Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 24

Thursday February 11, 2016

ICANN KSK Facility@Equinix LA3
1920 East Maple Avenue, El Segundo, CA 90245

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

Abbreviations

TEB =	Tamper Evident Bag (AMPAC, item #GCS1013, item #GCS0912 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large)	**SO =**	Security Officer	**CO =**	Crypto Officer
OP =	Operator	**CA =**	Ceremony Administrator	**IW =**	Internal Witness
SW =	Staff Witness	**SSC =**	Safe Security Controller	**EW =**	External Witness
MC =	Master of Ceremony	**IKOS =**	ICANN KSK Operations Security	**SA =**	System Administrator
AUD =	Third Party Auditor	**RZM =**	Root Zone Maintainer	**HSM =**	Hardware Security Module
FD =	Flash Drive	**KSR =**	Key Signing Request	**SKR =**	Signed Key Response

Participants

Instructions: At the end of the ceremony, participants sign on IW1's copy. IW1 records time upon completion.

Title	Printed Name	Signature	Date	Time
CA	Kim Davies / ICANN			
IW1	Yuko Green / ICANN			
SSC1	Marilia Hirano / ICANN			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian / TZ			
CO2	Dmitry Burkov / RU			
CO3	Joao Damas / PT			
CO6	Nicolas Antoniello / UY			
CO7	Subramanian Moonesamy / MU			
RZM	Alejandro Bolivar / Verisign			
RZM	Duane Wessels / Verisign			
RZM	Sanju Varghese/ Verisign			
~~RZM~~	~~Brad Verd / Verisign~~		11 February 2016	
AUD	Jackie Kwong / PricewaterhouseCoopers			
AUD	Abbey Beam / PricewaterhouseCoopers			
SA1	~~Connor Barthold~~ / ICANN Brian Martin			
SA2	Josh Jenkins / ICANN			
CA2 / IKOS	Alberto Duero / ICANN			
IW2 / IKOS	Andres Pavez / ICANN			
CA3	Edward Lewis / ICANN			
EW	Reg Levy			
EW	James Gannon			
SW	Sabrina Tanamal			
Locksmith	Rich Bowen (Industrial Lock and Security)			

Note: By signing this script, you are declaring that this is a true and accurate record of the Root DNSSEC KSK ceremony to the best of your knowledge.

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

Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.	Y.G.	22:31
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.	Y.G.	22:33

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	Y.G	22:33
4.	CA explains the use of personal electronics devices during ceremony.	Y.G	22:33
5.	CA briefly explains the purpose of the ceremony.	Y.G.	22:33

Verify Time and Date

Step	Activity	Initials	Time
6.	IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room: Date and time: 11 Feb 2016 22:33 All entries into this script or any logs should follow this common source of time.	Y.G	22:34

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.	Y.G.	22:35
8.	SSC2, while shielding combination from camera, opens Safe #2.	Y.G	22:37
9.	SSC2 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC2. SSC2 appends the new safe log then 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.**	Y.G.	22:38

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	One by one, the selected COs retrieves required OP cards and SO cards (if applicable) 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) Retains OP TEB and SO TEB (if applicable) and locks box. d) Makes an entry in safe log indicating OP TEB and SO TEB removal (if applicable) 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 required cards are removed. IW1 initials this entry when all COs have finished. **CO 1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46584261 (Retain)** **SO TEB # BB46584262 (Check and return)** **CO 2: Dmitry Burkov** **Box #: 1793** **OP TEB # BB46584255 (Retain)** **SO TEB # BB46584256 (Check and return)** **CO 3: Joao Damas** **Box # 1071** **OP TEB # BB21907274 (Retain)** **SO TEB # BB21820433 (Check and return)** **CO 6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB21368989 (Retain)** **SO TEB # BB21907266 (Retain)** **CO 7: Subramanian Moonesamy** **Box #: 1792** **OP TEB # BB46584257 (Retain)** **SO TEB # BB46584258 (Check and return)**	Y.G.	22:48

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. Note time.

Note Exception Time

Step	Activity	Initials	Time
1.	IW1 notes date and time of key ceremony exception and signs here:	Y.G.	22:52
2.	IW1 Describes exception and action below.		

~~Between~~

Lock Smith stayed at the beginning of the ceremony to ensure there is no issues with keys or locks.

Lock Smith was dismissed between steps 13 and 14 as there was no issue with opening the boxes.

– End of DNSSEC Script Exception –

Close Credential Safe #2

Step	Activity	Initials	Time
11.	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.**	Y.G.	22:49
12.	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.	Y.G	22:49
13.	IW1, CA, SSC2, and COs leave safe room, with OP cards and SO cards (if applicable) in TEBs, closing the door behind them.	Y.G	22:50

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	Y.G.	23:03
15.	SSC1, while shielding combination from camera, opens Safe #1.	Y.G	23:04
16.	SSC1 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 appends the new safe log then 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.**	Y.G.	23:07

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	**CA CAREFULLY removes HSM3 (in TEB)** from the safe and completes the entry on the safe log indicating HSM Removal, TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** **HSM3: TEB# BB24646665 / serial # H1403033** Verify the integrity of the other HSMs that will not be used and return them to the safe. **HSM1: TEB# BB24646605 / serial # K6002020** **HSM2: TEB# BB24646669 / serial # K6002018** **HSM4: TEB# BB24646664 / serial # H1411006**	Y.G	23:10
18.	CA takes out the items listed below from the safe and completes the entry on 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. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** **Laptop1 (Dell ATG6400): TEB# BB24646663** **O/S DVD (Rev600) + HSMFD: TEB# BB46584331** Verify the integrity of the other Laptop that will not be used this time and return it to the safe. **Laptop2 (Dell ATG6400): TEB# BB24646591 / serial# 7292928457**	Y.G	23:12

Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	SSC1 makes an entry including printed name, date, time and signature on 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.**	Y.G.	23:13
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.	Y.G.	23:14
21.	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.	Y.G.	23:14

Act 2. Confirm and Sign the Key Signing Request

Set Up Laptop

Step	Activity	Initials	Time
1.	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. **Laptop1 (Dell ATG6400): TEB# BB24646663 / serial # 37240147333**	Y.G.	23:16
2.	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# BB46584331**	Y.G.	23:17
3.	CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from O/S DVD.	Y.G.	23:24
4.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes `system-config-display --noui` c) CA executes `killall Xorg` d) CA confirms that external display works. e) CA logs in as root	Y.G.	23:25
5.	CA confirms that the printer is connected then configures printer as default and prints test page by going to **System > Administration > Printing** And follow the steps below: a) Click the **New Printer** icon (left side), leave everything default and then click the button **Forward** b) Under "Select Connection" choose the first device "**HP Laserjet xxxx**" and then click the button **Forward** c) (Note: The xxxx is the Printer Model) d) Select **HP** and click the button **Forward** e) Under "Models" scroll up and select **"Laserjet"**, and then click the button **Forward** f) To finish click the button **Apply** g) Under "Local Printers" from the left menu, select "**printer**" h) Click the button **"Make Default Printer"** and "**Print Test Page"**	Y.G.	23:30
6.	CA opens a terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal** Follow the additional steps to maximize the terminal window: a) Click the **View** menu and select **Zoom In** b) Repeat the step above as necessary	Y.G.	23:30

Step	Activity	Initials	Time
7.	CA checks and fixes the date and time on the laptop while referencing the laptop wall clock. On the laptop terminal windows, CA executes: `cp /usr/share/zoneinfo/UTC /etc/localtime` When "`cp: overwrite `/etc/localtime'?`" is displayed, type "`y`" and press enter. then `date -s "20160211 HH:MM:00"` where HH is two digit Hour, MM is two digit Minutes and 00 is Zero Seconds CA executes `date` using the Terminal window to confirm the date is properly configured.	Y.G.	23:31

Format and label blank FD

Step	Activity	Initials	Time

8.	CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system popup window and formats the drive by executing
	`df`
	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 and partition if necessary),
	`mkfs.vfat -n HSMFD -I /dev/sda1`
	to execute a FAT32 format and label it as HSMFD.
	CA unplugs the FD.
		Y.G	23:33

9.	CA repeats step 8 for the 2nd blank FD	Y.G	23:33
10.	CA repeats step 8 for the 3rd blank FD	Y.G.	23:34
11.	CA repeats step 8 for the 4th blank FD	Y.G.	23:34
12.	CA repeats step 8 for the 5th blank FD	Y.G.	23:35

Connect HSMFD

Step	Activity	Initials	Time
13.	CA plugs the previous HSMFD used in the **ceremony 22** into the free USB slot on the laptop and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.	Y.G.	23:37

Step	Activity	Initials	Time

14.	Calculate the sha256 hash of the contents on the copied HSMFD.
	`find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum`
	IW confirms that the result matches the sha256 hash of the HSMFD that is on the annotated script from the **Ceremony 22**.
	Previous hash should read as below (image from Ceremony 22 annotated script).
	`a3fac3770fc75ee69e48b9d40389d4717ab0f8b111e77bf8d65981a32fe0eb8b`
	Note: The CA should assign some attendees to confirm the hash displayed on the TV screen and the rest will confirm the hash written on the ceremony script.
		Y.G.	23:39

Start Logging Terminal Session

Step	Activity	Initials	Time
15.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`	Y.G.	23:39
16.	CA executes `script script-20160211.log` to start a capture of terminal output.	Y.G.	23:39

Start Logging HSM Output

Step	Activity	Initials	Time
17.	CA connects a serial to USB null modem cable to laptop.	Y.G.	23:39

18.	CA opens a second terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal.**
	Follow the additional steps to maximize the terminal window:
	a) Click the **View** menu and select **Zoom In**
	b) Repeat the step above as necessary
	and executes
	`cd /media/HSMFD`
	and executes
	`stty -F /dev/ttyUSB0 115200`
	`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.
		Y.G.	23:40

Power Up HSM

Step	Activity	Initials	Time
19.	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. **HSM3: TEB# BB24646665 / serial # H1403033**	Y.G.	23:41
20.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	Y.G.	23:42
21.	CA switches to the ttyaudit terminal window and connects power to HSM and switches the power ON. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) **HSM3: serial # H1403033** **Note: The HSM date and time was set from the factory.**	Y.G.	23:42

Enable/Activate HSM

Step	Activity	Initials	Time
22.	One by one, CA calls each COs listed below to inspect the TEB for tamper evidence, opens the TEB and hands the OP cards to the CA who places the cards in cardholder visible to all. **CO 1: Arbogast Fabian** **OP TEB # BB46584261** **CO 2: Dmitry Burkov** **OP TEB # BB46584255** **CO 3: Joao Damas** **OP TEB # BB21907274** **CO 6: Nicolas Antoniello** **OP TEB # BB21368989** **CO 7: Subramanian Moonesamy** **OP TEB # BB46584257**	Y.G.	23:46

Step	Activity	Initials	Time
23.	CA will perform the following steps to activate the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"1.Set Online"** hit **ENT** to confirm c) When **"Set Online?"** is displayed, hit **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card Confirm the **"READY"** led on the **HSM** is **ON.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 6 of 7 2nd OP card 1 of 7 3rd OP card 7 of 7	Y.G.	23:49

Check Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
24.	CA connects HSM to laptop using Ethernet cable in **LAN** port.	Y.G.	23:50
25.	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.	Y.G.	23:50

Insert Copy of KSR to be signed

Step	Activity	Initials	Time
26.	The KSR is downloaded to the KSRFD and transferred to the facility by the IKOS. 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.	Y.G.	23:52

VERISIGN

12061 Bluemont Way
Reston, Va. 20190
T: 703-948-3200
F: 703-948-3857

VerisignInc.com

February 4th, 2016

To Whom It May Concern:

This is a letter of Verification of Employment for Sanju Varghese. Verisign, Inc. has employed Sanju Varghese full-time since May 17th, 2004, currently as a Sr. Manager - CBO in our Operations organization.

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 Specialist | Verisign, Inc. | 703-948-4143 | dcarney@verisign.com

VERISIGN™

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

VerisignInc.com

11 February, 2016

The SHA256 hash of the 2016 Q2 KSR file is:

25d1a4a026ba40c90a4e6f13295c71e8b4f8a037eff84028fe49dd2d5 8e8f803

The PGP wordlist for the hash above is:

bombast scavenger regain Orlando bookshelf puberty crackdown retrospect allow distortion gremlin barbecue breakup fascinate hamlet typewriter scenic warranty ragtime consensus uncut warranty crackdown cellulose woodlark dinosaur swelter clergyman endorse typewriter Vulcan aggregate

Attested on behalf of VeriSign by:

Sanju Varghese
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

Execute KSR signer

Step	Activity	Initials	Time
27.	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2016-q2-0.xml`	Y.G.	23:53
28.	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 confirms 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.**	Y.G	23:53

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
29.	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: Sanju Oldaniel Varghese	Y.G.	23:54
30.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?	Y.G.	23:55
31.	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-2016-q2-0.xml`	Y.G.	23:56

```
$ 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-2016-q2-0.xml (at Thu Feb 11 23:52:27 2
016 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 9860-2
    Serial:          H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2016-01-01T00:00:00 2016-01-15T23:59:59  54549,62530   19036
2  2016-01-11T00:00:00 2016-01-25T23:59:59  54549         19036
3  2016-01-21T00:00:00 2016-02-04T23:59:59  54549         19036
4  2016-01-31T00:00:00 2016-02-14T23:59:59  54549         19036
5  2016-02-10T00:00:00 2016-02-24T23:59:59  54549         19036
6  2016-02-20T00:00:00 2016-03-05T23:59:59  54549         19036
7  2016-03-01T00:00:00 2016-03-15T23:59:59  54549         19036
8  2016-03-11T00:00:00 2016-03-25T23:59:59  54549         19036
9  2016-03-21T00:00:00 2016-04-05T23:59:59  54549,60615   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2016-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2016-04-01T00:00:00 2016-04-15T23:59:59  60615,54549
2  2016-04-11T00:00:00 2016-04-25T23:59:59  60615
3  2016-04-21T00:00:00 2016-05-05T23:59:59  60615
4  2016-05-01T00:00:00 2016-05-15T23:59:59  60615
5  2016-05-11T00:00:00 2016-05-25T23:59:59  60615
6  2016-05-21T00:00:00 2016-06-04T23:59:59  60615
7  2016-05-31T00:00:00 2016-06-14T23:59:59  60615
8  2016-06-10T00:00:00 2016-06-24T23:59:59  60615
9  2016-06-20T00:00:00 2016-07-05T23:59:59  46551,60615
...PASSED.

SHA256 hash of KSR:
25D1A4A026BA40C90A4E6F13295C71E8B4F8A037EFF84028FE49DD2D58E8F803
>> bombast scavenger regain Orlando bookshelf puberty crackdown retrospect allow distor
tion gremlin barbecue breakup fascinate hamlet typewriter scenic warranty ragtime conse
nsus uncut warranty crackdown cellulose woodlark dinosaur swelter clergyman endorse typ
ewriter Vulcan aggregate <<

Generated new SKR in /media/KSR/skr-root-2016-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2016-04-01T00:00:00 2016-04-15T23:59:59  54549,60615   19036
```

```
2  2016-04-11T00:00:00 2016-04-25T23:59:59  60615          19036
3  2016-04-21T00:00:00 2016-05-05T23:59:59  60615          19036
4  2016-05-01T00:00:00 2016-05-15T23:59:59  60615          19036
5  2016-05-11T00:00:00 2016-05-25T23:59:59  60615          19036
6  2016-05-21T00:00:00 2016-06-04T23:59:59  60615          19036
7  2016-05-31T00:00:00 2016-06-14T23:59:59  60615          19036
8  2016-06-10T00:00:00 2016-06-24T23:59:59  60615          19036
9  2016-06-20T00:00:00 2016-07-05T23:59:59  46551,60615    19036

SHA256 hash of SKR:
F6C667731366C46EDBDE84034090A09F1E5A0F10CEC8A11E1F0F7B8FB7208EAB
>> village responsive freedom hurricane Aztec gossamer snowslide headwaters suspense te
lephone mural aggregate crackdown millionaire ragtime opulent berserk existence artist
autopsy spyglass retrieval ratchet Burlington billiard atmosphere kickoff midsummer sea
bird butterfat orca Pegasus <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

```
Script started on Thu 11 Feb 2016 11:38:48 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.0.2
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=1.24 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.358 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.516 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.357 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.357/0.619/1.248/0.369 ms
\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]# ksrsi\007gner Kjqmt7v /m
edia/KSR/ksr-root-2016-q2-0.xml
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2016-q2-0.xml (at Thu Feb 11 23:52:27
2016 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 9860-2
    Serial:         H1403033

Validating last SKR with HSM...
#  Inception            Expiration           ZSK Tags     KSK Tag(CKA_LABEL)
1  2016-01-01T00:00:00  2016-01-15T23:59:59  54549,62530  19036
2  2016-01-11T00:00:00  2016-01-25T23:59:59  54549        19036
3  2016-01-21T00:00:00  2016-02-04T23:59:59  54549        19036
4  2016-01-31T00:00:00  2016-02-14T23:59:59  54549        19036
5  2016-02-10T00:00:00  2016-02-24T23:59:59  54549        19036
6  2016-02-20T00:00:00  2016-03-05T23:59:59  54549        19036
7  2016-03-01T00:00:00  2016-03-15T23:59:59  54549        19036
8  2016-03-11T00:00:00  2016-03-25T23:59:59  54549        19036
9  2016-03-21T00:00:00  2016-04-05T23:59:59  54549,60615  19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2016-q2-0.xml...
#  Inception            Expiration           ZSK Tags     KSK Tag(CKA_LABEL)
1  2016-04-01T00:00:00  2016-04-15T23:59:59  60615,54549
2  2016-04-11T00:00:00  2016-04-25T23:59:59  60615
3  2016-04-21T00:00:00  2016-05-05T23:59:59  60615
4  2016-05-01T00:00:00  2016-05-15T23:59:59  60615
5  2016-05-11T00:00:00  2016-05-25T23:59:59  60615
6  2016-05-21T00:00:00  2016-06-04T23:59:59  60615
7  2016-05-31T00:00:00  2016-06-14T23:59:59  60615
8  2016-06-10T00:00:00  2016-06-24T23:59:59  60615
9  2016-06-20T00:00:00  2016-07-05T23:59:59  46551,60615
...PASSED.

SHA256 hash of KSR:
25D1A4A026BA40C90A4E6F13295C71E8B4F8A037EFF84028FE49DD2D58E8F803
>> bombast scavenger regain Orlando bookshelf puberty crackdown retrospect allow disto
rtion gremlin barbecue breakup fascinate hamlet typewriter scenic warranty ragtime con
sensus uncut warranty crackdown cellulose woodlark dinosaur swelter clergyman endorse
typewriter Vulcan aggregate <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2016-q2-0.xml
#  Inception            Expiration           ZSK Tags     KSK Tag(CKA_LABEL)
1  2016-04-01T00:00:00  2016-04-15T23:59:59  54549,60615  19036
2  2016-04-11T00:00:00  2016-04-25T23:59:59  60615        19036
3  2016-04-21T00:00:00  2016-05-05T23:59:59  60615        19036
4  2016-05-01T00:00:00  2016-05-15T23:59:59  60615        19036
5  2016-05-11T00:00:00  2016-05-25T23:59:59  60615        19036
6  2016-05-21T00:00:00  2016-06-04T23:59:59  60615        19036
7  2016-05-31T00:00:00  2016-06-14T23:59:59  60615        19036
8  2016-06-10T00:00:00  2016-06-24T23:59:59  60615        19036
9  2016-06-20T00:00:00  2016-07-05T23:59:59  46551,60615  19036

SHA256 hash of SKR:
F6C667731366C46EDBDE84034090A09F1E5A0F10CEC8A11E1F0F7B8FB7208EAB
>> village responsive freedom hurricane Aztec gossamer snowslide headwaters suspense t
elephone mural aggregate crackdown millionaire ragtime opulent berserk existence artis
t autopsy spyglass retrieval ratchet Burlington billiard atmosphere kickoff midsummer
seabird butterfat orca Pegasus <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20160211-235227.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# for i in $(seq 15); do p
[illegible]0160211-235227
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 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 -ltr /media/KSR/
\033[00mtotal 112
-rwxr-xr-x 1 root root 18314 Jan 14 16:46 \033[00;32mskr.xml.20160211235227\033[00m
-rwxr-xr-x 1 root root 15371 Jan 14 17:22 \033[00;32mksr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 11 23:55 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 11 23:55 \033[00;32mskr-root-2016-q2-0.xml\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# synm%033[K033[Kc
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# um\007ount /media/KSR
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit

Script done on Fri 12 Feb 2016 12:07:28 AM UTC
```

```
2016-02-11T23:42:35+0000        ttyUSB0 ÿþþ
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0 H1403033 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0 BBL CRC32: 0x757574CA
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0 H1403033 011403 ABL 011 : Tamper Challenge Response Key
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:35+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2016-02-11T23:42:35+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 ####################################
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 ###     ABL tamper records       ###
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 ####################################
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 ========================================
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 vextoosTamperCount:     0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 vintoosTamperCount:     42
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 vbboosTamperCount:      0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 maxstrtempTamperCount:  0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 minstrtempTamperCount:  0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 meshTamperCount:        0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 extampSMKTamperCount:   0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 extampIMKTamperCount:   0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 tempdiffTamperCount:    0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 pfTamperCount:          42
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 restartTamperCount:     138
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 Current tamper bitmaps:
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 ========================
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
```

```
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0 ========================================
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:36+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0 Board is P2020RDB
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0 board_smp_init: 2 cpu
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:37+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2016-02-11T23:42:37+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 Starting next program at v0015183c
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 Starting K-Series Kernel
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 Thu Feb 11 23:26:11 2016
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 Starting auditd v2.0 ... started.
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:38+0000        ttyUSB0 Interface 0 configured for IPv6.
2016-02-11T23:42:38+0000        ttyUSB0
2016-02-11T23:42:39+0000        ttyUSB0 Interface 0 configured for IPv4.
2016-02-11T23:42:39+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0 Starting USB driver...
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0
2016-02-11T23:42:40+0000        ttyUSB0
```

```
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running DES POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 DES POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running Triple DES POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Triple DES POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running AES POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 AES POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running SHA1 POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 SHA1 POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running SHA2 POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 SHA2 POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running RandomGen POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 RandomGen POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running RSA POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 RSA POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running DSA POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 DSA POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 Running ECC POST Test
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:41+0000        ttyUSB0 ECC POST Test Passed
2016-02-11T23:42:41+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 Audit on 11/2/2016 23:26:14 00100008
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 Keyper 9860-2  Serial Number H1403033
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 Memory Usage:
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 RAM (free/total)        197Mb/256Mb
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0    black store          400b
```

```
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0    statistics           112b
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0    other                116b
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 RedStore (free/total)   109Kb/128Kb
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 Network Configuration:
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 IPv4: enabled
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 IPv6: enabled
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B2:40 / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b240/64
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 HSM Port: 05000
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 Software Versions:
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 BBL 010 ABL 011 App 023
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 CPLD Version:
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 1.9
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:42+0000        ttyUSB0 SCR Firmware Version:
2016-02-11T23:42:42+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0 OROS-R2.99-R1.20
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:42:43+0000        ttyUSB0 Audit on 11/2/2016 23:26:15 00100003
2016-02-11T23:42:43+0000        ttyUSB0
2016-02-11T23:47:42+0000        ttyUSB0 Audit on 11/2/2016 23:31:12 00200069 0A4000009DC6296E
2016-02-11T23:47:42+0000        ttyUSB0
2016-02-11T23:48:09+0000        ttyUSB0 Audit on 11/2/2016 23:31:41 00200069 0A400000B706296E
2016-02-11T23:48:09+0000        ttyUSB0
```

```
2016-02-11T23:48:34+0000        ttyUSB0 Audit on 11/2/2016 23:32:06 00200069 0A400000B7C6296E
2016-02-11T23:48:34+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0 TcpListener: Created IPv4 socket 14 on port 5000.
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0 TcpListener: Created IPv6 socket 15 on port 5000.
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:48:36+0000        ttyUSB0 Audit on 11/2/2016 23:32:09 00100002
2016-02-11T23:48:36+0000        ttyUSB0
2016-02-11T23:52:50+0000        ttyUSB0
2016-02-11T23:52:50+0000        ttyUSB0
2016-02-11T23:52:50+0000        ttyUSB0 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2016-02-11T23:52:50+0000        ttyUSB0
2016-02-11T23:55:30+0000        ttyUSB0
2016-02-11T23:55:30+0000        ttyUSB0
2016-02-11T23:55:30+0000        ttyUSB0 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2016-02-11T23:55:30+0000        ttyUSB0
2016-02-12T00:01:22+0000        ttyUSB0 Audit on 11/2/2016 23:44:54 00200069 0A400000B646296E
2016-02-12T00:01:22+0000        ttyUSB0
2016-02-12T00:01:36+0000        ttyUSB0 Audit on 11/2/2016 23:45:09 0020006a
2016-02-12T00:01:36+0000        ttyUSB0
2016-02-12T00:02:24+0000        ttyUSB0 Audit on 11/2/2016 23:45:57 00200069 0A4000009D06296E
2016-02-12T00:02:24+0000        ttyUSB0
2016-02-12T00:02:48+0000        ttyUSB0 Audit on 11/2/2016 23:46:21 00200069 0A4000009DC6296E
2016-02-12T00:02:48+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0 TcpListener: Closed IPv4 socket 14 on port 5000.
2016-02-12T00:02:55+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0 TcpListener: Closed IPv6 socket 15 on port 5000.
2016-02-12T00:02:55+0000        ttyUSB0
2016-02-12T00:02:55+0000        ttyUSB0 Audit on 11/2/2016 23:46:28 00100003
2016-02-12T00:02:55+0000        ttyUSB0
```

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
32.	CA prints out a sufficient number of copies for participants using `for i in $(seq X); do printlog ksrsigner-20160211-*.log; done` where ksrsigner-**20160211**-*.log is replaced by log output file displayed by program. This example generates **X** copies and hands copies to participants.	Y.G.	23:59
33.	IW1 attaches a copy to his/her script.	Y.G.	23:59

Backup Newly Created SKR

Step	Activity	Initials	Time
34.	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.	Y.G.	0:00

35.	CA lists contents of KSR FD which should now have an SKR by running
	`ls -ltr /media/KSR`
	flushes the system buffers:
	`sync`
	and then unmounts the KSR FD using
	`umount /media/KSR`
		Y.G.	0:00

36.	CA removes **KSR** FD containing SKR and gives it to the RZM representative.	Y.G.	0:00

Disable/Deactivate HSM

Step	Activity	Initials	Time
37.	CA makes sure to utilize the cards that were NOT used to activate the HSM are used to deactivate the HSM. CA will perform the following steps to deactivate the HSM: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"2.Set Offline"** hit **ENT** to confirm c) When **"Set Offline?"** is displayed, hit **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** hit **ENT** f) When **"Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP cards Confirm the **"READY"** led on the HSM is **OFF.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 3 of 7 2nd OP card 2 of 7 3rd OP card 6 of 7	Y.G.	0:03

Act 3. Secure Hardware and Close the Ceremony

Return HSM to a TEB

Step	Activity	Initials	Time
1.	CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.	Y.G.	0:04
2.	CA places the HSM into a prepared TEB and seals it.	Y.G.	0:06
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM3: TEB# BB24646618 / serial # H1403033** IW1 and CA initials the TEB and keeps the sealing strip for later inventory. CA places item on equipment cart.	Y.G	0:07

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
4.	**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".	Y.G.	0:07
5.	**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.	Y.G.	0:08

KSK 24


```
71eda78ef35290b984f3a6669cd9ba1ef0f76869279b612dea366b99a9675279  -
```

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA set dotglob by executing `shopt -s dotglob` This allows copying everything in the original HSMFD.	Y.G	0:08
7.	CA calculates the sha256hash of the contents on the original HSMFD. `find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum`	Y.G.	0:09
8.	CA copy and paste the sha256hash and paste it on Text Editor by going to **Applications > Accessories > Text Editor**	Y.G.	0:09
9.	CA prints two copies of the hash. One for the audit bundle and the other for the HSMFD package then writes "KSK 24" on the printed copies.	Y.G.	0:10
10.	CA displays contents of HSMFD by executing `ls -ltr`	Y.G	0:11
11.	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_`	Y.G	0:11
12.	CA displays contents of HSMFD_ by executing `ls -ltr /media/HSMFD_`	Y.G.	0:12
13.	Calculate the sha256hash of the contents on the copied HSMFD. `find -P /media/HSMFD_ -type f -print0 | sort -z | xargs -0 cat | sha256sum` Confirm that it matches the sha256hash of the original HSMFD by using the text editor to copy and paste the hash for comparison.	Y.G.	0:12
14.	CA unmounts new FD using `umount /media/HSMFD_`	Y.G.	0:12
15.	CA removes **HSMFD_** and places it on the table.	Y.G.	0:13
16.	CA repeats step 11 to 15 for the 2nd copy	Y.G.	0:14
17.	CA repeats step 11 to 15 for the 3rd copy	Y.G.	0:15
18.	CA repeats step 11 to 15 for the 4th copy	Y.G.	0:15
19.	CA repeats step 11 to 15 for the 5th copy	Y.G.	0:16

Print Logging Information

Step	Activity	Initials	Time

20.	CA prints out a hard copy of logging information by executing
	`enscript -2Gr -# 1 script-20160211.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20160211-*.log`
	for attachment to IW1 script.
	Note: Ignore the error regarding non-printable characters if prompted.
		Y.G.	0:17

Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initials	Time

21.	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
	CA removes HSMFD.
		Y.G.	0:18

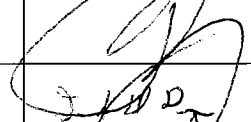
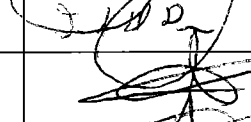
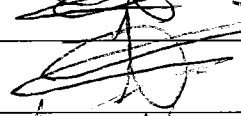
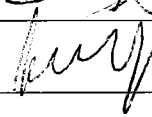
22.	After all print jobs are complete, CA a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch c) Remove the O/S DVD from the drive d) Turns off the laptop again by pressing the power switch	Y.G.	0:19
23.	CA places **TWO** HSMFDs and OS/DVD, paper with printed hash in prepared TEB; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **O/S DVD (Rev600) + HSMFD: TEB# BB46584278**	Y.G.	0:21
24.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.	Y.G	0:21

Distribute HSMFDs

Step	Activity	Initials	Time
25.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 2 for IKOS) to post SKR to RZM, and to review, analyze and improve on procedures.	Y.G.	0:22

Returning Laptop to a TEB

Step	Activity	Initials	Time
26.	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. **Laptop1 (Dell ATG6400): TEB# BB24646619 / serial # 37240147333**	Y.G.	0:24
27.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.	Y.G.	0:24

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584279	Arbogast Fabian		12 ~~11~~ February 2016	0:29	Y.G.
CO 2	OP 2 of 7	BB46584280	Dmitry Burkov		12 ~~11~~ February 2016	0:31	Y.G.
CO 3	OP 3 of 7	BB46584281	Joao Damas		12 ~~11~~ February 2016	0:32	Y.G.
CO 6	OP 6 of 7	BB46584283	Nicolas Antoniello		12 ~~11~~ February 2016	0:34	Y.G.
CO 6	SO 6 of 7	BB46584284	Nicolas Antoniello		12 ~~11~~ February 2016	0:38	Y.G.
CO 7	OP 7 of 7	BB46584285	Subramanian Moonesamy		12 ~~11~~ February 2016	0:35	Y.G.

Returning OP Cards to TEBs

Step	Activity	Initials	Time
28.	CA calls each COs to the front of the room one at a time and repeats the steps below. a) CA takes the 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) CO places the OP card into the plastic case. c) CA places the plastic case into the TEB, seals in front of IW1 and CO then the CA initials TEB and strip. d) IW1 inspects each TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. e) CA hands TEB containing the OP card to the CO. CO inspects and verifies TEB # and contents then initials his/her TEB. f) CO enters completion time and signs for TEB in the table below in IW1's script. IW1 initials table entry. g) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB. **CO 1: Arbogast Fabian** **OP TEB # BB46584279** **CO 2: Dmitry Burkov** **OP TEB # BB46584280** **CO 3: Joao Damas** **OP TEB # BB46584281** **CO 6: Nicolas Antoniello** **OP TEB # BB46584283** **CO 7: Subramanian Moonesamy** **OP TEB # BB46584285**	Y.G.	0:36

Change SO 6 card TEB

Step	Activity	Initials	Time
29.	CA calls the CO 6 with a SO card TEB to the front of the room and performs the steps below. a) CO opens the SO card TEB and confirms the contents b) CO places the SO card into the plastic case (if applicable) c) CA places the plastic case into the TEB, seals in front of IW1 and CO then the CA initials TEB and strip. d) IW1 inspects the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. e) CA hands TEB containing the SO cards to the CO. CO inspects and verifies TEB # and contents then initials his/her TEB. f) CO enters completion time and signs for TEB in the table below in IW1's script. IW1 initials table entry. g) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB. **CO 6: Nicolas Antoniello** **SO TEB # BB46584284**	Y.G.	0:39

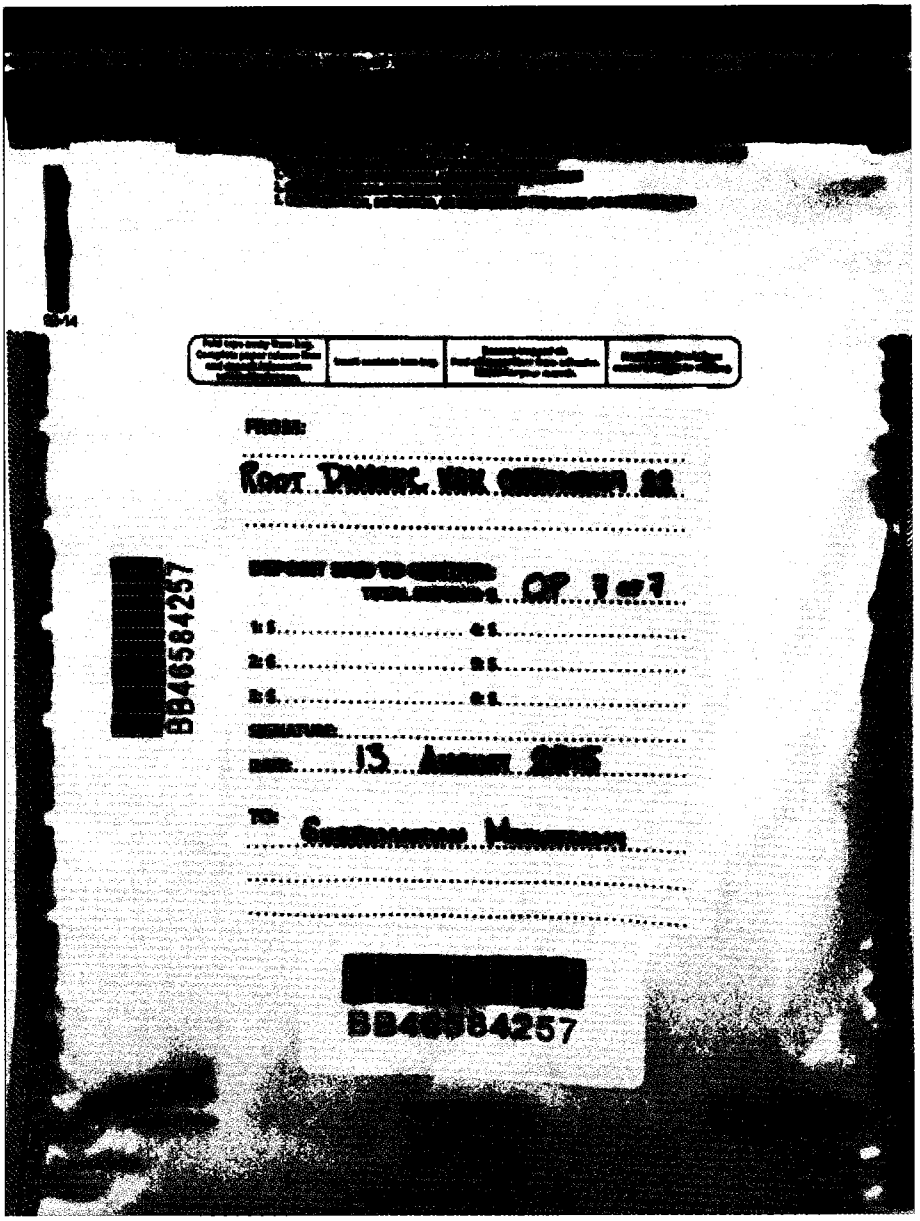


Figure 2

Returning Equipment to Safe #1

Step	Activity	Initials	Time
30.	CA, IW1, SSC1 open safe room and enter with equipment cart.	Y.G	0:40
31.	SSC1 opens Safe #1 shielding combination from camera.	Y.G.	0:41
32.	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.**	Y.G.	0:42
33.	CA records return of **HSM3** in next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA **CAREFULLY** places the HSMs into Safe #1 and IW1 initials the entry. **HSM3: TEB# BB24646618**	Y.G	0:43
34.	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. **Laptop1 (Dell ATG6400): TEB# BB24646619**	Y.G.	0:43
35.	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. **O/S DVD (Rev600) + HSMFD: TEB# BB46584278**	Y.G.	0:44

Close Equipment Safe #1

Step	Activity	Initials	Time
36.	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.**	Y.G.	0:44
37.	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.	Y.G.	0:45
38.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	Y.G.	0:45

Open Credential Safe #2

Step	Activity	Initials	Time
39.	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 and SO cards (if applicable) in TEBs with them.	Y.G.	0:47
40.	SSC2 opens Safe #2 while shielding combination from camera.	Y.G.	0:50
41.	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.**	Y.G.	0:51

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
42.	One by one, each COs 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. **# Common Key is bottom lock and CO Key is top lock** b) CO makes an entry into the safe log indicating the return of OP card and SO cards (if applicable) 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 each TEB 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. **CO 1: Arbogast Fabian** **Box #: 1791** **OP TEB # BB46584279** **CO 2: Dmitry Burkov** **Box #: 1793** **OP TEB # BB46584280** **CO 3: Joao Damas** **Box # 1071** **OP TEB # BB46584281** **CO 6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584283** **SO TEB # BB46584284** **CO 7: Subramanian Moonesamy** **Box #: 1792** **OP TEB # BB46584285**	Y.G.	0:57

Close Credential Safe #2

Step	Activity	Initials	Time
43.	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.**	Y.G	0:57
44.	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.	Y.G.	0:58
45.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	Y.G.	0:58

Participant Signing of IW1's Script

Step	Activity	Initials	Time
46.	One by one, all participants come to the front of the room, confirms printed name and date. **Then, the participant declares that this script is a true and accurate record of the ceremony by signing on IW1's script coversheet.** IW records the completion time once all participants have signed the coversheet. **Note: If entry is pre-printed, verify the entry and sign.**	Y.G	1:03
47.	CA reviews IW1's script and signs it.	Y.G.	1:04

Online Streaming Stops

Step	Activity	Initials	Time
48.	CA acknowledges the participation of online participants and confirms with SA to stop online streaming.	Y.G.	1:05

Signing Out of Ceremony Room

Step	Activity	Initials	Time
49.	IKOS 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.	Y.G.	1:14

Filming Stops

Step	Activity	Initials	Time
50.	CA confirms with SA to stop filming.	Y.G.	1:14

Copying and Storing the Script

Step	Activity	Initials	Time
51.	IW1 makes at least 1 copy of his/her script for off-site audit bundle. Audit bundles each contain: a) Output of signer system – HSMFD b) Copy of IW1's key ceremony script c) Audio-visual recording d) Logs from the Physical Access Control and Intrusion Detection System (Range is **08/13/2015 – 02/11/2016**) e) The IW attestation (A.1 below) f) SA attestation (A.2, A.3 below) All in a TEB labeled **"Root DNSSEC KSK Ceremony 24"**, 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.**	Y.G	2:22

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.

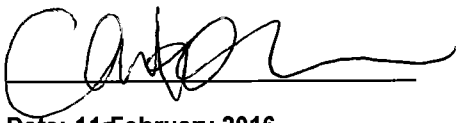
6. Configuration review of the Firewall System (SA)
SA's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3. Make sure the scrambled passwords are eliminated from the configuration before publishing it.

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.

Yuko Green



Date: ~~11~~ 12 February 2016

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 **13 August 2015 00:00 UTC** to now.

~~Connor Barthold~~ Brian Martin

Date: 4 February 2016

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.

~~Conner Bardhold~~ Brian Martin

Date: ~~14~~ 17 February 2016

```
jjenkins@srx> show configuration | no-more
## Last commit: 2014-12-12 18:55:44 UTC by cbarthold
version 12.1X44-D35.5;
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
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user reed {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
```

```
            authentication {
                encrypted-password
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
    }
    services;
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
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 10.100.1.1/24;
            }
        }
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 192.0.35.202/26;
            }
        }
    }
    vlan {
        unit 0 {
            family inet {
                address 10.4.28.1/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.0.35.201;
    }
}
security {
    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;
                        }
                    }
                }
            }
            rule-set wifi-to-untrust {
                from zone wifi;
                to zone untrust;
                rule source-nat-rule2 {
                    match {
                        source-address 0.0.0.0/0;
                    }
```

```
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy trust-to-untrust {
                match {
                    source-address localnet;
                    destination-address [ icann simplex1 simplex2
googledns1 googledns2 ];
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
        from-zone wifi to-zone untrust {
            policy internet {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    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 icann 192.0.32.0/20;
                address simplex1 216.224.218.31/32;
                address simplex2 216.224.219.32/32;
                address googledns1 8.8.8.8/32;
                address googledns2 8.8.4.4/32;
            }
            interfaces {
                ge-1/0/0.0 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
        security-zone wifi {
            interfaces {
                ge-0/0/0.0;
            }
        }
    }
}
vlans {
    vlan-trust {
        vlan-id 3;
        l3-interface vlan.0;
    }
}
```