ICANN

Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 11

Monday November 12, 2012

ICANN KSK Facility@Terremark NCR
18155 Technology Drive, Culpeper, VA 22701-3805

This ceremony is executed under the
DNSSEC Practices Statement for the Root Zone KSK Operator Version A Revision 1358

AbbreviationsDraft

TEB =	Tamper Evident Bag (AMPAC, item #GCS1013 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large)
HSM =	Hardware Security Module
FD =	Flash Drive
CA =	Ceremony Administrator
IW =	Internal Witness
CO=	Crypto Officer
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 sign on IW1's copy. IW1 records time upon completion.

Title	Printed Name/Citizenship	Signature	Date	Time
CA	Mehmet Akcin		12 November 2012	16:46
IW1	Francisco Arias			
SA1	Reed Quinn			
SSC1	Julie Hedlund			
SSC2	Steve Chan			
CO1	Frederico Neves / BR			
CO2	Anne-Marie Eklund Lowinder / SE			
CO4	Robert Seastrom / US			
CO7	Alain Aina /TG			
EW1	Edward Lewis			
EW2	Trung Tran			
EW3	Alejandro Bolivar			
EW4	Ethan Isleib			
EW5	Elizabeth White			
EW6	Sonia Wong			
EW7	Terry Manderson			
EW8	Martin Levy			
~~EW9~~	~~Vernita Harris~~			
IW2/IKOS	Tomofumi Okubo			

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 and/or escort other participants. 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 participant sign into the Ceremony Room log.	FA	14:53

Emergency Evacuation Procedures

Step	Activity	Initial	Time
2.	CA or IW reviews emergency evacuation procedures with participants.	FA	15:01

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: 12-Nov-2012 All entries into this script or any logs should follow this common source of time.	FA	15:01

Open Credential Safe #2

Step	Activity	Initial	Time
4.	CA and IW1 escort SSC2 and COs into the safe room together. CA brings a flashlight when entering the safe room.	FA	15:03
5.	SSC2, while shielding combination from camera, opens Safe #2.	FA	15:04
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. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	15:04

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. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** Repeat these steps until all cards are removed. IW1 initials this entry when all CO have finished. **CO 1: Frederico Neves** **Box # 1238** **OP TEB # A14365422** **SO TEB # A14377117** **CO 2: Anne-Marie Eklund Lowinder** **Box # 1259** **OP TEB # A14365412** **SO TEB # A14377119** **CO 4: Robert Seastrom** **Box # 1260** **OP TEB # A14365410** **SO TEB # A14377123** **CO 7: Alain Aina** **Box # 1242** **OP TEB # A14365373** **SO TEB # A14377129**	FA	15:16

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. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	15:11
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.	FA	—
10.	IW1, CA, SSC2, and COs leave safe room, with OP cards in TEBs, closing the door behind them.	FA	15:11

Open Equipment Safe #1

Step	Activity	Initial	Time
11.	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	FA	15:17
12.	SSC1, while shielding combination from camera, opens Safe #1.	FA	15:19
13.	SSC1 takes out safe log and prints name, date, time, signature and reason (i.e., "opened safe") in safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	15:19

Remove Equipment from Safe #1

Step	Activity	Initial	Time
14.	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# A2751160 / serial # K6002016** Verify the integrity of the other HSM that will not be in used this time. **HSM2: TEB# A2826763 / serial # K6002013 (last used)**	FA	FA ~~15:[illegible]~~ 15:21
15.	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. **Laptop2 (Dell ATG6400): TEB# A2826750 / serial# 35063364997** **O/S DVD (Rev600) + HSMFD: TEB# A14365408** Verify the integrity of the other Laptop that will not be in used this time. **Laptop1: TEB# A2826764 / serial # 41593712005**	FA	15:22

Close Equipment Safe #1 and exit safe room

Step	Activity	Initial	Time
16.	SSC1 makes an entry including printed name, date, time and signature into the safe log indicating, "Close safe". IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	15:22
17.	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.	FA	15:23
18.	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.	FA	15:24

Set Up Laptop

Step	Activity	Initial	Time
19.	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. **Laptop2 (Dell ATG6400): TEB# A2826750 / serial# 35063364997**	FA	15:25
20.	CA inspects the O/S DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. **O/S DVD (Rev600) + HSMFD: TEB# A14365408**	FA	15:25
21.	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 O/S DVD.	FA	15:28
22.	CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.	FA	15:30 FA

23.	CA enters the commands
	`system-config-display --noui`
	and
	`killall Xorg`
	CA ensures that external display works.
		FA	1530

24.	CA logs in as root.	FA	15:31
25.	CA configures printer as default and prints test page by going to **System > Administration > Printing**.	FA	15:33
26.	CA opens a terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal.**	FA	15:33
27.	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.**	FA	15:35
28.	CA inserts USB port expander into laptop.	FA	15:35

Format and label blank FD

Step	Activity	Initial	Time

29.	CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system window and formats the drive by executing
	`dmesg | grep -A 5 usb-storage`
	to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc),
	`umount /dev/sda1`
	to unmounts the drive (change drive letter if necessary),
	`mkfs.vfat -n HSMFD -I /dev/sda`
	to execute a FAT32 format and label it as HSMFD.
		FA	15:37

30.	CA repeats step 29 for the 2nd blank FD	FA	15:37
31.	CA repeats step 29 for the 3rd blank FD	FA	15:37
32.	CA repeats step 29 for the 4th blank FD	FA	15:38
33.	CA repeats step 29 for the 5th blank FD	FA	15:38

Connect HSMFD

Step	Activity	Initial	Time
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 the file system window.	FA	15:40

Start Logging Terminal Session

Step	Activity	Initial	Time
35.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`	FA	15:40
36.	CA executes `script script-20121112.log` to start a capture of terminal output.	FA	15:40

Start Logging HSM Output

Step	Activity	Initial	Time
37.	CA connects a serial to USB null modem cable to laptop.	FA	15:41

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	15:42

Power Up HSM

Step	Activity	Initial	Time
39.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM1: TEB# A2751160 / serial # K6002016**	FA	15:43
40.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	FA	15:43
41.	CA switches to the ttyaudit terminal window and 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	15:45

Enable/Activate HSM

Step	Activity	Initial	Time
42.	CA calls a CO, CO opens TEB with OP card and hands to CA who places card in cardholder visible to all.	FA	15:46
43.	Repeat the step above until all OP cards are placed on the cardholder.	FA	15:46
44.	CA inserts 3 cards into HSM to activate the unit (via "Set Online" menu item). Type in the default PIN "**11223344**" when prompted. IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card _2_ of 7 2nd OP card _7_ of 7 3rd OP card _1_ of 7	FA	15:49

VERISIGN

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200
f: 701-987-6543

VerisignInc.com

12 November 2012

The SHA256 hash of the 2013 Q1 KSR file is:

25374409e9bb0408bbace07ec045104491ef5d894c7a653fb9c2647f508d8ac9

The PGP wordlist for the hash above is:

bombast consensus crumpled applicant treadmill publisher adrift antenna shamrock penetrate tapeworm insurgent slowdown detector assume designing pheasant unravel exceed matchmaker drainage infancy fracture customer sentence repellent flytrap integrate drumbeat microscope Oakland retrospect

Attested on behalf of VeriSign by:

ABolivar

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

VERISIGN

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

VerisignInc.com

November 5th, 2012

To Whom It May Concern:

This is a letter of Verification of Employment for Alejandro A. Bolivar. Verisign, Inc. has employed Alejandro A. Bolivar full-time since September 8th, 1997 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's Network Intelligence and Availability team helps protect against distributed denial of service or DDoS attacks through an in-the-cloud monitoring and mitigation services. Verisign's iDefense Security Intelligence Services help identify and track vulnerabilities, malicious code, threats, and helps provide comprehensive intelligence to enable customers to proactively manage risk.

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

Check Network between Laptop and HSM

Step	Activity	Initial	Time
45.	CA connects HSM to laptop using Ethernet cable.	FA	15:49
46.	CA tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` on the laptop terminal window and looking for responses. Ctrl-C to exit program.	FA	15:49

Insert Copy of KSR to be signed

Step	Activity	Initial	Time
47.	CA plugs FD labeled "KSR" with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA points out the KSR file to be signed then closes the file system window.	FA	15:51

Execute KSR signer

Step	Activity	Initial	Time
48.	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2013-q1-0.xml`	FA	15:51
49.	The KSR signer will ask whether the HSM is activated or not as below. `Activate HSM prior to accepting in the affirmative!! (y/N):` CA cofirms that the HSM is online and then enters "y" to proceed to verification. **Note: DO NOT enter "y" for the "Is this correct y/n?" yet.**	FA	15:52

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	15:54
51.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there are any objections"?	FA	15:54
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-2013-q1-0.xml`	FA	15:55

```
$ 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-2013-q1-0.xml (at Mon Nov 12 15:51:52 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:          K6002016

Validating last SKR with HSM...
#  Inception           Expiration           ZSK Tags        KSK Tag(CKA_LABEL)
1  2012-10-01T00:00:00 2012-10-15T23:59:59  24220,50398     19036
2  2012-10-11T00:00:00 2012-10-25T23:59:59  24220           19036
3  2012-10-21T00:00:00 2012-11-04T23:59:59  24220           19036
4  2012-10-31T00:00:00 2012-11-14T23:59:59  24220           19036
5  2012-11-10T00:00:00 2012-11-24T23:59:59  24220           19036
6  2012-11-20T00:00:00 2012-12-04T23:59:59  24220           19036
7  2012-11-30T00:00:00 2012-12-14T23:59:59  24220           19036
8  2012-12-10T00:00:00 2012-12-25T00:00:00  24220           19036
9  2012-12-21T00:00:00 2013-01-05T23:59:59  24220,40323     19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2013-q1-0.xml...
#  Inception           Expiration           ZSK Tags        KSK Tag(CKA_LABEL)
1  2013-01-01T00:00:00 2013-01-15T23:59:59  40323,24220
2  2013-01-11T00:00:00 2013-01-25T23:59:59  40323
3  2013-01-21T00:00:00 2013-02-04T23:59:59  40323
4  2013-01-31T00:00:00 2013-02-14T23:59:59  40323
5  2013-02-10T00:00:00 2013-02-24T23:59:59  40323
6  2013-02-20T00:00:00 2013-03-06T23:59:59  40323
7  2013-03-02T00:00:00 2013-03-16T23:59:59  40323
8  2013-03-12T00:00:00 2013-03-26T23:59:59  40323
9  2013-03-21T00:00:00 2013-04-05T23:59:59  20580,40323
...PASSED.

SHA256 hash of KSR:
25374409E9BB0408BBACE07EC045104491EF5D894C7A653FB9C2647F508D8AC9
>> bombast consensus crumpled applicant treadmill publisher adrift antenna shamrock pen
etrate tapeworm insurgent slowdown detector assume designing pheasant unravel exceed ma
tchmaker drainage infancy fracture customer sentence repellent flytrap integrate drumbe
at microscope Oakland retrospect <<

Generated new SKR in /media/KSR/skr-root-2013-q1-0.xml
#  Inception           Expiration           ZSK Tags        KSK Tag(CKA_LABEL)
1  2013-01-01T00:00:00 2013-01-15T23:59:59  24220,40323     19036
```

```
2  2013-01-11T00:00:00 2013-01-25T23:59:59  40323          19036
3  2013-01-21T00:00:00 2013-02-04T23:59:59  40323          19036
4  2013-01-31T00:00:00 2013-02-14T23:59:59  40323          19036
5  2013-02-10T00:00:00 2013-02-24T23:59:59  40323          19036
6  2013-02-20T00:00:00 2013-03-06T23:59:59  40323          19036
7  2013-03-02T00:00:00 2013-03-16T23:59:59  40323          19036
8  2013-03-12T00:00:00 2013-03-26T23:59:59  40323          19036
9  2013-03-21T00:00:00 2013-04-05T23:59:59  20580,40323    19036

SHA256 hash of SKR:
0701625702552A4E41348453247D2391FAC4B2D733472BA896F1C586F7BBDDA6
>> ahead adviser flagpole Eskimo accrue equipment brickyard distortion cranky confidenc
e mural enterprise bluebird insincere blowtorch miracle wallet reproduce sawdust stetho
scope chisel determine briefcase paramount prefer vacancy solo letterhead virus publish
er swelter paragon <<
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-20121112-*.log N` where ksrsigner-**20121112**-*.log is replaced by log output file displayed by program. (this example generates **N** copies) and hands copies to participants.	FA	15:57
54.	IW1 attaches a copy to his/her script.	FA	15:57

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. Confirm overwrite by entering "y" when prompted.	FA	15:59

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	16:00

57.	CA removes **KSR** FD containing SKR and gives it to the RZM representative.	FA	16:00

Disable/Deactivate HSM

Step	Activity	Initial	Time
58.	CA inserts 3 cards into HSM to deactivate the unit (via "Set Offline" menu item). Type in the default PIN "**11223344**" when prompted. 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 2 of 7 2nd OP card 7 of 7 3rd OP card 1 of 7 Confirm the ready light turns off.	FA	16:02

```
[root@localhost HSMFD]# find -P /media/HSMFD -maxdepth 1 -type f -print | sort | xargs cat
| md5sum
c3805974f132dcd8b0cc3e2e989c4d48  -
[root@localhost HSMFD]#
```

Return HSM to a TEB

Step	Activity	Initial	Time
59.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.	FA	16:04
60.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM1: TEB# BB24049988 / serial # K6002016** IW1 initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.	FA	16:05

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initial	Time
61.	**Closing ttyaudit terminal window** CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of **ttyaudit terminal window** by typing "exit".	FA	16:06
62.	**Terminating the logging script** CA stops logging terminal output by entering "exit" in the other terminal window. This only stops the script logging and will **NOT** close window.	FA	16:07

Backup HSMFD Contents

Step	Activity	Initial	Time
63.	Set dotglob by executing `shopt -s dotglob` This allows copying everything in the original HSMFD.	FA	16:08
64.	Calculate the md5hash of the contents on the original HSMFD. `find -P /media/HSMFD -maxdepth 1 -type f -print | sort | xargs cat | md5sum`	FA	16:09
65.	Copy and paste the md5hash and paste it on Text Editor by going to **Applications > Accessories > Text Editor** Print two copies. One for the audit bundle and the other for the HSMFD package.	FA	16:10
66.	CA displays contents of HSMFD by executing `ls -ltr`	FA	16:10
67.	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	16:11

```
Script started on Mon 12 Nov 2012 03:41:00 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cd /med\033[K033[K033[K
\033[K0336K033¢K0B3$K0B3$KD0#7ping\092.168.0.2
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=1.00 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=0.256 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.261 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.256/0.443/1.001/0.322 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ks\007r\007sin\00Y033[Kg
\007ner\007 Kjmt033[K033[Kqmt7v.csr\033[K033[K033[K033[K033[K /media/KSR/ksr-root-2013
-q1-0.xml
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2013-q1-0.xml (at Mon Nov 12 15:51:52
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:         K6002016

Validating last SKR with HSM...
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2012-10-01T00:00:00 2012-10-15T23:59:59  24220,50398   19036
2  2012-10-11T00:00:00 2012-10-25T23:59:59  24220         19036
3  2012-10-21T00:00:00 2012-11-04T23:59:59  24220         19036
4  2012-10-31T00:00:00 2012-11-14T23:59:59  24220         19036
5  2012-11-10T00:00:00 2012-11-24T23:59:59  24220         19036
6  2012-11-20T00:00:00 2012-12-04T23:59:59  24220         19036
7  2012-11-30T00:00:00 2012-12-14T23:59:59  24220         19036
8  2012-12-10T00:00:00 2012-12-25T00:00:00  24220         19036
9  2012-12-21T00:00:00 2013-01-05T23:59:59  24220,40323   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2013-q1-0.xml...
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2013-01-01T00:00:00 2013-01-15T23:59:59  40323,24220
2  2013-01-11T00:00:00 2013-01-25T23:59:59  40323
3  2013-01-21T00:00:00 2013-02-04T23:59:59  40323
4  2013-01-31T00:00:00 2013-02-14T23:59:59  40323
5  2013-02-10T00:00:00 2013-02-24T23:59:59  40323
6  2013-02-20T00:00:00 2013-03-06T23:59:59  40323
7  2013-03-02T00:00:00 2013-03-16T23:59:59  40323
8  2013-03-12T00:00:00 2013-03-26T23:59:59  40323
9  2013-03-21T00:00:00 2013-04-05T23:59:59  20580,40323
...PASSED.

SHA256 hash of KSR:
25374409E9BB0408BBACE07EC045104491EF5D894C7A653FB9C2647F508D8AC9
>> bombast consensus crumpled applicant treadmill publisher adrift antenna shamrock pe
netrate tapeworm insurgent slowdown detector assume designing pheasant unravel exceed
```

```
matchmaker drainage infancy fracture customer sentence repellent flytrap integrate d
mbeat microscope Oakland retrospect <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2013-q1-0.xml
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2013-01-01T00:00:00 2013-01-15T23:59:59  24220,40323   19036
2  2013-01-11T00:00:00 2013-01-25T23:59:59  40323         19036
3  2013-01-21T00:00:00 2013-02-04T23:59:59  40323         19036
4  2013-01-31T00:00:00 2013-02-14T23:59:59  40323         19036
5  2013-02-10T00:00:00 2013-02-24T23:59:59  40323         19036
6  2013-02-20T00:00:00 2013-03-06T23:59:59  40323         19036
7  2013-03-02T00:00:00 2013-03-16T23:59:59  40323         19036
8  2013-03-12T00:00:00 2013-03-26T23:59:59  40323         19036
9  2013-03-21T00:00:00 2013-04-05T23:59:59  20580,40323   19036

SHA256 hash of SKR:
0701625702552A4E41348453247D2391FAC4B2D733472BA896F1C586F7BBDDA6
>> ahead adviser flagpole Eskimo accrue equipment brickyard distortion cranky confid
ce mural enterprise bluebird insincere blowtorch miracle wallet reproduce sawdust st
hoscope chisel determine briefcase paramount prefer vacancy solo letterhead virus pu
isher swelter paragon <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20121112-155152.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cat ks\007r\007
ksr-root-2010-q3-2.xml         ksrsigner-20101101-181303.log
ksr-root-2011-q1-0.xml         ksrsigner-20110511-181351.log
ksr-root-2011-q3-0.xml         ksrsigner-20110511-181632.log
ksr-root-2012-q1-0.xml         ksrsigner-20110930-181607.log
ksr-root-2012-q3-0.xml         ksrsigner-20120522-151741.log
ksrsigner-20100616-214329.log  ksrsigner-20121112-155152.log
[root@localhost HSMFD]# cat ksr
ksr-root-2010-q3-2.xml         ksrsigner-20101101-181303.log
ksr-root-2011-q1-0.xml         ksrsigner-20110511-181351.log
ksr-root-2011-q3-0.xml         ksrsigner-20110511-181632.log
ksr-root-2012-q1-0.xml         ksrsigner-20110930-181607.log
ksr-root-2012-q3-0.xml         ksrsigner-20120522-151741.log
ksrsigner-20100616-214329.log  ksrsigner-20121112-155152.log
[root@localhost HSMFD]# cat ksrsi\007gner-2011033[K2X033[K1112-155152.log
2012-11-12T15:51:52Z: [info] Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2013-q1
.xml (at Mon Nov 12 15:51:52 2012 UTC)
2012-11-12T15:51:52Z: [info] Use HSM /opt/dnssec/aep.hsmconfig?
2012-11-12T15:52:06Z: [info] HSM /opt/dnssec/aep.hsmconfig activated.
2012-11-12T15:52:06Z: [debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
2012-11-12T15:52:06Z: [debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/
cs11.GCC4.0.2.so.4.07
2012-11-12T15:52:08Z: [info] Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.
C4.0.2.so.4.07
2012-11-12T15:52:08Z: [info] HSM slot 0 included
2012-11-12T15:52:09Z: [info] Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.
 Slot=0
2012-11-12T15:52:09Z: [info] HSM Information:
2012-11-12T15:52:09Z: [info]     Label:          ICANNKSK
2012-11-12T15:52:09Z: [info]     ManufacturerID: AEP Networks
2012-11-12T15:52:09Z: [info]     Model:          Keyper Pro 0405
2012-11-12T15:52:09Z: [info]     Serial:         K6002016
2012-11-12T15:52:09Z: [info]
2012-11-12T15:52:09Z: [info] Validating last SKR with HSM...
2012-11-12T15:52:09Z: [info] #  Inception           Expiration           ZSK Tags
 KSK Tag(CKA_LABEL)
2012-11-12T15:52:09Z: [info] 1  2012-10-01T00:00:00 2012-10-15T23:59:59  24220,50398
```

```
 19036
2012-11-12T15:52:09Z: [info] 2  2012-10-11T00:00:00 2012-10-25T23:59:59  24220
 19036
2012-11-12T15:52:09Z: [info] 3  2012-10-21T00:00:00 2012-11-04T23:59:59  24220
 19036
2012-11-12T15:52:09Z: [info] 4  2012-10-31T00:00:00 2012-11-14T23:59:59  24220
 19036
2012-11-12T15:52:09Z: [info] 5  2012-11-10T00:00:00 2012-11-24T23:59:59  24220
 19036
2012-11-12T15:52:09Z: [info] 6  2012-11-20T00:00:00 2012-12-04T23:59:59  24220
 19036
2012-11-12T15:52:09Z: [info] 7  2012-11-30T00:00:00 2012-12-14T23:59:59  24220
 19036
2012-11-12T15:52:09Z: [info] 8  2012-12-10T00:00:00 2012-12-25T00:00:00  24220
 19036
2012-11-12T15:52:09Z: [info] 9  2012-12-21T00:00:00 2013-01-05T23:59:59  24220,40323
 19036
2012-11-12T15:52:09Z: [info] ...VALIDATED.
2012-11-12T15:52:09Z: [info]
2012-11-12T15:52:09Z: [info] Validate and Process KSR /media/KSR/ksr-root-2013-q1-0.xm
l...
2012-11-12T15:52:09Z: [info] #  Inception           Expiration          ZSK Tags
 KSK Tag(CKA_LABEL)
2012-11-12T15:52:09Z: [info] 1  2013-01-01T00:00:00 2013-01-15T23:59:59  40323,24220

2012-11-12T15:52:09Z: [info] 2  2013-01-11T00:00:00 2013-01-25T23:59:59  40323

2012-11-12T15:52:09Z: [info] 3  2013-01-21T00:00:00 2013-02-04T23:59:59  40323

2012-11-12T15:52:09Z: [info] 4  2013-01-31T00:00:00 2013-02-14T23:59:59  40323

2012-11-12T15:52:09Z: [info] 5  2013-02-10T00:00:00 2013-02-24T23:59:59  40323

2012-11-12T15:52:09Z: [info] 6  2013-02-20T00:00:00 2013-03-06T23:59:59  40323

2012-11-12T15:52:09Z: [info] 7  2013-03-02T00:00:00 2013-03-16T23:59:59  40323

2012-11-12T15:52:09Z: [info] 8  2013-03-12T00:00:00 2013-03-26T23:59:59  40323

2012-11-12T15:52:09Z: [info] 9  2013-03-21T00:00:00 2013-04-05T23:59:59  20580,40323

2012-11-12T15:52:09Z: [info] ...PASSED.
2012-11-12T15:52:09Z: [info]
2012-11-12T15:52:09Z: [info] SHA256 hash of KSR:
2012-11-12T15:52:09Z: [info] 25374409E9BB0408BBACE07EC045104491EF5D894C7A653FB9C2647F5
08D8AC9
2012-11-12T15:52:09Z: [info] >> bombast consensus crumpled applicant treadmill publish
er adrift antenna shamrock penetrate tapeworm insurgent slowdown detector assume desig
ning pheasant unravel exceed matchmaker drainage infancy fracture customer sentence re
pellent flytrap integrate drumbeat microscope Oakland retrospect <<
2012-11-12T15:55:14Z: [info]
2012-11-12T15:55:14Z: [info] Generated new SKR in /media/KSR/skr-root-2013-q1-0.xml
2012-11-12T15:55:14Z: [info] #  Inception           Expiration          ZSK Tags
 KSK Tag(CKA_LABEL)
2012-11-12T15:55:14Z: [info] 1  2013-01-01T00:00:00 2013-01-15T23:59:59  24220,40323
 19036
2012-11-12T15:55:14Z: [info] 2  2013-01-11T00:00:00 2013-01-25T23:59:59  40323
 19036
2012-11-12T15:55:14Z: [info] 3  2013-01-21T00:00:00 2013-02-04T23:59:59  40323
 19036
2012-11-12T15:55:14Z: [info] 4  2013-01-31T00:00:00 2013-02-14T23:59:59  40323
 19036
```

```
2012-11-12T15:55:14Z: [info] 5  2013-02-10T00:00:00 2013-02-24T23:59:59  40323
 19036
2012-11-12T15:55:14Z: [info] 6  2013-02-20T00:00:00 2013-03-06T23:59:59  40323
 19036
2012-11-12T15:55:14Z: [info] 7  2013-03-02T00:00:00 2013-03-16T23:59:59  40323
 19036
2012-11-12T15:55:14Z: [info] 8  2013-03-12T00:00:00 2013-03-26T23:59:59  40323
 19036
2012-11-12T15:55:14Z: [info] 9  2013-03-21T00:00:00 2013-04-05T23:59:59  20580,40323
 19036
2012-11-12T15:55:14Z: [info]
2012-11-12T15:55:14Z: [info] SHA256 hash of SKR:
2012-11-12T15:55:14Z: [info] 0701625702552A4E41348453247D2391FAC4B2D733472BA896F1C58
7BBDDA6
2012-11-12T15:55:14Z: [info] >> ahead adviser flagpole Eskimo accrue equipment brick
rd distortion cranky confidence mural enterprise bluebird insincere blowtorch miracl
wallet reproduce sawdust stethoscope chisel determine briefcase paramount prefer vac
cy solo letterhead virus publisher swelter paragon <<
2012-11-12T15:55:14Z: [info] Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.
07 Slot=0
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# printlog ks\007r\007s
\007igner-2012\0071112-15515Ⅹ0B8ḉC\033[C\033[C\033[C\033[C\033[C15
[ 2 pages * 15 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 -llt033[K033[Kt /mec
a/KSR
\033[00mtotal 76
-rwxr-xr-x 1 root root 18314 Nov 12 15:55 \033[00;32mskr-root-2013-q1-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Nov 12 15:55 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 15371 Oct 12 15:34 \033[00;32mksr-root-2013-q1-0.xml\033[00m
-rwxr-xr-x 1 root root 18324 Jul 26 19:58 \033[00;32mskr.xml.20121112155152\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

Script done on Mon 12 Nov 2012 04:07:25 PM UTC
```

```
2012-11-12T15:44:43+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2012-11-12T15:44:43+0000        ttyUSB0
2012-11-12T15:44:44+0000        ttyUSB0
2012-11-12T15:44:44+0000        ttyUSB0 Battery OK!
2012-11-12T15:44:44+0000        ttyUSB0
2012-11-12T15:44:44+0000        ttyUSB0
2012-11-12T15:44:44+0000        ttyUSB0 No Tamper Counts in BBRAM!
2012-11-12T15:44:44+0000        ttyUSB0
2012-11-12T15:44:45+0000        ttyUSB0  Loading Application (APP)
2012-11-12T15:44:45+0000        ttyUSB0
2012-11-12T15:44:46+0000        ttyUSB0  Starting loaded code.
2012-11-12T15:44:46+0000        ttyUSB0
2012-11-12T15:44:46+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2012-11-12T15:44:46+0000        ttyUSB0
2012-11-12T15:44:48+0000        ttyUSB0 wdog started
2012-11-12T15:44:48+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running DES POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 DES POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running Triple DES POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Triple DES POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running AES POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 AES POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running SHA1 POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 SHA1 POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running SHA2 POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 SHA2 POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running RSA POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 RSA POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running DSA POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 DSA POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Running RandomGen POST Test
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 RandomGen POST Test Passed
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
```

```
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 12/11/2012 at 14:59:32
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0  0x100008
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0 App Details Response:
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:51+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Part Number: Keyper Pro 0405
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Serial Number: Serial K6002016
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 App Build Number: App 020
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 ABL Build Number: ABL 029
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 AL Build Number: AL 02A
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 CS Build Number: CS 029
2012-11-12T15:44:52+0000        ttyUSB0
```

```
2012-11-12T15:44:52+0000        ttyUSB0 Total Private Memory 4173377
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Free Private Memory 4173377
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Total Dynamic Memory 14569472
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Free Dynamic Memory 14569472
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Date and Time: 14:59:32 on 12/11/2012
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 Created socket 1 on port 3000.
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:52+0000        ttyUSB0 12/11/2012 at 14:59:33
2012-11-12T15:44:52+0000        ttyUSB0
2012-11-12T15:44:53+0000        ttyUSB0  0x100003
2012-11-12T15:44:53+0000        ttyUSB0
2012-11-12T15:48:15+0000        ttyUSB0
2012-11-12T15:48:15+0000        ttyUSB0
2012-11-12T15:48:15+0000        ttyUSB0 12/11/2012 at 15:02:55
2012-11-12T15:48:15+0000        ttyUSB0
2012-11-12T15:48:15+0000        ttyUSB0  0x200023 0880004A7A73296D
2012-11-12T15:48:15+0000        ttyUSB0
2012-11-12T15:48:41+0000        ttyUSB0
2012-11-12T15:48:41+0000        ttyUSB0
2012-11-12T15:48:41+0000        ttyUSB0 12/11/2012 at 15:03:21
2012-11-12T15:48:41+0000        ttyUSB0
2012-11-12T15:48:41+0000        ttyUSB0  0x200023 0880004A7BB3296D
2012-11-12T15:48:41+0000        ttyUSB0
2012-11-12T15:49:08+0000        ttyUSB0
2012-11-12T15:49:08+0000        ttyUSB0
2012-11-12T15:49:08+0000        ttyUSB0 12/11/2012 at 15:03:48
2012-11-12T15:49:08+0000        ttyUSB0
2012-11-12T15:49:08+0000        ttyUSB0  0x200023 00800002714F156D
2012-11-12T15:49:08+0000        ttyUSB0
2012-11-12T15:49:10+0000        ttyUSB0
2012-11-12T15:49:10+0000        ttyUSB0
2012-11-12T15:49:10+0000        ttyUSB0
2012-11-12T15:49:10+0000        ttyUSB0
2012-11-12T15:49:10+0000        ttyUSB0 Created socket 1 on port 5000.
2012-11-12T15:49:10+0000        ttyUSB0
2012-11-12T15:49:10+0000        ttyUSB0 12/11/2012 at 15:03:51
2012-11-12T15:49:10+0000        ttyUSB0
2012-11-12T15:49:11+0000        ttyUSB0  0x100002
2012-11-12T15:49:11+0000        ttyUSB0
2012-11-12T15:52:08+0000        ttyUSB0
2012-11-12T15:52:08+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0 Accepted connection on address 182.199.192.168.0.1.
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0 ======================================================================
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0 Free memory down from 14569472 to 11843072 (last mechanism 0)!
```

```
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0 15:06:49 on 12-11-2012
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:52:09+0000        ttyUSB0 ====================================================================
2012-11-12T15:52:09+0000        ttyUSB0
2012-11-12T15:55:14+0000        ttyUSB0
2012-11-12T15:55:14+0000        ttyUSB0
2012-11-12T15:55:14+0000        ttyUSB0 Closing connection on address 182.199.192.168.0.1.
2012-11-12T15:55:14+0000        ttyUSB0
2012-11-12T16:01:59+0000        ttyUSB0
2012-11-12T16:01:59+0000        ttyUSB0
2012-11-12T16:01:59+0000        ttyUSB0 12/11/2012 at 15:16:39
2012-11-12T16:01:59+0000        ttyUSB0
2012-11-12T16:01:59+0000        ttyUSB0  0x200023 0880004A7A73296D
2012-11-12T16:01:59+0000        ttyUSB0
2012-11-12T16:02:21+0000        ttyUSB0
2012-11-12T16:02:21+0000        ttyUSB0
2012-11-12T16:02:21+0000        ttyUSB0 12/11/2012 at 15:17:01
2012-11-12T16:02:21+0000        ttyUSB0
2012-11-12T16:02:21+0000        ttyUSB0  0x200023 0880004A7BB3296D
2012-11-12T16:02:21+0000        ttyUSB0
2012-11-12T16:02:40+0000        ttyUSB0
2012-11-12T16:02:40+0000        ttyUSB0
2012-11-12T16:02:40+0000        ttyUSB0 12/11/2012 at 15:17:21
2012-11-12T16:02:40+0000        ttyUSB0
2012-11-12T16:02:40+0000        ttyUSB0  0x200023 00800002714F156D
2012-11-12T16:02:40+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closed socket 1 on port 5000.
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
```

```
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 Closing connection; address unavailable (errno 5009).
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0 12/11/2012 at 15:17:24
2012-11-12T16:02:44+0000        ttyUSB0
2012-11-12T16:02:44+0000        ttyUSB0  0x100003
2012-11-12T16:02:44+0000        ttyUSB0
```

Step	Activity	Initial	Time
68.	CA displays contents of HSMFD_ by executing `ls -ltr /media/HSMFD_`	FA	16:11
69.	Calculate the md5hash of the contents on the copied HSMFD. `find -P /media/HSMFD_ -maxdepth 1 -type f -print | sort | xargs cat | md5sum` Confirm that it matched the md5hash of the original HSMFD	FA	16:12
70.	CA unmounts new FD using `umount /media/HSMFD_`	FA	16:12
71.	CA removes **HSMFD_** and places on table.	FA	16:12
72.	CA repeats step 66 to 71 for the 2nd copy	FA	16:13
73.	CA repeats step 66 to 71 for the 3rd copy	FA	16:14
74.	CA repeats step 66 to 71 for the 4th copy	FA	16:14
75.	CA repeats step 66 to 71 for the 5th copy	FA	16:15

Print Logging Information

Step	Activity	Initial	Time

76.	CA prints out hard copies of logging information by executing
	`enscript -2Gr -# 2 script-20121112.log`
	`enscript -Gr -# 2 --font="Courier8" ttyaudit-ttyUSB*-20121112-*.log`
	for attachment to IW1 and CA scripts.
	Note: Ignore the error regarding non-printable characters if prompted.
		FA	16:17

Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initial	Time

77.	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
	CA removes HSMFD.
		FA	16:18

78.	After all print jobs are complete, CA a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch c) Remove the O/S DVD from the drive d) Turns off the laptop again by pressing the power switch	FA	16:19
79.	CA places two HSMFDs 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. **O/S DVD (Rev600) + HSMFD: TEB# BB21369020** IW1 initials the TEB. CA places TEB on equipment cart.	FA	16:20

Distribute HSMFDs

Step	Activity	Initial	Time
80.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 1 for himself), IKOS(1) to post SKR to RZM, and to review, analyze and improve on procedures.	FA	16:21

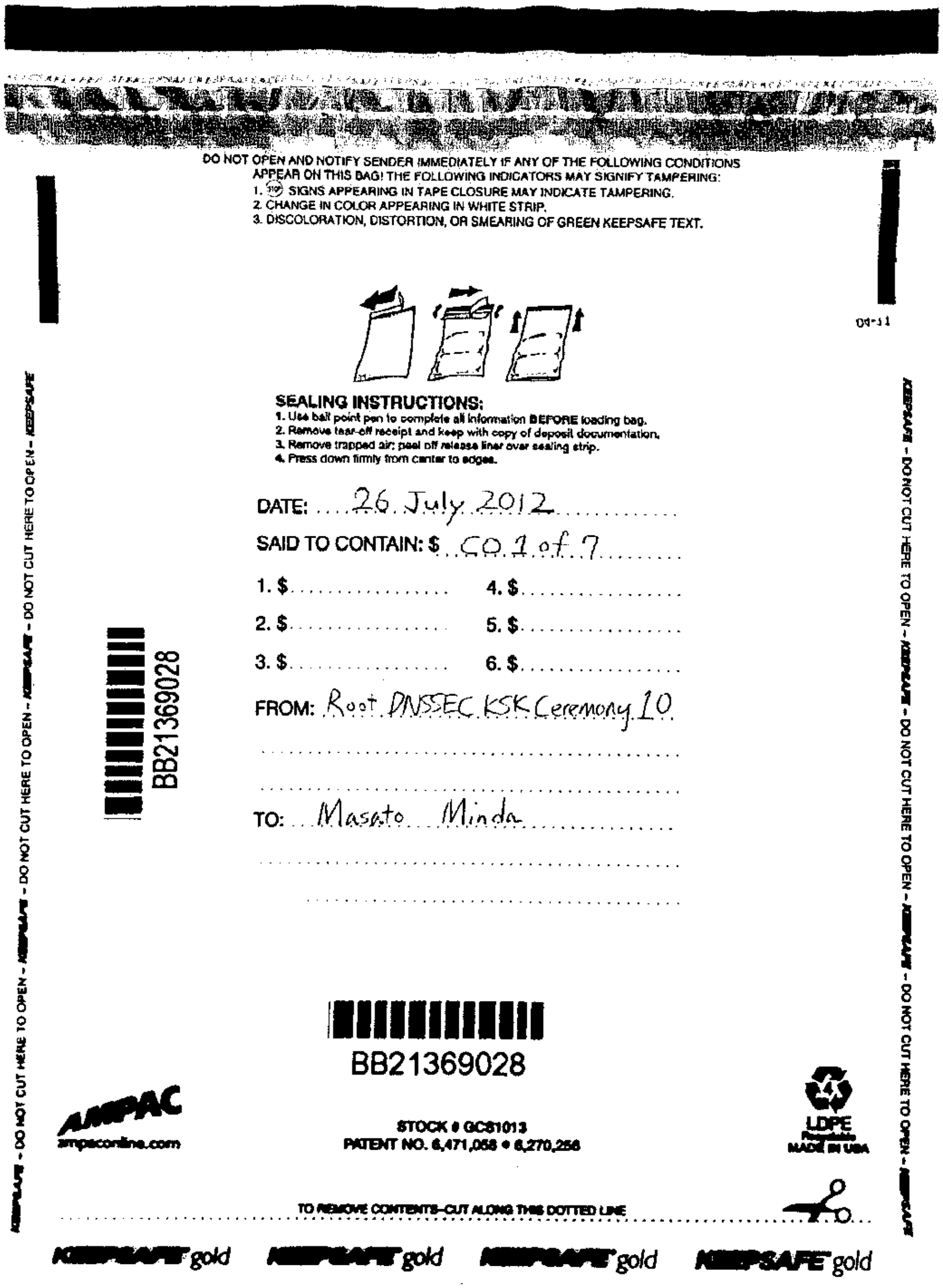
Returning Laptop to a TEB

Step	Activity	Initial	Time
81.	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. **Laptop2 (Dell ATG6400): TEB# BB24049937 / serial# 35063364997** IW1 initials the TEB and keep the sealing strips for later inventory. CA places TEB on equipment cart.	FA	16:23

Returning OP Smartcards to TEBs

Step	Activity	Initial	Time
82.	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 while showing the bag to IW1 and CO. Figure 2 below for an example. b) CA places OP into TEB, seals in front of IW1 and CO then initials bag and strip. c) IW1 inspects the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. d) CA hands the TEB containing the OP card to the CO. CO inspects and verifies TEB #s and contents then initials his/her bag. e) CO enters completion time and signs for each TEB in the table below in IW1's script. IW1 initials table entry. f) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB.	FA	16:31

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1
CO 1	OP 1 of 7	BB21369015	Frederico Neves	Frederico	12 November 2012	16:27	FA
CO 2	OP 2 of 7	BB21369016	Anne-Marie Eklund Lowinder		12 November 2012	16:26	FA
CO 4	OP 4 of 7	BB21369018	Robert Seastrom	—	12 November 2012	—	FA
CO 7	OP 7 of 7	BB21369019	Alain Aina		12 November 2012	16:29	FA



DO NOT OPEN AND NOTIFY SENDER IMMEDIATELY IF ANY OF THE FOLLOWING CONDITIONS APPEAR ON THIS BAG! THE FOLLOWING INDICATORS MAY SIGNIFY TAMPERING:
1. SIGNS APPEARING IN TAPE CLOSURE MAY INDICATE TAMPERING.
2. CHANGE IN COLOR APPEARING IN WHITE STRIP.
3. DISCOLORATION, DISTORTION, OR SMEARING OF GREEN KEEPSAFE TEXT.

SEALING INSTRUCTIONS:
1. Use ball point pen to complete all information BEFORE loading bag.
2. Remove tear-off receipt and keep with copy of deposit documentation.
3. Remove trapped air; peel off release liner over sealing strip.
4. Press down firmly from center to edges.

DATE: 26 July 2012

SAID TO CONTAIN: $ CO 1 of 7

1. $

2. $

3. $

4. $

5. $

6. $

FROM: Root DNSSEC KSK Ceremony 10

TO: Masato Minda

BB21369028

BB21369028

AMPAC
ampaconline.com

STOCK # GCS1013
PATENT NO. 6,471,058 • 6,270,258

LDPE
MADE IN USA

TO REMOVE CONTENTS-CUT ALONG THIS DOTTED LINE

KEEPSAFE - DO NOT CUT HERE TO OPEN - KEEPSAFE - DO NOT CUT HERE TO OPEN - KEEPSAFE - DO NOT CUT HERE TO OPEN - KEEPSAFE

KEEPSAFE gold KEEPSAFE gold KEEPSAFE gold KEEPSAFE gold

Figure 2

Returning Equipment to Safe #1

Step	Activity	Initial	Time
83.	CA, IW1, SSC1 open safe room and enter with equipment cart.	FA	16:32
84.	SSC1 opens Safe #1 shielding combination from camera.	FA	16:33
85.	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. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	16:34
86.	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	16:35
87.	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	16:35
88.	CA records return of **O/S DVD + HSMFD** in next entry field of safe log with TEB #, printed name, date, time, and signature; places the **O/S DVD + HSMFD** into Safe #1 and IW1 initials the entry.	FA	16:35

Close Equipment Safe #1

Step	Activity	Initial	Time
89.	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	16:35
90.	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.	FA	16:36
91.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	FA	16:36

Open Credential Safe #2

Step	Activity	Initial	Time
92.	After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP card TEB with them.	FA	16:37
93.	SSC2 opens Safe #2 while shielding combination from camera.	FA	16:38
94.	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	1639

CO returns OP cards to Safe #2

Step	Activity	Initial	Time
95.	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. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** c) CO **shows the bag to the camera** and then 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	16:42

Close Credential Safe #2

Step	Activity	Initial	Time
96.	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "Close safe" into the safe log. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	FA	16:43
97.	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.	FA	16:43
98.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	FA	16:44

Participant Signing of IW1's Script

Step	Activity	Initial	Time
99.	All participants enter printed name, date, time, and signature on IW1's script coversheet.	FA	16:46
100.	CA reviews IW1's script and signs it.	FA	16:48

Signing out of Ceremony Room

Step	Activity	Initial	Time
101.	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	16:54

Filming Stops

Step	Activity	Initial	Time
102.	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	16:54

Copying and Storing the Script

Step	Activity	Initial	Time
103.	IW1 makes at least 4 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 **05/22/2012 – 11/12/2012**) 5) The IW attestation (A.1 below) 6) SA attestation (A.2, A.3 below) All in a TEB labeled "**Key Ceremony 11**", 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.**	FA	19:12

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.

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: 12 November 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 other 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 log extraction on [date, time UTC] 5/22/12 00:00 to now.

Reed Quinn

Ree

Date: 12 November 2012

A.3 Firewall Configuration Review (by SA)

I have reviewed the firewall configuration from the other 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

Date: 12 November 2012

ICANN

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

1	IW notes date and time of key ceremony exception and signs here: ______________________________	FA	14:53
2	IW Describes exception and action below		

- CO4 forgot his key, therefore he participated in the ceremony as an EW. We did not used his card.

– End of DNSSEC Script Exception –

ICANN

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

1	IW notes date and time of key ceremony exception and signs here:	FA	15:16
2	IW Describes exception and action below		

- At step H8 the SSC2 closed the Safe door before putting the log in. We took the log with us (IW1 and CA) to bring it in when we come back to Safe 2.

– End of DNSSEC Script Exception –

```
reed@srx>

reed@srx> show configuration
## Last commit: 2011-08-19 06:26:50 UTC by alex
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
"$9$fQ6A0BIcre5QORSy
Kv-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
AAAAB3NzaC1yc2EAAAABIwAAAQEA4so1gB6EcqjcP7WTbIm4/6ZOqqYfFI3MRl7HiO2C2C
1
UML2jyaHAvQqO/5LtqbKyPoZ38huGEGgYMqsMDaga+lIiKpu+2sJysG6HHnH
+ZPw0eQ24RnTMxGaZjfCKR+/GDQDnrp
yZG0st8jlbSLPjVnQFzwMbAW2A0rcqDkSINEkb5vyzDeZxQTpBrHRwQDJeW9m87GxalHJo
7sqz91blpsC7K2XaE7ypM
QnEdOxY2mE4jzF/
OzNaNZVcWiN9YSeAPmRKybIbHcLX9Gn3K8IPJGlEVMMfwrWxhSj7iFl6Gr6gi
+rQvTVepDKgw0s6
JLJY2hTGHRIbFQ2/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;
                        ping;
                    }
                }
            }
        }
    }
}
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;
    }
}

reed@srx> exit


srx (ttyu0)
```