



Internet Corporation for Assigned Names and Numbers
Root DNSSEC KSK Ceremony 21
Thursday April 9, 2015

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



Abbreviations

TEB = Tamper Evident Bag (AMPAC, item #GCS1013 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large) SO = Security Officer OP = Operator
 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
 KSR = Key Signing Request SKR = Signed Key Response RZM = Root Zone Maintainer
 AUD = Third Party Auditor EW = External Witness

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	Francisco Arias / ICANN	<i>[Signature]</i>	9 April 2015	22:48
IW1	Gustavo Lozano / ICANN	<i>[Signature]</i>		
SSC1	Maria Otones / ICANN	<i>[Signature]</i>		
SSC2	Grace Abuhamad / ICANN	<i>[Signature]</i>		
CO2	Anne-Marie Eklund Lowinder / SE	<i>[Signature]</i>		
CO4	Robert Seastrom / US	<i>[Signature]</i>		
CO5	Christopher Griffiths / US	<i>[Signature]</i>		
CO6	Gaurab Upadhaya / NP	<i>[Signature]</i>		
CO7	Alain Aina / TG	<i>[Signature]</i>		
RZM	Alejandro Bolivar / Verisign	<i>[Signature]</i>		
RZM	Andrew Kim / Verisign	<i>[Signature]</i>		
AUD	Ken Michaels / PricewaterhouseCoopers	<i>[Signature]</i>		
AUD	Ryan Ung / PricewaterhouseCoopers	<i>[Signature]</i>		
AUD	Patricia Manning / PricewaterhouseCoopers	<i>[Signature]</i>		
SA1	Connor Barthold / ICANN	<i>[Signature]</i>		
SA2	Reed Quinn / ICANN	<i>[Signature]</i>		
Staff Witness	Kim Davies / ICANN	<i>[Signature]</i>		
Staff Witness	Richard Lamb / ICANN	<i>[Signature]</i>		
Staff Witness	Edward Lewis / ICANN	<i>[Signature]</i>		
IW2 / IKOS	Alberto Duero / ICANN	<i>[Signature]</i>		
IW3 / IKOS	Andres Pavez / ICANN	<i>[Signature]</i>		
IW4	Patrick Jones / ICANN	<i>[Signature]</i>		
EW1	Andrew Bagley	<i>[Signature]</i>		
EW2	Karin Grundskog			

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.	SA confirms that all audit cameras are recording and online streaming is live.	GL	16:57
✓ 2.	IW1 confirms that all participants are signed into the Ceremony Room.	GL	17:04

Emergency Evacuation Procedures

Step	Activity	Initials	Time
✓ 3.	CA reviews emergency evacuation procedures with participants.	GL	17:09

Verify Time and Date

Step	Activity	Initials	Time
✓ 4.	<p>IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room:</p> <p>Date and time: <u>09/10 4/2015 17:10</u></p> <p>All entries into this script or any logs should follow this common source of time.</p>	GL	17:10

Open Credential Safe #2

Step	Activity	Initials	Time
✓ 5.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.	GL	17:12
✓ 6.	SSC2, while shielding combination from camera, opens Safe #2.	GL	17:14
✓ 7.	<p>SSC2 takes out the existing safe log and shows the most current page to the camera.</p> <p>IW1 provides a blank pre-printed safe log to the SSC2.</p> <p>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.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p>	GL	17:15



COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
8.	<p>One by one, the selected COs retrieves required OP cards and SO cards following the steps shown below.</p> <p>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</p> <p>b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below.</p> <p>c) Retains OP TEB and SO TEB and locks box.</p> <p>d) Makes an entry in safe log indicating OP TEB and SO TEB removal with box #, printed name, date, time and signature.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>Repeat these steps until all required cards are removed. IW1 initials this entry when all COs have finished.</p> <p>CO 2: Anne-Marie Eklund Lowinder Box # 1259 OP TEB # BB21907187 (Retain) SO TEB # BB21820445 (Retain)</p> <p>CO 4: Robert Seastrom Box # 1260 OP TEB # BB21907190 (Retain) SO TEB # BB21820447 (Retain)</p> <p>CO 5: Christopher Griffiths Box # 1240 OP TEB # BB21820420 (Retain) SO TEB # BB21820449 (Retain)</p> <p>CO 6: Gaurab Upadhaya Box # 1261 OP TEB # BB21820421 (Retain) SO TEB # BB21820422 (Retain)</p> <p>CO 7: Alain Aina Box # 1242 OP TEB # BB21369019 (Retain) SO TEB # A14377129 (Retain)</p>	<p>GL</p>	<p>17:24</p>



Close Credential Safe #2

Step	Activity	Initials	Time
✓ 9.	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.	GL	17:25
✓ 10.	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.	GL	17:25
✓ 11.	IW1, CA, SSC2, and COs leave safe room, with OP cards and SO cards (if applicable) in TEBs, closing the door behind them.	GL	17:26

Open Equipment Safe #1

Step	Activity	Initials	Time
✓ 12.	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	GL	17:28
✓ 13.	SSC1, while shielding combination from camera, opens Safe #1.	GL	17:29
✓ 14.	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.	GL	17:31



Remove Equipment from Safe #1

Step	Activity	Initials	Time
✓ 15.	<p>CA CAREFULLY removes HSM2, HSM3 and HSM4 (in TEB) from the safe and completes the entry in 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.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>HSM2: TEB# BB24706800 / serial # K6002013 ✓</p> <p>HSM3: TEB# BB24646612 / serial # H1403032 ✓</p> <p>HSM4: TEB# BB24646680 / serial # H1411011 ✓</p> <p>Verify the integrity of the other HSM that will not be used this time and return it to the safe.</p> <p>HSM1: TEB# BB24706804 / serial # K6002016 (last used) ✓</p>	GL	17:36
✓ 16.	<p>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.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>Laptop1 (Dell ATG6400): TEB# BB24706801 / serial # 41593712005 ✓</p> <p>O/S DVD (Rev600) + HSMFD: TEB# BB21820430 ✓</p> <p>APP. Key: TEB# A14377114 ✓</p> <p>Verify the integrity of the other Laptop that will not be used this time and return it to the safe.</p> <p>Laptop2 (Dell ATG6400): TEB# BB24646602 / serial # 35063364997 ✓</p>	GL	17:41

Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
✓ 17.	<p>SSC1 makes an entry including printed name, date, time and signature into the safe log indicating, "Close safe". IW1 initials this entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p>	GL	17:42
✓ 18.	<p>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).</p> <p>CA and IW1 verify that the safe is locked and door indicator light is green.</p>	GL	17:42
✓ 19.	<p>CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.</p>	GL	17:43



Act 2. Confirm, Sign the Key Signing Request and Issue Authorization Key (AAK) and Storage Master Key (SMK) Cards

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# BB24706801 / serial # 41593712005	GL	17:45
✓ 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# BB21820430	GL	17:46
✓ 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.	GL	17:51
✓ 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 <code>system-config-display --noui</code> c) CA executes <code>killall Xorg</code> d) CA confirms that external display works. e) CA logs in as root	GL	17:53
✓ 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 <u>first device</u> " 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 "	GL	17:54



Step	Activity	Initials	Time
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	GL	17:55
7.	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 & Time CA executes <code>date</code> using the Terminal window to confirm the date is properly configured.	GL	17:56

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 <code>dmesg grep -A 5 usb-storage</code> to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc), <code>umount /dev/sda</code> to unmounts the drive (change drive letter and partition if necessary), <code>mkfs.vfat -n HSMFD -I /dev/sda</code> to execute a FAT32 format and label it as HSMFD. CA unplugs the FD.	GL	17:58
9.	CA repeats step 8 for the 2 nd blank FD	GL	17:59
10.	CA repeats step 8 for the 3 rd blank FD	GL	17:59
11.	CA repeats step 8 for the 4 th blank FD	GL	18:00
12.	CA repeats step 8 for the 5 th blank FD	GL	18:00

Connect HSMFD

Step	Activity	Initials	Time
13.	CA plugs the previous HSMFD used in the ceremony 19 into 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.	GL	18:02

Step	Activity	Initials	Time
14.	<p>Calculate the sha256 hash of the contents on the copied HSMFD.</p> <pre>find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum</pre> <p>IW confirms that the result matches the sha256 hash of the HSMFD that is on the annotated script from the Ceremony 19.</p> <p>Previous hash should read as below (image from Ceremony 19 annotated script).</p> <pre>be4943b2ab9b7bde230cf6abaa92f4fe69237dff8228fce6cb4d42dbeed4fc15</pre> <p>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.</p>	GL	18:04

Start Logging Terminal Session

Step	Activity	Initials	Time
15.	CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code>	GL	18:04
16.	CA executes <code>script script-20150409.log</code> to start a capture of terminal output.	GL	18:05

Start Logging HSM Output

Step	Activity	Initials	Time
17.	CA connects a serial to USB null modem cable to laptop.	GL	18:05
18.	<p>CA opens a second terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal.</p> <p>Follow the additional steps to maximize the terminal window:</p> <ul style="list-style-type: none"> a) Click the View menu and select Zoom In b) Repeat the step above as necessary <p>and executes <code>cd /media/HSMFD</code></p> <p>and executes <code>ttyaudit /dev/ttyUSB0</code></p> <p>to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.</p>	GL	18:07



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: <u>09/04/2015 18:18</u>	AL	18:18
2.	IW1 Describes exception and action below.	AL	18:18.

Page 11 of 56

Step 22

There is a typo, it should say SO instead of CO in step 22 instruction.

– End of DNSSEC Script Exception –



HSM2: Power Up

Step	Activity	Initials	Time
✓ 19.	CA inspects the HSM2 TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. HSM2: TEB# BB24706800 ✓ serial # K6002013 ✓	GL	18:09
✓ 20.	CA removes HSM2 from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	GL	18:11
✓ 21.	CA switches to the ttyaudit terminal window and connects power to HSM2. Status information should appear on the serial logging screen. IW1 matches displayed HSM2 serial number with below. (Time and date in the HSM2 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.) HSM2: Serial # K6002013 ✓ Note: The HSM2 date and time was set from the factory.	GL	18:12

HSM2: Enable/Activate

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 and SO cards to the CA who places the cards in cardholder visible to all. SO		
	CO 2: Anne-Marie Eklund Lowinder OP TEB # BB21907187 ✓ SO TEB # BB21820445 ✓		
	CO 4: Robert Seastrom OP TEB # BB21907190 ✓ SO TEB # BB21820447 ✓		
	CO 5: Christopher Griffiths OP TEB # BB21820420 ✓ SO TEB # BB21820449 ✓	GL	18:23
	CO 6: Gaurab Upadhaya OP TEB # BB21820421 ✓ SO TEB # BB21820422 ✓		
	CO 7: Alain Aina OP TEB # BB21369019 ✓ SO TEB # A14377129 ✓		



Step	Activity	Initials	Time
23.	<p>CA will perform the following steps to activate the HSM2:</p> <ul style="list-style-type: none"> 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 OP card from the cardholder e) When "PIN?" is displayed, enter "41223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP cards <p>Confirm the "READY" led on the HSM is ON.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <u>2</u> of 7 2nd OP card <u>4</u> of 7 3rd OP card <u>6</u> of 7</p>	GL	18:27

HSM2: Check Network Connectivity

Step	Activity	Initials	Time
24.	CA connects HSM2 to laptop using Ethernet cable.	GL	18:28
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.	GL	18:28

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.	GL	18:29



VERISIGN™

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

April 2nd, 2015

VerisignInc.com

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, currently as a Sr. Manager - CBO in our 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 Specialist | Verisign, Inc. | 703-948-4143 | dcarney@verisign.com



VERISIGN™

April 09, 2015

The SHA256 hash of the 2015 Q3 KSR file is:

**eleaca147d556444f8b4acba01902753a4babde0c0605efb9060b59ed
396f2c4**

The PGP wordlist for the hash above is:

tempest undaunted spellbind belowground klaxon equipment
flytrap designing Vulcan politeness ribcage puberty
absurd millionaire brackish enterprise regain puberty
skullcap tobacco slowdown fortitude eyeglass Wichita
peachy fortitude scorecard onlooker stapler monument
uproot reproduce

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

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

VerisignInc.com



Execute KSR signer

Step	Activity	Initials	Time
✓ 27.	CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR/ksr-root-2015-q3-0.xml</code>	GL	18:30
✓ 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 HSM2 is online and then enters "y" to proceed to verification. Note: DO NOT enter "y" for the "Is this correct y/n?" yet.	GL	18:30

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: <u>Alejandro Bulner</u>	GL	18:31
✓ 30.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections?"	GL	18:32
✓ 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 <code>/media/KSR/skr-root-2015-q3-0.xml</code>	GL	18:33



ICANN Root DNSSEC KSK Ceremony 21

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

Starting: krsigner 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:
A17E539793B261112C4F591A06AF4FBC2221DDDD71794BC72D5AEE910C72543
>> 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/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 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:
00CC34187B3BAE2E62B1AA6A58DEF07F02E4950E959E6A6ACBD7CEFF2741257
>> 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 ./krsigner-20100712-224426.log *****
```

Figure 1



Print Copies of the Operation for Participants

Step	Activity	Initials	Time
✓ 32.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog ksrsigner-20150409-*.log; done</code> where ksrsigner-20150409-*.log is replaced by log output file displayed by program. This example generates X copies and hands copies to participants.	GL	18:36
✓ 33.	IW1 attaches a copy to his/her script and writes "HSM2 SKR".	GL	18:37

Backup Newly Created SKR

Step	Activity	Initials	Time
✓ 34.	CA copies the contents of the KSR FD by running <code>cp -p /media/KSR/*</code> for posting back to RZM. Confirm overwrite by entering "y" when prompted.	GL	18:38
✓ 35.	CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR</code> flushes the system buffers: <code>sync</code> and then unmounts the KSR FD using <code>umount /media/KSR</code>	GL	18:38
✓ 36.	CA removes KSR FD containing SKR and gives it to the RZM representative.	GL	18:39

HSM2: Disable/Deactivate

Step	Activity	Initials	Time
✓ 37.	CA makes sure to utilize the cards that were NOT used to activate the HSM2 are used to deactivate the HSM2. CA will perform the following steps to deactivate the HSM2: 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" and 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 <u>5</u> of 7 2nd OP card <u>7</u> of 7 3rd OP card <u>2</u> of 7	GL	18:41

HSM2 SKR

Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2015-q3-0.xml (at Thu Apr 9 18:30:38 2015 UTC)

Use HSM /opt/dnssec/aep.hsmconfig?

HSM /opt/dnssec/aep.hsmconfig activated.

setenv KEYPER_LIBRARY_PATH=/opt/dnssec

setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07

Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07

HSM slot 0 included

Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

HSM Information:

Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper Pro 0405
Serial: K6002013

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2015-04-01T00:00:00	2015-04-15T23:59:59	16665,48613	19036
2	2015-04-11T00:00:00	2015-04-25T23:59:59	48613	19036
3	2015-04-21T00:00:00	2015-05-05T23:59:59	48613	19036
4	2015-05-01T00:00:00	2015-05-15T23:59:59	48613	19036
5	2015-05-11T00:00:00	2015-05-25T23:59:59	48613	19036
6	2015-05-21T00:00:00	2015-06-04T23:59:59	48613	19036
7	2015-05-31T00:00:00	2015-06-14T23:59:59	48613	19036
8	2015-06-10T00:00:00	2015-06-24T23:59:59	48613	19036
9	2015-06-20T00:00:00	2015-07-05T23:59:59	01518,48613	19036

...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2015-q3-0.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2015-07-01T00:00:00	2015-07-15T23:59:59	01518,48613	
2	2015-07-11T00:00:00	2015-07-25T23:59:59	01518	
3	2015-07-21T00:00:00	2015-08-04T23:59:59	01518	
4	2015-07-31T00:00:00	2015-08-14T23:59:59	01518	
5	2015-08-10T00:00:00	2015-08-24T23:59:59	01518	
6	2015-08-20T00:00:00	2015-09-03T23:59:59	01518	
7	2015-08-30T00:00:00	2015-09-13T23:59:59	01518	
8	2015-09-09T00:00:00	2015-09-24T00:00:00	01518	
9	2015-09-20T00:00:00	2015-10-05T23:59:59	62530,01518	

*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:

E1EACA147D556444F8B4ACBA01902753A4BABDE0C0605EFB9060B59ED396F2C4

>> tempest undaunted spellbind belowground klaxon equipment flytrap designing Vulcan po
liteness ribcage puberty absurd millionaire brackish enterprise regain puberty skullcap
tobacco slowdown fortitude eyeglass Wichita peachy fortitude scorecard onlooker staple
r monument uproot reproduce <<

Generated new SKR in /media/KSR/skr-root-2015-q3-0.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
---	-----------	------------	----------	--------------------

ASM2 SKR

1	2015-07-01T00:00:00	2015-07-15T23:59:59	01518,48613	19036
2	2015-07-11T00:00:00	2015-07-25T23:59:59	01518	19036
3	2015-07-21T00:00:00	2015-08-04T23:59:59	01518	19036
4	2015-07-31T00:00:00	2015-08-14T23:59:59	01518	19036
5	2015-08-10T00:00:00	2015-08-24T23:59:59	01518	19036
6	2015-08-20T00:00:00	2015-09-03T23:59:59	01518	19036
7	2015-08-30T00:00:00	2015-09-13T23:59:59	01518	19036
8	2015-09-09T00:00:00	2015-09-24T00:00:00	01518	19036
9	2015-09-20T00:00:00	2015-10-05T23:59:59	62530,01518	19036

SHA256 hash of SKR:

DD92D903CE328A6C577C47A3619680CC955A90AFA8869F4F99B43A285A8F038A

>> swelter misnomer sugar aggregate spyglass component Oakland handiwork eightball info
rmant dashboard pandemic fallout monument merit revolver preclude existence peachy phar
macy retouch letterhead quota document prowler politeness cleanup cellulose enlist mids
ummer acme maverick <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0



HSM2: Issuing Storage Master Key (SMK) Cards

Step	Activity	Initials	Time
38.	<p>CA makes sure to utilize 3 SO cards from the same set to make Storage Master key (SMK) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Key Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO 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 2nd and 3rd SO cards h) Select "1.SMK" hit ENT to confirm i) Select "2.Backup SMK" hit ENT to confirm j) When "Backup SMK?" is displayed, hit ENT to confirm k) When "Num Cards?" is displayed, enter "4" and press ENT to confirm l) When "Num Req Cards?" is displayed, enter "2" and press ENT to confirm m) When "Insert Card #?" is displayed, insert the proper sequence of SMK card from the cardholder n) When "Remove Card?" is displayed, remove card o) Repeat steps m) to n) for the 2nd, 3rd and 4th cards p) When "SMK Backed Up" is displayed, hit ENT to confirm q) Hit CLR to return to the previous menu <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>2</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p>	<p>GL</p>	<p>18:49</p>



HSM2: Issuing Authorization Key (AAK) Cards

Step	Activity	Initials	Time
39.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to make Authorization key (AAK) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Key Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO 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 2nd and 3rd SO cards h) Select "3.AAK" hit ENT to confirm i) Select "1.Backup AAK" hit ENT to confirm j) When "Backup AAK?", is displayed, hit ENT to confirm k) When "Num Cards?" is displayed, enter "2" and press ENT to confirm l) When "Insert Card #?" is displayed, insert the proper sequence of AAK card from the cardholder m) When "Remove Card?" is displayed, remove card n) Repeat steps l) to m) for the 2nd AAK card o) When "AAK Exported" is displayed, hit ENT to confirm p) Hit CLR to return to the previous menu <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>6</u> of 7</p> <p>2nd SO card <u>7</u> of 7</p> <p>3rd SO card <u>2</u> of 7</p>	SC	18:54



HSM2: Return to a TEB

Step	Activity	Initials	Time
✓ 40.	CA disconnects HSM2 from power and laptop (serial and Ethernet) if connected.	GL	18:55
✓ 41.	CA places the HSM2 into a prepared TEB and seals it.	GL	18:56
42.	CA reads out TEB # and HSM2 serial #, shows item to participants and IW1 confirms TEB # and HSM2 serial # below. HSM2: TEB# BB2464667# / serial # K6002013 IW1 and CA initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.	GL	18:58

HSM2: Stop Recording Serial Port Activity

Step	Activity	Initials	Time
✓ 43.	Closing ttyaudit terminal window CA terminates the HSMs serial output capture by disconnecting the USBs serial adaptors from laptop. CA then exits out of ttyaudit terminal window by typing "exit".	GL	18:59



Act. 3 HSM Replacement

Start Logging HSM Output

Step	Activity	Initials	Time
✓ 1.	CA connects a serial to USB null modem cable to laptop.	GL	18:59
✓ 2.	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 <code>cd /media/HSMFD</code> <code>stty -F /dev/ttyUSB0 115200</code> <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.	GL	19:01

HSM3: Power Up

Step	Activity	Initials	Time
✓ 3.	CA inspects the HSM3 TEB for tamper evidence; reads out TEB # and serial #. IW1 confirms TEB # and serial # below. HSM3: TEB# BB24646612 serial # H1403032	GL	19:02
✓ 4.	CA removes HSM3 from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	GL	19:03
✓ 5.	CA switches to the ttyaudit terminal window, connects power to HSM3 and turns on by pressing the power switch behind it. Status information should appear on the serial logging screen and after self test the HSM3 display should say " Important Read Manual " indicating the HSM3 is in the initialized state. IW1 matches displayed HSM3 serial number with below. HSM3: Serial # H1403032	GL	19:05



HSM3: Importing the AAK

Step	Activity	Initials	Time
6.	CA will perform the following steps to import the AAK: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "2.Restore AAK" hit ENT to confirm c) When "Restore AAK?" is displayed, hit ENT to confirm d) When "Insert Card #?" is displayed, insert the proper sequence of AAK card from the cardholder e) When "Remove Card?" is displayed, remove card f) Repeat steps d) to e) for the 2nd AAK card g) When "AAK Imported" is displayed, hit ENT to confirm As each card is used the CA places it in the cardholder.	FL	19:06



HSM3: Switching to Secure State

Step	Activity	Initials	Time
7.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to set the HSM3 in Secure State:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "3.Secure" hit ENT to confirm c) When "Secure?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO 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 SO card h) When "SMK AES Triple DES?" is displayed, hit CLR to skip i) When "SMK AES" is displayed, hit CLR to confirm j) When "Set HSM Port?" is displayed, hit CLR to skip k) When "Enable IPv4/IPv6?" is displayed, hit CLR to skip l) When "Set IPv4 Address?" is displayed, hit CLR to skip m) When "Set IPv4 NetMask?" is displayed, hit CLR to skip n) When "Set IPv4 Gateway?" is displayed, hit CLR to skip o) When "Set IPv6 Address?" is displayed, hit CLR to skip p) When "Set IPv6 NetMask?" is displayed, hit CLR to skip q) When "Set IPv6 Gateway?" is displayed, hit CLR to skip r) When "Change Clock?" is displayed, hit CLR to skip s) When "Import Config.?" is displayed, hit CLR to skip t) When "FIPS Mode On Disable?" is displayed, hit CLR to skip u) When "FIPS Mode On" is displayed, hit CLR to confirm v) When "Global Key Export Enabled" is displayed, hit CLR to confirm <p>Done Rebooting Device will be displayed and confirm that the HSM3 is in Secured State.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>2</u></p> <p>1st SO card <u>2</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p>	<p>SL</p>	<p>19:11</p>



HSM3: Issuing Crypto Officer (CO) Cards

Step	Activity	Initials	Time
8.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to make Crypto Officer (CO) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "7.Role Mgmt" hit ENT to confirm c) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd and 3rd SO card g) Select "1.Issue Cards" hit ENT to confirm h) Select "1.Issue CO Cards" hit ENT to confirm i) When "Issue CO Cards?" is displayed, hit ENT to confirm j) When "Num Cards?" is displayed, enter "3" and hit ENT to confirm k) When "Num Req Cards?" is displayed, enter "2" and hit ENT to confirm l) When "Insert Card #?" is displayed, insert the proper sequence of CO card from the cardholder m) When "PIN?" is displayed, enter "11223344" and hit ENT n) When "Remove Card?" is displayed, remove card o) Repeat steps l) to n) for the 2nd and 3rd CO cards p) When "CO Cards Issued" is displayed, hit ENT to confirm q) Hit CLR twice to return to the main menu "Secured" <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>2</u> 1st SO card <u>6</u> of 7 2nd SO card <u>8</u> of 7 3rd SO card <u>2</u> of 7</p>	<p>GL</p>	<p>19:17</p>



HSM3: Change and Verify API Settings

Step	Activity	Initials	Time
9. ✓	CA will perform the following steps to change the API settings: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "5. API Settings" hit ENT to confirm h) Select "1.Key Import" hit ENT to confirm i) When "Key Import On Disable?" is displayed, hit ENT to confirm j) Select "2.Key Export" hit ENT to confirm k) When "Key Export On Disable?" is displayed, hit ENT to confirm l) Select "5.Sym Key Der" hit ENT to confirm m) When "Sym Key Der On Disable?" is displayed, hit ENT to confirm n) Hit CLR twice to return to the main menu "Secured" As each card is created the CA places it in the cardholder.	RL	19:20



Step	Activity	Initials	Time
10.	<p>CA will perform the following steps to dumps the status of the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "4.HSM Info" hit ENT to confirm c) Select "8.Output Info" hit ENT to confirm d) When "Output Info?" is displayed, hit ENT to confirm e) Hit CLR to return to the main menu "Secured" <p>CA switches to the ttyaudit terminal window to confirm with IW the output of the HSM configuration matches with the list below:</p> <pre> Modes: (1=Enabled 0=Disabled) Global Key Export 1 ✓ App Key Import 0 ✓ App Key Export 0 ✓ Asymmetric Key Gen 1 ✓ Symmetric Key Gen 1 ✓ Symmetric Key Derive 0 ✓ Signing 1 ✓ Signature Verify 1 ✓ MAC Generation 1 ✓ MAC Verification 1 ✓ Encrypt / Decrypt 1 ✓ Delete Asym Key 1 ✓ Delete Sym Key 1 ✓ Output Key Details 1 ✓ Output Key Summary 1 ✓ Suite B Algorithms 1 ✓ Non Suite B Algs 1 ✓ Auto Online 0 ✓ AES SMK ✓ FIPS Mode ✓ </pre>	<p>GC</p>	<p>19:22</p>

HSM3: Importing the SMK

Step	Activity	Initials	Time
11.	<p>CA will perform the following steps to import the Storage Master Key (SMK) cards in to the HSM3:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "4.SMK" hit ENT to confirm h) Select "3.Restore SMK" hit ENT to confirm i) When "Restore SMK?" is displayed, hit ENT to confirm j) When "Insert Card SMK #?" is displayed, insert the SMK card from the cardholder k) When "Remove Card?" is displayed, remove card l) Repeat steps j) to k) for the 2nd SMK card m) When "SMK Restored" is displayed, hit ENT to confirm n) Hit CLR twice to return to the main menu "Secured" <p>As each card is used the CA places it in the cardholder.</p>	<p>GL</p>	<p>19:25</p>



HSM3: Importing APP. Key

Step	Activity	Initials	Time
12.	CA inspects the APP. Key TEB for tamper evidence; reads out TEB #. IW1 confirms the TEB # below. APP. Key: TEB# A14377114	GL	19:27
13.	CA opens the TEB; discards TEB and place the cards and the initial HSMFDs in the cardholder.	GL	19:28
14.	CA will perform the following steps to import the Application Key (APP. Key) card: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "3.App Keys" hit ENT to confirm h) Select "2.Restore" hit ENT to confirm i) When "Restore?" is displayed, hit ENT to confirm j) When "Which Media?" is displayed, select "2. From Card" and hit ENT to confirm k) When "Insert Card #?" is displayed, insert the proper card from the cardholder l) When "Remove Card?" is displayed, remove card m) When "Restore Complete" is displayed, hit ENT to confirm n) Hit CLR twice to return to the main menu "Secured" As card is used the CA places it in the cardholder.	GL	19:31

HSM3: Enable/Activate

Step	Activity	Initials	Time
15.	<p>CA will perform the following steps to activate the HSM3:</p> <ul style="list-style-type: none"> 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 <p>Confirm the "READY" led on the HSM3 is ON. IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <input checked="" type="checkbox"/> of 7 2nd OP card <input checked="" type="checkbox"/> of 7 3rd OP card <input checked="" type="checkbox"/> of 7</p>	GL	19:33

HSM3: Check Network Connectivity between Laptop and HSM3

Step	Activity	Initials	Time
16.	CA connects HSM3 to laptop using Ethernet cable in LAN port.	GL	19:34
17.	CA tests network connectivity between laptop and HSM by entering <code>ping 192.168.0.2</code> on the laptop terminal window and looking for responses. Ctrl-C to exit program.	GL	19:34

Insert Copy of KSR to be signed

Step	Activity	Initials	Time
18.	CA plugs FD labeled "KSR_COPY" that contains a copy of the 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.	GL	19:35



Execute KSR signer

Step	Activity	Initials	Time
✓ 19.	CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR_COPY/ksr-root-2015-q3-0.xml</code>	GL	19:36
✓ 20.	The KSR signer will ask whether the HSM is activated or not as below. <i>Activate HSM prior to accepting in the affirmative!! (y/N):</i> CA confirms that the HSM3 is online and then enters "y" to proceed to verification. <i>Note: DO NOT enter "y" for the "Is this correct y/n?" yet.</i>	GL	19:36

Verification of the Hash (validity) of the KSR Copy

Step	Activity	Initials	Time
✓ 21.	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN.	GL	19:37
✓ 22.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections?"	GL	19:37
✓ 23.	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 <code>/media/KSR_COPY/skr-root-2015-q3-0.xml</code>	GL	19:37

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
✓ 24.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog \$(ls -tr ksrsigner-20150409-*.log tail -n 1); done</code> This example generates X copies and hands copies to participants.	GL	19:39
✓ 25.	IW1 attaches a copy to his/her script and writes "HSM3 SKR".	GL	19:41

Verification of the Hash (validity) of the SKR Copy

Step	Activity	Initials	Time
✓ 26.	CA read out the SHA256 hash in PGP wordlist format for the generated HSM3 SKR and the ceremony participants match the hash with the previous HSM2 SKR.	GL	19:43

HSM3 SKR

Starting: ksrsigner Kjqmt7v /media/KSR_COPY/ksr-root-2015-q3-0.xml (at Thu Apr 9 19:36:35 2015 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: H1403032

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2015-04-01T00:00:00	2015-04-15T23:59:59	16665,48613	19036
2	2015-04-11T00:00:00	2015-04-25T23:59:59	48613	19036
3	2015-04-21T00:00:00	2015-05-05T23:59:59	48613	19036
4	2015-05-01T00:00:00	2015-05-15T23:59:59	48613	19036
5	2015-05-11T00:00:00	2015-05-25T23:59:59	48613	19036
6	2015-05-21T00:00:00	2015-06-04T23:59:59	48613	19036
7	2015-05-31T00:00:00	2015-06-14T23:59:59	48613	19036
8	2015-06-10T00:00:00	2015-06-24T23:59:59	48613	19036
9	2015-06-20T00:00:00	2015-07-05T23:59:59	01518,48613	19036

...VALIDATED.

Validate and Process KSR /media/KSR_COPY/ksr-root-2015-q3-0.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2015-07-01T00:00:00	2015-07-15T23:59:59	01518,48613	
2	2015-07-11T00:00:00	2015-07-25T23:59:59	01518	
3	2015-07-21T00:00:00	2015-08-04T23:59:59	01518	
4	2015-07-31T00:00:00	2015-08-14T23:59:59	01518	
5	2015-08-10T00:00:00	2015-08-24T23:59:59	01518	
6	2015-08-20T00:00:00	2015-09-03T23:59:59	01518	
7	2015-08-30T00:00:00	2015-09-13T23:59:59	01518	
8	2015-09-09T00:00:00	2015-09-24T00:00:00	01518	
9	2015-09-20T00:00:00	2015-10-05T23:59:59	62530,01518	

*** Requests signature expiration exceeds limit of 180 days! ***

...PASSED.

SHA256 hash of KSR:

E1EACA147D556444F8B4ACBA01902753A4BABDE0C0605EFB9060B59ED396F2C4

>> tempest undaunted spellbind belowground klaxon equipment flytrap designing Vulcan po
liteness ribcage puberty absurd millionaire brackish enterprise regain puberty skullcap
tobacco slowdown fortitude eyeglass Wichita peachy fortitude scorecard onlooker staple
r monument uproot reproduce <<

Generated new SKR in /media/KSR_COPY/skr-root-2015-q3-0.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
---	-----------	------------	----------	--------------------

HSM3 SKR

1	2015-07-01T00:00:00	2015-07-15T23:59:59	01518,48613	19036
2	2015-07-11T00:00:00	2015-07-25T23:59:59	01518	19036
3	2015-07-21T00:00:00	2015-08-04T23:59:59	01518	19036
4	2015-07-31T00:00:00	2015-08-14T23:59:59	01518	19036
5	2015-08-10T00:00:00	2015-08-24T23:59:59	01518	19036
6	2015-08-20T00:00:00	2015-09-03T23:59:59	01518	19036
7	2015-08-30T00:00:00	2015-09-13T23:59:59	01518	19036
8	2015-09-09T00:00:00	2015-09-24T00:00:00	01518	19036
9	2015-09-20T00:00:00	2015-10-05T23:59:59	62530,01518	19036

SHA256 hash of SKR:

DD92D903CE328A6C577C47A3619680CC955A90AFA8869F4F99B43A285A8F038A

>> swelter misnomer sugar aggregate spyglass component Oakland handiwork eightball info
rmant dashboard pandemic fallout monument merit revolver preclude existence peachy phar
macy retouch letterhead quota document prowler politeness cleanup cellulose enlist mids
ummer acme maverick <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0



HSM3: Remove SKR Copy FD

Step	Activity	Initials	Time
✓ 27.	CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR_COPY</code> flushes the system buffers: <code>sync</code> and then unmounts the KSR FD using <code>umount /media/KSR_COPY</code>	GL	19:44
✓ 28.	CA removes KSR_COPY FD containing SKR copy and retain for audit purpose.	GL	19:44

HSM3: Disable/Deactivate

Step	Activity	Initials	Time
✓ 29.	CA makes sure to utilize the cards that were NOT used to activate the HSM3 are used to deactivate the HSM3. 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 <u>5</u> of 7 2nd OP card <u>6</u> of 7 3rd OP card <u>4</u> of 7	GL	19:46



HSM3: Return to a TEB

Step	Activity	Initials	Time
✓ 30.	CA turns off the HSM3 by pressing the power switch behind it. Then CA disconnects HSM3 from power and laptop (serial and Ethernet) if connected.	GL	19:47
✓ 31.	CA places the HSM3 into a prepared TEB and seals it.	GL	19:48
✓ 32.	CA reads out TEB # and HSM3 serial #, shows item to participants and IW1 confirms TEB # and HSM3 serial # below. HSM3: TEB# BB24646676 / serial # H1403032 IW1 and CA initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.	GL	19:50

Stop Recording Serial Port Activity

Step	Activity	Initials	Time
✓ 33.	Closing ttyaudit terminal window CA terminates the HSMs serial output capture by disconnecting the USBs serial adaptors from laptop. CA then exits out of ttyaudit terminal window by typing "exit".	GL	19:50

Ceremony Break

Step	Activity	Initials	Time
✓ 34.	CA initiates the ceremony break and requests for IKOS to bring the facility security guard in the ceremony room to ensure that the cryptographic materials are protected from unauthorized access.	GL	19:57
✓ 35.	CA divides the participants that require ceremony break in groups and ensure the following: <ul style="list-style-type: none"> • Remaining participants are sufficient to maintain dual occupancy for the ceremony room • At least (2) Crypto Officer and (1) Auditor should remain in the ceremony room when each group is escorted for ceremony break • Audit Cameras are never obstructed IKOS will escort each group of participants out of the ceremony room for ceremony break.	GL	19:58
✓ 36.	Once all the groups returned to the ceremony room from break, CA ensures that all participants are present and resumes the ceremony.	GL	20:24



Start logging HSM Output

Step	Activity	Initials	Time
37.	CA connects a serial to USB null modem cable to laptop.	GL	20:27
38.	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 <code>cd /media/HSMFD</code> <code>stty -F /dev/ttyUSB0 115200</code> <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.	GL	20:28

HSM4: Power Up

Step	Activity	Initials	Time
39.	CA inspects the HSM4 TEB for tamper evidence; reads out TEB # and serial #. IW1 confirms TEB # and serial # below. HSM4: TEB# BB24646680 / serial # H1411011	GL	20:30
40.	CA removes HSM4 from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	GL	20:30
41.	CA switches to the ttyaudit terminal window, connects power to HSM4 and turns on by pressing the power switch behind it. Status information should appear on the serial logging screen and after self test the HSM4 display should say "Important Read Manual" indicating the HSM4 is in the initialized state. IW1 matches displayed HSM4 serial number with below HSM4: Serial # H1411011	GL	20:32



HSM4: Importing the AAK

Step	Activity	Initials	Time
42.	CA will perform the following steps to import the AAK: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "2.Restore AAK" hit ENT to confirm c) When "Restore AAK?" is displayed, hit ENT to confirm d) When "Insert Card #?" is displayed, insert the proper sequence of AAK card from the cardholder e) When "Remove Card?" is displayed, remove card f) Repeat steps d) to e) for the 2nd AAK card g) When "AAK Imported" is displayed, hit ENT to confirm As each card is used the CA places it in the cardholder.	GK	20:33



HSM4: Switching to Secure State

Step	Activity	Initials	Time
43.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to set the HSM4 in Secure State:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "3.Secure" hit ENT to confirm c) When "Secure?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO 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 SO card h) When "SMK AES Triple DES?" is displayed, hit CLR to skip i) When "SMK AES" is displayed, hit CLR to confirm j) When "Set HSM Port?" is displayed, hit CLR to skip k) When "Enable IPv4/IPv6?" is displayed, hit CLR to skip l) When "Set IPv4 Address?" is displayed, hit CLR to skip m) When "Set IPv4 NetMask?" is displayed, hit CLR to skip n) When "Set IPv4 Gateway?" is displayed, hit CLR to skip o) When "Set IPv6 Address?" is displayed, hit CLR to skip p) When "Set IPv6 NetMask?" is displayed, hit CLR to skip q) When "Set IPv6 Gateway?" is displayed, hit CLR to skip r) When "Change Clock?" is displayed, hit CLR to skip s) When "Import Config.?" is displayed, hit CLR to skip t) When "FIPS Mode On Disable?" is displayed, hit CLR to skip u) When "FIPS Mode On" is displayed, hit CLR to confirm v) When "Global Key Export Enabled" is displayed, hit CLR to confirm <p>Done Rebooting Device will be displayed and confirm that the HSM4 is in Secured State</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>2</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p>	<p>HL</p>	<p>20:36</p>



HSM4: Change and Verify API Settings

Step	Activity	Initials	Time
44. ✓	CA will perform the following steps to change the API settings: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "5. API Settings" hit ENT to confirm h) Select "1.Key Import" hit ENT to confirm i) When "Key Import On Disable?" is displayed, hit ENT to confirm j) Select "2.Key Export" hit ENT to confirm k) When "Key Export On Disable?" is displayed, hit ENT to confirm l) Select "5.Sym Key Der" hit ENT to confirm m) When "Sym Key Der On Disable?" is displayed, hit ENT to confirm n) Hit CLR twice to return to the main menu "Secured" As each card is created the CA places it in the cardholder.	K	20:38



Step	Activity	Initials	Time
45.	<p>CA will perform the following steps to dump the status of the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "4.HSM Info" hit ENT to confirm c) Select "8.Output Info" hit ENT to confirm d) When "Output info?" is displayed, hit ENT to confirm e) Hit CLR to return to the main menu "Secured" <p>CA switches to the ttyaudit terminal window to confirm with IW the output of the HSM configuration matches with the list below:</p> <pre> Modes: (1=Enabled 0=Disabled) Global Key Export 1 ✓ App Key Import 0 ✓ App Key Export 0 ✓ Asymmetric Key Gen 1 ✓ Symmetric Key Gen 1 ✓ Symmetric Key Derive 0 ✓ Signing 1 ✓ Signature Verify 1 ✓ MAC Generation 1 ✓ MAC Verification 1 ✓ Encrypt / Decrypt 1 ✓ Delete Asym Key 1 ✓ Delete Sym Key 1 ✓ Output Key Details 1 ✓ Output Key Summary 1 ✓ Suite B Algorithms 1 ✓ Non Suite B Algs 1 ✓ Auto Online 0 ✓ AES SMK ✓ FIPS Mode ✓ </pre>	<p>HL</p>	<p>20:40</p>

HSM4: Importing the SMK and APP. Key

Step	Activity	Initials	Time
46.	<p>CA will perform the following steps to import the Storage Master Key (SMK) cards in to the HSM4:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "4.SMK" hit ENT to confirm h) Select "3.Restore SMK" hit ENT to confirm i) When "Restore SMK?" is displayed, hit ENT to confirm j) When "Insert Card SMK #?" is displayed, insert the SMK card from the cardholder k) When "Remove Card?" is displayed, remove card l) Repeat steps j) to k) for the 2nd SMK card m) When "SMK Restored" is displayed, hit ENT to confirm n) Hit CLR to back to the previous menu "Key Mgmt" <p>As each card is used the CA places it in the cardholder.</p>	<p>GL</p>	<p>20:43</p>
47.	<p>CA makes sure to utilize the APP. Key card that was NOT used in the HSM3. CA will perform the following steps to import the Application Key (APP. Key) card:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "3.App Keys" from the same menu "Key Mgmt" and hit ENT to confirm c) Select "2.Restore" hit ENT to confirm d) When "Restore?" is displayed, hit ENT to confirm e) When "Which Media?" is displayed, select "2. From Card" and hit ENT to confirm f) When "Insert Card #?" is displayed, insert the proper card from the cardholder g) When "Remove Card?" is displayed, remove card h) When "Restore Complete" is displayed, hit ENT to confirm i) Hit CLR twice to return to the main menu "Secured" <p>As card is used the CA places it in the cardholder.</p>	<p>GL</p>	<p>20:45</p>



Returning APP. Key Cards to a TEB

Step	Activity	Initials	Time
✓ 48.	<p>CA places the APP Key cards in a plastic case and the initial HSMFDs into a prepared TEB and seals; reads out TEB # and shows item to participants and IW1 confirms TEB # below.</p> <p>APP. Key: TEB # BB21907213</p> <p>IW1 and CA initials the TEB and keep the sealing strips for later inventory.</p> <p>CA places item on equipment cart.</p>	GL	20:48

HSM4: Enable/Activate

Step	Activity	Initials	Time
✓ 49.	<p>CA will perform the following steps to activate the HSM4:</p> <ul style="list-style-type: none"> 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 <p>Confirm the "READY" led on the HSM4 is ON.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <u>4</u> of 7 2nd OP card <u>7</u> of 7 3rd OP card <u>5</u> of 7</p>	GL	20:49

HSM4: Check Network between Laptop and HSM4

Step	Activity	Initials	Time
✓ 50.	CA connects HSM4 to laptop using Ethernet cable in LAN port.	GL	20:50
✓ 51.	<p>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.</p>	GL	20:50



Insert Copy of KSR to be signed

Step	Activity	Initials	Time
✓ 52.	CA plugs FD labeled "KSR_COPY" that contains a copy of the 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.	GL	20:51

Execute KSR signer

Step	Activity	Initials	Time
✓ 53.	CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR_COPY/ksr-root-2015-q3-0.xml</code>	GL	20:52
✓ 54.	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 HSM4 is online and then enters "y" to proceed to verification. Note: DO NOT enter "y" for the "Is this correct y/n?" yet.	GL	20:52

Verification of the Hash (validity) of the KSR Copy

Step	Activity	Initials	Time
✓ 55.	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN.	GL	20:53
✓ 56.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?	GL	20:53
✓ 57.	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 <code>/media/KSR_COPY/skr-root-2015-q3-0.xml</code>	GL	20:53

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
✓ 58.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog \$(ls -tr ksrsigner-20150409-*.log tail -n 1); done</code> This example generates X copies and hands copies to participants.	GL	20:54
✓ 59.	IW1 attaches a copy to his/her script and writes "HSM4 SKR".	GL	20:56



Verification of the Hash (validity) of the SKR Copy

Step	Activity	Initials	Time
60.	CA read out the SHA256 hash in PGP wordlist format for the generated HSM4 SKR and the ceremony participants match the hash with the previous HSM2 SKR.	FL	20:58

HSM4: Remove SKR Copy FD

Step	Activity	Initials	Time
61.	CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR_COPY</code> flushes the system buffers: <code>sync</code> and then unmounts the KSR FD using <code>umount /media/KSR_COPY</code>	FL	20:59
62.	CA removes KSR_COPY FD containing SKR copy and retain for audit purpose.	FL	20:59

HSM4: Disable/Deactivate

Step	Activity	Initials	Time
63.	CA makes sure to utilize the cards that were NOT used to activate the HSM4 are used to deactivate the HSM4. 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 <u>2</u> of 7 2nd OP card <u>6</u> of 7 3rd OP card <u>5</u> of 7	FL	21:02

HSM y SKR

Starting: ksrsigner Kjqmt7v /media/KSR_COPY/ksr-root-2015-q3-0.xml (at Thu Apr 9 20:52:27 2015 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: H1411011

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2015-04-01T00:00:00	2015-04-15T23:59:59	16665,48613	19036
2	2015-04-11T00:00:00	2015-04-25T23:59:59	48613	19036
3	2015-04-21T00:00:00	2015-05-05T23:59:59	48613	19036
4	2015-05-01T00:00:00	2015-05-15T23:59:59	48613	19036
5	2015-05-11T00:00:00	2015-05-25T23:59:59	48613	19036
6	2015-05-21T00:00:00	2015-06-04T23:59:59	48613	19036
7	2015-05-31T00:00:00	2015-06-14T23:59:59	48613	19036
8	2015-06-10T00:00:00	2015-06-24T23:59:59	48613	19036
9	2015-06-20T00:00:00	2015-07-05T23:59:59	01518,48613	19036

...VALIDATED.

Validate and Process KSR /media/KSR_COPY/ksr-root-2015-q3-0.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2015-07-01T00:00:00	2015-07-15T23:59:59	01518,48613	
2	2015-07-11T00:00:00	2015-07-25T23:59:59	01518	
3	2015-07-21T00:00:00	2015-08-04T23:59:59	01518	
4	2015-07-31T00:00:00	2015-08-14T23:59:59	01518	
5	2015-08-10T00:00:00	2015-08-24T23:59:59	01518	
6	2015-08-20T00:00:00	2015-09-03T23:59:59	01518	
7	2015-08-30T00:00:00	2015-09-13T23:59:59	01518	
8	2015-09-09T00:00:00	2015-09-24T00:00:00	01518	
9	2015-09-20T00:00:00	2015-10-05T23:59:59	62530,01518	

*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:

E1EACA147D556444F8B4ACBA01902753A4BABDE0C0605EFB9060B59ED396F2C4

>> tempest undaunted spellbind belowground klaxon equipment flytrap designing Vulcan po
liteness ribcage puberty absurd millionaire brackish enterprise regain puberty skullcap
tobacco slowdown fortitude eyeglass Wichita peachy fortitude scorecard onlooker staple
r monument uproot reproduce <<

Generated new SKR in /media/KSR_COPY/skr-root-2015-q3-0.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
---	-----------	------------	----------	--------------------

HSM 4SKR

1	2015-07-01T00:00:00	2015-07-15T23:59:59	01518,48613	19036
2	2015-07-11T00:00:00	2015-07-25T23:59:59	01518	19036
3	2015-07-21T00:00:00	2015-08-04T23:59:59	01518	19036
4	2015-07-31T00:00:00	2015-08-14T23:59:59	01518	19036
5	2015-08-10T00:00:00	2015-08-24T23:59:59	01518	19036
6	2015-08-20T00:00:00	2015-09-03T23:59:59	01518	19036
7	2015-08-30T00:00:00	2015-09-13T23:59:59	01518	19036
8	2015-09-09T00:00:00	2015-09-24T00:00:00	01518	19036
9	2015-09-20T00:00:00	2015-10-05T23:59:59	62530,01518	19036

SHA256 hash of SKR:

DD92D903CE328A6C577C47A3619680CC955A90AFA8869F4F99B43A285A8F038A

>> swelter misnomer sugar aggregate spyglass component Oakland handiwork eightball info
rmant dashboard pandemic fallout monument merit revolver preclude existence peachy phar
macy retouch letterhead quota document prowler politeness cleanup cellulose enlist mids
ummer acme maverick <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0



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: <u>09/04/2015 21:05</u>	SL	21:05
2.	IW1 Describes exception and action below.	SL	21:05

Page 40, Step 64

SMK #1 card was removed before the "Remove card" message was displayed in the HSM.

Restarting from step, 64, a)

– End of DNSSEC Script Exception –



HSM:4 Clear and Destroy SMK Cards

Step	Activity	Initials	Time
64.	<p>CA will perform the following steps to clear SMK cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "4.SMK" hit ENT to confirm h) Select "4.Clear Cards" hit ENT to confirm i) When "Clear Card?" is displayed, hit ENT to confirm j) When "Insert Card SMK 1?" is displayed, take the SMK #1 card from the cardholder, show the SMK #1 card to the audit camera and then insert the SMK #1 card into the HSM's card reader k) When "Num Cards?" is displayed, enter "4" and hit ENT to confirm l) When "Remove Card?" is displayed, remove card m) When "Insert Card SMK #?" is displayed, take the proper sequence of the SMK card form the cardholder, show the SMK card to the audit camera and then insert the SMK into the HSM's card reader n) When "Remove Card?" is displayed, remove card o) Repeat steps m) to n) for the 3rd and 4th SMK cards p) Hit CLR twice to return to the main menu "Secured" <p>CA uses the shredder to destroy the cleared SMK cards.</p>	<p>GL</p>	<p>21:11</p>



HSM:4 Clear and Destroy CO Cards

Step	Activity	Initials	Time
65.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to clear Crypto Officer (CO) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "7.Role Mgmt" hit ENT to confirm c) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd and 3rd SO card g) Select "4.Clear RoleCard" hit ENT to confirm h) When "Clear Card?" is displayed, hit ENT to confirm i) When "Num Cards?" is displayed, enter "3" and hit ENT to confirm j) When "Insert Card #?" is displayed, take the proper sequence of the CO card form the cardholder, show the CO card to the audit camera and then insert the CO into the HSM's card reader k) When "PIN?" is displayed, enter "11223344" and hit ENT l) When "Remove Card?" is displayed, remove card m) Repeat steps j) to l) for the 2nd and 3rd CO cards n) Hit CLR to return to the main menu "Secured" <p>IW1 records the used cards below.</p> <p>Set # <u>2</u></p> <p>1st SO card <u>2</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p> <p>CA uses the shredder to destroy the cleared CO cards.</p>	<p>FL</p>	<p>21:17</p>

HSM:4 Clear and Destroy AAK Cards

Step	Activity	Initials	Time
66.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to clear AAK cards:</p> <p>a) Utilize the HSM's keyboard and scroll through menu using <> key</p> <p>b) Select "7.Role Mgmt" hit ENT to confirm</p> <p>c) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder</p> <p>d) When "PIN?" is displayed, enter "11223344" and hit ENT</p> <p>e) When "Remove Card?" is displayed, remove card</p> <p>f) Repeat steps c) to e) for the 2nd and 3rd SO card</p> <p>g) Select "5.Clear AAK Card" hit ENT to confirm</p> <p>h) When "Clear AAK Card?" is displayed, hit ENT to confirm</p> <p>i) When "Num Cards?" is displayed, enter "2" and hit ENT to confirm</p> <p>j) When "Insert Card AAK #?" is displayed, take the proper sequence of the AAK card form the cardholder, show the AAK card to the audit camera and then insert the AAK into the HSM's card reader</p> <p>k) When "Remove Card?" is displayed, remove card</p> <p>l) Repeat steps j) to k) for the 2nd AAK cards</p> <p>m) Hit CLR to return to the main menu "Secured"</p> <p>IW1 records the used cards below. Set # <u>2</u> 1st SO card <u>6</u> of 7 2nd SO card <u>7</u> of 7 3rd SO card <u>1</u> of 7</p> <p>CA uses the shredder to destroy the cleared AAK cards.</p>	GC	21:21

HSM:4 Return to a TEB

Step	Activity	Initials	Time
67.	CA turns off the HSM4 by pressing the power switch behind it. Then CA disconnects HSM4 from power and laptop (serial and Ethernet) if connected.	GC	21:22
68.	CA places the HSM4 into a prepared TEB and seals it.	GC	21:23
69.	<p>CA reads out TEB # and HSM4 serial #, shows item to participants and IW1 confirms TEB # and HSM4 serial # below.</p> <p>HSM4: TEB# BB24646675 / serial # H1411011 ✓</p> <p>IW1 and CA initials the TEB and keep the sealing strips for later inventory.</p> <p>CA places item on equipment cart.</p>	GC	21:25



Act. 4 Close the Ceremony

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
✓ 1.	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".	GL	21:26
✓ 2.	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.	GL	21:26

Backup HSMFD Contents

Step	Activity	Initials	Time
✓ 3.	Set dotglob by executing <code>shopt -s dotglob</code> This allows copying everything in the original HSMFD.	GL	21:27
✓ 4.	Calculate the sha256hash of the contents on the original HSMFD. <code>find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum</code>	GL	21:27
✓ 5.	Copy and paste the sha256hash and paste it on Text Editor by going to Applications > Accessories > Text Editor	GL	21:28
✓ 6.	Print two copies. One for the audit bundle and the other for the HSMFD package.	GL	21:29
✓ 7.	CA displays contents of HSMFD by executing <code>ls -ltr</code>	GL	21:29
✓ 8.	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 <code>cp -Rp * /media/HSMFD_</code>	GL	21:30
✓ 9.	CA displays contents of HSMFD_ by executing <code>ls -ltr /media/HSMFD_</code>	GL	21:30
✓ 10.	Calculate the sha256hash of the contents on the copied HSMFD. <code>find -P /media/HSMFD_ -type f -print0 sort -z xargs -0 cat sha256sum</code> Confirm that it matches the sha256hash of the original HSMFD	GL	21:31
✓ 11.	CA unmounts new FD using <code>umount /media/HSMFD_</code>	GL	21:31
✓ 12.	CA removes HSMFD_ and places on table.	GL	21:31
✓ 13.	CA repeats step 8 to 12 for the 2 nd copy	GL	21:32
✓ 14.	CA repeats step 8 to 12 for the 3 rd copy	GL	21:33
✓ 15.	CA repeats step 8 to 12 for the 4 th copy	GL	21:34
✓ 16.	CA repeats step 8 to 12 for the 5 th copy	GL	21:34

Print Logging Information

Step	Activity	Initials	Time
✓ 17.	CA prints out a hard copy of logging information by executing <code>enscript -2Gr -# 1 script-20150409.log</code> <code>enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20150409-*.log</code> for attachment to IW1 and CA scripts. Note: Ignore the error regarding non-printable characters if prompted.	GL	21:39

4ca2ccbe6d4be643d8c13742e9a3d450754328dae04cddce494eaa33223bdaed

04/09/15
21:26:44

script-20150409.log

```
-rwxr-xr-x 1 root root 18314 Apr  2 00:09 \033[00;32mskr.xml.20150409205227\033[00m
-rwxr-xr-x 1 root root 15353 Apr  2 00:09 \033[00;32mskr-root-2015-q3-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Apr  9 20:53 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 18314 Apr  9 20:53 \033[00;32mskr-root-2015-q3-0.xml\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# sync
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /#033[Kmedia/$033
[KKSR_COPY/
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit
```

Script done on Thu 09 Apr 2015 09:26:44 EM UTC

04/09/15
18:59:08

ttyaudit-ttyUSB0-20150409-180743.log

Application Boot Loader - Feb 25 2010 11:08:16

```
2015-04-09T18:12:22+0000 ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2015-04-09T18:12:22+0000 ttyUSB0
2015-04-09T18:12:23+0000 ttyUSB0 Battery OK!
2015-04-09T18:12:23+0000 ttyUSB0
2015-04-09T18:12:23+0000 ttyUSB0 No Tamper Counts in BBRAM!
2015-04-09T18:12:23+0000 ttyUSB0 Loading Application (APP)
2015-04-09T18:12:23+0000 ttyUSB0 Starting loaded code.
2015-04-09T18:12:24+0000 ttyUSB0
2015-04-09T18:12:24+0000 ttyUSB0 \000Application - Feb 25 2010 11:08:02
2015-04-09T18:12:25+0000 ttyUSB0 wdog started
2015-04-09T18:12:26+0000 ttyUSB0
2015-04-09T18:12:26+0000 ttyUSB0
2015-04-09T18:12:29+0000 ttyUSB0 Running DES POST Test
2015-04-09T18:12:29+0000 ttyUSB0 DES POST Test Passed
2015-04-09T18:12:29+0000 ttyUSB0
2015-04-09T18:12:29+0000 ttyUSB0 Running Triple DES POST Test
2015-04-09T18:12:29+0000 ttyUSB0 Triple DES POST Test Passed
2015-04-09T18:12:29+0000 ttyUSB0
2015-04-09T18:12:29+0000 ttyUSB0 Running AES POST Test
2015-04-09T18:12:29+0000 ttyUSB0 AES POST Test Passed
2015-04-09T18:12:29+0000 ttyUSB0
2015-04-09T18:12:29+0000 ttyUSB0 Running SHA1 POST Test
2015-04-09T18:12:29+0000 ttyUSB0 SHA1 POST Test Passed
2015-04-09T18:12:29+0000 ttyUSB0
2015-04-09T18:12:29+0000 ttyUSB0 Running SHA2 POST Test
2015-04-09T18:12:29+0000 ttyUSB0 SHA2 POST Test Passed
2015-04-09T18:12:29+0000 ttyUSB0
2015-04-09T18:12:30+0000 ttyUSB0 Running RandomGen SHA1 POST Test
2015-04-09T18:12:30+0000 ttyUSB0 Randomgen SHA1 POST Test Passed
2015-04-09T18:12:30+0000 ttyUSB0
2015-04-09T18:12:30+0000 ttyUSB0 Running RSA POST Test
2015-04-09T18:12:30+0000 ttyUSB0 RSA POST Test Passed
2015-04-09T18:12:30+0000 ttyUSB0
2015-04-09T18:12:30+0000 ttyUSB0 Running DSA POST Test
2015-04-09T18:12:30+0000 ttyUSB0 DSA POST Test Passed
2015-04-09T18:12:30+0000 ttyUSB0
2015-04-09T18:12:30+0000 ttyUSB0 Running RandomGen POST Test
2015-04-09T18:12:30+0000 ttyUSB0 RandomGen POST Test Passed
2015-04-09T18:12:30+0000 ttyUSB0
2015-04-09T18:12:30+0000 ttyUSB0 Additional RandomGen POST Test Passed
```


04/09/15
18:59:08

ttyaudit-ttyUSB0-20150409-180743.log

```
2015-04-09T18:52:18+0000 ttyUSB0 9/4/2013 at 17:16:19
2015-04-09T18:52:18+0000 ttyUSB0
2015-04-09T18:52:18+0000 ttyUSB0 0x200023 004000000C8A2156D
2015-04-09T18:52:18+0000 ttyUSB0
2015-04-09T18:53:51+0000 ttyUSB0
2015-04-09T18:53:51+0000 ttyUSB0 9/4/2013 at 17:17:52
2015-04-09T18:53:51+0000 ttyUSB0
2015-04-09T18:53:51+0000 ttyUSB0 0x20002c 4780000007E2D2972
2015-04-09T18:53:51+0000 ttyUSB0
2015-04-09T18:54:28+0000 ttyUSB0
2015-04-09T18:54:28+0000 ttyUSB0 9/4/2013 at 17:18:29
2015-04-09T18:54:28+0000 ttyUSB0
2015-04-09T18:54:28+0000 ttyUSB0 0x20002c 4780000007DAD2972
2015-04-09T18:54:28+0000 ttyUSB0
2015-04-09T18:54:41+0000 ttyUSB0
2015-04-09T18:54:41+0000 ttyUSB0 9/4/2013 at 17:18:42
2015-04-09T18:54:41+0000 ttyUSB0
2015-04-09T18:54:41+0000 ttyUSB0 0x200010 4780000007DAD2972
2015-04-09T18:54:41+0000 ttyUSB0
```


04/09/15
19:50:48

ttyaudit-ttyUSB0-20150409-190117.log

```
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0 HmcListener: Created IPv4 socket 7 on port 3000.
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0 HmcListener: Created IPv6 socket 9 on port 3000.
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0 Audit on 9/4/2015 19:04:22 00100003
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0 Shutting down daemons...
2015-04-09T19:10:59+0000 ttyUSB0 AuditBuffer rx'd [-1] (3)
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:10:59+0000 ttyUSB0 shutting down audit service.
2015-04-09T19:10:59+0000 ttyUSB0
2015-04-09T19:11:00+0000 ttyUSB0 Terminated
2015-04-09T19:11:00+0000 ttyUSB0
2015-04-09T19:11:00+0000 ttyUSB0 HmcListener::accept(): No such process
2015-04-09T19:11:00+0000 ttyUSB0
2015-04-09T19:11:00+0000 ttyUSB0 Shutting down filesystems...
2015-04-09T19:11:00+0000 ttyUSB0
2015-04-09T19:11:01+0000 ttyUSB0
2015-04-09T19:11:01+0000 ttyUSB0
2015-04-09T19:11:01+0000 ttyUSB0
2015-04-09T19:11:01+0000 ttyUSB0
2015-04-09T19:11:01+0000 ttyUSB0 H1403032 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-04-09T19:11:01+0000 ttyUSB0 BBL CRC32: 0x757574CA
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 Running applicationBootLoader at 0xEFD00000
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 H1403032 011403 ABL 011 : Tamper Challenge Response Key
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 ABL CRC32: 0xE7E0FA6A
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 #####
2015-04-09T19:11:02+0000 ttyUSB0 ## ABL tamper records ###
2015-04-09T19:11:02+0000 ttyUSB0 #####
2015-04-09T19:11:02+0000 ttyUSB0 Current Tamper Counts (decimal 0-255):
2015-04-09T19:11:02+0000 ttyUSB0 =====
2015-04-09T19:11:02+0000 ttyUSB0 vextoosTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 vintooosTamperCount: 43
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 vbboosTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 maxsttempTamperCount: 0
```

04/09/15
19:50:48

ttyaudit-ttyUSB0-20150409-190117.log

```
2015-04-09T19:11:02+0000 ttyUSB0 minstrtempTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0 meshTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0 extampSMKTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0 extampIMKTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0 tempdiffTamperCount: 0
2015-04-09T19:11:02+0000 ttyUSB0 pfTamperCount: 43
2015-04-09T19:11:02+0000 ttyUSB0 restartTamperCount: 137
2015-04-09T19:11:02+0000 ttyUSB0 Current tamper bitmaps:
2015-04-09T19:11:02+0000 =====
2015-04-09T19:11:02+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-04-09T19:11:02+0000 ttyUSB0 lastTamper bitmap: 0x0080 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2015-04-09T19:11:02+0000 =====
2015-04-09T19:11:02+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2015-04-09T19:11:02+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2015-04-09T19:11:02+0000 ttyUSB0 Board is P2020RDB
2015-04-09T19:11:02+0000 ttyUSB0 board_smp_init: 2 cpu
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=500000000
2015-04-09T19:11:02+0000 ttyUSB0
2015-04-09T19:11:02+0000 ttyUSB0 System page at phys:000b0000 user:000b0000 kern:000b0000
2015-04-09T19:11:02+0000 ttyUSB0 Starting next program at v0015183c
2015-04-09T19:11:02+0000 ttyUSB0 Starting K-Series Kernel
2015-04-09T19:11:02+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2015-04-09T19:11:02+0000 ttyUSB0
```


04/09/15
19:50:48

ttysuidit-ttyUSB0-20150409-190117.log

```
2015-04-09T19:11:04+0000 ttyUSB0 Thu Apr 9 19:04:27 2015
2015-04-09T19:11:04+0000 ttyUSB0
2015-04-09T19:11:04+0000 ttyUSB0 Starting auditd v2.0 ... started.
2015-04-09T19:11:04+0000 ttyUSB0
2015-04-09T19:11:05+0000 ttyUSB0 Interface 0 configured for IPv6.
2015-04-09T19:11:05+0000 ttyUSB0
2015-04-09T19:11:05+0000 ttyUSB0 Interface 0 configured for IPv4.
2015-04-09T19:11:05+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0 add net default: gateway :: Network is unreachable
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0 Starting USB driver...
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:06+0000 ttyUSB0
2015-04-09T19:11:07+0000 ttyUSB0 Running DES POST Test
2015-04-09T19:11:07+0000 ttyUSB0 DES POST Test Passed
2015-04-09T19:11:07+0000 ttyUSB0 Running Triple DES POST Test
2015-04-09T19:11:07+0000 ttyUSB0 Triple DES POST Test Passed
2015-04-09T19:11:07+0000 ttyUSB0 Running AES POST Test
2015-04-09T19:11:07+0000 ttyUSB0 AES POST Test Passed
2015-04-09T19:11:07+0000 ttyUSB0 Running SHA1 POST Test
2015-04-09T19:11:07+0000 ttyUSB0 SHA1 POST Test Passed
2015-04-09T19:11:07+0000 ttyUSB0 Running SHA2 POST Test
2015-04-09T19:11:07+0000 ttyUSB0 SHA2 POST Test Passed
2015-04-09T19:11:08+0000 ttyUSB0 Running RandomGen POST Test
2015-04-09T19:11:08+0000 ttyUSB0 RandomGen POST Test Passed
2015-04-09T19:11:08+0000 ttyUSB0 Running RSA POST Test
2015-04-09T19:11:08+0000 ttyUSB0 RSA POST Test Passed
2015-04-09T19:11:08+0000 ttyUSB0 Running DSA POST Test
2015-04-09T19:11:08+0000 ttyUSB0 DSA POST Test Passed
```


04/09/15
19:50:48

ttyaudit-ttyUSB0-20150409-190117.log

```
2015-04-09T19:21:21+0000 ttyUSB0 capabilities tx=0
2015-04-09T19:21:21+0000 ttyUSB0 enabled=0
2015-04-09T19:21:21+0000 ttyUSB0 address: 00:e0:06:c0:b2:3d
2015-04-09T19:21:21+0000 ttyUSB0 media: Ethernet none
2015-04-09T19:21:21+0000 ttyUSB0 inet 192.168.0.2 netmask 0xfffff00 broadcast 192.168.0.255
2015-04-09T19:21:21+0000 ttyUSB0 inet6 2001::2e0:6ff:fec0:b23d prefixlen 64
2015-04-09T19:21:21+0000 ttyUSB0 inet6 fe80::2e0:6ff:fec0:b23dH\037\220@ec0 prefixlen 64 scopeid 0x2

2015-04-09T19:21:21+0000 ttyUSB0 Current HSM State: Secured Off-Line

2015-04-09T19:21:21+0000 ttyUSB0 Modes: (1=Enabled 0=Disabled)
2015-04-09T19:21:21+0000 ttyUSB0 Global Key Export 1 App Key Import 0 App Key Export 0 Asymmetric Key Gen 1
2015-04-09T19:21:21+0000 ttyUSB0 Symmetric Key Gen 1 Symmetric Key Derive 0 Signing 1 Signature Verify 1
2015-04-09T19:21:21+0000 ttyUSB0 MAC Generation 1 MAC Verification 1 Encrypt / Decrypt 1 Delete Asym Key 1
2015-04-09T19:21:21+0000 ttyUSB0 Delete Sym Key 1 Output Key Details 1 Output Key Summary 1 Suite B Algorithms 1
2015-04-09T19:21:21+0000 ttyUSB0 Non Suite B Algs 1 Auto Online 0
2015-04-09T19:21:21+0000 ttyUSB0 Other Modes:
2015-04-09T19:21:21+0000 ttyUSB0 AES SMK FIPS Mode
2015-04-09T19:21:21+0000 ttyUSB0 Battery ok
2015-04-09T19:21:21+0000 ttyUSB0 #####
2015-04-09T19:21:21+0000 ttyUSB0 ## ABL tamper records ###
2015-04-09T19:21:21+0000 ttyUSB0 #####
2015-04-09T19:21:21+0000 ttyUSB0 Current Tamper Counts (decimal 0-255):
2015-04-09T19:21:21+0000 ttyUSB0 =====
2015-04-09T19:21:21+0000 ttyUSB0 vextoosTamperCount: 0
```

04/09/15
19:50:48

ttyaudit-ttyUSB0-20150409-190117.log

```
2015-04-09T19:21:21+0000 ttyUSB0 vintoolsTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 vboosTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 maxstrtempTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 minstrtempTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 meshTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 extampSMKTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 extampIMKTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 tempdiffTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 pfTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 restartTamperCount: 0
2015-04-09T19:21:21+0000 ttyUSB0 Current tamper bitmaps:
2015-04-09T19:21:21+0000 =====
2015-04-09T19:21:21+0000 currentTamper bitmap: 0x0000 0b .... .... .... ....
2015-04-09T19:21:21+0000 lastTamper bitmap: 0x0000 0b .... .... .... ....
2015-04-09T19:21:21+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2015-04-09T19:21:21+0000 =====
2015-04-09T19:21:21+0000 DRBG Instantiate Health Test On Demand Passed
2015-04-09T19:21:21+0000 DRBG Generate Health Test On Demand Passed
2015-04-09T19:21:21+0000 DRBG Reseed Health Test On Demand Passed
2015-04-09T19:21:21+0000 Audit on 9/4/2015 19:17:34 0020006b 47800000796D2972
2015-04-09T19:21:21+0000 Audit on 9/4/2015 19:17:57 0020006b 478000007B6D2972
2015-04-09T19:21:21+0000 Audit on 9/4/2015 19:18:57 00200025 478000007CAD2972
2015-04-09T19:21:21+0000 Audit on 9/4/2015 19:19:15 00200025 478000007D2D2972
```


04/09/15
21:26:20

ttyaudit-ttyUSB0-20150409-202837.log

```
2015-04-09T20:31:41+0000 ttyUSB0 lastTamper bitmap: 0x0000 0b .....  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0 Bitmapped Change Record (most recent first):  
2015-04-09T20:31:41+0000 =====  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0  
2015-04-09T20:31:41+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000  
2015-04-09T20:31:42+0000 ttyUSB0 Jumping to startup @ 0x001037B4  
2015-04-09T20:31:42+0000 ttyUSB0 Board is P2020RDB  
2015-04-09T20:31:42+0000 ttyUSB0 board_smp_init: 2 cpu  
2015-04-09T20:31:42+0000 ttyUSB0  
2015-04-09T20:31:42+0000 ttyUSB0  
2015-04-09T20:31:42+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=5000000000  
2015-04-09T20:31:42+0000 ttyUSB0  
2015-04-09T20:31:42+0000 ttyUSB0  
2015-04-09T20:31:42+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000  
2015-04-09T20:31:42+0000 ttyUSB0 Starting next program at v0015183c  
2015-04-09T20:31:43+0000 ttyUSB0 Starting K-Series Kernel  
2015-04-09T20:31:43+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.  
2015-04-09T20:31:43+0000 ttyUSB0 Thu Apr 9 20:23:57 2015  
2015-04-09T20:31:43+0000 ttyUSB0 Starting auditd v2.0 ... started.  
2015-04-09T20:31:43+0000 ttyUSB0 Interface 0 configured for IPv6.  
2015-04-09T20:31:43+0000 ttyUSB0 Interface 0 configured for IPv4.  
2015-04-09T20:31:44+0000 ttyUSB0 route: writing to routing socket: Network is unreachable  
2015-04-09T20:31:44+0000 ttyUSB0 add net default: gateway :: Network is unreachable  
2015-04-09T20:31:45+0000 ttyUSB0 route: writing to routing socket: Network is unreachable  
2015-04-09T20:31:45+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable  
2015-04-09T20:31:45+0000 ttyUSB0 Starting USB driver...  
2015-04-09T20:31:45+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33  
2015-04-09T20:31:45+0000 ttyUSB0  
2015-04-09T20:31:45+0000 ttyUSB0
```


04/09/15
21:26:20

ityaudit-ityUSB0-20150409-202837.log

```
2015-04-09T20:36:46+0000 ttyUSB0
2015-04-09T20:36:46+0000 ttyUSB0 HmcListener: Created IPv4 socket 7 on port 3000.
2015-04-09T20:36:46+0000 ttyUSB0
2015-04-09T20:36:46+0000 ttyUSB0
2015-04-09T20:36:46+0000 ttyUSB0
2015-04-09T20:36:46+0000 ttyUSB0 HmcListener: Created IPv6 socket 9 on port 3000.
2015-04-09T20:36:46+0000 ttyUSB0
2015-04-09T20:36:47+0000 ttyUSB0 Audit on 9/4/2015 20:29:00 00100003
2015-04-09T20:36:47+0000 ttyUSB0 Shutting down daemons...
2015-04-09T20:36:47+0000 ttyUSB0
2015-04-09T20:36:47+0000 ttyUSB0 AuditBuffer rx'd [-1] (3)
2015-04-09T20:36:47+0000 ttyUSB0 shutting down audit service.
2015-04-09T20:36:47+0000 ttyUSB0 Terminated
2015-04-09T20:36:47+0000 ttyUSB0 HmcListener::accept(): No such process
2015-04-09T20:36:47+0000 ttyUSB0 Shutting down filesystems...
2015-04-09T20:36:47+0000 ttyUSB0
2015-04-09T20:36:47+0000 ttyUSB0
2015-04-09T20:36:47+0000 ttyUSB0
2015-04-09T20:36:47+0000 ttyUSB0 H1411011 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-04-09T20:36:49+0000 ttyUSB0 BBL CRC32: 0x757574CA
2015-04-09T20:36:49+0000 ttyUSB0 Running applicationBootLoader at 0xEFD0C000
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 H1411011 011403 ABL 011 : Tamper Challenge Response Key
2015-04-09T20:36:49+0000 ttyUSB0 ABL CRC32: 0xE7E0FA6A
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 #####
2015-04-09T20:36:49+0000 ttyUSB0 ## ABL tamper records ##
2015-04-09T20:36:49+0000 ttyUSB0 #####
2015-04-09T20:36:49+0000 ttyUSB0 Current Tamper Counts (decimal 0-255):
2015-04-09T20:36:49+0000 ttyUSB0 =====
2015-04-09T20:36:49+0000 ttyUSB0 vextoosTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0 vintcoosTamperCount: 11
2015-04-09T20:36:49+0000 ttyUSB0 vbboosTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0 maxstrtempTamperCount: 0
```

04/09/15
21:26:20

tyaudit-ttyUSB0-20150409-202837.log

```

2015-04-09T20:36:49+0000 ttyUSB0 mInstrtempTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 meshTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 extampSMKTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 extampIMKTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 tempdiffTamperCount: 0
2015-04-09T20:36:49+0000 ttyUSB0 pFTamperCount: 11
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 restartTamperCount: 23
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Current tamper bitmaps:
2015-04-09T20:36:49+0000 ttyUSB0 =====
2015-04-09T20:36:49+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b ..... 0x0000 0b .....
2015-04-09T20:36:49+0000 ttyUSB0 lastTamper bitmap: 0x0000 0b ..... 0x0000 0b .....
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2015-04-09T20:36:49+0000 ttyUSB0 =====
2015-04-09T20:36:49+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Board is P2020RDB
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 board_smp_init: 2 cpu
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=i000000000, CCB=5000000000
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-04-09T20:36:49+0000 ttyUSB0 Starting next program at v00i5183c
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Starting K-Series Kernel
2015-04-09T20:36:49+0000 ttyUSB0
2015-04-09T20:36:49+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2015-04-09T20:36:49+0000 ttyUSB0

```

04/09/15
21:26:20

ttyauditi-ttyUSB0-20150409-202837.log

```
2015-04-09T20:36:51+0000 ttyUSB0 Thu Apr 9 20:29:05 2015
2015-04-09T20:36:51+0000 ttyUSB0 Starting auditt v2.0 ... started.
2015-04-09T20:36:52+0000 ttyUSB0 Interface 0 configured for IPv6.
2015-04-09T20:36:52+0000 ttyUSB0 Interface 0 configured for IPv4.
2015-04-09T20:36:52+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-04-09T20:36:53+0000 ttyUSB0 add net default: gateway :: Network is unreachable
2015-04-09T20:36:53+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-04-09T20:36:53+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2015-04-09T20:36:53+0000 ttyUSB0 Starting USB driver...
2015-04-09T20:36:53+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-04-09T20:36:53+0000 ttyUSB0 Running DES POST Test
2015-04-09T20:36:53+0000 ttyUSB0 DES POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running Triple DES POST Test
2015-04-09T20:36:55+0000 ttyUSB0 Triple DES POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running AES POST Test
2015-04-09T20:36:55+0000 ttyUSB0 AES POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running SHA1 POST Test
2015-04-09T20:36:55+0000 ttyUSB0 SHA1 POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running SHA2 POST Test
2015-04-09T20:36:55+0000 ttyUSB0 SHA2 POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running RandomGen POST Test
2015-04-09T20:36:55+0000 ttyUSB0 RandomGen POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running RSA POST Test
2015-04-09T20:36:55+0000 ttyUSB0 RSA POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0 Running DSA POST Test
2015-04-09T20:36:55+0000 ttyUSB0 DSA POST Test Passed
```

04/09/15
21:26:20

ttyaudit-ttyUSB0-20150409-202837.log

```
2015-04-09T20:36:55+0000 ttyUSB0 Running ECC POST Test
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0 ECC POST Test Passed
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:55+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0 Keyper 9860-2 Serial Number H1411011
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0 Memory Usage:
2015-04-09T20:36:56+0000 ttyUSB0 RAM (free/total) 197Mb/256Mb
2015-04-09T20:36:56+0000 ttyUSB0 Flash (free/total) 127Mb/128Mb
2015-04-09T20:36:56+0000 ttyUSB0 black store 192b
2015-04-09T20:36:56+0000 ttyUSB0 statistics 112b
2015-04-09T20:36:56+0000 ttyUSB0 other 116b
2015-04-09T20:36:56+0000 ttyUSB0 RedStore (free/total) 109Kb/128Kb
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0 Network Configuration:
2015-04-09T20:36:56+0000 ttyUSB0 IPv4: enabled
2015-04-09T20:36:56+0000 ttyUSB0 IPv6: enabled
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B3:2A / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b32a/64
2015-04-09T20:36:56+0000 ttyUSB0 HSM Port: 05000
2015-04-09T20:36:56+0000 ttyUSB0 HSM Gateway(s): 0.0.0.0 :
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0 Software Versions:
2015-04-09T20:36:56+0000 ttyUSB0 BBL 010 ABL 011 App 023
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0 CPLD Version:
2015-04-09T20:36:56+0000 ttyUSB0 1.9
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
2015-04-09T20:36:56+0000 ttyUSB0
```


04/09/15
21:26:20

tyaudit-tyUSB0-20150409-202837.log

```
2015-04-09T20:50:11+0000    ttyUSB0
2015-04-09T20:50:11+0000    ttyUSB0
2015-04-09T20:50:11+0000    TcpListener: Created IPv4 socket 11 on port 5000.
2015-04-09T20:50:11+0000    ttyUSB0
2015-04-09T20:50:11+0000    ttyUSB0
2015-04-09T20:50:11+0000    ttyUSB0
2015-04-09T20:50:11+0000    TcpListener: Created IPv6 socket 16 on port 5000.
2015-04-09T20:50:11+0000    ttyUSB0
2015-04-09T20:50:12+0000    ttyUSB0
2015-04-09T20:50:12+0000    ttyUSB0
2015-04-09T20:50:12+0000    ttyUSB0
2015-04-09T20:52:43+0000    ttyUSB0
2015-04-09T20:52:43+0000    TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2015-04-09T20:52:43+0000    ttyUSB0
2015-04-09T20:52:43+0000    ttyUSB0
2015-04-09T20:53:54+0000    ttyUSB0
2015-04-09T20:53:54+0000    CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2015-04-09T20:53:54+0000    ttyUSB0
2015-04-09T20:53:54+0000    Audit on 9/4/2015 20:53:42 00200069 08800004A7A73296D
2015-04-09T21:01:29+0000    ttyUSB0
2015-04-09T21:01:29+0000    Audit on 9/4/2015 20:54:09 00200069 08800004A7B73296D
2015-04-09T21:01:56+0000    ttyUSB0
2015-04-09T21:01:56+0000    Audit on 9/4/2015 20:54:34 00200069 08800004A7B33296D
2015-04-09T21:02:21+0000    ttyUSB0
2015-04-09T21:02:21+0000    Audit on 9/4/2015 20:54:37 00100003
2015-04-09T21:02:23+0000    ttyUSB0
2015-04-09T21:02:23+0000    TcpListener: Closed IPv4 socket 11 on port 5000.
2015-04-09T21:02:23+0000    ttyUSB0
2015-04-09T21:02:23+0000    Audit on 9/4/2015 20:55:48 0020006b 478000007AED2972
2015-04-09T21:03:35+0000    ttyUSB0
2015-04-09T21:03:35+0000    Audit on 9/4/2015 20:56:15 0020006b 478000007B6D2972
2015-04-09T21:04:02+0000    ttyUSB0
2015-04-09T21:04:02+0000    Audit on 9/4/2015 21:00:35 0020002d 478000007CAD2972
2015-04-09T21:08:23+0000    ttyUSB0
2015-04-09T21:08:23+0000    Audit on 9/4/2015 21:01:18 0020002d 478000007D2D2972
2015-04-09T21:09:05+0000    ttyUSB0
2015-04-09T21:09:05+0000    Audit on 9/4/2015 21:01:48 0020002d 478000007C2D2972
2015-04-09T21:09:35+0000    ttyUSB0
2015-04-09T21:09:35+0000    Audit on 9/4/2015 21:02:21 0020002d 478000007BAD2972
2015-04-09T21:10:08+0000    ttyUSB0
2015-04-09T21:10:08+0000    Audit on 9/4/2015 21:05:23 00200023 00800002A4CF156D
2015-04-09T21:13:10+0000    ttyUSB0
2015-04-09T21:13:36+0000    ttyUSB0
2015-04-09T21:13:36+0000    Audit on 9/4/2015 21:05:48 00200023 00800002A48F156D
2015-04-09T21:14:02+0000    ttyUSB0
2015-04-09T21:14:02+0000    Audit on 9/4/2015 21:06:15 00200023 008000029ECF156D
2015-04-09T21:15:24+0000    ttyUSB0
2015-04-09T21:15:24+0000    Audit on 9/4/2015 21:07:37 00200070 478000007B6D2972
2015-04-09T21:16:01+0000    ttyUSB0
2015-04-09T21:16:01+0000    Audit on 9/4/2015 21:08:14 00200070 478000007AED2972
```

04/09/15
21:26:20

ttyaudit-ttyUSB0-20150409-202837.log

```
2015-04-09T21:16:01+0000
2015-04-09T21:16:38+0000
2015-04-09T21:16:38+0000
2015-04-09T21:18:51+0000
2015-04-09T21:18:51+0000
2015-04-09T21:19:14+0000
2015-04-09T21:19:14+0000
2015-04-09T21:19:39+0000
2015-04-09T21:19:39+0000
2015-04-09T21:20:50+0000
2015-04-09T21:20:50+0000
2015-04-09T21:21:24+0000
2015-04-09T21:21:24+0000

ttyUSB0 Audit on 9/4/2015 21:08:51 00200070 47800000796D2972
ttyUSB0
ttyUSB0 Audit on 9/4/2015 21:11:04 00200023 008000002A50F156D
ttyUSB0
ttyUSB0 Audit on 9/4/2015 21:11:27 00200023 00800000294CF156D
ttyUSB0
ttyUSB0 Audit on 9/4/2015 21:11:51 00200023 008000002A4CF156D
ttyUSB0
ttyUSB0 Audit on 9/4/2015 21:13:01 0020002c 478000007E2D2972
ttyUSB0
ttyUSB0 Audit on 9/4/2015 21:13:37 0020002c 478000007DAD2972
ttyUSB0
```



Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initials	Time
✓ 18.	CA unmounts HSMFD by executing cd /tmp then umount /media/HSMFD CA removes HSMFD.	GL	21:39
✓ 19.	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	GL	21:40
✓ 20.	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# BB21907244 ✓	GL	21:42
✓ 21.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.	GL	21:43

Distribute HSMFDs

Step	Activity	Initials	Time
✓ 22.	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.	GL	21:43

Returning Laptop to a TEB

Step	Activity	Initials	Time
✓ 23.	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# BB24646672 / serial # 41593712005 ✓	GL	21:45
✓ 24.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.	GL	21:46



Returning OP and SO Cards to TEBs

Step	Activity	Initials	Time
25.	<p>CA calls each COs to the front of the room one at a time and repeats the steps below.</p> <ul style="list-style-type: none"> a) CA takes the two TEBs 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) CO places the SO cards into the plastic case. d) CA places each plastic case into the proper TEBs, seals in front of IW1 and CO then the CA initials TEB and strip. e) IW1 inspects each TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. f) CA hands each TEB containing the OP and the SO cards to the CO. CO inspects and verifies TEB #s and contents then initials his/her TEB. g) CO enters completion time and signs for each TEB in the table below in IW1's script. IW1 initials table entry. h) CO returns to his/her seat with the TEBs, being careful not to poke or puncture TEBs. <p>CO 2: Anne-Marie Eklund ✓ OP TEB # BB21907214 ✓ SO TEB # BB21907211 ✓</p> <p>CO 4: Robert Seastrom ✓ OP TEB # BB21907204 ✓ SO TEB # BB21907203 ✓</p> <p>CO 5: Christopher Griffiths ✓ OP TEB # BB21907208 ✓ SO TEB # BB21907206 ✓</p> <p>CO 6: Gaurab Upadhaya ✓ OP TEB # BB21907210 ✓ SO TEB # BB21907207 ✓</p> <p>CO 7: Alain Aina ✓ OP TEB # BB21907209 ✓ SO TEB # BB21907212 ✓</p>	<p>GL</p>	<p>27:12</p>



ICANN

ICANN Root DNSSEC KSK Ceremony 21

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 2	OP 2 of 7	BB21907214	Anne-Marie Eklund Lowinder		9 April 2015	21:52	GL
CO 2	SO 2 of 7	BB21907211	Anne-Marie Eklund Lowinder		9 April 2015	21:52	GL
CO 4	OP 4 of 7	BB21907204	Robert Seastrom		9 April 2015	21:57	GL
CO 4	SO 4 of 7	BB21907203	Robert Seastrom		9 April 2015	21:57	GL
CO 5	OP 5 of 7	BB21907208	Christopher Griffiths		9 April 2015	22:02	GL
CO 5	SO 5 of 7	BB21907206	Christopher Griffiths		9 April 2015	22:02	GL
CO 6	OP 6 of 7	BB21907210	Gaurab Upadhaya		9 April 2015	22:06	GL
CO 6	SO 6 of 7	BB21907207	Gaurab Upadhaya		9 April 2015	22:07	GL
CO 7	OP 7 of 7	BB21907209	Alain Aina		9 April 2015	22:11	GL
CO 7	SO 7 of 7	BB21907212	Alain Aina		9 April 2015	22:12	GL

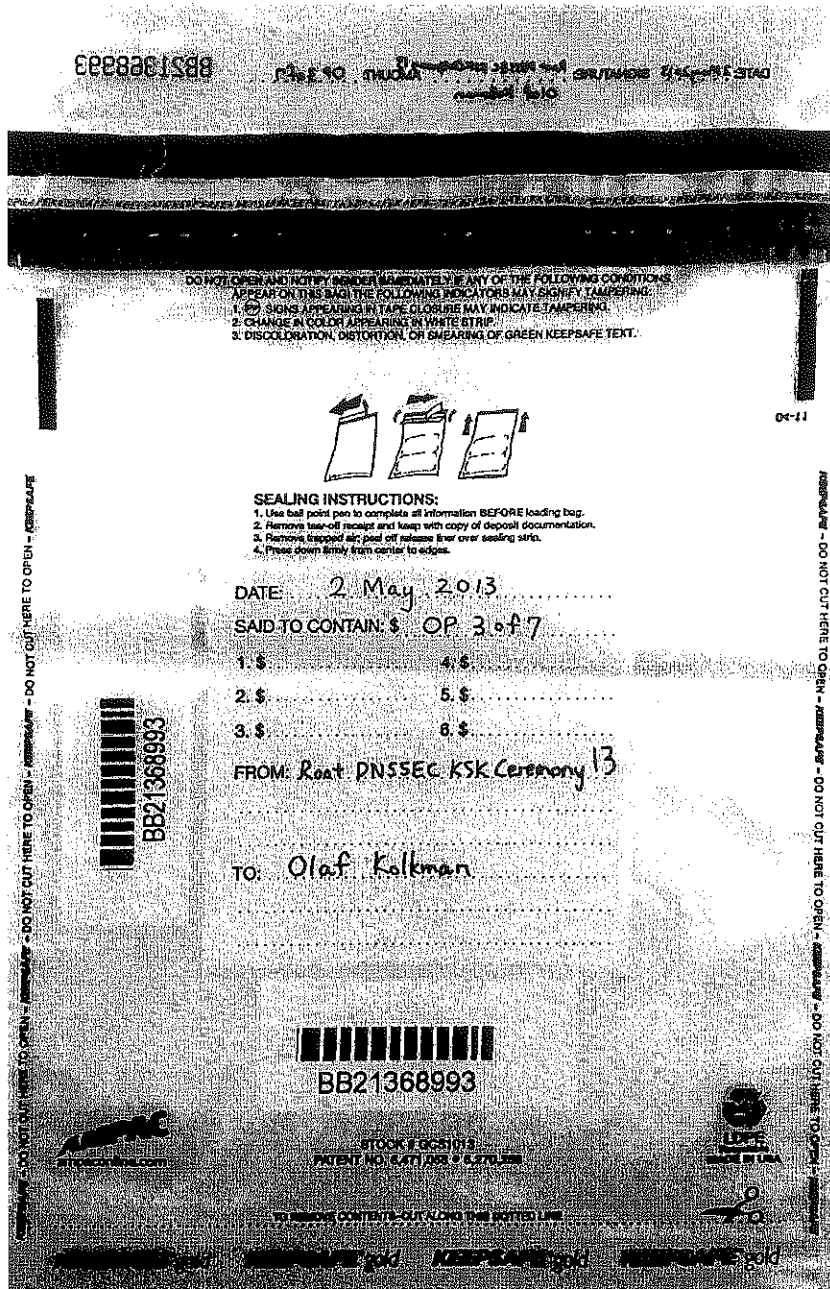


Figure 2



Returning Equipment to Safe #1

Step	Activity	Initials	Time
✓ 26.	CA, IW1, SSC1 open safe room and enter with equipment cart.	GL	22:13
✓ 27.	SSC1 opens Safe #1 shielding combination from camera.	GL	22:14
✓ 28.	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.	GL	22:15
✓ 29.	CA records return of HSM2, HSM3 and HSM4 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. HSM2: TEB# BB24646674 / serial # K6002013 ✓ HSM3: TEB# BB24646676 / serial # H14030321 ✓ HSM4: TEB# BB24646675 / serial # H14110111 ✓	GL	22:18
✓ 30.	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# BB24646672 / serial # 41593712005 ✓	GL	22:19
✓ 31.	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# BB21907244 ✓	GL	22:20
✓ 32.	CA records return of APP. Key in next entry field of safe log with TEB #, printed name, date, time, and signature; places the APP. Key into Safe #1 and IW1 initials the entry. APP. Key: TEB # BB21907213 ✓	GL	22:24

Close Equipment Safe #1

Step	Activity	Initials	Time
✓ 33.	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.	GL	22:21
✓ 34.	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.	GL	22:22
✓ 35.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	GL	22:22



Open Credential Safe #2

Step	Activity	Initials	Time
✓ 36.	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 TEB with them.	GL	22:24
✓ 37.	SSC2 opens Safe #2 while shielding combination from camera.	GL	22:26
✓ 38.	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.	GL	22:26



CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
39.	<p>One by one, each COs along with the CA (using his/her common key):</p> <ul style="list-style-type: none"> 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 card including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB# s and card type to his/her script. c) Note: If log entry is pre-printed, verify the entry, record time of completion and sign. d) CO shows each 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. <p>Repeat the steps above until all cards are returned to the deposit box.</p> <p>CO 2: Anne-Marie Eklund Lowinder Box # 1259 ✓ OP TEB # BB21907214 ✓ SO TEB # BB21907211 ✓</p> <p>CO 4: Robert Seaström Box # 1260 ✓ OP TEB # BB21907204 ✓ SO TEB # BB21907203 ✓</p> <p>CO 5: Christopher Griffiths Box # 1240 ✓ OP TEB # BB21907208 ✓ SO TEB # BB21907206 ✓</p> <p>CO 6: Gaurab Upadhaya Box # 1261 ✓ OP TEB # BB21907210 ✓ SO TEB # BB21907207 ✓</p> <p>CO 7: Alain Aina Box # 1242 ✓ OP TEB # BB21907209 ✓ SO TEB # BB21907212 ✓</p>	<p>SL</p>	<p>22:39</p>



Close Credential Safe #2

Step	Activity	Initials	Time
✓ 40.	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.	GL	22:40
✓ 41.	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.	GL	22:40
✓ 42.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	GL	22:41

Participant Signing of IW1's Script

Step	Activity	Initials	Time
✓ 43.	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.	GL	22:45
✓ 44.	CA reviews IW1's script and signs it.	GL	22:47

[Handwritten signature]

Signing Out of Ceremony Room

Step	Activity	Initials	Time
✓ 45.	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.	GL	22:57

Filming Stops

Step	Activity	Initials	Time
✓ 46.	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.	GL	22:00



Copying and Storing the Script

Step	Activity	Initials	Time
47.	<p>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.</p> <p>Audit bundles each contain:</p> <ul style="list-style-type: none"> a) Output of signer system – HSMFD b) Copy of the KSR_COPY FD used for HSM3 and HSM4 c) Copy of IW1's key ceremony script d) Audio-visual recording e) Logs from the Physical Access Control and Intrusion Detection System (Range is 11/20/2014 – 04/09/2015) f) The IW attestation (A.1 below) g) SA attestation (A.2, A.3 below) <p>All in a TEB labeled "Root DNSSEC KSK Ceremony 21", 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.</p>		

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.

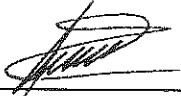
7. Other items

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.

Gustavo Lozano



Date: 9 April 2015

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 **20 November 2014 00:00 UTC** to now.

Connor Barthold



Date: 9 April 2015

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.

Connor Barthold



Date: 9 April 2015

```
cbarthold@srx> show configuration | no-more
## Last commit: 2015-03-20 05:33:11 UTC by reed
version 12.1X44-D35.5;
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 "XXXXXXXXXXXX"; ## SECRET-DATA
  }
  name-server {
    8.8.8.8;
    8.8.4.4;
  }
  login {
    user cbarthold {
      full-name "Connor A. Barthold";
      uid 2007;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user reed {
      full-name "Reed Quinn";
      uid 2003;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
  }
  services {
    ssh {
      root-login allow;
    }
  }
  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-rollback 20;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
processes {
    idp-policy disable;
}
ntp {
    server 129.6.15.28;
    server 129.6.15.29;
    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 {
    unit 0 {
        family inet {
            address 10.100.1.1/24;
        }
    }
}

```

```

    }
  }
  ge-1/0/0 {
    unit 0 {
      family inet {
        address 152.194.1.148/28;
      }
    }
  }
  vlan {
    unit 0 {
      family inet {
        address 10.4.29.1/24;
      }
    }
  }
}
routing-options {
  static {
    route 0.0.0.0/0 next-hop 152.194.1.145;
  }
}
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 media-to-untrust {
      from zone media;
      to zone untrust;
      rule source-nat-rule-1 {
        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 [ icanndns simplexgrinnell
simplexgrinnell2 simplex simplex2 icann google ];
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
  from-zone media to-zone untrust {
    policy media-to-untrust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
}
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 icann dns 199.4.28.0/22;
        address simplexgrinnell 12.30.47.110/32;
        address simplexgrinnell2 205.145.182.128/32;
        address simplex 216.224.218.31/32;
        address simplex2 216.224.219.32/32;
        address icann 192.0.32.0/20;
        address google 8.8.8.8/32;
    }
    interfaces {
        ge-1/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone media {
    interfaces {
        fe-0/0/7.0;
    }
}
}
}
applications {
    application sg {
        protocol udp;
        source-port 3060;
        destination-port 3061;
    }
    application sg2 {
        protocol udp;
        source-port 3065;
        destination-port 3061;
    }
    application simplexout {
        protocol udp;
        source-port 3060;
        destination-port 18031;
    }
    application simplexout2 {
        protocol udp;
    }
}

```

```
        source-port 3065;
        destination-port 18031;
    }
}
vlans {
    vlan-trust {
        vlan-id 3;
        l3-interface vlan.0;
    }
}
```

cbarthold@srx>