ICANN DNSSEC Key Ceremony 8 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

J. ABLEY CA.

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	Joseph Abley		2 Feb 2012	23 47.
IW1/IKOS	Tomofumi Okubo		2 Feb 2012	23:51
SA1	Alexander Kulik		2 Feb 2012	23:48
SSC1	Anand Mishra		2 Feb 2012	23:50
SSC2	Geoff Bickers		2 Feb 2012	23:48
CO1	Masato Minda /JP		2 Feb 2012	
CO4	Carlos Martinez /UY		2 Feb 2012	2349
CO5	Edward Lewis /US		2 Feb 2012	2350
CO7	Subramanian Moonesamy /MU		2 Feb 2012	23:49
EW1	Alejandro Bolivar		2 Feb 2012	23:48
EW2	James Adair		2 Feb 2012	23:48
EW3	~~Desiree Miloshevic~~		2 Feb 2012	
EW4	Kenneth Michaels		2 Feb 2012	23:49
EW5	~~Exavier Chabata~~		2 Feb 2012	
EW6	Naela Sarras		2 Feb 2012	23:50
EW7	Nicoleta Munteanu		2 Feb 2012	23:50
EW8	~~Martin Levy~~		2 Feb 2012	
EW9	Selina Harrington		2 Feb 2012	23:50
CA2	Mehmet Akcin		2 Feb 2012	
IW2	Francisco Arias		2 Feb 2012	23:49
SA2	Matt Childs		2 Feb 2012	23:51

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	SA starts video recording and online streaming. SAs or IWs escort participants into the Ceremony Room and all participants sign into the Ceremony Room log.	J.A	21:14

Emergency Evacuation Procedures

Step	Activity	Initial	Time
2	CA or IW reviews emergency evacuation procedures with participants.	J.A	21:15

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: 2/2/2012 21:15 All entries into this script or any logs should follow this common source of time.	J.A	21:15

Open Credential Safe #2

Step	Activity	Initial	Time
4	CA and IW1 escort SSC2 and COs into the safe room together.	J.A	21:16
5	SSC2, while shielding combination from camera, opens Safe #2.	J.A	21:18
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.	J.A	21:19

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. **# Common Key is bottom lock and CO Key is top lock** 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: Masato Minda** **Box 1788** ✓ **OP TEB # A14365423** ✓ **SO TEB # A13004340** ✓ **CO4: Carlos Martinez** **Box 1068** ✓ **OP TEB # A14365443** ✓ **SO TEB # A13004311** ✓ **CO5: Edward Lewis** **Box 1790** ✓ **OP TEB # A16608560** ✓ **SO TEB # A13004326** ✓ **CO7: Subramanian Moonesamy** **Box 1792** ✓ **OP TEB # A14365378** ✓ **SO TEB # A16608556** ✓	JC	21:29

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.	JC	21:30
9	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and card reader indicator is green.	JC	21:30
10	IW1, CA, SSC2, and COs leave safe room, with OP cards in TEBs, closing the door behind them.	JC	21:31

OS/DVD Acceptance Test

Step	Activity	Initial	Time

11	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/disk1 (or /dev/scd0..etc)` < sub-i
	`openssl dgst -sha256 /dev/disc1 (or /dev/scd0..etc)`
	`hdiutil eject /dev/disk1 (or /dev/scd0..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
		T.O	21:43

12	CA repeats above for a second new O/S DVD.	T.O	21:44
13	IW records date, time and signature here upon successful completion: Date 2/2/2012 Time 21:44 Printed Name **Tomofumi Okubo** Signature	T.O	21:44

Open Equipment Safe #1

Step	Activity	Initial	Time
14	CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	T.O	21:46
15	SSC1, while shielding combination from camera, opens Safe #1.	T.O	21:48
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.	T.O	21:49

Remove Equipment from Safe #1

Step	Activity	Initial	Time
17	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# A2826715 / serial # K6002020** Verify the integrity of the other HSM that will not be in used this time. **HSM2: TEB# A2826772 / serial # K6002018 (last used)**	T.O	21:52

Step	Activity	Initial	Time
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# A2826774 / serial# 37240147333** **O/S DVDs (Rev 575): TEB# A14365427** **HSMFD: TEB # A14365428** **Verify the integrity of the other Laptop that will not be in used this time.** **Laptop #2: TEB A2734916 / serial # 7292928457**	J.G	21:56

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.	J.G	21:57
20	SSC1 puts log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and door indicator light is green.	J.G	21:57
21	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.	J.G	21:58

Set Up Laptop

Step	Activity	Initial	Time
22	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# A2826774 / serial# 37240147333**	J.G	21:59
23	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).	J.G	22:03
24	CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.	J.G	22:04

25	CA enters the commands
	`system-config-display --noui`
	and
	`killall Xorg`
	CA ensures that external display works.
		J.G	22:10

26	CA logs in as root.	J.G	22:11
27	CA configures printer as default and prints test page by going to **System > Administration > Printing**.	J.G	22:12
28	CA opens a terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal**.	J.G	22:13

(Exception)

Step	Activity	Initial	Time
29	CA checks and fixes date and time on laptop based on wall clock ensuring UTC time zone has been chosen by going to **System > Administration > Date and Time.**		
30	CA inserts USB port expander into laptop.		
31	CA inspects the HSMFD TEB for tamper evidence; reads out TEB # and 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 # A14365428** ✓		
32	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
33	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`		
34	CA executes `script script-20120202.log` to start a capture of terminal output.		

Start Logging HSM Output

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

36	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
37	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# A2826715 / serial # K6002020**	T.A	22:19
38	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	T.A	22:20
39	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.)	T.A	22:21

Enable/Activate HSM

Step	Activity	Initial	Time
40	CA calls the CO, CO opens TEB with OP card and hands to CA who places card in cardholder visible to all.	T.A	22:22
41	Repeat the step above until all OP cards are placed on the cardholder.	T.A	22:23
42	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 1 of 7 2nd OP card 5 of 7 3rd OP card 7 of 7	T.A	22:26

Check Network between Laptop and HSM

Step	Activity	Initial	Time
43	CA connects HSM to laptop using Ethernet cable.	T.A	22:27
44	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.	T.A	22:27

VERISIGN

12061 Bluemont Way
Reston, Va. 20190
T: 703-948-3200
F: 701-987-6543

VerisignInc.com

January 9th, 2012

To Whom It May Concern:

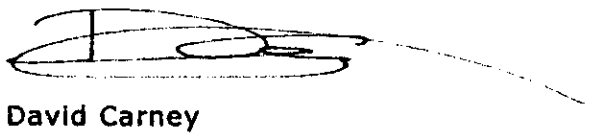
This is a letter of Verification of Employment for James Adair. Verisign, Inc. has employed James Adair full-time since October 4th, 2004 as a Senior Engineer in our Info Services/Corporate Naming Resolution Operations department.

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,



David Carney
HR Services Consultant | Verisign, Inc. | 703-948-4143 | dcarney@verisign.com

VERISIGN

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200
f: 703-987-6543

VerisignInc.com

2 February 2012

The SHA256 hash of the 2012 Q2 KSR file is:

B6A08C6354664251352BC30470D703CC685DA25F36889FC22C895DD0B
B180661

The PGP wordlist for the hash above is:

Scotland Orlando offload Galveston eating gossamer
crowfoot enchanting chopper Cherokee snowcap alkali
guidance stethoscope acme revolver frighten filament
rebirth forever Christmas maritime quota repellent
Burbank matchmaker exceed savagery shamrock
borderline afflict frequency

Attested on behalf of VeriSign by:

James Adair
Senior Engineer, Cryptographic Business Operations
VeriSign, Inc.

Insert Copy of KSR to be signed

Step	Activity	Initial	Time
45	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.	7.Q	22:29

Sign it with our KSK

Step	Activity	Initial	Time
46	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2012-q2-0.xml`	7.Q	22:30

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initial	Time
47	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: James Adair	7.Q	22:31
48	Participants match the hash read out with that displayed on the terminal. CA asks "are there are any objections"?	7.Q	22:32
49	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-q2-0.xml`	7.Q	22:32

```
$ 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-2012-q2-0.xml (at Thu Feb  2 22:29:28 2
012 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:          K6002020

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-01-01T00:00:00 2012-01-15T23:59:59  55231,51201   19036
2  2012-01-11T00:00:00 2012-01-25T23:59:59  51201         19036
3  2012-01-21T00:00:00 2012-02-04T23:59:59  51201         19036
4  2012-01-31T00:00:00 2012-02-14T23:59:59  51201         19036
5  2012-02-10T00:00:00 2012-02-24T23:59:59  51201         19036
6  2012-02-20T00:00:00 2012-03-05T23:59:59  51201         19036
7  2012-03-01T00:00:00 2012-03-15T23:59:59  51201         19036
8  2012-03-11T00:00:00 2012-03-25T23:59:59  51201         19036
9  2012-03-21T00:00:00 2012-04-05T23:59:59  56158,51201   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2012-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-04-01T00:00:00 2012-04-15T23:59:59  56158,51201
2  2012-04-11T00:00:00 2012-04-25T23:59:59  56158
3  2012-04-21T00:00:00 2012-05-05T23:59:59  56158
4  2012-05-01T00:00:00 2012-05-15T23:59:59  56158
5  2012-05-11T00:00:00 2012-05-25T23:59:59  56158
6  2012-05-21T00:00:00 2012-06-04T23:59:59  56158
7  2012-05-31T00:00:00 2012-06-14T23:59:59  56158
8  2012-06-10T00:00:00 2012-06-24T23:59:59  56158
9  2012-06-20T00:00:00 2012-07-05T23:59:59  50398,56158
...PASSED.

SHA256 hash of KSR:
B6A08C6354664251352BC30470D703CC685DA25F36889FC22C895DD0BB180661
>> Scotland Orlando offload Galveston eating gossamer crowfoot enchanting chopper Chero
kee snowcap alkali guidance stethoscope acme revolver frighten filament rebirth forever
 Christmas maritime quota repellent Burbank matchmaker exceed savagery shamrock borderl
ine afflict frequency <<

Generated new SKR in /media/KSR/skr-root-2012-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-04-01T00:00:00 2012-04-15T23:59:59  56158,51201   19036
```

```
2  2012-04-11T00:00:00 2012-04-25T23:59:59  56158          19036
3  2012-04-21T00:00:00 2012-05-05T23:59:59  56158          19036
4  2012-05-01T00:00:00 2012-05-15T23:59:59  56158          19036
5  2012-05-11T00:00:00 2012-05-25T23:59:59  56158          19036
6  2012-05-21T00:00:00 2012-06-04T23:59:59  56158          19036
7  2012-05-31T00:00:00 2012-06-14T23:59:59  56158          19036
8  2012-06-10T00:00:00 2012-06-24T23:59:59  56158          19036
9  2012-06-20T00:00:00 2012-07-05T23:59:59  56158,50398    19036

SHA256 hash of SKR:
1298680C128C29505E03ED1FC34BB15855DF092BAF45A140FBF2DE4C5A8BE07D
>> atlas narrative frighten article atlas megaton breakup embezzle eyeglass aggregate t
unnel businessman snowcap disable sailboat everyday edict therapist Algol Cherokee rock
er detector ratchet Dakota watchword vagabond tactics disbelief enlist Medusa tapeworm
insincere <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Print Copies of the Operation for Participants

Step	Activity	Initial	Time
50	CA prints out a sufficient number of copies for participants using `printlog ksrsigner-20120202-*.log N` where ksrsigner-20120202-*.log is replaced by log output file displayed by program. (this example generates N copies) and hands copies to participants.	J.A	22:36
51	IW1 attaches a copy to his/her script.	J.A	22:38

Backup Newly Created SKR

Step	Activity	Initial	Time
52	CA copies the contents of the KSR FD by running `cp -p /media/KSR/* .` for posting back to RZM.	J.A	22:38

53	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`
		J.A	22:39

54	CA removes **KSR** FD containing SKR and gives it to the RZM representative.	J.A	22:40

Disable/Deactivate HSM

Step	Activity	Initial	Time
55	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 4 of 7 2nd OP card 7 of 7 3rd OP card 1 of 7 Confirm the ready light turns off.	J.A	22:42

```
Script started on Thu 02 Feb 2012 10:16:41 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=1.06 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.257 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.253 ms

--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.253/0.525/1.066/0.382 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner Kjqmt7\033[Kv
/media/KSR/ksr-root\033[K-2012-q2-0.xml
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2012-q2-0.xml (at Thu Feb  2 22:29:28
2012 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:         K6002020

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-01-01T00:00:00 2012-01-15T23:59:59 55231,51201   19036
2  2012-01-11T00:00:00 2012-01-25T23:59:59 51201         19036
3  2012-01-21T00:00:00 2012-02-04T23:59:59 51201         19036
4  2012-01-31T00:00:00 2012-02-14T23:59:59 51201         19036
5  2012-02-10T00:00:00 2012-02-24T23:59:59 51201         19036
6  2012-02-20T00:00:00 2012-03-05T23:59:59 51201         19036
7  2012-03-01T00:00:00 2012-03-15T23:59:59 51201         19036
8  2012-03-11T00:00:00 2012-03-25T23:59:59 51201         19036
9  2012-03-21T00:00:00 2012-04-05T23:59:59 56158,51201   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2012-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-04-01T00:00:00 2012-04-15T23:59:59 56158,51201
2  2012-04-11T00:00:00 2012-04-25T23:59:59 56158
3  2012-04-21T00:00:00 2012-05-05T23:59:59 56158
4  2012-05-01T00:00:00 2012-05-15T23:59:59 56158
5  2012-05-11T00:00:00 2012-05-25T23:59:59 56158
6  2012-05-21T00:00:00 2012-06-04T23:59:59 56158
7  2012-05-31T00:00:00 2012-06-14T23:59:59 56158
8  2012-06-10T00:00:00 2012-06-24T23:59:59 56158
9  2012-06-20T00:00:00 2012-07-05T23:59:59 50398,56158
...PASSED.

SHA256 hash of KSR:
B6A08C6354664251352BC30470D703CC685DA25F36889FC22C895DD0BB180661
>> Scotland Orlando offload Galveston eating gossamer crowfoot enchanting chopper Cher
okee snowcap alkali guidance stethoscope acme revolver frighten filament rebirth forev
er Christmas maritime quota repellent Burbank matchmaker exceed savagery shamrock bord
erline afflict frequency <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2012-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-04-01T00:00:00 2012-04-15T23:59:59 56158,51201   19036
2  2012-04-11T00:00:00 2012-04-25T23:59:59 56158         19036
3  2012-04-21T00:00:00 2012-05-05T23:59:59 56158         19036
4  2012-05-01T00:00:00 2012-05-15T23:59:59 56158         19036
5  2012-05-11T00:00:00 2012-05-25T23:59:59 56158         19036
6  2012-05-21T00:00:00 2012-06-04T23:59:59 56158         19036
7  2012-05-31T00:00:00 2012-06-14T23:59:59 56158         19036
8  2012-06-10T00:00:00 2012-06-24T23:59:59 56158         19036
9  2012-06-20T00:00:00 2012-07-05T23:59:59 56158,50398   19036

SHA256 hash of SKR:
1298680C128C29505E03ED1FC34BB15855DF092BAF45A140FBF2DE4C5A8BE07D
>> atlas narrative frighten article atlas megaton breakup embezzle eyeglass aggregate
tunnel businessman snowcap disable sailboat everyday edict therapist Algol Cherokee ro
cker detector ratchet Dakota watchword vagabond tactics disbelief enlist Medusa tapewo
rm insincere <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20120202-222928.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# printlog ksrsigner-20120
202-2229\033[K\033[K\033[K\033[K\033[K*.log 20
[ 2 pages * 20 copy ] sent to printer
3 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -p /media/KSR/* .
cp: overwrite './skr.xml'? y
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -lt /media/KSR
\033[00mtotal 112
-rwxr-xr-x 1 root root 18424 Feb  2 22:32 \033[00;32mskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18424 Feb  2 22:32 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 15591 Jan  9 19:14 \033[00;32mksr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18422 Sep 30 18:18 \033[00;32mskr.xml.20120202222928\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]#
\033[00mtotal 904
-rwxr-xr-x 1 root root   8290 Feb  2 22:44 \033[00;32mttyaudit-ttyUSB0-20120202-22181
.log\033[00m
-rwxr-xr-x 1 root root   5509 Feb  2 22:32 \033[00;32mksrsigner-20120202-222928.log
\033[00m
-rwxr-xr-x 1 root root   4096 Feb  2 22:32 \033[00;32mscript-20120202.log\033[00m
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 \033[00;32mskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 \033[00;32mskr.xml\033[00m
drwxr-xr-x 2 root root   4096 Feb  2 22:32 \033[00;34mtmp\033[00m
-rwxr-xr-x 1 root root  15591 Jan  9 19:14 \033[00;32mksr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root  18422 Sep 30 18:18 \033[00;32mskr.xml.20120202222928\033[00m
-rwxr-xr-x 1 root root  32768 Jul 20  2011 \033[00;32mscript-20110720.log\033[00m
-rwxr-xr-x 1 root root   8044 Jul 20  2011 \033[00;32mttyaudit-ttyUSB0-20110720-20501
.log\033[00m
-rwxr-xr-x 1 root root   5508 Jul 20  2011 \033[00;32mksrsigner-20110720-205839.log
\033[00m
-rwxr-xr-x 1 root root  18404 Jul 20  2011 \033[00;32mskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root  15551 Jul 19  2011 \033[00;32mksr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root  18402 May 11  2011 \033[00;32mskr.xml.20110720205839\033[00m
-rwxr-xr-x 1 root root  20709 Feb  7  2011 \033[00;32mscript-20110207.log\033[00m
-rwxr-xr-x 1 root root  13997 Feb  7  2011 \033[00;32mttyaudit-ttyUSB0-20110207-22181
.log\033[00m
-rwxr-xr-x 1 root root   5524 Feb  7  2011 \033[00;32mksrsigner-20110207-223256.log
\033[00m
-rwxr-xr-x 1 root root  18402 Feb  7  2011 \033[00;32mskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root    188 Feb  7  2011 \033[00;32mksrsigner-20110207-223245.log
```

```
\033[00m
-rwxr-xr-x 1 root root  15547 Jan  2  2011 \033[00;32mksr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root  18402 Nov  1  2010 \033[00;32mskr.xml.20110207223256\033[00m
-rwxr-xr-x 1 root root  12956 Jul 13  2010 \033[00;32mscript-20100712.log\033[00m
-rwxr-xr-x 1 root root  38221 Jul 13  2010 \033[00;32mttyaudit-ttyUSB1-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root  36885 Jul 13  2010 \033[00;32mttyaudit-ttyUSB0-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root   5506 Jul 12  2010 \033[00;32mksrsigner-20100712-224426.log
\033[00m
-rwxr-xr-x 1 root root  18364 Jul 12  2010 \033[00;32mskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root  18364 Jul 12  2010 \033[00;32mskr.xml.20100712224426\033[00m
-rwxr-xr-x 1 root root   1400 Jul 12  2010 \033[00;32mksrsigner-20100712-224252.log
\033[00m
-rwxr-xr-x 1 root root  15547 Jul  8  2010 \033[00;32mksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root  15547 Jul  8  2010 \033[00;32mwksr_1_20100708144111_14165_198.
41.3.50_ksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root  30915 Jul  8  2010 \033[00;32mwksr-20100708-144111.log\033[00m
-rwxr-xr-x 1 root root   4096 Jun 16  2010 \033[00;32mscript-20100616-2209utc.log\033[
00m
-rwxr-xr-x 1 root root 196608 Jun 16  2010 \033[00;32mscript-20100616.log\033[00m
-rwxr-xr-x 1 root root   4473 Jun 16  2010 \033[00;32mksrsigner-20100616-214329.log
\033[00m
-rwxr-xr-x 1 root root  18364 Jun 16  2010 \033[00;32mskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root  45056 Jun 16  2010 \033[00;32mttyaudit-ttyUSB0-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root  36864 Jun 16  2010 \033[00;32mttyaudit-ttyUSB1-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root    765 Jun 16  2010 \033[00;32mKjqmt7v.csr\033[00m
-rwxr-xr-x 1 root root   2668 Jun 16  2010 \033[00;32mkskgen-20100616-211906.log\033[0
0m
-rwxr-xr-x 1 root root   1487 Jun 16  2010 \033[00;32mKSKSlotDB.db\033[00m
-rwxr-xr-x 1 root root    190 Jun 16  2010 \033[00;32mKSKSlotDB.config.db\033[00m
-rwxr-xr-x 1 root root  40555 Jun  9  2010 \033[00;32mwksr-20100517-172720.log\033[00m
-rwxr-xr-x 1 root root  15547 Jun  9  2010 \033[00;32mksr-root-2010-q3-2.xml\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# date
Thu Feb  2 22:45:57 UTC 2012
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# mount
/dev/mapper/live-rw on / type ext3 (rw,noatime)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
/dev/sda1 on /media/HSMFD type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
/dev/sdb1 on /media/disk type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# %033[K\007mount
/dev/mapper/live-rw on / type ext3 (rw,noatime)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
/dev/sda1 on /media/HSMFD type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
/dev/sdb1 on /media/disk type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/disk
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -Rp * /media/HSMF%033
[KD%033[K_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -lt /d%033[K033[Kmedi
a/HSMFD_
\033[00mtotal 908
-rwxr-xr-x 1 root root   8192 Feb  2 22:45 \033[00;32mscript-20120202.log\033[00m
-rwxr-xr-x 1 root root   8290 Feb  2 22:44 \033[00;32mttyaudit-ttyUSB0-20120202-221813
.log\033[00m
-rwxr-xr-x 1 root root   5509 Feb  2 22:32 \033[00;32mksrsigner-20120202-222928.log
\033[00m
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 \033[00;32mskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 \033[00;32mskr.xml\033[00m
drwxr-xr-x 2 root root   4096 Feb  2 22:32 \033[00;34mtmp\033[00m
-rwxr-xr-x 1 root root  15591 Jan  9 19:14 \033[00;32mksr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root  18422 Sep 30 18:18 \033[00;32mskr.xml.20120202222928\033[00m
-rwxr-xr-x 1 root root  32768 Jul 20  2011 \033[00;32mscript-20110720.log\033[00m
-rwxr-xr-x 1 root root   8044 Jul 20  2011 \033[00;32mttyaudit-ttyUSB0-20110720-20501
.log\033[00m
-rwxr-xr-x 1 root root   5508 Jul 20  2011 \033[00;32mksrsigner-20110720-205839.log
\033[00m
-rwxr-xr-x 1 root root  18404 Jul 20  2011 \033[00;32mskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root  15551 Jul 19  2011 \033[00;32mksr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root  18402 May 11  2011 \033[00;32mskr.xml.20110720205839\033[00m
-rwxr-xr-x 1 root root  20709 Feb  7  2011 \033[00;32mscript-20110207.log\033[00m
-rwxr-xr-x 1 root root  13997 Feb  7  2011 \033[00;32mttyaudit-ttyUSB0-20110207-22181
.log\033[00m
-rwxr-xr-x 1 root root   5524 Feb  7  2011 \033[00;32mksrsigner-20110207-223256.log
\033[00m
-rwxr-xr-x 1 root root  18402 Feb  7  2011 \033[00;32mskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root    188 Feb  7  2011 \033[00;32mksrsigner-20110207-223245.log
\033[00m
-rwxr-xr-x 1 root root  15547 Jan  2  2011 \033[00;32mksr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root  18402 Nov  1  2010 \033[00;32mskr.xml.20110207223256\033[00m
-rwxr-xr-x 1 root root  12956 Jul 13  2010 \033[00;32mscript-20100712.log\033[00m
-rwxr-xr-x 1 root root  38221 Jul 13  2010 \033[00;32mttyaudit-ttyUSB1-20100712-21254
.log\033[00m
-rwxr-xr-x 1 root root  36885 Jul 13  2010 \033[00;32mttyaudit-ttyUSB0-20100712-21254
.log\033[00m
-rwxr-xr-x 1 root root   5506 Jul 12  2010 \033[00;32mksrsigner-20100712-224426.log
\033[00m
-rwxr-xr-x 1 root root  18364 Jul 12  2010 \033[00;32mskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root  18364 Jul 12  2010 \033[00;32mskr.xml.20100712224426\033[00m
-rwxr-xr-x 1 root root   1400 Jul 12  2010 \033[00;32mksrsigner-20100712-224252.log
\033[00m
-rwxr-xr-x 1 root root  15547 Jul  8  2010 \033[00;32mksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root  15547 Jul  8  2010 \033[00;32mwksr_1_20100708144111_14165_198
41.3.50_ksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root  30915 Jul  8  2010 \033[00;32mwksr-20100708-144111.log\033[00
-rwxr-xr-x 1 root root   4096 Jun 16  2010 \033[00;32mscript-20100616-2209utc.log\033
00m
-rwxr-xr-x 1 root root 196608 Jun 16  2010 \033[00;32mscript-20100616.log\033[00m
-rwxr-xr-x 1 root root   4473 Jun 16  2010 \033[00;32mksrsigner-20100616-214329.log
\033[00m
-rwxr-xr-x 1 root root  18364 Jun 16  2010 \033[00;32mskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root  45056 Jun 16  2010 \033[00;32mttyaudit-ttyUSB0-20100616-18215
.log\033[00m
-rwxr-xr-x 1 root root  36864 Jun 16  2010 \033[00;32mttyaudit-ttyUSB1-20100616-18215
.log\033[00m
-rwxr-xr-x 1 root root    765 Jun 16  2010 \033[00;32mKjqmt7v.csr\033[00m
-rwxr-xr-x 1 root root   2668 Jun 16  2010 \033[00;32mkskgen-20100616-211906.log\033[
0m
-rwxr-xr-x 1 root root   1487 Jun 16  2010 \033[00;32mKSKSlotDB.db\033[00m
-rwxr-xr-x 1 root root    190 Jun 16  2010 \033[00;32mKSKSlotDB.config.db\033[00m
-rwxr-xr-x 1 root root  40555 Jun  9  2010 \033[00;32mwksr-20100517-172720.log\033[0
-rwxr-xr-x 1 root root  15547 Jun  9  2010 \033[00;32mksr-root-2010-q3-2.xml\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/HSM
D_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/disk
```

```
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# mount
/dev/mapper/live-rw on / type ext3 (rw,noatime)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
/dev/sda1 on /media/HSMFD type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
/dev/sdb1 on /media/KSK7-AUDIT type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0
)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/KSK7-AUDIT
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# uM033[K033[KmpouN033[K
\033[K033[K033[KopuN033[K033[K033[Kunt
/dev/mapper/live-rw on / type ext3 (rw,noatime)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
/dev/sda1 on /media/HSMFD type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
/dev/sdb1 on /media/KSK7-AUDIT type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0
)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/KSK7-AUDIT
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# M033[Knkfs\033[K033[K033
[K033[K033[Kmkfs.vfat /dev/sdl033[Kb1
mkfs.vfat 2.11 (12 Mar 2005)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# which fslabel
/usr/bin/which: no fslabel in (.:/opt/icann/bin:/opt/Keyper/bin:/usr/kerberos/sbin:/us
r/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6
/bin:/root/bin)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# fdisk -l /dev/sdb1

Disk /dev/sdb1: 2102 MB, 2102349312 bytes
65 heads, 62 sectors/track, 1018 cylinders
Units = cylinders of 4030 * 512 = 2063360 bytes

     Device Boot      Start         End      Blocks   Id  System
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# mount
/dev/mapper/live-rw on / type ext3 (rw,noatime)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
/dev/sda1 on /media/HSMFD type vfat (rw,noexec,nosuid,nodev,shortname=winnt,uid=0)
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -Rp * /media/HSMFD_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -lt /media/HSMFD_ | m
ore
total 916
-rwxr-xr-x 1 root root  16384 Feb  2 22:52 script-20120202.log
-rwxr-xr-x 1 root root   8290 Feb  2 22:44 ttyaudit-ttyUSB0-20120202-221813.log
-rwxr-xr-x 1 root root   5509 Feb  2 22:32 ksrsigner-20120202-222928.log
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 skr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 skr.xml
drwxr-xr-x 2 root root   4096 Feb  2 22:32 tmp
-rwxr-xr-x 1 root root  15591 Jan  9 19:14 ksr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root  18422 Sep 30 18:18 skr.xml.20120202222928
-rwxr-xr-x 1 root root  32768 Jul 20  2011 script-20110720.log
-rwxr-xr-x 1 root root   8044 Jul 20  2011 ttyaudit-ttyUSB0-20110720-205011.log
-rwxr-xr-x 1 root root   5508 Jul 20  2011 ksrsigner-20110720-205839.log
-rwxr-xr-x 1 root root  18404 Jul 20  2011 skr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root  15551 Jul 19  2011 ksr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root  18402 May 11  2011 skr.xml.20110720205839
-rwxr-xr-x 1 root root  20709 Feb  7  2011 script-20110207.log
-rwxr-xr-x 1 root root  13997 Feb  7  2011 ttyaudit-ttyUSB0-20110207-221818.log
-rwxr-xr-x 1 root root   5524 Feb  7  2011 ksrsigner-20110207-223256.log
-rwxr-xr-x 1 root root  18402 Feb  7  2011 skr-root-2011-q2-0.xml
-rwxr-xr-x 1 root root    188 Feb  7  2011 ksrsigner-20110207-223245.log
-rwxr-xr-x 1 root root  15547 Jan  2  2011 ksr-root-2011-q2-0.xml
-rwxr-xr-x 1 root root  18402 Nov  1  2010 skr.xml.20110207223256
-rwxr-xr-x 1 root root  12956 Jul 13  2010 script-20100712.log
-rwxr-xr-x 1 root root  38221 Jul 13  2010 ttyaudit-ttyUSB1-20100712-212549.log
-rwxr-xr-x 1 root root  36885 Jul 13  2010 ttyaudit-ttyUSB0-20100712-212549.log
-rwxr-xr-x 1 root root   5506 Jul 12  2010 ksrsigner-20100712-224426.log
-rwxr-xr-x 1 root root  18364 Jul 12  2010 skr-root-2010-q4-1.xml
\033[7mr-Mo[re\033[0m 18364 Jul 12  2010 skr.xml.20100712224426
-rwxr-xr-x 1 root root   1400 Jul 12  2010 ksrsigner-20100712-224252.log
-rwxr-xr-x 1 root root  15547 Jul  8  2010 ksr-root-2010-q4-1.xml
-rwxr-xr-x 1 root root  15547 Jul  8  2010 wksr_1_20100708144111_14165_198.41.3.50_
ksr-root-2010-q4-1.xml
-rwxr-xr-x 1 root root  30915 Jul  8  2010 wksr-20100708-144111.log
-rwxr-xr-x 1 root root   4096 Jun 16  2010 script-20100616-2209utc.log
-rwxr-xr-x 1 root root 196608 Jun 16  2010 script-20100616.log
-rwxr-xr-x 1 root root   4473 Jun 16  2010 ksrsigner-20100616-214329.log
-rwxr-xr-x 1 root root  18364 Jun 16  2010 skr-root-2010-q3-2.xml
-rwxr-xr-x 1 root root  45056 Jun 16  2010 ttyaudit-ttyUSB0-20100616-182157.log
-rwxr-xr-x 1 root root  36864 Jun 16  2010 ttyaudit-ttyUSB1-20100616-182157.log
-rwxr-xr-x 1 root root    765 Jun 16  2010 Kjqmt7v.csr
-rwxr-xr-x 1 root root   2668 Jun 16  2010 kskgen-20100616-211906.log
-rwxr-xr-x 1 root root   1487 Jun 16  2010 KSKSlotDB.db
-rwxr-xr-x 1 root root    190 Jun 16  2010 KSKSlotDB.config.db
-rwxr-xr-x 1 root root  40555 Jun  9  2010 wksr-20100517-172720.log
-rwxr-xr-x 1 root root  15547 Jun  9  2010 ksr-root-2010-q3-2.xml
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/HSNBK033[
\033[K033[KMFD_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -Rp * /media/HSMFD+
\033[K_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# [illegible]
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 | more
total 916
-rwxr-xr-x 1 root root  16384 Feb  2 22:52 script-20120202.log
-rwxr-xr-x 1 root root   8290 Feb  2 22:44 ttyaudit-ttyUSB0-20120202-221813.log
-rwxr-xr-x 1 root root   5509 Feb  2 22:32 ksrsigner-20120202-222928.log
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 skr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root  18424 Feb  2 22:32 skr.xml
drwxr-xr-x 2 root root   4096 Feb  2 22:32 tmp
-rwxr-xr-x 1 root root  15591 Jan  9 19:14 ksr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root  18422 Sep 30 18:18 skr.xml.20120202222928
-rwxr-xr-x 1 root root  32768 Jul 20  2011 script-20110720.log
-rwxr-xr-x 1 root root   8044 Jul 20  2011 ttyaudit-ttyUSB0-20110720-205011.log
-rwxr-xr-x 1 root root   5508 Jul 20  2011 ksrsigner-20110720-205839.log
-rwxr-xr-x 1 root root  18404 Jul 20  2011 skr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root  15551 Jul 19  2011 ksr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root  18402 May 11  2011 skr.xml.20110720205839
-rwxr-xr-x 1 root root  20709 Feb  7  2011 script-20110207.log
-rwxr-xr-x 1 root root  13997 Feb  7  2011 ttyaudit-ttyUSB0-20110207-221818.log
-rwxr-xr-x 1 root root   5524 Feb  7  2011 ksrsigner-20110207-223256.log
-rwxr-xr-x 1 root root  18402 Feb  7  2011 skr-root-2011-q2-0.xml
-rwxr-xr-x 1 root root    188 Feb  7  2011 ksrsigner-20110207-223245.log
-rwxr-xr-x 1 root root  15547 Jan  2  2011 ksr-root-2011-q2-0.xml
-rwxr-xr-x 1 root root  18402 Nov  1  2010 skr.xml.20110207223256
-rwxr-xr-x 1 root root  12956 Jul 13  2010 script-20100712.log
-rwxr-xr-x 1 root root  38221 Jul 13  2010 ttyaudit-ttyUSB1-20100712-212549.log
-rwxr-xr-x 1 root root  36885 Jul 13  2010 ttyaudit-ttyUSB0-20100712-212549.log
```

```
-rwxr-xr-x 1 root root  5506 Jul 12  2010 ksrsigner-20100712-224426.log
-rwxr-xr-x 1 root root 18364 Jul 12  2010 skr-root-2010-q4-1.xml
\033[7m--More--\033[0m 18364 Jul 12  2010 skr.xml.20100712224426
-rwxr-xr-x 1 root root  1400 Jul 12  2010 ksrsigner-20100712-224252.log
-rwxr-xr-x 1 root root 15547 Jul  8  2010 ksr-root-2010-q4-1.xml
-rwxr-xr-x 1 root root 15547 Jul  8  2010 wksr_1_20100708144111_14165_198.41.3.50_
ksr-root-2010-q4-1.xml
-rwxr-xr-x 1 root root 30915 Jul  8  2010 wksr-20100708-144111.log
-rwxr-xr-x 1 root root  4096 Jun 16  2010 script-20100616-2209utc.log
-rwxr-xr-x 1 root root 196608 Jun 16  2010 script-20100616.log
-rwxr-xr-x 1 root root  4473 Jun 16  2010 ksrsigner-20100616-214329.log
-rwxr-xr-x 1 root root 18364 Jun 16  2010 skr-root-2010-q3-2.xml
-rwxr-xr-x 1 root root 45056 Jun 16  2010 ttyaudit-ttyUSB0-20100616-182157.log
-rwxr-xr-x 1 root root 36864 Jun 16  2010 ttyaudit-ttyUSB1-20100616-182157.log
-rwxr-xr-x 1 root root   765 Jun 16  2010 Kjqmt7v.csr
-rwxr-xr-x 1 root root  2668 Jun 16  2010 kskgen-20100616-211906.log
-rwxr-xr-x 1 root root  1487 Jun 16  2010 KSKSlotDB.db
-rwxr-xr-x 1 root root   190 Jun 16  2010 KSKSlotDB.config.db
-rwxr-xr-x 1 root root 40555 Jun  9  2010 wksr-20100517-172720.log   \033[2Pumount\033[C\033[C
-rwxr-xr-x 1 root root 15547 Jun  9  2010 ksr-root-2010-q3-2.xml
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -lt /media/HSMFD_ | m
\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[5Pcp -Rp * /media/HSM
33[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]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/HSMFD_ | m
\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[5Pcp -Rp * /media/HSM
FD_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# [illegible]
[illegible]
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[7Pumount /media/HSMFD
SMFD_ | more
total 920
-rwxr-xr-x 1 root root 20480 Feb  2 22:55 script-20120202.log
-rwxr-xr-x 1 root root  8290 Feb  2 22:44 ttyaudit-ttyUSB0-20120202-221813.log
-rwxr-xr-x 1 root root  5509 Feb  2 22:32 ksrsigner-20120202-222928.log
-rwxr-xr-x 1 root root 18424 Feb  2 22:32 skr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root 18424 Feb  2 22:32 skr.xml
drwxr-xr-x 2 root root  4096 Feb  2 22:32 tmp
-rwxr-xr-x 1 root root 15591 Jan  9 19:14 ksr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root 18422 Sep 30 18:18 skr.xml.20120202222928
-rwxr-xr-x 1 root root 32768 Jul 20  2011 script-20110720.log
-rwxr-xr-x 1 root root  8044 Jul 20  2011 ttyaudit-ttyUSB0-20110720-205011.log
-rwxr-xr-x 1 root root  5508 Jul 20  2011 ksrsigner-20110720-205839.log
-rwxr-xr-x 1 root root 18404 Jul 20  2011 skr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root 15551 Jul 19  2011 ksr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root 18402 May 11  2011 skr.xml.20110720205839
-rwxr-xr-x 1 root root 20709 Feb  7  2011 script-20110207.log
-rwxr-xr-x 1 root root 13997 Feb  7  2011 ttyaudit-ttyUSB0-20110207-221818.log
-rwxr-xr-x 1 root root  5524 Feb  7  2011 ksrsigner-20110207-223256.log
-rwxr-xr-x 1 root root 18402 Feb  7  2011 skr-root-2011-q2-0.xml
-rwxr-xr-x 1 root root   188 Feb  7  2011 ksrsigner-20110207-223245.log
-rwxr-xr-x 1 root root 15547 Jan  2  2011 ksr-root-2011-q2-0.xml
-rwxr-xr-x 1 root root 18402 Nov  1  2010 skr.xml.20110207223256
-rwxr-xr-x 1 root root 12956 Jul 13  2010 script-20100712.log
-rwxr-xr-x 1 root root 38221 Jul 13  2010 ttyaudit-ttyUSB1-20100712-212549.log
-rwxr-xr-x 1 root root 36885 Jul 13  2010 ttyaudit-ttyUSB0-20100712-212549.log
-rwxr-xr-x 1 root root  5506 Jul 12  2010 ksrsigner-20100712-224426.log
-rwxr-xr-x 1 root root 18364 Jul 12  2010 skr-root-2010-q4-1.xml
\033[7m--More--\033[0m 18364 Jul 12  2010 skr.xml.20100712224426
-rwxr-xr-x 1 root root  1400 Jul 12  2010 ksrsigner-20100712-224252.log
-rwxr-xr-x 1 root root 15547 Jul  8  2010 ksr-root-2010-q4-1.xml
-rwxr-xr-x 1 root root 15547 Jul  8  2010 wksr_1_20100708144111_14165_198.41.3.50_
ksr-root-2010-q4-1.xml
-rwxr-xr-x 1 root root 30915 Jul  8  2010 wksr-20100708-144111.log
-rwxr-xr-x 1 root root  4096 Jun 16  2010 script-20100616-2209utc.log
-rwxr-xr-x 1 root root 196608 Jun 16  2010 script-20100616.log
-rwxr-xr-x 1 root root  4473 Jun 16  2010 ksrsigner-20100616-214329.log
-rwxr-xr-x 1 root root 18364 Jun 16  2010 skr-root-2010-q3-2.xml
-rwxr-xr-x 1 root root 45056 Jun 16  2010 ttyaudit-ttyUSB0-20100616-182157.log
-rwxr-xr-x 1 root root 36864 Jun 16  2010 ttyaudit-ttyUSB1-20100616-182157.log
-rwxr-xr-x 1 root root   765 Jun 16  2010 Kjqmt7v.csr
-rwxr-xr-x 1 root root  2668 Jun 16  2010 kskgen-20100616-211906.log
-rwxr-xr-x 1 root root  1487 Jun 16  2010 KSKSlotDB.db
-rwxr-xr-x 1 root root   190 Jun 16  2010 KSKSlotDB.config.db
-rwxr-xr-x 1 root root 40555 Jun  9  2010 wksr-20100517-172720.log
-rwxr-xr-x 1 root root 15547 Jun  9  2010 ksr-root-2010-q3-2.xml
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -lt /media/HSMFD_ | m
\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[5Pcp -Rp * /media/HSM
\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]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/HSMFD_ | m
\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[5Pcp -Rp * /media/HSM
FD_
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# [illegible]
C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[illegible] | more
total 924
-rwxr-xr-x 1 root root 24576 Feb  2 22:55 script-20120202.log
-rwxr-xr-x 1 root root  8290 Feb  2 22:44 ttyaudit-ttyUSB0-20120202-221813.log
-rwxr-xr-x 1 root root  5509 Feb  2 22:32 ksrsigner-20120202-222928.log
-rwxr-xr-x 1 root root 18424 Feb  2 22:32 skr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root 18424 Feb  2 22:32 skr.xml
drwxr-xr-x 2 root root  4096 Feb  2 22:32 tmp
-rwxr-xr-x 1 root root 15591 Jan  9 19:14 ksr-root-2012-q2-0.xml
-rwxr-xr-x 1 root root 18422 Sep 30 18:18 skr.xml.20120202222928
-rwxr-xr-x 1 root root 32768 Jul 20  2011 script-20110720.log
-rwxr-xr-x 1 root root  8044 Jul 20  2011 ttyaudit-ttyUSB0-20110720-205011.log
-rwxr-xr-x 1 root root  5508 Jul 20  2011 ksrsigner-20110720-205839.log
-rwxr-xr-x 1 root root 18404 Jul 20  2011 skr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root 15551 Jul 19  2011 ksr-root-2011-q4-0.xml
-rwxr-xr-x 1 root root 18402 May 11  2011 skr.xml.20110720205839
-rwxr-xr-x 1 root root 20709 Feb  7  2011 script-20110207.log
-rwxr-xr-x 1 root root 13997 Feb  7  201
```

```
2012-02-02T22:20:19+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2012-02-02T22:20:19+0000        ttyUSB0
2012-02-02T22:20:20+0000        ttyUSB0
2012-02-02T22:20:20+0000        ttyUSB0 Battery OK!
2012-02-02T22:20:20+0000        ttyUSB0
2012-02-02T22:20:20+0000        ttyUSB0
2012-02-02T22:20:20+0000        ttyUSB0 No Tamper Counts in BBRAM!
2012-02-02T22:20:20+0000        ttyUSB0
2012-02-02T22:20:21+0000        ttyUSB0  Loading Application (APP)
2012-02-02T22:20:21+0000        ttyUSB0
2012-02-02T22:20:22+0000        ttyUSB0  Starting loaded code.
2012-02-02T22:20:22+0000        ttyUSB0
2012-02-02T22:20:22+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2012-02-02T22:20:22+0000        ttyUSB0
2012-02-02T22:20:24+0000        ttyUSB0 wdog started
2012-02-02T22:20:24+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running DES POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 DES POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running Triple DES POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Triple DES POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running AES POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 AES POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running SHA1 POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 SHA1 POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running SHA2 POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 SHA2 POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running RSA POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 RSA POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running DSA POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 DSA POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Running RandomGen POST Test
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 RandomGen POST Test Passed
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 Additional RandomGen POST Test Passed
```

```
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 2/2/2012 at 21:29:30
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0  0x100008
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0 App Details Response:
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:27+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Part Number: Keyper Pro 0405
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Serial Number: Serial K6002020
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 App Build Number: App 020
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 ABL Build Number: ABL 029
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 AL Build Number: AL 02A
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 CS Build Number: CS 029
2012-02-02T22:20:28+0000        ttyUSB0
```

```
2012-02-02T22:20:28+0000        ttyUSB0 Total Private Memory 4173393
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Free Private Memory 4173393
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Total Dynamic Memory 14569472
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Free Dynamic Memory 14569472
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Date and Time: 21:29:30 on 02/02/2012
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 Created socket 1 on port 3000.
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:28+0000        ttyUSB0 2/2/2012 at 21:29:31
2012-02-02T22:20:28+0000        ttyUSB0
2012-02-02T22:20:29+0000        ttyUSB0  0x100003
2012-02-02T22:20:29+0000        ttyUSB0
2012-02-02T22:25:08+0000        ttyUSB0
2012-02-02T22:25:08+0000        ttyUSB0
2012-02-02T22:25:08+0000        ttyUSB0 2/2/2012 at 21:34:11
2012-02-02T22:25:08+0000        ttyUSB0
2012-02-02T22:25:08+0000        ttyUSB0  0x200023 0A400000B706296E
2012-02-02T22:25:08+0000        ttyUSB0
2012-02-02T22:25:23+0000        ttyUSB0
2012-02-02T22:25:23+0000        ttyUSB0
2012-02-02T22:25:23+0000        ttyUSB0 2/2/2012 at 21:34:25
2012-02-02T22:25:23+0000        ttyUSB0
2012-02-02T22:25:23+0000        ttyUSB0  0x200024 0A4000009D86296E
2012-02-02T22:25:23+0000        ttyUSB0
2012-02-02T22:25:49+0000        ttyUSB0
2012-02-02T22:25:49+0000        ttyUSB0
2012-02-02T22:25:49+0000        ttyUSB0 2/2/2012 at 21:34:51
2012-02-02T22:25:49+0000        ttyUSB0
2012-02-02T22:25:49+0000        ttyUSB0  0x200023 0A4000009D86296E
2012-02-02T22:25:49+0000        ttyUSB0
2012-02-02T22:26:13+0000        ttyUSB0
2012-02-02T22:26:13+0000        ttyUSB0
2012-02-02T22:26:13+0000        ttyUSB0 2/2/2012 at 21:35:16
2012-02-02T22:26:13+0000        ttyUSB0
2012-02-02T22:26:13+0000        ttyUSB0  0x200023 0A400000B7C6296E
2012-02-02T22:26:13+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0 Created socket 1 on port 5000.
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0 2/2/2012 at 21:35:18
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:26:16+0000        ttyUSB0  0x100002
2012-02-02T22:26:16+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0 Accepted connection on address 210.147.192.168.0.1.
```

```
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0 ================================================================
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0 Free memory down from 14569472 to 11843072 (last mechanism 0)!
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0 21:38:48 on 02-02-2012
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:29:45+0000        ttyUSB0 ================================================================
2012-02-02T22:29:45+0000        ttyUSB0
2012-02-02T22:32:01+0000        ttyUSB0
2012-02-02T22:32:01+0000        ttyUSB0
2012-02-02T22:32:01+0000        ttyUSB0 Closing connection on address 210.147.192.168.0.1.
2012-02-02T22:32:01+0000        ttyUSB0
```

Return HSM to a TEB

Step	Activity	Initial	Time
56	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.	J.A	22:43
57	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM1: TEB# A2826760 / serial # K6002020** IW1 initials the TEB. CA places item on equipment cart.	J.A	22:44

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initial	Time
58	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of serial output terminal window.	J.A	22:45
59	CA stops logging terminal output by entering "exit" in the terminal window.	J.A	22:46

Backup HSM FD Contents (Approximately 10 minutes)

Step	Activity	Initial	Time
60	CA displays contents of HSMFD by executing `ls -lt`	J.A	22:46
61	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_`	J.A	22:48
62	CA displays contents of HSMFD_ by executing `ls -lt /media/HSMFD_`	J.A	22:48
63	CA unmounts new FD using `umount /media/HSMFD_`	J.A	22:49
64	CA removes HSMFD_ and places on table.	J.A	22:49
65	CA repeats steps above and creates 4 more copies. Check when completed. 2nd copy ✓ 3rd copy ✓ 4th copy ✓ 5th copy ✓	J.A	22:57

<exception!

<exception!

Print Logging Information

Step	Activity	Initial	Time

66	CA prints out hard copies of logging information by executing
	`enscript -2Gr -# 2 script-20120202.log`
	`enscript -Gr -# 2 --font="Courier8" ttyaudit-ttyUSB*-20120202-*.log`
	for attachment to IW1 and CA scripts.
		J.L	22:55

Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initial	Time

67	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
	CA removes HSMFD.
		J.A	23:12

68	After all print jobs are complete, CA executes `shutdown -hP now` removes DVD and turns off laptop.	J.A	23:13
69	CA places HSMFD and OS/DVD in TEB; writes date, time and "HSMFD" in amount field; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **HSMFD + O/S DVDs (Rev 600): TEB # A14365385** IW1 initials the TEB. CA places TEB on equipment cart.	J.A	23:15

Distribute HSMFDs

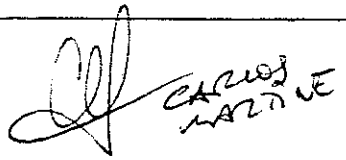
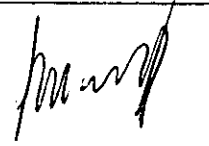
Step	Activity	Initial	Time
70	Remaining HSMFDs are distributed to IW1 (2 for audit bundles), CA (1), IKOS(1) to post SKR to RZM, and to review, analyze and improve on procedures.	J.A	23:16

Returning Laptop to a TEB

Step	Activity	Initial	Time
71	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# A2826759 / serial# 37240147333** IW1 initials the TEB. CA places TEB on equipment cart.	J.A	23:18

Returning OP Smartcards to TEBs

Step	Activity	Initial	Time
72	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.	JA	23:29

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1
CO1	OP 1 of 7	A14365386	Masato Minda		2 Feb 2012	23:24	
CO4	OP 4 of 7	A14365387	Carlos Martinez		2 Feb 2012	23:24	
CO5	OP 5 of 7	A14365388	Edward Lewis		2 Feb 2012	2326	
CO7	OP 7 of 7	A14365389	Subramanian Moonesamy		2 Feb 2012	23:27	

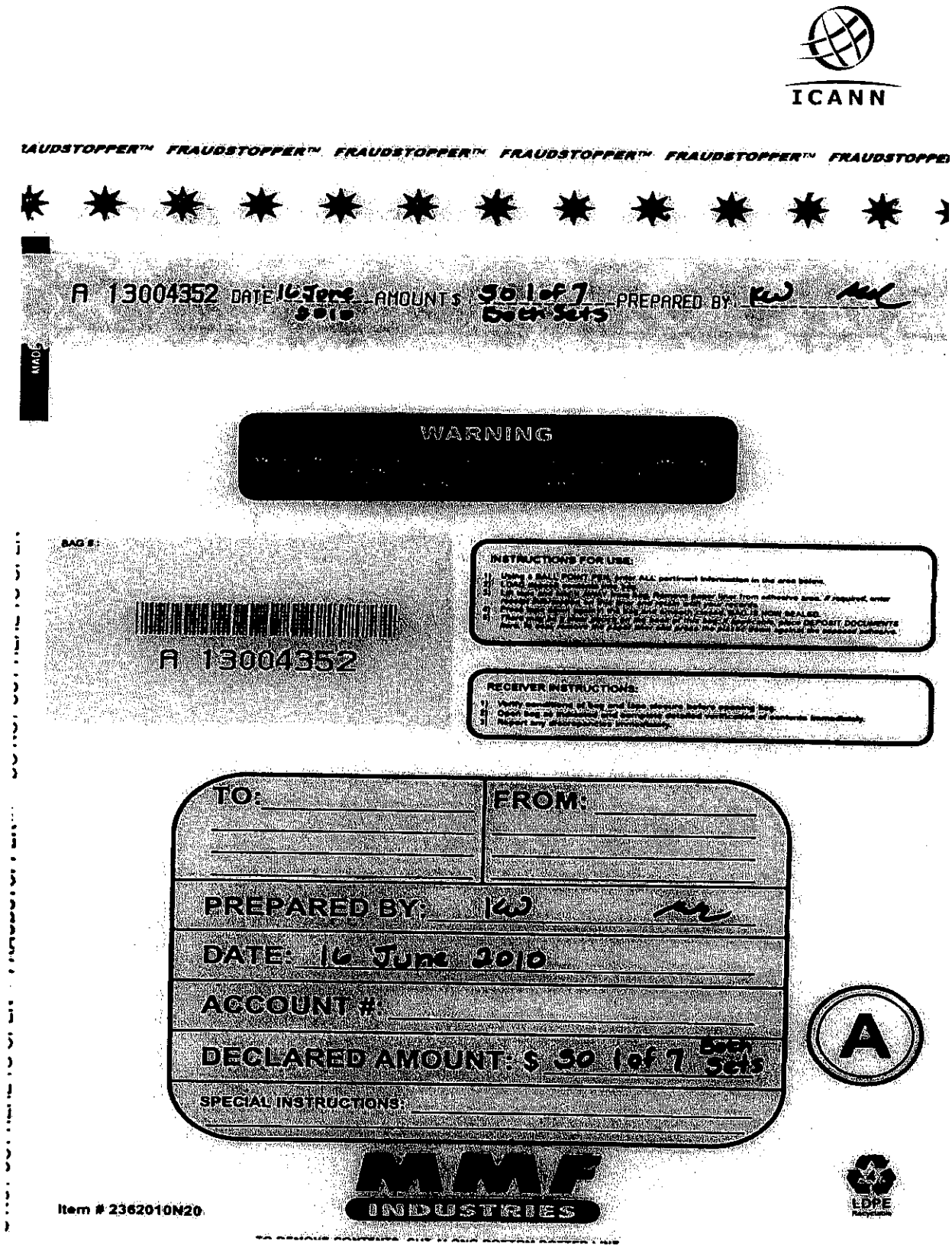

FRAUDSTOPPER™
A 13004352 DATE 16 June 2010 AMOUNT $ 30 1 of 7 Dark Sets PREPARED BY: KW
WARNING
BAG #:
A 13004352
INSTRUCTIONS FOR USE:
RECEIVER INSTRUCTIONS:
TO:
FROM:
PREPARED BY: KW
DATE: 16 June 2010
ACCOUNT #:
DECLARED AMOUNT: $ 30 1 of 7 Dark Sets
SPECIAL INSTRUCTIONS:
A
MMF INDUSTRIES
Item # 2362010N20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

Figure 2

Returning Equipment in TEBs to Safe #1

Step	Activity	Initial	Time
73	CA, IW1, SSC1 open safe room and enter with equipment cart.	J.C	23:30
74	SSC1 opens Safe #1 shielding combination from camera.	J.C	23:32
75	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.	J.C	23:33
76	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.	J.C	23:33
77	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.	J.C	23:34
78	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. HSMFD	J.C	23:35
79	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.		

Last (79)

Close Equipment Safe #1

Step	Activity	Initial	Time
80	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log.	J.C	23:35
81	SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise). IW1 and CA verify safe is locked and door indicator light is green.	J.C	23:36
82	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	J.C	23:36

Open Credential Safe #2

Step	Activity	Initial	Time
83	After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. COs bring their OP card TEB with them.	J.C	23:38
84	SSC2 opens Safe #2 while shielding combination from camera.	J.C	23:40
85	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.	J.C	23:40

CO returns OP cards to Safe #2

Step	Activity	Initial	Time
86	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.	T.K	23:46

Last (79)

Close Credential Safe #2

Step	Activity	Initial	Time
87	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.	T.K	23:46
88	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). IW1 and CA verify safe is locked and door indicator light is green.	T.O	23:46
89	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	T.K	23:47

Participant Signing of IW1's Script

Step	Activity	Initial	Time
90	All participants enter printed name, date, time, and signature on IW1's script coversheet.	T.O	23:51
91	CA reviews IW1's script and signs it.	T.O	23:55

Signing out of Ceremony Room

Step	Activity	Initial	Time
92	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.	T.O	0:02

Filming Stops

Step	Activity	Initial	Time
93	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.	T.O	0:03

Copying and Storing the Script

Step	Activity	Initial	Time
94	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 7/21/2011 – 2/2/2012) 5) SA attestation (A.2, A.3 below) 6) The IW attestation (A.1 below) All in a TEB labeled **"Key Ceremony 8"**, 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.**	T.O	2:06

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

Audit Bundle Checklist:

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)
One set for the original audit bundle and the other for duplicate.

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.

IW confirms the contents of the logs before placing the logs in the audit bundle.

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.

ICANN DNSSEC Script Exception

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

Step	Activity	Initial	Time
1	IW notes date and time of key ceremony exception and signs here: 2/2/2012 22:09	TLe	22:09
2	IW Describes exception and action below		

On step 25. HDMI did not work and was repeated
& it turned out to be the cable that is bad

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

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

Step	Activity	Initial	Time
1	IW notes date and time of key ceremony exception and signs here: 2/2/2012 22:52	T.A	22:52
2	IW Describes exception and action below		

On step 64 — HSMFD was not formatted

SA to format the HSMFD's

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

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

Step	Activity	Initial	Time
1	IW notes date and time of key ceremony exception and signs here: 2/2/2012	T.O	23:03
2	IW Describes exception and action below		

On step 65 HSM FD was not unmountable as the script was still running

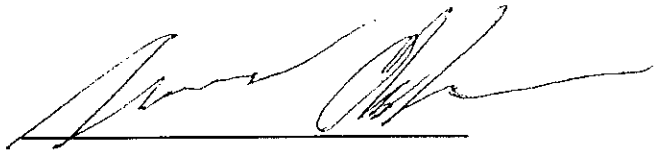
Delete and
→ Recopy all HSM FD contents to × 5 by repeating 60 to 65

– End of DNSSEC Script Exception –

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.

Tomofumi Okubo



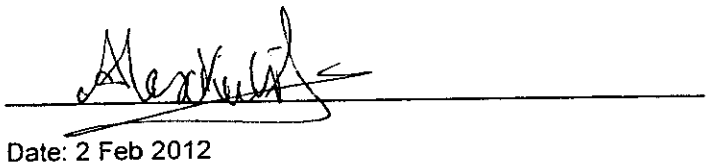
Date: 2 Feb 2012

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: 2 Feb 2012

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] 2/2/2012 1:55 to now.

Alexander Kulik

Date: 2 Feb 2012

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

```
root@srx# show
## Last changed: 2012-02-03 09:41:48 UTC
version 10.1R1.8;
system {
    host-name srx;
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "$1$XlzwmIYq$i50YWAfS7h4SW4U27m.qM."; ## SECRET-
DATA
    }
    name-server {
        199.4.28.18;
        199.4.28.28;
    }
    login {
        user akulik {
            full-name "Alex Kulik";
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "$1$209TLzzv$v9GNTNKqLHj9snvqUHZD21"; ##
SECRET-DATA
            }
        }
        user reed {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "$1$KqBOyZR6$6S3oixOhSklN/j1TUXK210"; ##
SECRET-DATA
            }
        }
```

```
    }
    services;
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        host 199.4.28.21 {
            any any;
            match RT_FLOW_SESSION;
            log-prefix SRX-KSK-LAX;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
        source-address 199.4.28.145;
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    archival {
        configuration {
            transfer-on-commit;
            archive-sites {
                "scp://srxkskcjr@199.4.28.21:/home/srxkskcjr" password
"$9$GHiHmpu1ylM36reW8Vbs24Ji.Qz6"; ## SECRET-DATA
            }
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    ntp {
        server 199.4.28.17;
        server 199.4.28.27;
        source-address 10.4.28.1;
    }
}
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 fe-0/0/7;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 199.4.28.145/26;
            }
        }
    }
    vlan {
        unit 0 {
            family inet {
                address 10.4.28.1/24;
            }
        }
    }
}
snmp {
    community dnss3c {
        clients {
            10.4.28.253/32;
        }
    }
    trap-options {
        source-address 199.4.28.145;
        agent-address outgoing-interface;
    }
    trap-group kskwest {
        categories {
            authentication;
            link;
            routing;
            startup;
            configuration;
```

```
            services;
        }
        targets {
            199.4.28.21;
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 199.4.28.129;
    }
}
security {
    ssh-known-hosts {
        host 199.4.28.21 {
            rsa-key
AAAAB3NzaC1yc2EAAAABIwAAAQEAuMQSnC2+tk7W4nBHLZFk1FfFlSTiYP2w/5XR/
x2hxxP2soZ4uFppRdaB+G9DICkvm27ovL/QsEtR2holMK2C+ilAwPaqgPfo9XFQby/
cwS400sYQHZAXqAV2wM4eGF8l7eGI2BKJcjgpWmD+YTZ
+d9jOd7bVd6248xIPF4eQmsyXsxwT2ecm2e2I9q99G5M5+aR15NTXLJ4fTYgLmODMZlIThER2zd
nZYYxUh7cD2BTij9RQwfk8oVJipGZc0q4eNNZyrUKArBXRqcuNOjQAqVzktS+BByI4JBfq/
nlXzKdvd8rXkPoavCe9lNP0zAEbAKhKgfPc6QlfTFycpI34Ew==;
        }
    }
    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 10.4.28.0/24;
```

```
            }
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                vlan.0;
            }
        }
        security-zone untrust {
            address-book {
                address icanndns 199.4.28.0/22;
            }
            interfaces {
                ge-0/0/0.0 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy trust-to-untrust {
                match {
                    source-address localnet;
                    destination-address icanndns;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
    }
}
```

```
vlans {
    vlan-trust {
        vlan-id 3;
        l3-interface vlan.0;
    }
}

[edit]
```