	SSC1 makes an entry including printed name, date, time and signature into the safe log indicating, “closing of the safe”. IW1 initials this entry.		
21	SSC1 puts log back in safe and locks Safe #1 (spin dial at least two full revolutions).		
22	CA and IW1 verify that the safe is locked and door indicator light is green.		
23	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.		

Set Up Laptop

Step	Activity	Initial	Time
24	CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. **Laptop #2: TEB# A2751140 / serial# 35063364997**		
25	CA takes the laptop out of TEBs placing them on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from the tested OS/DVD (**Rev 600**) and discards old OS/DVD (Rev 575).		
26	CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.		

27	CA enters the commands
	`system-config-display --noui`
	and
	`killall Xorg`
	CA ensures that external display works.		

28	CA logs in as root.		
29	CA configures printer as default and prints test page.		

Step	Activity	Initial	Time
30	CA opens a terminal window and maximizes its size for visibility.		
31	CA checks and fixes date and time on laptop based on wall clock ensuring UTC time zone has been chosen.		
32	CA inserts USB port expander into laptop.		
33	CA inspects the HSMFD TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. **HSMFD: TEB # A14365372**		
34	CA plugs HSMFD into free USB slot on the laptop – not expander - and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes pop up FD window.		

Start Logging Terminal Session

Step	Activity	Initial	Time
35	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`		
36	CA executes `script script-20110930.log` to start a capture of terminal output.		

Start Logging HSM Output

Step	Activity	Initial	Time
37	CA connects a serial to USB null modem cable to laptop.		

38	CA opens a second terminal screen and executes
	`cd /media/HSMFD`
	and executes
	`ttyaudit /dev/ttyUSB0`
	to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.		

Power Up HSM

Step	Activity	Initial	Time
39	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM1: TEB# A2751142 / serial # K6002016**		
40	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		
41	CA connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with above. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it since the scripts that does the logging to the laptop adds a timestamp.)		

Enable/Activate HSM

Step	Activity	Initial	Time
42	CA calls the CO, CO opens TEB with OP card and hands to CA who places card in cardholder visible to all.		
43	Repeat the step above until all OP cards are placed on the cardholder.		
44	CA inserts 3 cards into HSM to activate the unit (via "Set Online" menu item). IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7		

Check Network between Laptop and HSM

Step	Activity	Initial	Time
45	CA connects HSM to laptop using Ethernet cable.		
46	CA 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. Switch back to ttyaudit screen when done.		

Insert Copy of KSR to be signed

Step	Activity	Initial	Time
47	CA plugs FD labeled "KSR" with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA points out the KSR file to be signed.		

Sign it with our KSK

Step	Activity	Initial	Time
48	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2012-q1-0.xml`		

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initial	Time
49	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to identify him/herself, present identification document for IW1 to retain and read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN. IW1 enters RZM representative's name here: _____		
50	Participants match the hash read out with that displayed on the terminal. CA asks "are there are any objections"?		
51	CA then enters "y" in response to "Is this correct y/n?" to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in `/media/KSR/skr-root-2012-q1-0.xml`		

```
$ ksrsigner Kjqmt7v ksr-root-2010-q4-1.xml

Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2010-q4-1.xml (at Mon Jul 12 22:44:26 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper Pro 0405
    Serial:          K6002018

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-07-01T00:00:00 2010-07-15T23:59:59  55138,41248   19036
2  2010-07-11T00:00:00 2010-07-25T23:59:59  41248         19036
3  2010-07-21T00:00:00 2010-08-04T23:59:59  41248         19036
4  2010-07-31T00:00:00 2010-08-14T23:59:59  41248         19036
5  2010-08-10T00:00:00 2010-08-24T23:59:59  41248         19036
6  2010-08-20T00:00:00 2010-09-03T23:59:59  41248         19036
7  2010-08-30T00:00:00 2010-09-13T23:59:59  41248         19036
8  2010-09-09T00:00:00 2010-09-24T00:00:00  41248         19036
9  2010-09-20T00:00:00 2010-10-05T23:59:59  40288,41248   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2010-q4-1.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  40288,41248
2  2010-10-11T00:00:00 2010-10-25T23:59:59  40288
3  2010-10-21T00:00:00 2010-11-04T23:59:59  40288
4  2010-10-31T00:00:00 2010-11-14T23:59:59  40288
5  2010-11-10T00:00:00 2010-11-24T23:59:59  40288
6  2010-11-20T00:00:00 2010-12-04T23:59:59  40288
7  2010-11-30T00:00:00 2010-12-14T23:59:59  40288
8  2010-12-10T00:00:00 2010-12-25T00:00:00  40288
9  2010-12-21T00:00:00 2011-01-05T23:59:59  21639,40288
...PASSED.

SHA256 hash of KSR:
A17E539793B2611112C4F591A06AF4FBC2221DDDD71794BC72D5AEE910C72543
>> ratchet insurgent dwelling mosquito playhouse pioneer fallout Babylon atlas reproduce vapor miracle
ragtime hamburger upshot Wichita snapshot candidate Belfast tambourine stopwatch bookseller Pluto
pyramid highchair specialist robust ultimate assume retraction bombast decimal <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2010-q4-1.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  40288,41248   19036
2  2010-10-11T00:00:00 2010-10-25T23:59:59  40288         19036
3  2010-10-21T00:00:00 2010-11-04T23:59:59  40288         19036
4  2010-10-31T00:00:00 2010-11-14T23:59:59  40288         19036
5  2010-11-10T00:00:00 2010-11-24T23:59:59  40288         19036
6  2010-11-20T00:00:00 2010-12-04T23:59:59  40288         19036
7  2010-11-30T00:00:00 2010-12-14T23:59:59  40288         19036
8  2010-12-10T00:00:00 2010-12-25T00:00:00  40288         19036
9  2010-12-21T00:00:00 2011-01-05T23:59:59  40288,21639   19036

SHA256 hash of SKR:
00CC341B7B3BAEE2E62B1AA6A58DEF07F02E4950E959E6A6ACBD7CEFF2741257
>> aardvark revolver choking bravado kickoff councilman robust tomorrow tracker Cherokee beehive
paragon reindeer microscope uncut amusement unearth coherence deckhand embezzle treadmill examine
tracker paragon ribcage quantity kiwi unravel uproot hydraulic atlas Eskimo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20100712-224426.log **********
```

Figure 1

Print Copies of the Operation for Participants

Step	Activity	Initial	Time
52	CA prints out a sufficient number of copies for participants using **`printlog ksrsigner-20110930-*.log N`** where ksrsigner-20110720-*.log is replaced by log output file displayed by program. (this example generates **N** copies) and hands copies to participants.		
53	IW1 attaches a copy to his/her script.		

Backup Newly Created SKR

Step	Activity	Initial	Time
54	CA copies the contents of the KSR FD by running **`cp –p /media/KSR/* .`** for posting back to RZM.		
55	CA lists contents of KSR FD which should now have an SKR by running **`ls –lt /media/KSR`** and then unmounts the KSR FD using **`umount /media/KSR`**		
56	CA removes **KSR** FD containing SKR and gives it to the RZM representative.		

Disable/Deactivate HSM

Step	Activity	Initial	Time
57	CA inserts 3 cards into HSM to deactivate the unit (via “Set Offline” menu item). IW1 records the used cards below. Each card is returned to cardholder after use. CA makes sure the card(s) NOT used to activate are used to deactivate the HSM. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7 Confirm the ready light turns off.		

Return HSM to a TEB

Step	Activity	Initial	Time
58	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.		
59	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM1: TEB# A2826751 / serial # K6002016** IW1 initials the TEB.		
60	CA places item on equipment cart.		

Stop Recording Serial Port Activity

Step	Activity	Initial	Time
61	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of serial output terminal window.		

Stop Logging Terminal Output

Step	Activity	Initial	Time
62	CA stops logging terminal output by entering “exit” in the terminal window.		

Backup HSM FD Contents (Approximately 10 minutes)

Step	Activity	Initial	Time
63	CA displays contents of HSMFD by executing **`ls -lt`**		
64	CA plugs a blank FD labeled HSMFD into the laptop, then 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_`**		
65	CA displays contents of HSMFD_ by executing **`ls -lt /media/HSMFD_`**		
66	CA unmounts new FD using **`umount /media/HSMFD_`**		
67	CA removes HSMFD_ and places on table.		
68	CA repeats steps above and creates 4 more copies.		

Print Logging Information

Step	Activity	Initial	Time

69	CA prints out hard copies of logging information by executing
	`enscript -2Gr -# 2 script-20110930.log`
	`enscript -Gr -# 2 --font="Courier8" ttyaudit-ttyUSB*-20110930-*.log`
	for attachment to IW1 and CA scripts.		

Returning HSMFD to a TEB

Step	Activity	Initial	Time
70	CA unmounts HSMFD by executing **`cd /tmp`** then **`umount /media/HSMFD`**		
71	CA removes HSMFD and places it in a new TEB; writes date, time and "HSMFD" in amount field; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **HSMFD: TEB # A14365418** IW1 initials the TEB. CA places TEB on equipment cart.		

Distribute HSMFDs

Step	Activity	Initial	Time
72	Remaining HSMFDs are distributed to IW1 (2 for audit bundles), CA (2), IKOS(1) to post SKR to RZM, and to review, analyze and improve on procedures.		

Packing O/S DVD to a TEB

Step	Activity	Initial	Time
73	After all print jobs are complete, CA executes **`shutdown -hP now`** removes DVD and turns off laptop.		
74	CA places DVDs in new TEB and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **O/S DVDs (Rev 600): TEB# A14365419** IW1 initials the TEB. CA places TEB on equipment cart.		

Returning Laptop to a TEB

Step	Activity	Initial	Time
75	CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. **Laptop #2: TEB# A2826750 / serial# 35063364997** IW1 initials the TEB. CA places TEB on equipment cart.		

Returning OP Smartcards to TEBs

Step	Activity	Initial	Time
76	CA calls each CO to the front of the room one at a time and repeats the steps below. a) CA takes a TEB prepared for the CO and reads out the number and description (e.g., "OP 2 of 7" on "amount" line) while showing the bag to IW1 and CO. Figure 2 below for an example. b) CA places OP into TEB. c) IW1 inspects then initials TEB and sealing strip (next to CA's initials). d) CA initials bag and strip, seals TEB in front of IW1 and CO then hands sealing strip to IW1. IW1 keeps sealing strips for later inventory. e) IW1 confirms TEB and description in table below. f) CA hands the TEB containing the OP card to the CO. CO inspects and verifies TEB #s and contents and enters date, time and signs for each TEB in the table below in IW1's script. CO initials his/her bag. IW1 initials table entry. CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB. IW1 initials table entry.		

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1
CO1	OP 1 of 7	A14365422	Frederico Neves		30 Sep 2011		
CO2	OP 2 of 7	A14365421	Anne-Marie Eklund Lowinder		30 Sep 2011		
CO4	OP 4 of 7	A14365420	Robert Seastrom		30 Sep 2011		

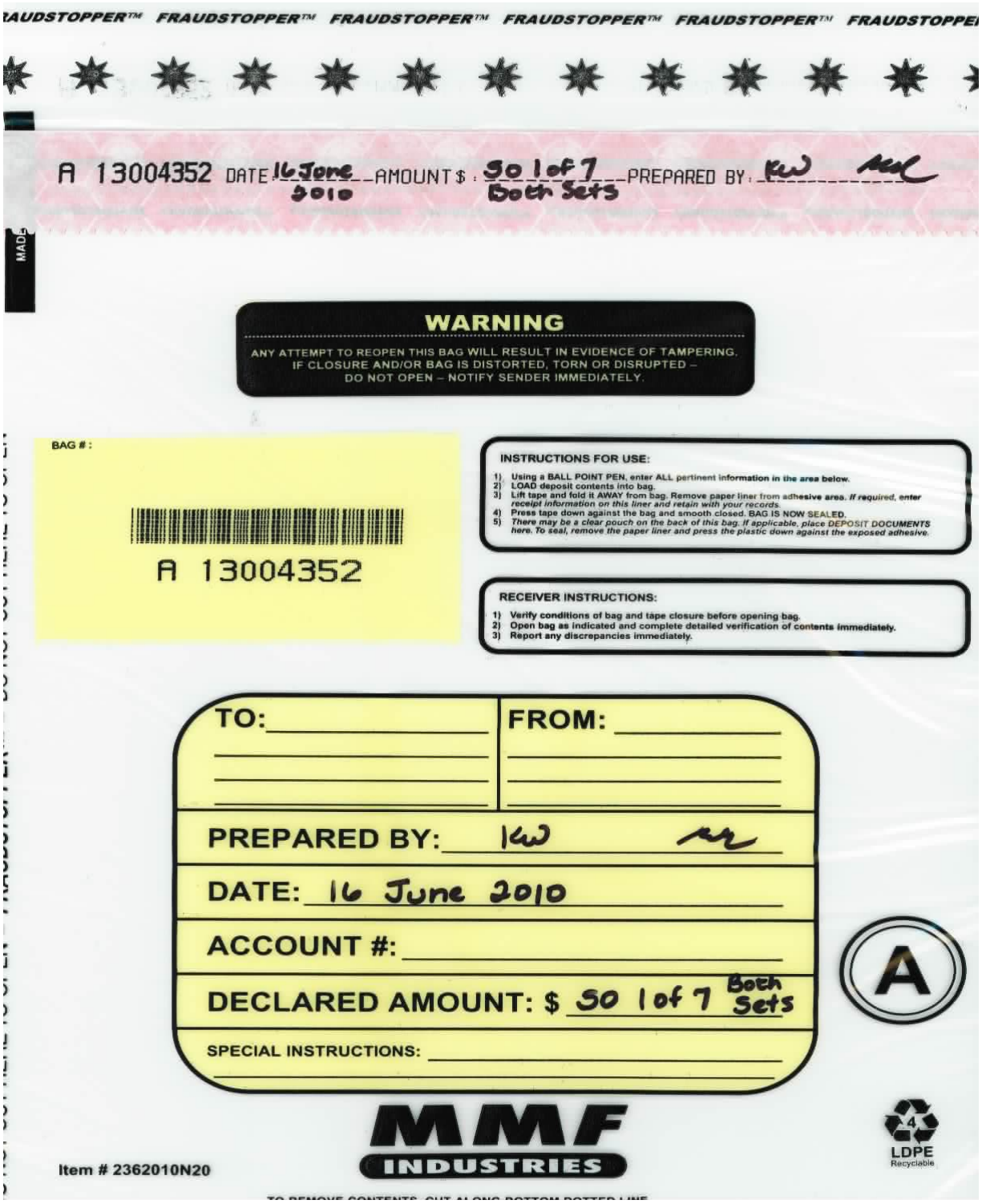
FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™
A 13004352 DATE 16 June 2010 AMOUNT $ 50 1 of 7 Both Sets PREPARED BY KW
WARNING
ANY ATTEMPT TO REOPEN THIS BAG WILL RESULT IN EVIDENCE OF TAMPERING.
IF CLOSURE AND/OR BAG IS DISTORTED, TORN OR DISRUPTED –
DO NOT OPEN – NOTIFY SENDER IMMEDIATELY.
BAG # :
A 13004352
INSTRUCTIONS FOR USE:
1) Using a BALL POINT PEN, enter ALL pertinent information in the area below.
2) LOAD deposit contents into bag.
3) Lift tape and fold it AWAY from bag. Remove paper liner from adhesive area. If required, enter receipt information on this liner and retain with your records.
4) Press tape down against the bag and smooth closed. BAG IS NOW SEALED.
5) There may be a clear pouch on the back of this bag. If applicable, place DEPOSIT DOCUMENTS here. To seal, remove the paper liner and press the plastic down against the exposed adhesive.
RECEIVER INSTRUCTIONS:
1) Verify conditions of bag and tape closure before opening bag.
2) Open bag as indicated and complete detailed verification of contents immediately.
3) Report any discrepancies immediately.
TO:
FROM:
PREPARED BY: KW
DATE: 16 June 2010
ACCOUNT #:
DECLARED AMOUNT: $ 50 1 of 7 Both Sets
SPECIAL INSTRUCTIONS:
A
MMF INDUSTRIES
Item # 2362010N20
4 LDPE Recyclable

Figure 2

Returning Equipment in TEBs to Safe #1

Step	Activity	Initial	Time
77	CA, IW1, SSC1 open safe room and enter with equipment cart.		
78	SSC1 opens Safe #1 shielding combination from camera.		
79	SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry.		
80	CA records return of **HSM** in next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA **CAREFULLY** places the HSM into Safe #1 and IW1 initials the entry.		
81	CA records return of **laptop** in next entry field of safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry.		
82	CA records return of **O/S DVDs** in next entry field of safe log with TEB #, printed name, date, time, and signature; places the O/S DVD into Safe #1 and IW1 initials the entry.		
83	CA records return of **HSMFD** in next entry field of safe log with TEB #, printed name, date, time, and signature; places the HSMFD into Safe #1 and IW1 initials the entry.		

Close Equipment Safe #1

Step	Activity	Initial	Time
84	SSC1 makes an entry including printed name, date, time, signature and notes “closing safe” in the safe log.		
85	SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions).		
86	IW1 and CA verify safe is locked and door indicator light is green.		
87	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.		

Open Credential Safe #2

Step	Activity	Initial	Time
88	After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. COs bring their OP card TEB with them.		
89	SSC2 opens Safe #2 while shielding combination from camera.		
90	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the re-opening of the safe. IW1 initials the entry.		

CO returns OP cards to Safe #2

Step	Activity	Initial	Time
91	One by one, each CO along with the CA (using his/her common key): a) Open his/her respective safe deposit box and read out box number inside Safe #2. b) CO makes an entry into the safe log indicating the return of OP card including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB# s and card type to his/her script. c) CO places his/her TEB into his/her box and locks the safe deposit box with the help of the CA. Repeat the steps above until all cards are returned to the deposit box.		

Close Credential Safe #2

Step	Activity	Initial	Time
92	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes “closing safe” into the safe log.		
93	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions).		
94	IW1 and CA verify safe is locked and door indicator light is green.		
95	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.		

Participant Signing of IW1’s Script

Step	Activity	Initial	Time
96	All participants enter printed name, date, time, and signature on IW1’s script coversheet.		
97	CA reviews IW1’s script and signs it.		

Signing out of Ceremony Room

Step	Activity	Initial	Time
98	IW2 ensures that all participants sign out of Ceremony Room log and are escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.		

Filming Stops

Step	Activity	Initial	Time
99	SA stops filming and makes 2 copies of film, one for on-site and one for off-site storage along with IW1 script copies made below.		

Copying and Storing the Script

Step	Activity	Initial	Time
100	IW1 makes at least 5 copies of his/her script: one for off-site audit bundle, one for IW1, one for IKOS and copies for other participants, as requested. Audit bundles each contain 1) Output of signer system – HSMFD 2) Copy of IW1's key ceremony script 3) Audio-visual recording 4) Logs from the Physical Access Control and Intrusion Detection System (Range is 5/12/2011 – 9/30/2011) 5) SA attestation (A.2, A.3 below) 6) The IW attestation (A.1 below) All in a TEB labeled "Key Ceremony 7", dated and signed by **IW1 and CA**. Off-site audit bundle is delivered to off-site storage. **The CA holds the ultimate responsibility for finalizing the audit bundle.**		

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

Notes from the Audit Bundle Checklist Document:

1. Output of Signer System (CA)
One electronic copy (physical flash drive) of the HSMFD in each audit bundle, each placed within a tamper-evident bag, labeled, dated and signed by the CA and the IW1

2. Key Ceremony Scripts (IW1)
Hard copies of the IW1's key ceremony scripts, including the IW's notes and the IW's attestation. See Appendix A.1.

3. Audio-visual recordings from the key ceremony (SA)

4. Logs from the Physical Access Control and Intrusion Detection System (SA)
One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC-IDS configuration review, the list of the enrolled users, the event log file and the configuration audit log file in each audit bundle, each placed in a tamper-evident bag, labeled, dated and signed by the SA and the IW

5. Configuration review of the Physical Access Control and Intrusion Detection System (SA)
SA's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix A.2.

6. Configuration review of the Firewall System (SA)
SA's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3.

7. Other items
If applicable.

A.1 Key Ceremony Script (by IW)

I hereby attest that the Key Ceremony was conducted in accordance with this script and any exceptions that may have occurred were accurately and properly documented.

Francisco Arias

_____

Date: _____

A.2 Access Control System Configuration Review (by SA)

I have reviewed the access control system configuration, the configuration audit log and the assigned authorizations from the West Coast KMF and not found any discrepancies or anything else out of the ordinary.

Enclosed are the configuration audit log, the list of assigned authorizations and the screenshots of the roles configurations.

Enclosed is also an electronic copy of the event log from the access control system ranging from the last extraction at East Coast KMF [date, time UTC]_____ to now.

Alexander Kulik

_____

Date: _____

A.3 Firewall Configuration Review (by SA)

I have reviewed the firewall configuration from the West Coast KMF and not found any discrepancies or anything else out of the ordinary.

Enclosed is the configuration extract from the firewall unit.

Alexander Kulik

_____

Date: _____

A.4 Re-sealing of Audit Bundle Information

I have opened the TEB from KSK ceremony N, dated [date] labeled “audit N" for the purpose of _____. The original TEB is enclosed within this new packaging.

[Name] _____

[Signature] _____

[Date] _____