ICANN DNSSEC Key Ceremony 5 Script

Abbreviations

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 /US		11 May 2011	19:05
IW1	Francisco Arias /MX		11 May 2011	19:05
SA1	Reed Quinn /US		11 May 2011	19:05
SA2	Alex Kulik /US		11 May 2011	19:06
SSC1	Julie Hedlund /US		11 May 2011	19:08
SSC2	Patrick Jones /US		11 May 2011	19:08
CO2	Anne-Marie Eklund Lowinder /SE		11 May 2011	19:07
CO3	Olaf Kolkman /NL		11 May 2011	19:06
CO4	Robert Seastrom /US		11 May 2011	19:09
CO6	Guarab Upadhaya /NP		11 May 2011	19:06
CO7	Alain Aina /TG		11 May 2011	19:08
EW1	Al Bolivar /US		11 May 2011	19:08
EW2	Crist Malekyan/ US		11 May 2011	—
EW3	Paul Kane /UK		11 May 2011	19-08
EW4	Spencer Roessner /US		11 May 2011	19:09
EW5	Bevil Wooding /TT		11 May 2011	19:07
EW6/CA2	Richard Lamb /US		11 May 2011	19:07
IKOS/IW2	Tomofumi Okubo /JP		11 May 2011	19:07

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.

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

Step	Activity	Initial	Time
1	SAs or IWs escort participants into the Ceremony Room.	FA	17:01

Sign into Key Ceremony Room

Step	Activity	Initial	Time
2	SA and IWs have all participants sign into the Ceremony Room log.	FA	17:01

Emergency Evacuation Procedures

Step	Activity	Initial	Time
3	CA or IW reviews emergency evacuation procedures with participants.	FA	17:01

Verify Time and Date

Step	Activity	Initial	Time
4	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: 11 May 2011 17:01 UTC All entries into this script or any logs should follow this common source of time.	FA	17:01

CO Selection

Step	Activity	Initial	Time
5	After reaching a consensus with the TCRs, CA announces the 3 COs to retrieve the cards for the ceremony. CO 2 of 7 CO 6 of 7 CO 7 of 7	FA	17:03

Open Credential Safe #2

Step	Activity	Initial	Time
6	CA and IW1 escort SSC2 and COs into the safe room together.	FA	17:04
7	SSC2, while shielding combination from camera, opens Safe #2.	FA	17:05
8	SSC2 takes out safe log and prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry.	FA	17:05

COs extract OP Cards from safe deposit boxes

Step	Activity	Initial	Time
9	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 3 cards are removed. IW1 initials this entry when all CO have finished. IW also checks the selected CO below. COs that were not selected this time, performs a) and b), then returns both set of cards and perform d). Repeat until the remaining COs complete the verification. CO2: Anne-Marie Eklund Lowinder Check if removed ✓ **Box 1259** **OP TEB # A15473418** **SO TEB # A14377119** CO3: Olaf Kolkman Check if removed NO **Box 1239** **OP TEB # A14377120** **SO TEB # A14377121** CO4: Robert Seastrom Check if removed NO **Box 1260** **OP TEB # A15473415** **SO TEB # A14377123** CO6: Guarab Upadhaya Check if removed ✓ **Box 1261** **OP TEB # A14377126** **SO TEB # A14377127** CO7: Alain Aina Check if removed ✓ **Box 1262** **OP TEB # A14377128** **SO TEB # A14377129**	FA	17:18

Close Credential Safe #2

Step	Activity	Initial	Time
10	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.	FA	17:19

Step	Activity	Initial	Time
11	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions).	FA	17:20
12	CA and IW1 verify that the safe is locked and card reader indicator is green.	FA	17:20
13	IW1, CA, SSC2, and COs leave safe room, with OP cards in TEBs, closing the door behind them.	FA	17:20

Open Equipment Safe #1 (Approximately 3 minutes)

Step	Activity	Initial	Time
14	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	FA	17:22
15	SSC1, while shielding combination from camera, opens Safe #1.	FA	17:23
16	SSC1 takes out safe log and prints name, date, time, signature and reason (i.e., "opened safe") in safe log. IW1 initials this entry.	FA	17:24

Remove Equipment from Safe #1

Step	Activity	Initial	Time
17	CA **CAREFULLY** removes HSM2 (in TEB) from the safe and completes the entry in the safe log indicating "HSM2 Removal," TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry. **HSM2: TEB# A2751117 / serial # K6002013** Note: HSM1: TEB# A2751142 / serial # K6002016 (last used)	FA	17:25
18	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 #1: TEB# A2751116 / serial# 41593712005** Note: Laptop #2: TEB A2751140 / serial # 35063364997 (last used) **O/S DVDs (Rev 575): TEB# A15473414** **HSMFD: TEB # A15473413**	FA	17:29

Close Equipment Safe #1 and exit safe room

Step	Activity	Initial	Time
19	SSC1 makes an entry including printed name, date, time and signature into the safe log indicating, "closing of the safe". IW1 initials this entry.	FA	17:29
20	SSC1 puts log back in safe and locks Safe #1 (spin dial at least two full revolutions).	FA	17:32
21	CA and IW1 verify that the safe is locked and door indicator light is green.	FA	17:32
22	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.	FA	17:45

Set Up Laptop

Step	Activity	Initial	Time
23	CA inspects the r575 O/S DVD TEB for tamper evidence; reads out TEB # 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 # below. **O/S DVDs (Rev 575): TEB# A15473414**	FA	17:53
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 #1: TEB A2751116 / serial# 41593712005** Note: Laptop #2: TEB A2751140 / serial # 35063364997 (last used)	FA	17:54
25	CA takes above O/S DVDs and laptop out of TEBs placing them on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from DVD.	FA	17:59
26	CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.	FA	17:59

27	CA enters the commands
	`system-config-display --noui`
	and
	`killall Xorg`
	CA ensures that external display works.
		FA	17:59

28	CA logs in as root.	FA	17:59
29	CA configures printer as default and prints test page.	FA	18:01
30	CA opens a terminal window and maximizes its size for visibility.	FA	18:01
31	CA checks and fixes date and time on laptop based on wall clock ensuring UTC time zone has been chosen.	FA	18:03
32	CA inserts USB port expander into laptop.	FA	18:03
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 # A15473413**	FA	18:03
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.	FA	18:04

Start Logging Terminal Session

Step	Activity	Initial	Time
35	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`	FA	18:04
36	CA executes `script script-20110511.log` to start a capture of terminal output.	FA	18:05

Start Logging HSM Output

Step	Activity	Initial	Time
37	CA connects a serial to USB null modem cable to laptop.	FA	18:05

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.
		FA	18:06

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. **HSM2: TEB# A2751117 / serial # K6002013** Note HSM1: TEB# A2751142 / serial # K6002016 (last used)	FA	18:06
40	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	FA	18:07
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.)	FA	18:08

Enable/Activate HSM

Step	Activity	Initial	Time
42	CA calls the CO, CO opens TEB with OP card __2__ of 7 and hands to CA who places card in cardholder visible to all.	FA	18:09
43	CA calls the CO, CO opens TEB with OP card __6__ of 7 and hands to CA who places card in cardholder visible to all.	FA	18:09
44	CA calls the CO, CO opens TEB with OP card __7__ of 7 and hands to CA who places card in cardholder visible to all.	FA	18:09
45	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 __2__ of 7 2nd OP card __6__ of 7 3rd OP card __7__ of 7	FA	18:11

VERISIGN

21355 Ridgetop Circle
Dulles, VA 20166
t: 703-948-3200
f: 650-237-8827

VerisignInc.com

April 29, 2011

To Whom It May Concern:

This is a letter of Verification of Employment for Alejandro Bolivar. Verisign, Inc. has employed Alejandro Bolivar full-time since September 8, 1997 as a Senior Engineer, with our Naming Product Operations Department.

Verisign is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day our identity protection and registry services allow companies and consumers all over the world to engage in trusted communications and commerce.

For over 10 years, Verisign Internet infrastructure has been at the very heart of the Internet, enabling key transactions and protecting valuable data. Verisign facilitates as many as 31 billion authoritative Domain Name System (DNS) queries a day, and has been providing this service since 1998 with 100% availability. Over the years the Verisign Internet infrastructure has scaled quickly and dramatically, and has the capacity to scale just as dramatically in the coming years, as the world moves to Internet-based transactions. Verisign SSL Certificates have provided a strong foundation for e-commerce, and the Verisign Secured® Seal, the most recognized symbol of trust on the Internet (TNS Study, 2006), is viewed over 100 million times a day on browsers all over the world.

Should you have further questions, please contact me at the number below.

Sincerely,

Natalie Fuentes
HR Services Consultant | VeriSign, Inc. | 703-948-4175 | nfuentes@verisign.com

VERISIGN

21355 Ridgetop Circle
Dulles, VA 20166
t: 703-948-3200
f: 701-987-6543

VerisignInc.com

11 May 2011

The SHA256 hash of the 2011 Q3 KSR file is:

eeaf9d0207be84063f20e809bd2cc25e570665ec8d04a75ab2e278365
527e77a

The PGP wordlist for the hash above is:

Tycoon pharmacy quadrant aftermath ahead racketeer mural
amulet cowbell butterfat trauma applicant skullcap
Chicago snapshot finicky eightball amulet fracture
unicorn optic alkali repay existence sawdust tomorrow
island congregate edict celebrate transit infancy

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer, Cryptographic Business Operations
VeriSign, Inc.

Check Network between Laptop and HSM

Step	Activity	Initial	Time
46	CA connects HSM to laptop using Ethernet cable.	FA	18:11
47	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.	FA	18:12

Insert Copy of KSR to be signed

Step	Activity	Initial	Time
48	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.	FA	18:12

Sign it with our KSK

Step	Activity	Initial	Time
49	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2011-q3-0.xml`	FA	18:17

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initial	Time
50	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: Alejandro Bolivar	FA	18:19
51	Participants match the hash read out with that displayed on the terminal. CA asks "are there are any objections"?	FA	18:19
52	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-2011-q3-0.xml`	FA	18:19

```
$ 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

```
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2011-q3-0.xml (at Wed May 11 18:16:32 2
011 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
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:          K6002013

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2011-04-01T00:00:00 2011-04-15T23:59:59  34525,21639   19036
2  2011-04-11T00:00:00 2011-04-25T23:59:59  34525         19036
3  2011-04-21T00:00:00 2011-05-05T23:59:59  34525         19036
4  2011-05-01T00:00:00 2011-05-15T23:59:59  34525         19036
5  2011-05-11T00:00:00 2011-05-25T23:59:59  34525         19036
6  2011-05-21T00:00:00 2011-06-04T23:59:59  34525         19036
7  2011-05-31T00:00:00 2011-06-14T23:59:59  34525         19036
8  2011-06-10T00:00:00 2011-06-24T23:59:59  34525         19036
9  2011-06-20T00:00:00 2011-07-05T23:59:59  39283,34525   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2011-q3-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2011-07-01T00:00:00 2011-07-15T23:59:59  39283,34525
2  2011-07-11T00:00:00 2011-07-25T23:59:59  39283
3  2011-07-21T00:00:00 2011-08-04T23:59:59  39283
4  2011-07-31T00:00:00 2011-08-14T23:59:59  39283
5  2011-08-10T00:00:00 2011-08-24T23:59:59  39283
6  2011-08-20T00:00:00 2011-09-03T23:59:59  39283
7  2011-08-30T00:00:00 2011-09-13T23:59:59  39283
8  2011-09-09T00:00:00 2011-09-24T00:00:00  39283
9  2011-09-20T00:00:00 2011-10-05T23:59:59  55231,39283
...PASSED.

SHA256 hash of KSR:
EEAF9D0207BE84063F20E809BD2CC25E570665EC8D04A75AB2E278365527E77A
>> tycoon pharmacy quadrant aftermath ahead racketeer mural amulet cowbell butterfat tr
auma applicant skullcap Chicago snapshot finicky eightball amulet fracture unicorn opti
c alkali repay existence sawdust tomorrow island congregate edict celebrate transit inf
ancy <<

Generated new SKR in /media/KSR/skr-root-2011-q3-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2011-07-01T00:00:00 2011-07-15T23:59:59  39283,34525   19036
```

```
2  2011-07-11T00:00:00 2011-07-25T23:59:59  39283         19036
3  2011-07-21T00:00:00 2011-08-04T23:59:59  39283         19036
4  2011-07-31T00:00:00 2011-08-14T23:59:59  39283         19036
5  2011-08-10T00:00:00 2011-08-24T23:59:59  39283         19036
6  2011-08-20T00:00:00 2011-09-03T23:59:59  39283         19036
7  2011-08-30T00:00:00 2011-09-13T23:59:59  39283         19036
8  2011-09-09T00:00:00 2011-09-24T00:00:00  39283         19036
9  2011-09-20T00:00:00 2011-10-05T23:59:59  55231,39283   19036

SHA256 hash of SKR:
6FD52BDC5D38B6EC97C61020C8FAAC68C694ABAB8241F075EBB47E0329B789F9
>> gremlin specialist briefcase sympathy exceed consulting Scotland unicorn preshrunk r
esponsive assume butterfat spaniel whimsical ribcage gravity southward molecule rhythm
Pegasus miser decadence unearth impartial trouble politeness locale aggregate breakup p
rocessor nightbird Waterloo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Print Copies of the Operation for Participants

Step	Activity	Initial	Time
53	CA prints out a sufficient number of copies for participants using `printlog ksrsigner-20110511-*.log N` where ksrsigner-20110511-*.log is replaced by log output file displayed by program. (this example generates **N** copies) and hands copies to participants.	FA	18:22
54	IW1 attaches a copy to his/her script.	FA	18:22

Backup Newly Created SKR

Step	Activity	Initial	Time
55	CA copies the contents of the KSR FD by running `cp -p /media/KSR/* .` for posting back to RZM.	FA	18:23

56	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`
		FA	18:24

57	CA removes **KSR** FD containing SKR and gives it to the RZM representative.	FA	18.24

Returning HSM to a TEB

Step	Activity	Initial	Time
58	CA presses RESTART button and waits for self test to complete.	FA	18:24
59	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.	FA	18:25
60	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM2: TEB# A2826709 / serial # K6002013** IW1 initials the TEB.	FA	18:26
61	CA places item on equipment cart.	FA	18:27

Stop Recording Serial Port Activity

Step	Activity	Initial	Time
62	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of serial output terminal window.	FA	18:27

Stop Logging Terminal Output

Step	Activity	Initial	Time
63	CA stops logging terminal output by entering "exit" in the terminal window.	FA	18:27

```
Script started on Wed 11 May 2011 06:04:50 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]#
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=0.784 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.255 ms

--- 192.168.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.255/0.519/0.784/0.265 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigned K033[K033[Kr
\033[K033[Kr kK033[K033[KLKy033[K033[K033[KKjmtk033[K033[K033[Kqmt7v /media/KSR/ks\007
mkroot-2011-q3-0.xm
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2011-q3-0.xml (at Wed May 11 18:13:51
2011 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:          K6002013

Validating last SKR with HSM...
[error] Cannot open last KSR response file /media/KSR/skr.xml
[error] If this is first KSR, you may want to override with -Override if authorized.
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20110511-181351.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner Kjqmt7v /media
mKSR033[A033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[
C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[K
\033[K\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[Cksrsigner Kjqm
mIv\033[A033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[
C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[Cping 192.168.0.2\033[K
\033[K\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[Cv
mmedia/KSR033[A033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[
C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[K
\033[K\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]#
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner Kjqmt7v /media
mKSR033[A033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[C033[
C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[Cping 192.168.0.2\033[K
\033[K\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[Cv
mmedia/KSR/ksr-root-2011-q3-0.xm
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2011-q3-0.xml (at Wed May 11 18:16:32
2011 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:          K6002013

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2011-04-01T00:00:00 2011-04-15T23:59:59  34525,21639   19036
2  2011-04-11T00:00:00 2011-04-25T23:59:59  34525         19036
3  2011-04-21T00:00:00 2011-05-05T23:59:59  34525         19036
4  2011-05-01T00:00:00 2011-05-15T23:59:59  34525         19036
5  2011-05-11T00:00:00 2011-05-25T23:59:59  34525         19036
6  2011-05-21T00:00:00 2011-06-04T23:59:59  34525         19036
7  2011-05-31T00:00:00 2011-06-14T23:59:59  34525         19036
8  2011-06-10T00:00:00 2011-06-24T23:59:59  34525         19036
9  2011-06-20T00:00:00 2011-07-05T23:59:59  39283,34525   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2011-q3-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2011-07-01T00:00:00 2011-07-15T23:59:59  39283,34525
2  2011-07-11T00:00:00 2011-07-25T23:59:59  39283
3  2011-07-21T00:00:00 2011-08-04T23:59:59  39283
4  2011-07-31T00:00:00 2011-08-14T23:59:59  39283
5  2011-08-10T00:00:00 2011-08-24T23:59:59  39283
6  2011-08-20T00:00:00 2011-09-03T23:59:59  39283
7  2011-08-30T00:00:00 2011-09-13T23:59:59  39283
8  2011-09-09T00:00:00 2011-09-24T00:00:00  39283
9  2011-09-20T00:00:00 2011-10-05T23:59:59  55231,39283
...PASSED.

SHA256 hash of KSR:
EEAF9D0207BE84063F20E809BD2CC25E570665EC8D04A75AB2E278365527E77A
>> tycoon pharmacy quadrant aftermath ahead racketeer mural amulet cowbell butterfat t
rauma applicant skullcap Chicago snapshot finicky eightball amulet fracture unicorn op
tic alkali repay existence sawdust tomorrow island congregate edict celebrate transit
infancy <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2011-q3-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2011-07-01T00:00:00 2011-07-15T23:59:59  39283,34525   19036
2  2011-07-11T00:00:00 2011-07-25T23:59:59  39283         19036
3  2011-07-21T00:00:00 2011-08-04T23:59:59  39283         19036
4  2011-07-31T00:00:00 2011-08-14T23:59:59  39283         19036
5  2011-08-10T00:00:00 2011-08-24T23:59:59  39283         19036
6  2011-08-20T00:00:00 2011-09-03T23:59:59  39283         19036
7  2011-08-30T00:00:00 2011-09-13T23:59:59  39283         19036
8  2011-09-09T00:00:00 2011-09-24T00:00:00  39283         19036
9  2011-09-20T00:00:00 2011-10-05T23:59:59  55231,39283   19036

SHA256 hash of SKR:
6FD52BDC5D38B6EC97C61020C8FAAC68C694ABAB8241F075EBB47E0329B789F9
>> gremlin specialist briefcase sympathy exceed consulting Scotland unicorn preshrunk
responsive assume butterfat spaniel whimsical ribcage gravity southward molecule rhyth
```

```
m Pegasus miser decadence unearth impartial trouble politeness locale aggregate breaku
p processor nightbird Waterloo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20110511-181632.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# prin\033[Ktlog ksr\007-s
\033[K033[Ksi\007gner-2011\0070511-181\007
ksrsigner-20110511-181351.log  ksrsigner-20110511-181632.log
[root@localhost HSMFD]# printlog ksrsigner-20110511-1812\007\033[K*.lo\033[K033[K033[K
\033[K033[K033[K033[K033[K*.log 20
[ 1 pages * 0 copy ] sent to printer
1 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# printlog ksrsigner-20110
511-\033[1P\007\033[3@181\007
ksrsigner-20110511-181351.log  ksrsigner-20110511-181632.log
[root@localhost HSMFD]# printlog ksrsigner-20110511-181\033[C\033[C\033[C\033[C\033[1P
\033[1P\033[1P\033[1P6200log 20
[ 2 pages * 20 copy ] sent to printer
3 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# printlog ksrsigner-20110
511-181\033[C\033[C\033[C\033[1P033[1P033[1P033[1P033[1P033[1P\033[1@\033[1P\033[1@*
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[Cksrsigner Kjqmt7v /media/K
SR/\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[
C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[13Pprintlog ksrsigner-20110511-*
.log 20
\033[K\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[K\007\007\007\007\007
\007\007\007\007\007CP\033[K033[K033[Kcp -p /media/KSR/\033[K* .
cp: overwrite './skr.xml'? y
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -lt /m\033[Kedia\033[
K/KSR
\033[00mtotal 76
-rwxr-xr-x 1 root root 18402 May 11 18:19 \033[00;32mskr-root-2011-q3-0.xml\033[00m
-rwxr-xr-x 1 root root 18402 May 11 18:19 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 15547 Apr 25 17:30 \033[00;32mksr-root-2011-q3-0.xml\033[00m
-rwxr-xr-x 1 root root 18402 Feb  7 22:36 \033[00;32mskr.xml.20110511181632\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/KSR
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit

Script done on Wed 11 May 2011 06:27:29 PM UTC
```

```
2011-05-11T18:07:33+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2011-05-11T18:07:33+0000        ttyUSB0
2011-05-11T18:07:34+0000        ttyUSB0
2011-05-11T18:07:34+0000        ttyUSB0 Battery OK!
2011-05-11T18:07:34+0000        ttyUSB0
2011-05-11T18:07:35+0000        ttyUSB0
2011-05-11T18:07:35+0000        ttyUSB0 No Tamper Counts in BBRAM!
2011-05-11T18:07:35+0000        ttyUSB0
2011-05-11T18:07:35+0000        ttyUSB0  Loading Application (APP)
2011-05-11T18:07:35+0000        ttyUSB0
2011-05-11T18:07:36+0000        ttyUSB0  Starting loaded code.
2011-05-11T18:07:36+0000        ttyUSB0
2011-05-11T18:07:36+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2011-05-11T18:07:36+0000        ttyUSB0
2011-05-11T18:07:38+0000        ttyUSB0 wdog started
2011-05-11T18:07:38+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running DES POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 DES POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running Triple DES POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Triple DES POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running AES POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 AES POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running SHA1 POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 SHA1 POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running SHA2 POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 SHA2 POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running RSA POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 RSA POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running DSA POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 DSA POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Running RandomGen POST Test
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 RandomGen POST Test Passed
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 Additional RandomGen POST Test Passed
```

```
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0 11/5/2009 at 17:46:50
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:41+0000        ttyUSB0  0x100008
2011-05-11T18:07:41+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 App Details Response:
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Part Number: Keyper Pro 0405
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Serial Number: Serial K6002013
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 App Build Number: App 020
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 ABL Build Number: ABL 029
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 AL Build Number: AL 02A
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 CS Build Number: CS 029
2011-05-11T18:07:42+0000        ttyUSB0
```

```
2011-05-11T18:07:42+0000        ttyUSB0 Total Private Memory 4173393
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Free Private Memory 4173393
2011-05-11T18:07:42+0000        ttyUSB0
2011-05-11T18:07:42+0000        ttyUSB0 Total Dynamic Memory 14569472
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0 Free Dynamic Memory 14569472
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0 Date and Time: 17:46:50 on 11/05/2009
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0 Created socket 1 on port 3000.
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0 11/5/2009 at 17:46:51
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:07:43+0000        ttyUSB0  0x100003
2011-05-11T18:07:43+0000        ttyUSB0
2011-05-11T18:10:24+0000        ttyUSB0
2011-05-11T18:10:24+0000        ttyUSB0
2011-05-11T18:10:24+0000        ttyUSB0 11/5/2009 at 17:49:32
2011-05-11T18:10:24+0000        ttyUSB0
2011-05-11T18:10:24+0000        ttyUSB0  0x200023 0880004A7A73296D
2011-05-11T18:10:24+0000        ttyUSB0
2011-05-11T18:10:47+0000        ttyUSB0
2011-05-11T18:10:47+0000        ttyUSB0
2011-05-11T18:10:47+0000        ttyUSB0 11/5/2009 at 17:49:55
2011-05-11T18:10:47+0000        ttyUSB0
2011-05-11T18:10:47+0000        ttyUSB0  0x200023 0880004A7B73296D
2011-05-11T18:10:47+0000        ttyUSB0
2011-05-11T18:11:06+0000        ttyUSB0
2011-05-11T18:11:06+0000        ttyUSB0
2011-05-11T18:11:06+0000        ttyUSB0 11/5/2009 at 17:50:14
2011-05-11T18:11:06+0000        ttyUSB0
2011-05-11T18:11:06+0000        ttyUSB0  0x200023 0880004A7BB3296D
2011-05-11T18:11:06+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0 Created socket 1 on port 5000.
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0 11/5/2009 at 17:50:16
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:11:08+0000        ttyUSB0  0x100002
2011-05-11T18:11:08+0000        ttyUSB0
2011-05-11T18:14:12+0000        ttyUSB0
2011-05-11T18:14:12+0000        ttyUSB0
2011-05-11T18:14:12+0000        ttyUSB0 Accepted connection on address 215.92.192.168.0.1.
2011-05-11T18:14:12+0000        ttyUSB0
2011-05-11T18:14:12+0000        ttyUSB0
2011-05-11T18:14:12+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0 ========================================================================
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0 Free memory down from 14569472 to 11843072 (last mechanism 0)!
```

```
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0 17:53:21 on 11-05-2009
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0 ================================================================
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:14:13+0000        ttyUSB0 Closing connection on address 215.92.192.168.0.1.
2011-05-11T18:14:13+0000        ttyUSB0
2011-05-11T18:16:41+0000        ttyUSB0
2011-05-11T18:16:41+0000        ttyUSB0
2011-05-11T18:16:41+0000        ttyUSB0 Accepted connection on address 215.93.192.168.0.1.
2011-05-11T18:16:41+0000        ttyUSB0
2011-05-11T18:19:06+0000        ttyUSB0
2011-05-11T18:19:06+0000        ttyUSB0
2011-05-11T18:19:06+0000        ttyUSB0 Closing connection on address 215.93.192.168.0.1.
2011-05-11T18:19:06+0000        ttyUSB0
2011-05-11T18:24:29+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2011-05-11T18:24:29+0000        ttyUSB0
2011-05-11T18:24:30+0000        ttyUSB0
2011-05-11T18:24:30+0000        ttyUSB0 Battery OK!
2011-05-11T18:24:30+0000        ttyUSB0
2011-05-11T18:24:31+0000        ttyUSB0
2011-05-11T18:24:31+0000        ttyUSB0 No Tamper Counts in BBRAM!
2011-05-11T18:24:31+0000        ttyUSB0
2011-05-11T18:24:31+0000        ttyUSB0  Loading Application (APP)
2011-05-11T18:24:31+0000        ttyUSB0
2011-05-11T18:24:32+0000        ttyUSB0  Starting loaded code.
2011-05-11T18:24:32+0000        ttyUSB0
2011-05-11T18:24:32+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2011-05-11T18:24:32+0000        ttyUSB0
2011-05-11T18:24:33+0000        ttyUSB0 wdog started
2011-05-11T18:24:33+0000        ttyUSB0
2011-05-11T18:24:36+0000        ttyUSB0
2011-05-11T18:24:36+0000        ttyUSB0
2011-05-11T18:24:36+0000        ttyUSB0 Running DES POST Test
2011-05-11T18:24:36+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 DES POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running Triple DES POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Triple DES POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running AES POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 AES POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running SHA1 POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 SHA1 POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running SHA2 POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 SHA2 POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
```

```
2011-05-11T18:24:37+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running RSA POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 RSA POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running DSA POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 DSA POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Running RandomGen POST Test
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 RandomGen POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 11/5/2009 at 18:03:45
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0  0x100008
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 App Details Response:
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:37+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:37+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
```

```
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Additional RandomGen POST Test Passed
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Part Number: Keyper Pro 0405
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Serial Number: Serial K6002013
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 App Build Number: App 020
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 ABL Build Number: ABL 029
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 AL Build Number: AL 02A
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 CS Build Number: CS 029
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Total Private Memory 4173393
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Free Private Memory 4173393
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Total Dynamic Memory 14569472
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Free Dynamic Memory 14569472
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Date and Time: 18:03:45 on 11/05/2009
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 Created socket 1 on port 3000.
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0 11/5/2009 at 18:03:47
2011-05-11T18:24:38+0000        ttyUSB0
2011-05-11T18:24:38+0000        ttyUSB0  0x100003
2011-05-11T18:24:38+0000        ttyUSB0
```

Backup HSM FD Contents (Approximately 10 minutes)

Step	Activity	Initial	Time
64	CA displays contents of HSMFD by executing `ls -lt`	FA	18:28
65	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_`	FA	18:28
66	CA displays contents of HSMFD_ by executing `ls -lt /media/HSMFD_`	FA	18:28
67	CA unmounts new FD using `umount /media/HSMFD_`	FA	18:28
68	CA removes HSMFD_ and places on table.	FA	18:28
69	CA repeats steps above and creates 4 more copies.	FA	18:30

Print Logging Information

Step	Activity	Initial	Time

70	CA prints out hard copies of logging information by executing
	`enscript -2Gr -# 2 script-20110511.log`
	`enscript -Gr -# 2 --font="Courier8" ttyaudit-ttyUSB*-20110511-*.log`
	for attachment to IW1 and CA scripts.
		FA	18:33

Returning HSMFD to a TEB

Step	Activity	Initial	Time

71	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
		FA	18:33

72	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 # A14365372** IW1 initials the TEB. CA places TEB on equipment cart.	FA	18:34

Distribute HSMFDs

Step	Activity	Initial	Time
73	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.	FA	18:35

Returning O/S DVD to a TEB

Step	Activity	Initial	Time
74	After all print jobs are complete, CA executes `shutdown -hP now` removes DVD and turns off laptop.	FA	18:36
75	CA places DVDs in new TEB and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **O/S DVDs (Rev 575): TEB# A14365371** IW1 initials the TEB. CA places TEB on equipment cart.	FA	18:36

Returning Laptop to a TEB

Step	Activity	Initial	Time
76	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 #1: TEB A2826708 / serial# 41593712005** IW1 initials the TEB. CA places TEB on equipment cart.	FA	18:39

Returning OP Smartcards to TEBs

Step	Activity	Initial	Time
77	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.	FA	18:45

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1
CO2	OP 2 of 7	A14365375	Anne-Marie Eklund Löwinder		11 May 2011	18.41	FA
CO6	OP 6 of 7	A14365374	UPADHAYA GAURAB RAJ		11 May 2011	18:43	FA
CO7	OP 7 of 7	A14365373	AINA Alain		11 May 2011	18:44	FA

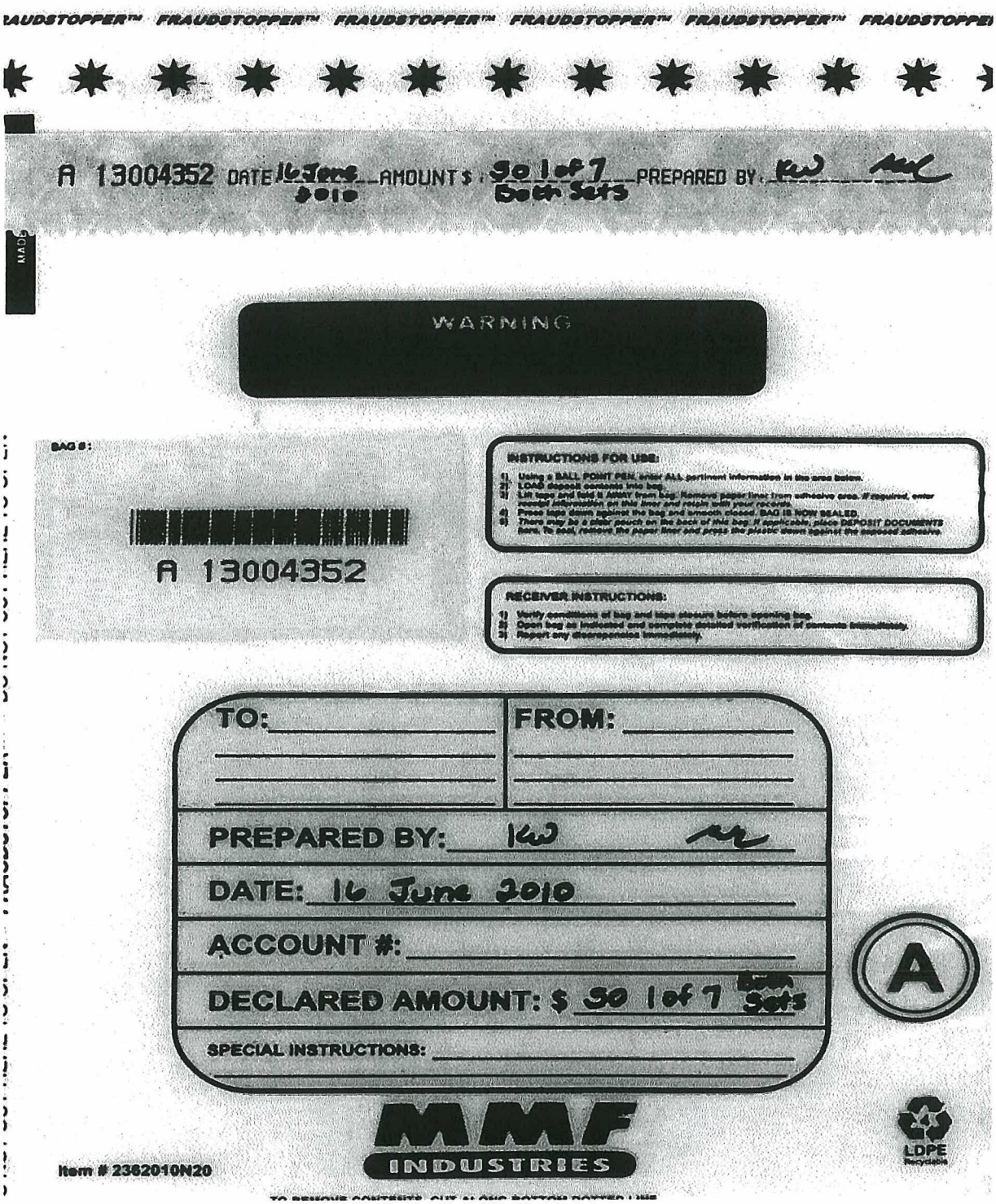

FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™
A 13004352 DATE 16 June 2010 AMOUNT $: 30 1 of 7 Both Sets PREPARED BY: kw
WARNING
BAG #:
A 13004352
INSTRUCTIONS FOR USE:
RECEIVER INSTRUCTIONS:
TO:
FROM:
PREPARED BY: kw
DATE: 16 June 2010
ACCOUNT #:
DECLARED AMOUNT: $ 30 1 of 7 Both Sets
SPECIAL INSTRUCTIONS:
A
MMF INDUSTRIES
Item # 2362010N20
LDPE

Figure 2

Returning Equipment in TEBs to Safe #1

Step	Activity	Initial	Time
78	CA, IW1, SSC1 open safe room and enter with equipment cart.	FA	18:46
79	SSC1 opens Safe #1 shielding combination from camera.	FA	18:49
80	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.	FA	18:50
81	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.	FA	18:51
82	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.	FA	18:52
83	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.	FA	18:53
84	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.	FA	18:53

Closing Equipment Safe #1

Step	Activity	Initial	Time
85	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. #64	FA	18:54
86	SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions).	FA	18:55
87	IW1 and CA verify safe is locked and door indicator light is green.	FA	18:55
88	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	FA	18:55

Returning CO OP/SO cards to Credential Safe #2

Step	Activity	Initial	Time
89	After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. COs bring their OP card TEB with them.	FA	18:57
90	SSC2 opens Safe #2 while shielding combination from camera.	FA	18:58
91	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.	FA	18:59

CO returns OP cards to Safe #2

Step	Activity	Initial	Time
92	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.	FA	19:03

Closing Credential Safe #2

Step	Activity	Initial	Time
93	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.	FA	19:04
94	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions).	FA	19:04
95	IW1 and CA verify safe is locked and door indicator light is green.	FA	19:04
96	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	FA	19:05

Participant Signing of IW1's Script

Step	Activity	Initial	Time
97	All participants enter printed name, date, time, and signature on IW1's script coversheet.	FA	19:09
98	CA reviews IW1's script and signs it.	FA	19:11

Signing out of Ceremony Room

Step	Activity	Initial	Time
99	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.	FA	19:20

Filming Stops

Step	Activity	Initial	Time
100	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.	FA	19:20

Copying and Storing the Script

Step	Activity	Initial	Time
101	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 is11/2/2010 – 5/11/2011) 5) SA attestation (A.2, A.3 below) 6) The IW attestation (A.1 below) All in a TEB labeled "Key Ceremony 4", 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.

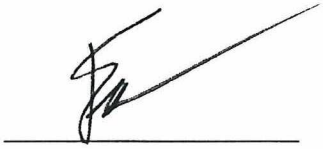
6. Configuration review of the Firewall System (SA)

SA's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3.

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: 11 May 2011

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] 11/2/11 00:01 to now.

Reed Quinn

Reed Quinn

Date: 5/11/11

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.

Reed Quinn

Reed Quinn

Date: 5/11/11

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] _____

Not used FA

ICANN DNSSEC Script Exception

1

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

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

Note Exception Time

1	IW notes date and time of key ceremony exception and signs here:	FA	17:17
2	IW Describes exception and action below	FA	17:18

-On step 9 Alain Aina had box 1241 instead of 1262. that the script said.

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

2

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

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

Note Exception Time

1	IW notes date and time of key ceremony exception and signs here:	FA	17:21
2	IW Describes exception and action below	FA	17:35

- On stp 21 the ~~green~~ light didn't go green until a couple of minutes.

– End of DNSSEC Script Exception –

ICANN

ICANN DNSSEC Script Exception

3

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

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

Note Exception Time

1	IW notes date and time of ~~key~~ ceremony exception and signs here: _____	FA	17:37
2	IW Describes exception and action below	FA	17:45

- On step2 while trying to leave the system won't let us, the light wont red since ~~CA or IW~~ the moment CA or IW first bolge out.
- CA let SA1 in tier 5 by forcing door - 17:37
- SA1 logs into console to check the issue, the ~~console~~ ACS showed 5 people on tier 5, while it should be 3. SA1 tried adjusting counters, it won't work. SA1 forced door so we could leave tier 5.

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

4

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

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

Note Exception Time

1	IW notes date and time of key ceremony exception and signs here: _____	FA	17:46
2	IW Describes exception and action below	FA	17:49

- At 17:46 all left tier4 to tier 3 by forcing the door
- ~~A~~CA and IW2 badged in to tier 4 taking everyone without badge with them
- CA2, SA1, SA2 and IW badged in - 17:49
- CA returned OP cards to the COs
- Equipment and OP cards were left on the table visible on camera with a watch from Olaf at aside before leaving tier 4.

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

5

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

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

Note Exception Time

1	IW notes date and time of key ceremony exception and signs here:	FA	18:16
2	IW Describes exception and action below	FA	18:16

- On step 49 the USB didn't have the previous SKR.
- CA brough another usb that had it having previously dismounted the other USB

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

6

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

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

Note Exception Time

1	IW notes date and time of key ceremony exception and signs here:	FA	18:48
2	IW Describes exception and action below	FA	

- Before step 79 CA, IW and SSC1 left tier5 leaving the cart with the equipment in front of the camera.
- CA, IW, SSC1 enter back in tier5 - 18:49

– End of DNSSEC Script Exception –

```
reed@srx> show configuration | no-more
## Last commit: 2011-05-12 06:20:45 UTC by reed
version 10.1R3.7;
system {
    host-name srx;
    domain-name ksk.cjr.dns.icann.org;
    location {
        country-code US;
        postal-code 22701;
        building Terremark-Admin;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "$1$aHyrnTM5$Qel./kgTz6hmmTZqWI9P00"; ## SECRET-
DATA
    }
    name-server {
        199.4.29.19;
        199.4.29.29;
    }
    login {
        user alex {
            full-name "Alexander Kulik";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "$1$vDDB4N6q$aRBlkIJ58FJm7lIWt.Sp7."; ##
SECRET-DATA
            }
        }
        user jsamora {
            full-name "Jesse Samora";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "$1$4OeS8C4z$YrYay5Ro33uFFuF7JC.Kx1"; ##
SECRET-DATA
            }
        }
```

```
        user reed {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "$1$KqBOyZR6$6S3oixOhSklN/j1TUXK210"; ##
SECRET-DATA
            }
        }
    }
    services {
        web-management {
            http;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        host 199.4.29.21 {
            any any;
            match RT_FLOW_SESSION;
            log-prefix SRX-KSK-CJR;
        }
        host 199.4.28.21 {
            any any;
            match RT_FLOW_SESSION;
            log-prefix SRX-KSK-CJR;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
        source-address 199.4.29.196;
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    archival {
        configuration {
            transfer-on-commit;
            archive-sites {
                "scp://srxkskcjr@199.4.29.21:/home/srxkskcjr" password
```

```
"$9$fQ6A0BIcre5QORSyKv-VwYoGik.TF/
"; ## SECRET-DATA
            }
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    processes {
        idp-policy disable;
    }
    ntp {
        server 199.4.29.17;
        server 199.4.29.27;
        source-address 10.4.29.1;
    }
}
interfaces {
    interface-range interfaces-trust {
        member ge-0/0/1;
        member fe-0/0/2;
        member fe-0/0/3;
        member fe-0/0/4;
        member fe-0/0/5;
        member fe-0/0/6;
        member ge-0/0/0;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/7 {
        speed 100m;
        link-mode full-duplex;
        fastether-options {
            no-auto-negotiation;
        }
        unit 0 {
            family inet {
                address 199.4.29.196/29;
            }
```

```
        }
    }
    vlan {
        unit 0 {
            family inet {
                address 10.4.29.1/32;
            }
        }
    }
}
snmp {
    community dnss3c {
        clients {
            10.4.29.253/32;
        }
    }
    trap-options {
        source-address 199.4.29.196;
        agent-address outgoing-interface;
    }
    trap-group kskeast {
        categories {
            authentication;
            link;
            routing;
            startup;
            configuration;
            services;
        }
        targets {
            199.4.29.21;
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 199.4.29.193;
    }
}
security {
    ssh-known-hosts {
        host 199.4.29.21 {
            rsa-key
AAAAB3NzaC1yc2EAAAABIwAAAQEA4so1gB6EcqjcP7WTbIm4/6ZOqqYfFI3MRl7HiO2C2C1UML2
jyaHAvQqO/
5LtqbKyPoZ38huGEGgYMqsMDaga+lIiKpu+2sJysG6HHnH+ZPw0eQ24RnTMxGaZjfCKR+/
```

```
GDQDnrpyZG0st8jlbSLPjVnQFzwMbAW2A0r
cqDkSINEkb5vyzDeZxQTpBrHRwQDJeW9m87GxalHJo7sqz91blpsC7K2XaE7ypMQnEdOxY2mE4j
zF/OzNaNZVcWiN9YSeAPmRKybIbHcL
X9Gn3K8IPJGlEVMMfwrWxhSj7iFl6Gr6gi+rQvTVepDKgw0s6JLJY2hTGHRIbFQ2/c/
PpxsrqmQ==;
        }
    }
    nat {
        source {
            rule-set trust-to-untrust {
                from zone trust;
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
    zones {
        security-zone trust {
            address-book {
                address localnet 10.4.29.0/24;
            }
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                vlan.0;
            }
        }
        security-zone untrust {
            address-book {
                address icanndns 199.4.28.0/22;
                address simplexgrinnell 12.30.47.110/32;
```

```
                address simplexgrinnell2 205.145.182.128/32;
            }
            interfaces {
                fe-0/0/7.0 {
                    host-inbound-traffic {
                        system-services {
                            dhcp;
                        }
                    }
                }
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy trust-to-untrust {
                match {
                    source-address localnet;
                    destination-address [ icanndns simplexgrinnell
simplexgrinnell2 ];
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
    }
}
applications {
    application sg {
        protocol udp;
        source-port 3060;
        destination-port 3061;
    }
    application sg2 {
        protocol udp;
        source-port 3065;
        destination-port 3061;
    }
}
vlans {
    vlan-trust {
```

```
        vlan-id 3;
        l3-interface vlan.0;
    }
}
```