



**Internet Corporation for Assigned Names and Numbers**

**Root DNSSEC HSM Acceptance  
Testing Ceremony  
Monday July 20, 2015**

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

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



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:

<b>A</b>	Alfa	AL-FAH
<b>B</b>	Bravo	BRAH-VOH
<b>C</b>	Charlie	CHAR-LEE
<b>D</b>	Delta	DELL-TAH
<b>E</b>	Echo	ECK-OH
<b>F</b>	Foxtrot	FOKS-TROT
<b>G</b>	Golf	GOLF
<b>H</b>	Hotel	HOH-TEL
<b>I</b>	India	IN-DEE-AH
<b>J</b>	Juliet	JEW-LEE-ETT
<b>K</b>	Kilo	KEY-LOH
<b>L</b>	Lima	LEE-MAH
<b>M</b>	Mike	MIKE
<b>N</b>	November	NO-VEM-BER
<b>O</b>	Oscar	OSS-CAH
<b>P</b>	Papa	PAH-PAH
<b>Q</b>	Quebec	KEH-BECK
<b>R</b>	Romeo	ROW-ME-OH
<b>S</b>	Sierra	SEE-AIR-RAH
<b>T</b>	Tango	TANG-GO
<b>U</b>	Uniform	YOU-NEE-FORM
<b>V</b>	Victor	VIK-TAH
<b>W</b>	Whiskey	WISS-KEY
<b>X</b>	Xray	ECKS-RAY
<b>Y</b>	Yankee	YANG-KEY
<b>Z</b>	Zulu	ZOO-LOO
<b>1</b>	One	WUN
<b>2</b>	Two	TOO
<b>3</b>	Three	TREE
<b>4</b>	Four	FOW-ER
<b>5</b>	Five	FIFE
<b>6</b>	Six	SIX
<b>7</b>	Seven	SEV-EN
<b>8</b>	Eight	AIT
<b>9</b>	Nine	NIN-ER
<b>0</b>	Zero	ZEE-RO

# Act 1. Initiate Ceremony and Verify the Chain of Custody

## Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	SA confirms that all audit cameras are recording.	AP	16:50
2.	IW1 confirms that all participants are signed into the Ceremony Room.	AP	16:50

## Emergency Evacuation Procedures

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	AP	16:50

## 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>July 20 2015 16:51</u></p> <p>All entries into this script or any logs should follow this common source of time.</p>	AP	16:51

## Verify Chain of Custody

Step	Activity	Initials	Time
5.	CA unpacks the HSMs boxes while leaving HSMs enclosed in vendor supplied TEBs.	AP	16:55
6.	<p>CA match HSMs serial number and vendor TEBs to digitally signed email from the vendor Figure 1. If these do not match, re-package HSMs, terminate the ceremony and return HSMs.</p> <p>HSM: TEB# 02736035 / serial # H1403033 ✓</p> <p>HSM: TEB# 02668316 / serial # H1411006 ✓</p>	AP	16:56

**Shipment Details UE00610 (El Segundo)**

Peter Clements

Sent: Wednesday, June 10, 2015 at 3:58  
 To: Andres Pavez; Punky Duero  
 Cc: jrose@citsus.com; Rob Stubbs; Daryl Hyett

This message was digitally signed by "Peter.Clements@ULTRA-AEP.COM".

Dear Andres and Punky,

Please find details of your order dispatched on 10/06/2015. This email has been signed with a digital signature. Please let me know if you require any further assistance.

This is a part shipment as per your schedule. The destination is Equinix Facility, El Segundo.

Your order has been dispatched please see details below:

Date	10/06/15
Customer PO#	PO# 15JR7177
AEP Ref#	UE00610
Courier Used	Fedex
AWB/Tracking #	773796340230
Product Type	KEY-PLUS

Serial Number	Tamper Bag Ref
H1403033 ✓	02736035 ✓
H1411006 ✓	02668316 ✓

Upon receipt please check that the serial number and tamper evident bag number match the details above. If they do not it could indicate the goods have tampered with. If you believe the goods have been tampered with during transit please contact AEP immediately at [customerorders@ultra-aep.com](mailto:customerorders@ultra-aep.com)

**Peter Clements**  
 Head of Compliance

Ultra Electronics  
 Communication & Integrated Systems  
 419 Bridport Road  
 Greenford  
 Middlesex  
 UB6 8UA

[peter.clements@ultra-cis.com](mailto:peter.clements@ultra-cis.com)  
 Tel: +44 (0) 208 813 4701

<http://www.ultra-cis.com/>



Communication & Integrated Systems

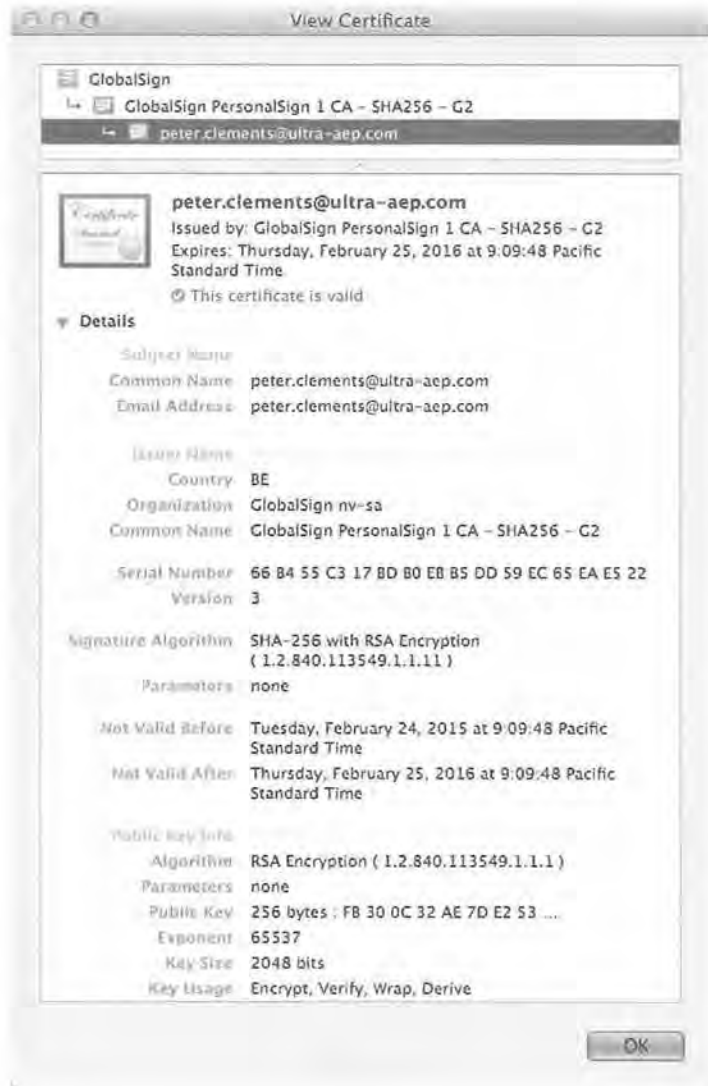


Figure 1

## Act 2. Perform the HSM Acceptance Testing

### Set Up Laptop

Step	Activity	Initials	Time
1.	CA takes the general purpose laptop, connects laptop power, external display, printer and boots laptop from test O/S DVD (same of production version which is publicly available).	AP	17:00
2.	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	AP	17:01
3.	CA confirms that the printer is connected then configures printer as default and prints test page by going to <b>System &gt; Administration &gt; Printing</b> And follow the steps below: a) Click the <b>New Printer</b> icon (left side), leave everything default and then click the button <b>Forward</b> b) Under "Select Connection" choose the first device "HP Laserjet xxxx" and then click the button <b>Forward</b> (Note: The xxxx is the Printer Model) c) Select <b>HP</b> and click the button <b>Forward</b> d) Under "Models" scroll up and select "Laserjet", and then click the button <b>Forward</b> e) To finish click the button <b>Apply</b> f) Under "Local Printers" from the left menu, select "printer" g) Click the button "Make Default Printer" and "Print Test Page"	AP	17:04
4.	CA opens a terminal window and maximizes its size for visibility by going to <b>Applications &gt; Accessories &gt; Terminal</b> Follow the additional steps to maximize the terminal window: a) Click the <b>View</b> menu and select <b>Zoom In</b> b) Repeat the step above as necessary	AP	17:05
5.	CA checks and fixes date and time on laptop based on wall clock. On the laptop terminal windows, CA executes: <code>cp /usr/share/zoneinfo/UTC /etc/localtime</code> When "cp: overwrite '/etc/localtime'?" is displayed, type "y" and press enter. Then CA executes <code>date -s "20150720 HH:MM:SS"/</code> where HH is two digit Hour, MM is two digit Minutes and SS is two digit Seconds CA executes <code>date</code> using the Terminal window to confirm the date is properly configured.	AP	17:07

**Format and label blank FD**

Step	Activity	Initials	Time
6.	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 1</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.	AP	17:09
7.	CA repeats step 6 for the 2 <sup>nd</sup> blank FD	AP	17:09
8.	CA repeats step 6 for the 3 <sup>rd</sup> blank FD	AP	17:10

**Connect HSMFD**

Step	Activity	Initials	Time
9.	CA plugs an empty HSMFD into free USB slot on the laptop and waits for O/S to recognize the FD. CA lets participants view that the HSMFD is empty and then closes the file system window.	AP	17:10

**Start Logging Terminal Session**

Step	Activity	Initials	Time
10.	CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code>	AP	17:11
11.	CA executes <code>script script-20150720.log</code> to start a capture of terminal output.	AP	17:11

**Start Logging HSM Output**

Step	Activity	Initials	Time
12.	CA connects two (2) serial to USB null modem cable to laptop. Note that the first USB cable connected will be "ttyUSB0", the second will be "ttyUSB1".	AP	17:12
13.	CA opens a second terminal window and maximizes its size for visibility by going to <b>Applications &gt; Accessories &gt; Terminal</b> . Follow the additional steps to maximize the terminal window: <ul style="list-style-type: none"> <li>a) Click the <b>View</b> menu and select <b>Zoom In</b></li> <li>b) Repeat the step above as necessary</li> </ul> and executes <pre>cd /media/HSMFD</pre> <pre>stty -F /dev/ttyUSB0 115200</pre> <pre>stty -F /dev/ttyUSB1 115200</pre> <pre>ttyaudit /dev/ttyUSB0 /dev/ttyUSB1</pre> to start logging HSM serial port outputs. Note: <b>DO NOT</b> unplug USB serial port from laptop as this causes logging to stop.	AP	17:14



**HSM3: Power Up**

Step	Activity	Initials	Time
14.	CA inspects the HSM vendor supplied TEB for tamper evidence; reads out TEB # and serial #. IW1 confirms TEB # and serial # below. HSM: TEB# 02736035 / serial # H1403033 ✓	AP	17:15
15.	CA removes HSM from TEB; discards TEB, label the HSM with the label HSM3 and plugs ttyUSB0 null modem serial cable to the back.	AP	17:17
16.	CA removes the small packet on top of the HSM3 containing the HSM3 physical key and verify the serial # on the packet matches with the HSM3's serial #, then verify the number in the key matches with the number in the packet. Note: The HSM physical key is used to enable/disable the LCD display and the Keypad.	AP	17:18
17.	CA returns the physical key inside the small packet and places it in a prepared TEB and seals it. Reads out TEB # and shows it to the participants and IW1 to confirm the TEB # below. HSM3 Physical Key: TEB# BB21907221 ✓	AP	17:19
18.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	AP	17:20
19.	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 and the application version with below. HSM3: Serial # H1403033 ✓ Keyper Application: v2.3 ✓	AP	17:24

**HSM3: Issuing Security Officer (SO) Cards**

Step	Activity	Initials	Time
20.	CA will perform the following steps to make <b>Security Officer (SO)</b> cards: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "1.Issue SO Cards" hit ENT to confirm c) When "Issue SO Cards?" is displayed, hit ENT to confirm d) When "Num Cards?" is displayed, enter "3" and hit ENT to confirm e) When "Num Req Cards?" is displayed, enter "2" and hit ENT to confirm f) When "Insert Card SO #?" is displayed, insert the proper sequence of SO card from the cardholder g) When "PIN?" is displayed, enter "11223344" and hit ENT h) When "Remove Card?" is displayed, remove card i) Repeat steps f) to h) for the 2nd and 3rd SO cards j) When "SO Cards Issued" is displayed, hit ENT to confirm  As each card is created the CA places it in the cardholder.	AP	17:27

**HSM3: Switching to Secure State**

Step	Activity	Initials	Time
21.	<p>CA will perform the following steps to set the HSM Secure State using Security Officer (SO) cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "3.Secure" hit ENT to confirm</li> <li>c) When "Secure?" is displayed, hit ENT to confirm</li> <li>d) When "Insert Card SO #?" is displayed, insert the SO from the cardholder</li> <li>e) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>f) When "Remove Card?" is displayed, remove card</li> <li>g) Repeat steps d) to f) for the 2nd SO card</li> <li>h) When "SMK AES Triple DES?" is displayed, hit CLR to skip</li> <li>i) When "SMK AES" is displayed, hit CLR to confirm</li> <li>j) When "Set HSM Port?" is displayed, hit CLR to skip</li> <li>k) When "Enable IPv4/IPv6?" is displayed, hit CLR to skip</li> <li>l) When "Set IPv4 Address?" is displayed, hit CLR to skip</li> <li>m) When "Set IPv4 NetMask?" is displayed, hit CLR to skip</li> <li>n) When "Set IPv4 Gateway?" is displayed, hit CLR to skip</li> <li>o) When "Set IPv6 Address?" is displayed, hit CLR to skip</li> <li>p) When "Set IPv6 NetMask?" is displayed, hit CLR to skip</li> <li>q) When "Set IPv6 Gateway?" is displayed, hit CLR to skip</li> <li>r) When "Change Clock?" is displayed, hit CLR to skip</li> <li>s) When "Import Config.?" is displayed, hit CLR to skip</li> <li>t) When "FIPS Mode On Disable?" is displayed, hit CLR to skip</li> <li>u) When "FIPS Mode On" is displayed, hit CLR to confirm</li> <li>v) When "Global Key Export Enabled" is displayed, hit CLR to confirm</li> </ul> <p>Done Rebooting Device will be displayed.</p> <p>As each card is used the CA places it in the cardholder.</p>	AP	17:30

**HSM3: Issuing Crypto Officer (CO), Operator (OP) and Adapter Authorization key (AAK) Cards**

Step	Activity	Initials	Time
22.	<p>CA will perform the following steps to make <b>Crypto Officer (CO)</b> cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"7.Role Mgmt"</b> hit <b>ENT</b> to confirm</li> <li>c) When <b>"Insert Card SO #?"</b> is displayed, insert the SO card from the cardholder</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b> and hit <b>ENT</b></li> <li>e) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd SO card</li> <li>g) Select <b>"1.Issue Cards"</b> hit <b>ENT</b> to confirm</li> <li>h) Select <b>"1.Issue CO Cards"</b> hit <b>ENT</b> to confirm</li> <li>i) When <b>"Issue CO Cards?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>j) When <b>"Num Cards?"</b> is displayed, enter <b>"3"</b> and hit <b>ENT</b> to confirm</li> <li>k) When <b>"Num Req Cards?"</b> is displayed, enter <b>"2"</b> and hit <b>ENT</b> to confirm</li> <li>l) When <b>"Insert Card #?"</b> is displayed, insert the proper sequence of <b>CO</b> card from the cardholder</li> <li>m) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b> and hit <b>ENT</b></li> <li>n) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>o) Repeat steps l) to n) for the 2nd and 3rd CO cards</li> <li>p) When <b>"CO Cards Issued"</b> is displayed, hit <b>ENT</b> to confirm</li> </ul> <p>As each card is created the CA places it in the cardholder.</p>	AP	17:34
23.	<p>CA will perform the following steps to make <b>Operator (OP)</b> cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"2.Issue OP Cards"</b> from the same menu <b>"Issue Cards"</b> and hit <b>ENT</b> to confirm</li> <li>c) When <b>"Issue OP Cards?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>d) When <b>"Num Cards?"</b> is displayed, enter <b>"3"</b> and hit <b>ENT</b> to confirm</li> <li>e) When <b>"Num Req Cards?"</b> is displayed, enter <b>"2"</b> and hit <b>ENT</b> to confirm</li> <li>f) When <b>"Insert Card #?"</b> is displayed, insert the proper sequence of <b>OP</b> card from the cardholder</li> <li>g) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b> and hit <b>ENT</b></li> <li>h) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>i) Repeat steps f) to h) for the 2nd and 3rd OP cards</li> <li>j) When <b>"OP Cards Issued"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>k) Hit <b>CLR</b> to return to the previous menu <b>"Role Mgmt"</b></li> </ul> <p>As each card is created the CA places it in the cardholder.</p>	AP	17:37

Step	Activity	Initials	Time
24.	<p>CA will perform the following steps to make <b>Adapter Authorization key (AAK)</b> cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"3.Backup AAK"</b> from the same menu <b>"Role Mgmt"</b> and hit <b>ENT</b> to confirm</li> <li>c) When <b>"Backup AAK?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>d) When <b>"Num Cards?"</b> is displayed, enter <b>"2"</b> and hit <b>ENT</b> to confirm</li> <li>e) When <b>"Insert Card #?"</b> is displayed, insert the proper sequence of <b>AAK</b> card from the cardholder</li> <li>f) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>g) Repeat steps e) to g) for the 2nd AAK card</li> <li>h) When <b>"AAK Exported"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>i) Hit <b>CLR</b> to return to the main menu <b>"Secured"</b></li> </ul> <p>As each card is created the CA places it in the cardholder.</p>	AP	17:39

**HSM3: Change and Verify API Settings**

Step	Activity	Initials	Time
25.	<p>CA will perform the following steps to change the API settings:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"5.Key Mgmt"</b> hit <b>ENT</b> to confirm</li> <li>c) When <b>"Insert Card CO #?"</b> is displayed, insert the CO card from the cardholder</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b> and hit <b>ENT</b></li> <li>e) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd CO card</li> <li>g) Select <b>"5. API Settings"</b> hit <b>ENT</b> to confirm</li> <li>h) Select <b>"1.Key Import"</b> hit <b>ENT</b> to confirm</li> <li>i) When <b>"Key Import On Disable?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>j) Select <b>"2.Key Export"</b> hit <b>ENT</b> to confirm</li> <li>k) When <b>"Key Export On Disable?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>l) Select <b>"5.Sym Key Der"</b> hit <b>ENT</b> to confirm</li> <li>m) When <b>"Sym Key Der On Disable?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>n) Hit <b>CLR</b> to return to the menu <b>"Key Mgmt"</b></li> </ul> <p>As each card is created the CA places it in the cardholder.</p>	AP	17:41

Step	Activity	Initials	Time
26.	<p>CA will perform the following steps to dump the status of the HSM:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "8.HSM Info" from the same menu "Key Mgmt" and hit ENT to confirm</li> <li>c) Select "8.Output Info" hit ENT to confirm</li> <li>d) When "Output Info?" is displayed, hit ENT to confirm</li> <li>e) Hit CLR twice to return to the main menu "Secured"</li> </ul> <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>	AP	17:44

**HSM4: Power Up**

Step	Activity	Initials	Time
27.	CA inspects the HSM vendor supplied TEB for tamper evidence; reads out TEB # and serial #. IW1 confirms TEB # and serial # below. <b>HSM: TEB# 026683167 serial # H1411006 ✓</b>	AP	17:45
28.	CA removes HSM from TEB; discards TEB, label the HSM with the label <b>HSM4</b> and plugs ttyUSB1 null modem serial cable to the back.	AP	17:47
29.	CA removes the small packet on top of the HSM4 containing the HSM4 physical key and verify the serial # on the packet matches with the HSM4's serial #, then verify the number in the key matches with the number in the packet. <b>Note: The HSM physical key is used to enable/disable the LCD display and the Keypad.</b>	AP	17:48
30.	CA places the small packet with the HSM4 physical key in a prepared TEB and seals it. reads out TEB # and shows it to participants and IW1 to confirm TEB # below. <b>HSM4 Physical Key: TEB# BB21907222 ✓</b>	AP	17:49
31.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	AP	17:50
32.	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 and the application version with below. <b>HSM4: serial # H1411006 ✓</b> <b>Keyper Application: v2.3 ✓</b>	AP	17:52

**HSM4: Importing the AAK**

Step	Activity	Initials	Time
33.	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.	AP	17:53

**HSM4: Switching to Secure State**

Step	Activity	Initials	Time
34.	<p>CA will perform the following steps to set the HSM4 Secure State using Security Officer (SO) cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "3.Secure" hit ENT to confirm</li> <li>c) When "Secure?" is displayed, hit ENT to confirm</li> <li>d) When "Insert Card SO #?" is displayed, insert the SO from the cardholder</li> <li>e) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>f) When "Remove Card?" is displayed, remove card</li> <li>g) Repeat steps d) to f) for the 2nd SO card</li> <li>h) When "SMK AES Triple DES?" is displayed, hit CLR to skip</li> <li>i) When "SMK AES" is displayed, hit CLR to confirm</li> <li>j) When "Set HSM Port?" is displayed, hit CLR to skip</li> <li>k) When "Enable IPv4/IPv6?" is displayed, hit CLR to skip</li> <li>l) When "Set IPv4 Address?" is displayed, hit CLR to skip</li> <li>m) When "Set IPv4 NetMask?" is displayed, hit CLR to skip</li> <li>n) When "Set IPv4 Gateway?" is displayed, hit CLR to skip</li> <li>o) When "Set IPv6 Address?" is displayed, hit CLR to skip</li> <li>p) When "Set IPv6 NetMask?" is displayed, hit CLR to skip</li> <li>q) When "Set IPv6 Gateway?" is displayed, hit CLR to skip</li> <li>r) When "Change Clock?" is displayed, hit CLR to skip</li> <li>s) When "Import Config.?" is displayed, hit CLR to skip</li> <li>t) When "FIPS Mode On Disable?" is displayed, hit CLR to skip</li> <li>u) When "FIPS Mode On" is displayed, hit CLR to confirm</li> <li>v) When "Global Key Export Enabled" is displayed, hit CLR to confirm</li> </ul> <p>Done Rebooting Device will be displayed.</p> <p>As each card is used the CA places it in the cardholder.</p>	<p>AP</p>	<p>17:56</p>

**HSM4: Change and Verify API Settings**

Step	Activity	Initials	Time
35.	<p>CA will perform the following steps to change the API settings:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "5.Key Mgmt" hit ENT to confirm</li> <li>c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder</li> <li>d) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>e) When "Remove Card?" is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd CO card</li> <li>g) Select "5. API Settings" hit ENT to confirm</li> <li>h) Select "1.Key Import" hit ENT to confirm</li> <li>i) When "Key Import On Disable?" is displayed, hit ENT to confirm</li> <li>j) Select "2.Key Export" hit ENT to confirm</li> <li>k) When "Key Export On Disable?" is displayed, hit ENT to confirm</li> <li>l) Select "5.Sym Key Der" hit ENT to confirm</li> <li>m) When "Sym Key Der On Disable?" is displayed, hit ENT to confirm</li> <li>n) Hit CLR to return to the menu "Key Mgmt"</li> </ul> <p>As each card is created the CA places it in the cardholder.</p>	AP	17:58



Step	Activity	Initials	Time
36.	<p>CA will perform the following steps to dumps the status of the HSM:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "8.HSM Info" from the same menu "Key Mgmt" and hit ENT to confirm</li> <li>c) Select "8.Output Info" hit ENT to confirm</li> <li>d) When "Output Info?" is displayed, hit ENT to confirm</li> <li>e) Hit CLR to return to the menu "Key Mgmt"</li> </ul> <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>	AP	18:00

**HSM4: Generate and Backup Storage Master Key (SMK)**

Step	Activity	Initials	Time
37.	CA will perform the following steps to generate <b>Storage Master Key (SMK)</b> : a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select <b>"4.SMK"</b> from the same menu <b>"Key Mgmt"</b> and hit <b>ENT</b> to confirm c) Select <b>"1.Generate SMK"</b> hit <b>ENT</b> to confirm d) When <b>"Generate SMK?"</b> is displayed, hit <b>ENT</b> to confirm e) When <b>"SMK Generated"</b> is displayed, hit <b>ENT</b> to confirm	AP	18:01
38.	CA will perform the following steps to make <b>Storage Master Key (SMK)</b> cards: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select <b>"2.Backup SMK"</b> from the same menu <b>"SMK"</b> and hit <b>ENT</b> to confirm c) When <b>"Backup SMK?"</b> is displayed, hit <b>ENT</b> to confirm d) When <b>"Num Cards?"</b> is displayed, enter <b>"4"</b> and hit <b>ENT</b> to confirm e) When <b>"Num Req Cards?"</b> is displayed, enter <b>"2"</b> and hit <b>ENT</b> to confirm f) When <b>"Insert Card #?"</b> is displayed, insert the proper sequence of SMK card from the cardholder g) When <b>"Remove Card?"</b> is displayed, remove card h) Repeat steps f) to g) for the 2nd, 3rd and 4th SMK cards i) When <b>"Verify Card #?"</b> is displayed, insert the proper sequence of SMK card from the cardholder j) When <b>"Remove Card?"</b> is displayed, remove card k) Repeat steps i) to j) for the 2nd, 3rd and 4th SMK cards l) When <b>"SMK Backed Up"</b> is displayed, hit <b>ENT</b> to confirm m) Hit <b>CLR</b> twice to return to the main menu <b>"Secured"</b>  As each card is created the CA places it in the cardholder.	AP	18:06

**HSM4: Enable/Activate**

Step	Activity	Initials	Time
39.	<p>CA will perform the following steps to activate the HSM4:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "1.Set Online" hit ENT to confirm</li> <li>c) When "Set Online?" is displayed, hit ENT to confirm</li> <li>d) When "Insert Card OP #?" is displayed, insert the OP card from the cardholder</li> <li>e) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>f) When "Remove Card?" is displayed, remove card</li> <li>g) Repeat steps e) to g) for the 2nd OP card</li> </ul> <p>As each card is used the CA places it in the cardholder. Confirm the "READY" led on the HSM4 is ON.</p>	AP	18:08

**HSM4: Check Network Connectivity between Laptop and HSM4**

Step	Activity	Initials	Time
40.	CA connects HSM4 to laptop using Ethernet cable in LAN port.	AP	18:08
41.	<p>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.</p>	AP	18:09

**HSM4: Initialize**

Step	Activity	Initials	Time
42.	<p>On the laptop terminal window, CA executes:</p> <pre>. /opt/dnssec/fixenv</pre> <p>to set environment variables for HSM then runs <code>inittoken</code> for the slot number enter:</p> <pre>0</pre> <p>for the PKCS11 Token name enter:</p> <pre>ICANNTEST</pre> <p>for the User PIN enter and re-enter:</p> <pre>123456</pre> <p>for Security Officer PIN enter and re-enter:</p> <pre>123456</pre> <p>this should return</p> <pre>Token initialized OK</pre>	AP	18:11

**HSM4: Generate New Test Key**

Step	Activity	Initials	Time
43.	<p>On the laptop terminal window, CA executes:</p> <pre>kkskgen</pre> <p>to generate new test KSK inside the HSM and Certificate Signing Request (CSR).</p> <p>When "Activate HSM prior to accepting in the affirmative! (y/n)" is displayed, confirm the hardware security module's "READY" LED is on and type "y" and press enter.</p> <p>If "slot" is asked type 0.</p> <p>Sample output should look like Figure 2.</p>	AP	18:12

```
Starting: kkskgen (at Sat Feb 14 00:40:14 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:          ICANNTEST
  ManufacturerID: AEP Networks
  Model:          Keyper 9860-2
  Serial:         H1404001

Generating 2048 bit RSA keypair...
Created keypair labeled "Kktpjs4"

SHA256 DS resource record and hash:
. IN DS 32579 8 2 A6F2B99E0E9193A9258701E0EB139E559A957587B9685FF1BEF9CCC334E15445
>> rematch vagabond sentence onlooker apple miracle playhouse passenger bombast liberty absurd tobacco
trouble barbecue quiver equipment pupil Montana indulge liberty sentence gravity eyetooth vacancy
skydive Waterloo spigot replica choking tolerance eating detector <<

Created CSR file "Kktpjs4.csr":
O: ICANN
OU: IANA
CN: Root Zone KSK 2015-02-14T00:40:22+00:00
1.3.6.1.4.1.1000.53: . IN DS 32579 8 2
A6F2B99E0E9193A9258701E0EB139E559A957587B9685FF1BEF9CCC334E15445

Kktpjs4.csr SHA256 thumbprint and hash:
DBB4890B093189A285A0F6CS4340D728DF12FA17A5E5F9F89F62B09499DDCFAB
>> suspense politeness nightbird armistice Algol company nightbird Pacific music Orlando village
resistor crucial Dakota stopwatch cellulose talon backwater wallet bookseller reindeer travesty waffle
warranty quota gadgetry ruffled molecule prowler tambourine stagehand Pegasus <<

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

Figure 2

**HSM4: Print Thumbprint**

Step	Activity	Initials	Time
44.	CA prints out hard copy of the log output file of kskgen by executing <code>printlog kskgen-20150720-*.log</code> for attachment to IW1 script.	AP	18:13

**HSM4: Record Test Keypair Label**

Step	Activity	Initials	Time
45.	IW1 records the keypair label here <u>Kkwwtts</u>	AP	18:14

**HSM4: Verify CSR**

Step	Activity	Initials	Time
46.	CA checks the integrity of the CSR by executing in to the terminal windows: <code>displaycsr XXXX.csr</code> Where XXXX would be replaced with the keypair label generated above. Hit SPACE bar until end of display and then "q". Sample output should look like Figure 3.	AP	18:15

```

Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: O=ICANN, OU=IANA, CN=Root Zone KSK 2015-02-14T00:40:22+00:00/1.3.6.1.4.1.1000.53-. IN
DS 32579 8 2 A6F2B99E0E9193A9258701E0EB139E559A957587B9685FF1BEF9CCC334E15445
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:d4:68:77:51:16:b9:d0:fa:21:25:38:b8:12:91:
          [...]
          f0:95
        Exponent: 65537 (0x10001)
    Attributes:
      a0:00
    Signature Algorithm: sha256WithRSAEncryption
    60:aa:a9:03:5e:36:b1:df:6f:ca:c9:42:49:70:7b:69:2f:59:
    [...]
    81:ae:ee:95
  
```

Figure 3

```
Starting: kskgen (at Mon Jul 20 18:11:06 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:          ICANNTEST
  ManufacturerID: AEP Networks
  Model:          Keyper 9860-2
  Serial:         H1411006
```

```
Generating 2048 bit RSA keypair...
Created keypair labeled "Kkwwtts"
```

```
SHA256 DS resource record and hash:
```

```
. IN DS 60817 8 2 52E00F223B2FC0E063CAE41981D49F227648363CBC5F117B8C186962C8382D4C
>> Dupont tobacco artist candidate clockwork combustion slowdown tobacco flatfoot reven
ue tonic bottomless minnow souvenir quota candidate inverse dictator Christmas crossove
r showgirl forever Athens inferno offload borderline gazelle gadgetry spaniel consultin
g button disbelief <<
```

```
Created CSR file "Kkwwtts.csr":
```

```
O: ICANN
OU: IANA
CN: Root Zone KSK 2015-07-20T18:11:24+00:00
1.3.6.1.4.1.1000.53: . IN DS 60817 8 2 52E00F223B2FC0E063CAE41981D49F227648363CBC5F117B
8C186962C8382D4C
```

```
Kkwwtts.csr SHA256 thumbprint and hash:
```

```
520845D38C7AA05E96091B3D507FCCA0FECB1CF98BA1F6AB1784C75CDD796729
>> Dupont antenna crusade sociable offload infancy ragtime finicky prefer applicant bee
swax crucifix drumbeat integrate spigot Orlando woodlark revival befriend Waterloo obtu
se outfielder village Pegasus banjo Jupiter soybean fascinate swelter inertia freedom c
ertify <<
```

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

**HSM4: Backup Test Key**

Step	Activity	Initials	Time
47.	CA presses <b>RESTART</b> button on <b>HSM4</b> to take <b>OFFLINE</b> and waits for <b>SELT TEST</b> to complete. Confirm the <b>"READY"</b> led on the <b>HSM4</b> is <b>OFF</b> .	AP	18:16
48.	CA will perform the following steps to make <b>Application Key (APP. Key)</b> card: <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"5.Key Mgmt"</b> hit <b>ENT</b> to confirm</li> <li>c) When <b>"Insert Card CO #?"</b> is displayed, insert the CO card from the cardholder</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b> and hit <b>ENT</b></li> <li>e) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd CO card</li> <li>g) Select <b>"3.App Keys"</b> hit <b>ENT</b> to confirm</li> <li>h) Select <b>"1.Backup"</b> hit <b>ENT</b> to confirm</li> <li>i) When <b>"Backup?"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>j) When <b>"Which Media?"</b> is displayed, select <b>"2.Backup to Card"</b> and hit <b>ENT</b> to confirm</li> <li>k) Select <b>"2.Specify key"</b> hit <b>ENT</b> to confirm</li> <li>l) Hit <b>"A"</b> to select the key generate above and hit <b>ENT</b> to confirm</li> <li>m) When <b>"Insert B/U Card?"</b> is displayed insert the proper AAP. Key card from the cardholder</li> <li>n) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>o) When <b>"Backup Success"</b> is displayed, hit <b>ENT</b> to confirm</li> <li>p) Hit <b>CLR twice</b> to return to the main menu <b>"Secured"</b></li> </ul> <p>As card is created the CA places it in the cardholder.</p>	AP	18:19
49.	CA disconnects Ethernet cable from back of <b>HSM4</b> .	AP	18:19

**HSM3: Importing the SMK and APP. Key**

Step	Activity	Initials	Time
50.	<p>CA will perform the following steps to import the <b>Storage Master Key (SMK)</b> cards in to the HSM3:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"5.Key Mgmt"</b> hit ENT to confirm</li> <li>c) When <b>"Insert Card CO #?"</b> is displayed, insert the CO card from the cardholder</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b> and hit ENT</li> <li>e) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd CO card</li> <li>g) Select <b>"4.SMK"</b> hit ENT to confirm</li> <li>h) Select <b>"3.Restore SMK"</b> hit ENT to confirm</li> <li>i) When <b>"Restore SMK?"</b> is displayed, hit ENT to confirm</li> <li>j) When <b>"Insert Card SMK #?"</b> is displayed, insert the SMK card from the cardholder</li> <li>k) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>l) Repeat steps j) to k) for the 2nd SMK card</li> <li>m) When <b>"SMK Restored"</b> is displayed, hit ENT to confirm</li> <li>n) Hit CLR to return to the previous menu <b>"Key Mgmt"</b></li> </ul> <p>As each card is used the CA places it in the cardholder.</p>	AP	18:23
51.	<p>CA will perform the following steps to import the <b>Application Key (APP. Key)</b> cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select <b>"3.App Keys"</b> hit ENT to confirm</li> <li>c) Select <b>"2.Restore"</b> hit ENT to confirm</li> <li>d) When <b>"Restore?"</b> is displayed, hit ENT to confirm</li> <li>e) When <b>"Which Media?"</b> is displayed, select <b>"2. From Card"</b> and hit ENT to confirm</li> <li>f) When <b>"Insert Card #?"</b> is displayed, insert the proper card from the cardholder</li> <li>g) When <b>"Remove Card?"</b> is displayed, remove card</li> <li>h) When <b>"Restore Complete"</b> is displayed, hit ENT to confirm</li> <li>i) Hit CLR twice to return to the main menu <b>"Secured"</b></li> </ul> <p>As card is used the CA places it in the cardholder.</p>	AP	18:24



**HSM3: Enable/Activate**

Step	Activity	Initials	Time
52.	<p>CA will perform the following steps to activate the HSM3:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "1.Set Online" hit ENT to confirm</li> <li>c) When "Set Online?" is displayed, hit ENT to confirm</li> <li>d) When "Insert Card OP #?" is displayed, insert the OP card from the cardholder</li> <li>e) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>f) When "Remove Card?" is displayed, remove card</li> <li>g) Repeat steps d) to f) for the 2nd OP card</li> </ul> <p>As each card is used the CA places it in the cardholder. Confirm the "READY" led on the HSM3 is ON.</p>	AP	18:26

**HSM3: Check Network Connectivity between Laptop and HSM3**

Step	Activity	Initials	Time
53.	CA connects HSM3 to laptop using Ethernet cable in LAN port.	AP	18:26
54.	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.	AP	18:27

**HSM3: Verify the Test Key**

Step	Activity	Initials	Time
55.	CA checks the Test Key by executing in to the terminal windows: keybackup -l -P 123456 and confirms the Testing Key Label generated in the step 45.	AP	18:28

**HSM3: Re-Initialize Erase All / Zeroize / Unsecure**

Step	Activity	Initials	Time
56.	CA disconnects Ethernet cable from back of HSM3.	AP	18:28
57.	CA presses <b>RESTART</b> button on <b>HSM3</b> to take OFFLINE and waits for SELT TEST to complete. Confirm the "READY" led on the HSM3 is OFF.	AP	18:29
58.	CA switches to the ttyaudit terminal window to display the output of the HSM3.	AP	18:29
59.	<p>CA will perform the following steps to return the HSM3 to "Unsecure" state as if just shipped from vendor. This will erase all keys (AAK, SMK, AAP), settings and configuration.</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "6.HSM Mgmt" hit ENT to confirm</li> <li>c) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder</li> <li>d) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>e) When "Remove Card?" is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd SO card</li> <li>g) Select "5.Unsecure" hit ENT to confirm</li> <li>h) When "Unsecure?" is displayed, hit ENT to confirm</li> <li>i) When "Done" is displayed, hit ENT to confirm</li> </ul> <p>It may take a few minutes for HSM to restart after erasing all keys.</p> <p>When this operation is complete the HSM3 will reboot into the 'Unsecured State' and after self test the HSM3 display should say "Important Read Manual" indicating the HSM3 is in the initialized state.</p> <p>Note: Material on the cards becomes useless once the HSMs are returned to an initialized state.</p>	AP	18:32
60.	CA turns off the HSM3 by pressing the power switch behind it.	AP	18:33

**HSM4: Re-Initialize Erase All / Zeroize / Unsecure**

Step	Activity	Initials	Time
61.	CA confirms the <b>READY</b> led on the HSM4 is <b>OFF</b> .	AP	18:33
62.	<p>CA will perform the following steps to return the HSM4 to "Unsecure" state as if just shipped from vendor. This will erase all keys (AAK, SMK, AAP), settings and configuration.</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard and scroll through menu using &lt;&gt; key</li> <li>b) Select "6.HSM Mgmt" hit ENT to confirm</li> <li>c) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder</li> <li>d) When "PIN?" is displayed, enter "11223344" and hit ENT</li> <li>e) When "Remove Card?" is displayed, remove card</li> <li>f) Repeat steps c) to e) for the 2nd SO card</li> <li>g) Select "5.Unsecure" hit ENT to confirm</li> <li>h) When "Unsecure?" is displayed, hit ENT to confirm</li> <li>i) When "Done" is displayed, hit ENT to confirm</li> </ul> <p>It may take a few minutes for HSM to restart after erasing all keys.</p> <p>When this operation is complete the HSM4 will reboot into the 'Unsecured State' and after self test the HSM4 display should say "Important Read Manual" indicating the HSM4 is in the initialized state.</p> <p>Note: Material on the cards becomes useless once the HSMs are returned to an initialized state.</p>	AP	18:35
63.	CA turns off the HSM4 by pressing the power switch behind it.	AP	18:35

## Act. 3 Secure Hardware and Close the Ceremony

### Return HSMs to a TEB

Step	Activity	Initials	Time
1.	CA disconnects each HSMs from power and laptop (serials and Ethernet) if connected.	AP	18:36
2.	CA places HSM3 into a prepared TEB and seals it.	AP	18:37
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM3: TEB# BB24646668 ✓ serial # H1403033 ✓ IW1 and CA initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.	AP	18:39
4.	CA places HSM4 into a prepared TEB and seals it.	AP	18:40
5.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM4: TEB# BB24646667 ✓ serial # H1411006 ✓ IW1 and CA initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.	AP	18:41

### Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
6.	<b>Closing ttyaudit terminal window</b> 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".	AP	18:42
7.	<b>Terminating the logging script</b> CA stops logging terminal output by entering "exit" in the other terminal window. This only stops the script logging and will NOT close window.	AP	18:43

**Backup HSMFD Contents**

Step	Activity	Initials	Time
8.	Set dotglob by executing <code>shopt -s dotglob</code> This allows copying everything in the original HSMFD.	AP	18:43
9.	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>	AP	18:44
10.	Copy and paste the sha256hash and paste it on Text Editor by going to <b>Applications &gt; Accessories &gt; Text Editor</b>	AP	18:45
11.	Print one copy for the audit bundle.	AP	18:46
12.	CA displays contents of HSMFD by executing <code>ls -ltr</code>	AP	18:46
13.	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>	AP	18:47
14.	CA displays contents of HSMFD_ by executing <code>ls -ltr /media/HSMFD_</code>	AP	18:48
15.	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	AP	18:48
16.	CA unmounts new FD using <code>umount /media/HSMFD_</code>	AP	18:49
17.	CA removes HSMFD_ and places on table.	AP	18:49
18.	CA repeats step 13 to 17 for the 2 <sup>nd</sup> copy	AP	18:50

**Print Logging Information**

Step	Activity	Initials	Time
19.	CA print out hard copy of logging information by executing <code>enscript -Gr -# 1 script-20150720.log</code> <code>enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20150720-*.log</code> for attachment to IW1 script. <b>Note: Ignore the error regarding non-printable characters if prompted.</b>	AP	18:54

65d622e2ae826ea06bf2e8a6722508894987dc660bf3632c83388f7f6e78533c



script-20150720.log

```
66:19a1c0:9e:91:67:12:09:80:f0:15:d0:34:6e:25:
1b:9cd5:e7:cb:4f:45:8c:2e:da:32:6b:35:40:d0:
48:1176:f2:6e:8e:b7:a5:ba:a6:7d:f1:ac:b1:ed:59:
b1:20:fc:fd:2a:26:13:c7:b4:0f:da:ac:5c:c3:db:
0f:bc:4b:ba:0a:16:64:1d:e2:8c:1b:ce:f8:d8:6b:
18:c0:c1:7b:50:ea:ea:a8:02:76:5b:b7:66:be:ac:
40:7f:37:41:1f:2c:d2:86:4f:d8:1e:2a:3:ff:57:90:
ca:02:ab:be:13:dc:0d:f5:f0:f9:bc:53:21:40:7d:
cf:b7:4c:ce:84:5b:f7:30:5c:28:78:21:25:56:5a:
38:b4:83:9f:17:7c:d1:2e:d1:b7:0b:5c:13:83:75:
d1:0a:8b:89:ca:27:01:99:65:36:30:41:02:d6:ff:
c8:7b:66:79:ce:ee:10:01:9e:37:9b:cb:97:17:03:
6d:76:28:fd:e2:5a:50:5b:2d:45:9a:02:70:10:61:
fe:4f
```

Exponent: 65537 (0x10001)

Attributes:
a0:00

Signature Algorithm: sha256WithRSAEncryption
18:a9:ed:e5:eb:b6:0d:75:40:eb:47:53:80:8b:48:a5:a5:79:
5e:06:c9:5b:da:b1:de:16:e5:16:5a:e6:ed:ca:94:9c:54:87:
9b:c8:ef:4f:6f:78:75:19:2a:19:05:00:d9:72:9f:62:5d:cb:
73:d0:77:b3:2c:15:74:44:c0:97:51:es:c4:ea:d6:4b:e0:89:51:
19:41:93:7b:7a:b9:e5:34:2f:db:e6:12:3b:77:2d:a0:a3:9e:
c4:42:cd:95:22:3a:bb:d5:6b:60:c9:0a:74:62:c5:2a:c2:98:
76:d7:69:d6:1b:70:d4:f2:e:68:08:f3:a2:1b:re:3:83:08:92:f8:
ed:8c:94:2d:52:b0:67:5c:26:82:06:51:94:f7:20:75:4c:19:
a9:c9:41:a4:84:e3:a7:61:32:52:5e:62:74:e3:19:60:99:db:
11:a1:ac:f3:20:76:96:51:f3:02:de:89:23:d2:98:8b:41:1e:
6c:33:6c:9a:ff:0e:17:80:64:a4:26:5b:34:6d:61:93:f1:2c:
07:4d:07:63:07:7f:3f:de:d2:33:10:97:47:00:4f:65:d0:b4:
95:73:8a:42:166:a6:2e:3a:e6:7d:9f:e8:6e:0b:cf:8a:a6:a7:
23:14:29:1e:3f:51:f9:48:c8:7d:38:a1:2d:08:64:6e:b1:08:
ab:08:a8:9b

\033[40m\033[33m\033[38m\033[49m\033[0mroot@localhost:/media/HSMFD\007[root@localhost HS

```
MFD]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data:
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=0.953 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.363 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.666 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.367 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=255 time=0.506 ms
64 bytes from 192.168.0.2: icmp_seq=6 ttl=255 time=0.360 ms
```

```
--- 192.168.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.360/0.535/0.953/0.218 ms
\033[0mroot@localhost:/media/HSMFD\007[root@localhost HSMFD]# keybackup -l --P 123456
Starting: keybackup -l --P 123456 (at Mon Jul 20 18:27:04 2015 UTC)
```

```
1 public keys:
label:Kkwttts
1 private keys:
label:Kkwttts
```

```
***** Log output in ./keybackup-20150720-182704.log *****
\033[0mroot@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit
```

```
Script done on Mon 20 Jul 2015 06:42:29 PM UTC
```



07/20/15  
15:41:40

1

tyaudit-tyUSB0-20150720-171329.log

```
2015-07-20T17:21:32+0000 ttyUSB0 bbb
2015-07-20T17:21:32+0000 ttyUSB0 HI403033 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T17:21:32+0000 ttyUSB0 BBL CRC32: 0x757574CA
2015-07-20T17:21:32+0000 ttyUSB0 Running applicationBootloader at 0xEFDC0000
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 HI403033 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T17:21:32+0000 ttyUSB0 ABL CRC32: 0xE7E0FA6A
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 #####
2015-07-20T17:21:32+0000 ttyUSB0 ## ABL tamper records ##
2015-07-20T17:21:32+0000 ttyUSB0 #####
2015-07-20T17:21:32+0000 ttyUSB0 Current Tamper Counts (decimal 0-255):
=====
2015-07-20T17:21:32+0000 ttyUSB0 vextoosTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 vintoosTamperCount: 40
2015-07-20T17:21:32+0000 ttyUSB0 vbboosTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 maxstrtempTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 minstrtempTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 meshTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 extampSMKTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 extampIMKTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 tempdiffTamperCount: 0
2015-07-20T17:21:32+0000 ttyUSB0 pftamperCount: 40
2015-07-20T17:21:32+0000 ttyUSB0 restartTamperCount: 128
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 Current tamper bitmaps:
=====
2015-07-20T17:21:32+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b ..... .....
```

tttyaudit-ttyUSB0-20150720-171329.log

```

2015-07-20T17:21:32+0000 ttyUSB0 lastTamper bitmap: 0x0080 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2015-07-20T17:21:32+0000 ttyUSB0
=====
2015-07-20T17:21:32+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2015-07-20T17:21:32+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2015-07-20T17:21:32+0000 ttyUSB0 Board is P2020RDB
2015-07-20T17:21:32+0000 ttyUSB0 board_smp_init: 2 cpu
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=5000000000
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-07-20T17:21:32+0000 ttyUSB0 Starting next program at v0015183c
2015-07-20T17:21:32+0000 ttyUSB0 Starting K-Series Kernel
2015-07-20T17:21:32+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T17:21:32+0000 ttyUSB0 Mon Jul 20 17:15:59 2015
2015-07-20T17:21:32+0000 ttyUSB0 Starting auditd v2.0 ... started.
2015-07-20T17:21:32+0000 ttyUSB0 Interface 0 configured for IPv6.
2015-07-20T17:21:32+0000 ttyUSB0 Interface 0 configured for IPv4.
2015-07-20T17:21:32+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T17:21:32+0000 ttyUSB0 add net default: gateway ::: Network is unreachable
2015-07-20T17:21:32+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T17:21:32+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T17:21:32+0000 ttyUSB0 Starting USB driver...
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-07-20T17:21:32+0000 ttyUSB0
2015-07-20T17:21:32+0000 ttyUSB0

```

07/20/15  
16:41:49

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:21:38+0000 ttyUSB0
2015-07-20T17:21:38+0000 ttyUSB0 Running DES POST Test
2015-07-20T17:21:38+0000 ttyUSB0 DES POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running Triple DES POST Test
2015-07-20T17:21:38+0000 ttyUSB0 Triple DES POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running AES POST Test
2015-07-20T17:21:38+0000 ttyUSB0 AES POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running SHA1 POST Test
2015-07-20T17:21:38+0000 ttyUSB0 SHA1 POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running SHA2 POST Test
2015-07-20T17:21:38+0000 ttyUSB0 SHA2 POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running RandomGen POST Test
2015-07-20T17:21:38+0000 ttyUSB0 RandomGen POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running RSA POST Test
2015-07-20T17:21:38+0000 ttyUSB0 RSA POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running DSA POST Test
2015-07-20T17:21:38+0000 ttyUSB0 DSA POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Running ECC POST Test
2015-07-20T17:21:38+0000 ttyUSB0 ECC POST Test Passed
2015-07-20T17:21:38+0000 ttyUSB0 Audit on 20/7/2015 17:16:02 001000006
2015-07-20T17:21:38+0000 ttyUSB0
2015-07-20T17:21:38+0000 ttyUSB0
2015-07-20T17:21:38+0000 ttyUSB0
2015-07-20T17:21:38+0000 ttyUSB0
2015-07-20T17:21:38+0000 ttyUSB0 Keyper 9860-2 Serial Number H1403033
2015-07-20T17:21:38+0000 ttyUSB0
2015-07-20T17:21:38+0000 ttyUSB0 Memory Usage:
2015-07-20T17:21:38+0000 ttyUSB0 RAM (free/total) 197Mb/256Mb
2015-07-20T17:21:38+0000 ttyUSB0 Flash (free/total) 127Mb/128Mb
2015-07-20T17:21:38+0000 ttyUSB0 black store 44b
```

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 statistics 112b
2015-07-20T17:21:39+0000 ttyUSB0 other 116b
2015-07-20T17:21:39+0000 ttyUSB0 RedStore (free/total) 109Kb/128Kb
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Network Configuration:
2015-07-20T17:21:39+0000 ttyUSB0 IPv4: enabled
2015-07-20T17:21:39+0000 ttyUSB0 IPv6: enabled
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 MAC/IP address(es): 00:E0:06:C0:E2:40 / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b240/64
2015-07-20T17:21:39+0000 ttyUSB0 HSM Port: 05000
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Software Versions:
2015-07-20T17:21:39+0000 ttyUSB0 BBL 010 ABL 011 App 023
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 CPLD Version:
2015-07-20T17:21:39+0000 ttyUSB0 1.9
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 SCR Firmware Version:
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 OROS-R2.99-R1.20
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Audit on 20/7/2015 17:16:03 00100001
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Audit on 20/7/2015 17:19:12 00200062
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Audit on 20/7/2015 17:20:31 00200019 00400000C662156D
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Audit on 20/7/2015 17:22:01 00200023 00400000C662156D
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Audit on 20/7/2015 17:22:30 00200023 15400006AEB3296E
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0
2015-07-20T17:21:39+0000 ttyUSB0 Hmclistener: Created IPv4 socket 7 on port 3000.
2015-07-20T17:21:39+0000 ttyUSB0
```

ttyaudit-ttyUSB0-20150720-171329.log

```

2015-07-20T17:29:12+0000 ttyUSB0
2015-07-20T17:29:12+0000 ttyUSB0 HmcListener: Created IPv6 socket 9 on port 3000.
2015-07-20T17:29:12+0000 ttyUSB0
2015-07-20T17:29:12+0000 ttyUSB0 Audit on 20/7/2015 17:23:36 00100003
2015-07-20T17:29:12+0000 ttyUSB0
2015-07-20T17:29:12+0000 ttyUSB0 Shutting down daemons...
2015-07-20T17:29:12+0000 ttyUSB0
2015-07-20T17:29:12+0000 ttyUSB0 AuditBuffer rx'd [-1] (3)
2015-07-20T17:29:12+0000 ttyUSB0 shutting down audit service.
2015-07-20T17:29:12+0000 ttyUSB0
2015-07-20T17:29:12+0000 ttyUSB0 Terminated
2015-07-20T17:29:12+0000 ttyUSB0
2015-07-20T17:29:13+0000 ttyUSB0 HmcListener::accept(): No such process
2015-07-20T17:29:13+0000 ttyUSB0
2015-07-20T17:29:13+0000 ttyUSB0 Shutting down filesystems...
2015-07-20T17:29:14+0000 ttyUSB0
2015-07-20T17:29:14+0000 ttyUSB0 H1403033 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T17:29:14+0000 ttyUSB0
2015-07-20T17:29:14+0000 ttyUSB0 BBL CRC32: 0x757574CA
2015-07-20T17:29:14+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 Running applicationBootLoader at 0xEFD00000
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 H1403033 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 ABL CRC32: 0xE7E0FA6A
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 #####
2015-07-20T17:29:15+0000 ttyUSB0 ## ABL tamper records ###
2015-07-20T17:29:15+0000 ttyUSB0 #####
2015-07-20T17:29:15+0000 ttyUSB0 Current Tamper Counts (decimal 0-255):
2015-07-20T17:29:15+0000 ttyUSB0 =====
2015-07-20T17:29:15+0000 ttyUSB0 vextoostamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 vintoostamperCount: 40
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 vbboosTamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 maxstrtempTamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 minstrtempTamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 meshTamperCount: 0

```

07/20/15  
18:41:49

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:29:15+0000 ttyUSB0 extLampSMKTamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 extLampIMKTamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 tempdiffTamperCount: 0
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 pfTamperCount: 40
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 restartTamperCount: 128
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 Current tamper bitmaps:
2015-07-20T17:29:15+0000 =====
2015-07-20T17:29:15+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b ..... 1.... 1.... |EXT_POWER_DOWN
2015-07-20T17:29:15+0000 ttyUSB0 lastTamper bitmap: 0x0080 0b ..... 1.... 1.... |EXT_POWER_DOWN
2015-07-20T17:29:15+0000 ttyUSB0
2015-07-20T17:29:15+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2015-07-20T17:29:15+0000 =====
2015-07-20T17:29:15+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2015-07-20T17:29:16+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2015-07-20T17:29:16+0000 ttyUSB0 Board is P2020RDB
2015-07-20T17:29:16+0000 ttyUSB0 board_smp_init: 2 cpu
2015-07-20T17:29:16+0000 ttyUSB0
2015-07-20T17:29:16+0000 ttyUSB0 Cpu_clk=100000000, Sys_clk=100000000, CCB=500000000
2015-07-20T17:29:17+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-07-20T17:29:17+0000 ttyUSB0 Starting next program at v0015183c
2015-07-20T17:29:17+0000 ttyUSB0
2015-07-20T17:29:17+0000 ttyUSB0 Starting K-Series Kernel
2015-07-20T17:29:17+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T17:29:17+0000 ttyUSB0 Mon Jul 20 17:23:42 2015
2015-07-20T17:29:17+0000 ttyUSB0 Starting auditd v2.0 ... started.
2015-07-20T17:29:17+0000 ttyUSB0
```

07/20/15  
18:41:49

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:29:18+0000 ttyUSB0 Interface 0 configured for IPv6.
2015-07-20T17:29:18+0000 ttyUSB0
2015-07-20T17:29:18+0000 ttyUSB0 Interface 0 configured for IPv4.
2015-07-20T17:29:18+0000 ttyUSB0
2015-07-20T17:29:18+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T17:29:19+0000 ttyUSB0
2015-07-20T17:29:19+0000 ttyUSB0 add net default: gateway :: Network is unreachable
2015-07-20T17:29:19+0000 ttyUSB0
2015-07-20T17:29:19+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T17:29:19+0000 ttyUSB0
2015-07-20T17:29:19+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T17:29:19+0000 ttyUSB0
2015-07-20T17:29:19+0000 ttyUSB0 Starting USB driver...
2015-07-20T17:29:19+0000 ttyUSB0
2015-07-20T17:29:19+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Running DES POST Test
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 DES POST Test Passed
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Running Triple DES POST Test
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Triple DES POST Test Passed
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Running AES POST Test
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 AES POST Test Passed
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Running SHA1 POST Test
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 SHA1 POST Test Passed
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Running SHA2 POST Test
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 SHA2 POST Test Passed
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 Running RandomGen POST Test
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:20+0000 ttyUSB0 RandomGen POST Test Passed
2015-07-20T17:29:20+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 Running RSA POST Test
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 RSA POST Test Passed
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 Running DSA POST Test
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 DSA POST Test Passed
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 Running ECC POST Test
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 ECC POST Test Passed
```

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 Keyper 9860-2 Serial Number H1403033
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 Memory Usage:
2015-07-20T17:29:21+0000 ttyUSB0 RAM (free/total) 197Mb/256Mb
2015-07-20T17:29:21+0000 ttyUSB0 Flash (free/total) 127Mb/128Mb
2015-07-20T17:29:21+0000 ttyUSB0 black store 192b
2015-07-20T17:29:21+0000 ttyUSB0 statistics 112b
2015-07-20T17:29:21+0000 ttyUSB0 other 116b
2015-07-20T17:29:21+0000 ttyUSB0 RedStore (free/total) 109Kb/128Kb
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 Network Configuration:
2015-07-20T17:29:21+0000 ttyUSB0 IPv4: enabled
2015-07-20T17:29:21+0000 ttyUSB0 IPv6: enabled
2015-07-20T17:29:21+0000 ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B2:40 / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b240/64
2015-07-20T17:29:21+0000 ttyUSB0 HSM Port: 05000
2015-07-20T17:29:21+0000 ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 Software Versions:
2015-07-20T17:29:21+0000 ttyUSB0 BBL 010 ABL 011 App 023
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 CPLD Version:
2015-07-20T17:29:21+0000 ttyUSB0 1.9
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 SCR Firmware Version:
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0 OROS-R2.99-R1.20
2015-07-20T17:29:21+0000 ttyUSB0
```



07/20/15  
18:41:49

9

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:21+0000 ttyUSB0
2015-07-20T17:29:22+0000 ttyUSB0
2015-07-20T17:29:22+0000 ttyUSB0
2015-07-20T17:29:22+0000 HmcListener: Created IPv4 socket 7 on port 3000.
2015-07-20T17:29:22+0000 ttyUSB0
2015-07-20T17:29:22+0000 ttyUSB0
2015-07-20T17:29:22+0000 HmcListener: Created IPv6 socket 8 on port 3000.
2015-07-20T17:29:22+0000 ttyUSB0
2015-07-20T17:29:22+0000 Audit on 20/7/2015 17:23:46 00100003
2015-07-20T17:29:22+0000 ttyUSB0
2015-07-20T17:30:33+0000 Audit on 20/7/2015 17:24:58 00200023 15400006E4F3296E
2015-07-20T17:30:33+0000 ttyUSB0
2015-07-20T17:30:42+0000 Audit on 20/7/2015 17:25:06 00200024
2015-07-20T17:30:42+0000 ttyUSB0
2015-07-20T17:31:06+0000 Audit on 20/7/2015 17:25:30 00200023 15400006AEB3296E
2015-07-20T17:31:06+0000 ttyUSB0
2015-07-20T17:33:25+0000 Audit on 20/7/2015 17:27:47 00200077 00400000E962156D
2015-07-20T17:33:25+0000 ttyUSB0
2015-07-20T17:36:01+0000 Audit on 20/7/2015 17:30:25 00200063 00400000ECE2156D
2015-07-20T17:36:01+0000 ttyUSB0
2015-07-20T17:38:07+0000 Audit on 20/7/2015 17:32:31 00200010 00400000E922156D
2015-07-20T17:38:07+0000 ttyUSB0
2015-07-20T17:39:24+0000 Audit on 20/7/2015 17:33:48 0020006c
2015-07-20T17:39:24+0000 ttyUSB0
2015-07-20T17:39:46+0000 Audit on 20/7/2015 17:34:11 0020006b 00400000E8E2156D
2015-07-20T17:39:46+0000 ttyUSB0
2015-07-20T17:40:09+0000 Audit on 20/7/2015 17:34:33 0020006b 00400000E962156D
2015-07-20T17:40:09+0000 ttyUSB0
2015-07-20T17:40:38+0000 Audit on 20/7/2015 17:35:02 00200039
2015-07-20T17:40:38+0000 ttyUSB0
2015-07-20T17:40:51+0000 Audit on 20/7/2015 17:35:15 0020003b
2015-07-20T17:40:51+0000 ttyUSB0
2015-07-20T17:41:05+0000 Audit on 20/7/2015 17:35:29 00200041
2015-07-20T17:41:05+0000 ttyUSB0
2015-07-20T17:41:58+0000 HSM Status
2015-07-20T17:41:58+0000 =====
2015-07-20T17:41:58+0000 Keyper 9860-2
2015-07-20T17:41:58+0000 Serial Number H1403033
2015-07-20T17:41:58+0000 Date(dd/mm/yyyy) 20/7/2015 Time 17:36:22
2015-07-20T17:41:58+0000 ttyUSB0
2015-07-20T17:41:58+0000 Software Versions:
2015-07-20T17:41:58+0000 BBL 010 ABL 011 App 023
2015-07-20T17:41:58+0000
```



ttyaudit-ttyUSB0-20150720-171329.log

```

2015-07-20T17:41:58+0000 ttyUSB0 address: 00:e0:06:c0:b2:40
2015-07-20T17:41:58+0000 ttyUSB0 media: Ethernet none
2015-07-20T17:41:58+0000 ttyUSB0 inet 192.168.0.2 netmask 0xfffff00 broadcast 192.168.0.255
2015-07-20T17:41:58+0000 ttyUSB0 inet6 2001::2e0:6ff:fec0:b240 prefixlen 64
2015-07-20T17:41:58+0000 ttyUSB0 inet6 fe80::2e0:6ff:fec0:b240H\037\220@ec0 prefixlen 64 scopeid 0x2

Current HSM State: Secured Off-line

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

Other Modes:
AES SMK FIPS Mode
Battery ok

#####
## ABL tamper records ##
#####

Current Tamper Counts (decimal 0-255):
=====
vextoosTamperCount: 0
vintoosTamperCount: 0
vbboosTamperCount: 0

```

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T17:41:58+0000 ttyUSB0 maxstrtempTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 minstrtempTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 meshTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 extampSMKTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 extampIMKTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 tempdiffTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 pfTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 restartTamperCount: 0
2015-07-20T17:41:58+0000 ttyUSB0 Current tamper bitmaps:
=====
2015-07-20T17:41:58+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b ..... ..... .....
2015-07-20T17:41:58+0000 ttyUSB0 lastTamper bitmap: 0x0000 0b ..... ..... .....
2015-07-20T17:41:58+0000 ttyUSB0 Bitmapped Change Record (most recent first):
=====
2015-07-20T17:41:58+0000 ttyUSB0 DRBG Instantiate Health Test On Demand Passed
2015-07-20T17:41:58+0000 ttyUSB0 DRBG Generate Health Test On Demand Passed
2015-07-20T17:41:58+0000 ttyUSB0 DRBG Reseed Health Test On Demand Passed
2015-07-20T17:41:58+0000 ttyUSB0 Audit on 20/7/2015 18:15:13 0020006b 00400000E962156D
2015-07-20T17:41:58+0000 ttyUSB0 Audit on 20/7/2015 18:15:35 0020006b 00400000ED62156D
2015-07-20T17:41:58+0000 ttyUSB0 Audit on 20/7/2015 18:16:22 00200025 00400000EAA2156D
2015-07-20T17:41:58+0000 ttyUSB0 Audit on 20/7/2015 18:16:38 00200025 00400000EAA62156D
2015-07-20T17:41:58+0000 ttyUSB0 Audit on 20/7/2015 18:16:39 00200005
2015-07-20T17:41:58+0000 ttyUSB0 Audit on 20/7/2015 18:17:57 00200016 Kkwwtts
```



ttysaudit-ttyUSB0-20150720-171329.log

```

2015-07-20T18:28:36+0000 ttyUSB0 vbboosTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 maxstrtempTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 minstrtempTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 meshTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 extampSMKTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 extampIMKTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 tempdiffTamperCount: 0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 pfTamperCount: 40
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 restartTamperCount: 130
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 Current tamper bitmaps:
2015-07-20T18:28:36+0000
2015-07-20T18:28:36+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b ..... ..... .....
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 lastTamper bitmap: 0x0080 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0
2015-07-20T18:28:36+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2015-07-20T18:28:36+0000
2015-07-20T18:28:36+0000
2015-07-20T18:28:36+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2015-07-20T18:28:37+0000 ttyUSB0
2015-07-20T18:28:37+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2015-07-20T18:28:37+0000 ttyUSB0
2015-07-20T18:28:37+0000 ttyUSB0 Board is P2020RDB
2015-07-20T18:28:37+0000 ttyUSB0
2015-07-20T18:28:37+0000 ttyUSB0 board_smp_init: 2 cpu
2015-07-20T18:28:37+0000 ttyUSB0
2015-07-20T18:28:37+0000 ttyUSB0
2015-07-20T18:28:37+0000 ttyUSB0 Cpu_clk=100000000, Sys_clk=100000000, CCB=500000000
2015-07-20T18:28:37+0000 ttyUSB0
2015-07-20T18:28:38+0000 ttyUSB0
2015-07-20T18:28:38+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-07-20T18:28:38+0000 ttyUSB0
2015-07-20T18:28:38+0000 ttyUSB0 Starting next program at v0015183c
2015-07-20T18:28:38+0000 ttyUSB0
2015-07-20T18:28:38+0000

```

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T18:28:38+0000 ttyUSB0 Starting K-Series Kernel
2015-07-20T18:28:38+0000 ttyUSB0
2015-07-20T18:28:38+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T18:28:38+0000 ttyUSB0
2015-07-20T18:28:38+0000 ttyUSB0 Mon Jul 20 18:23:03 2015
2015-07-20T18:28:38+0000 ttyUSB0
2015-07-20T18:28:38+0000 ttyUSB0 Starting auditd v2.0 ... started.
2015-07-20T18:28:39+0000 ttyUSB0
2015-07-20T18:28:39+0000 ttyUSB0 Interface 0 configured for IPv6.
2015-07-20T18:28:39+0000 ttyUSB0
2015-07-20T18:28:39+0000 ttyUSB0 Interface 0 configured for IPv4.
2015-07-20T18:28:40+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T18:28:40+0000 ttyUSB0 add net default: gateway :: Network is unreachable
2015-07-20T18:28:40+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T18:28:40+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T18:28:40+0000 ttyUSB0 Starting USB driver...
2015-07-20T18:28:40+0000 ttyUSB0
2015-07-20T18:28:40+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-07-20T18:28:40+0000 ttyUSB0
2015-07-20T18:28:40+0000 ttyUSB0
2015-07-20T18:28:42+0000 ttyUSB0 Running DES POST Test
2015-07-20T18:28:42+0000 ttyUSB0 DES POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running Triple DES POST Test
2015-07-20T18:28:42+0000 ttyUSB0 Triple DES POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running AES POST Test
2015-07-20T18:28:42+0000 ttyUSB0 AES POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running SHA1 POST Test
2015-07-20T18:28:42+0000 ttyUSB0 SHA1 POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running SHA2 POST Test
2015-07-20T18:28:42+0000 ttyUSB0 SHA2 POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running RandomGen POST Test
2015-07-20T18:28:42+0000 ttyUSB0 RandomGen POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running RSA POST Test
2015-07-20T18:28:42+0000 ttyUSB0 RSA POST Test Passed
```

ttyaudit-ttyUSB0-20150720-171329.log

```

2015-07-20T18:28:42+0000 ttyUSB0 Running DSA POST Test
2015-07-20T18:28:42+0000 ttyUSB0 DSA POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Running ECC POST Test
2015-07-20T18:28:42+0000 ttyUSB0 ECC POST Test Passed
2015-07-20T18:28:42+0000 ttyUSB0 Audit on 20/7/2015 18:23:06 00100008
2015-07-20T18:28:42+0000 ttyUSB0
2015-07-20T18:28:42+0000 ttyUSB0
2015-07-20T18:28:42+0000 ttyUSB0
2015-07-20T18:28:42+0000 ttyUSB0
2015-07-20T18:28:42+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 Keyper 9860-2 Serial Number H1403033
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 Memory Usage:
2015-07-20T18:28:43+0000 ttyUSB0 RAM (free/total) 197Mb/256Mb
2015-07-20T18:28:43+0000 ttyUSB0 Flash (free/total) 127Mb/128Mb
2015-07-20T18:28:43+0000 ttyUSB0 black store 400b
2015-07-20T18:28:43+0000 ttyUSB0 statistics 112b
2015-07-20T18:28:43+0000 ttyUSB0 other 116b
2015-07-20T18:28:43+0000 ttyUSB0 RedStore (free/total) 109Kb/128Kb
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 Network Configuration:
2015-07-20T18:28:43+0000 ttyUSB0 IPv4: enabled
2015-07-20T18:28:43+0000 ttyUSB0 IPv6: enabled
2015-07-20T18:28:43+0000 ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B2:40 / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b240/64
2015-07-20T18:28:43+0000 ttyUSB0 HSM Port: 05000
2015-07-20T18:28:43+0000 ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 Software Versions:
2015-07-20T18:28:43+0000 ttyUSB0 BBL 010 ABL 011 App 023
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0

```



ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T18:28:43+0000 ttyUSB0 CPLD Version:
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 1.9
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 SCR Firmware Version:
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 OROS-R2.99-R1.20
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 Audit on 20/7/2015 18:23:07 001000003
2015-07-20T18:28:43+0000 ttyUSB0
2015-07-20T18:28:43+0000 ttyUSB0 Audit on 20/7/2015 18:24:40 002000023 00400000C662156D
2015-07-20T18:30:16+0000 ttyUSB0
2015-07-20T18:30:16+0000 ttyUSB0 Audit on 20/7/2015 18:24:51 002000024
2015-07-20T18:30:27+0000 ttyUSB0
2015-07-20T18:30:27+0000 ttyUSB0 Audit on 20/7/2015 18:25:20 002000023 154000006AEB3296E
2015-07-20T18:30:56+0000 ttyUSB0
2015-07-20T18:31:15+0000 ttyUSB0 Audit on 20/7/2015 18:25:39 00200001f
2015-07-20T18:31:24+0000 ttyUSB0
2015-07-20T18:31:24+0000 ttyUSB0 Shutting down daemons...
2015-07-20T18:31:24+0000 ttyUSB0
2015-07-20T18:31:24+0000 ttyUSB0 AuditBuffer rx'd [-] (3)
2015-07-20T18:31:24+0000 ttyUSB0
2015-07-20T18:31:24+0000 ttyUSB0 shutting down audit service.
2015-07-20T18:31:24+0000 ttyUSB0
2015-07-20T18:31:24+0000 ttyUSB0 HmcListener::accept(): No such process
2015-07-20T18:31:24+0000 ttyUSB0
2015-07-20T18:31:24+0000 ttyUSB0 Shutting down filesystems...
2015-07-20T18:31:25+0000 ttyUSB0
2015-07-20T18:31:26+0000 ttyUSB0
2015-07-20T18:31:26+0000 ttyUSB0
2015-07-20T18:31:26+0000 ttyUSB0
2015-07-20T18:31:26+0000 ttyUSB0 HI403033 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T18:31:26+0000 ttyUSB0 BEL CRC32: 0x757574CA
2015-07-20T18:31:26+0000 ttyUSB0
2015-07-20T18:31:26+0000 ttyUSB0 Running applicationBootLoader at 0xEEDC0000
2015-07-20T18:31:27+0000 ttyUSB0
2015-07-20T18:31:27+0000 ttyUSB0
2015-07-20T18:31:27+0000 ttyUSB0
2015-07-20T18:31:27+0000 ttyUSB0 HI403033 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T18:31:27+0000 ttyUSB0 ABL CRC32: 0xE7E0FA6A
2015-07-20T18:31:27+0000 ttyUSB0
2015-07-20T18:31:27+0000 ttyUSB0
```



```

2015-07-20T18:31:28+0000 ttyUSB0 Board is P2020RDB
2015-07-20T18:31:28+0000 ttyUSB0
2015-07-20T18:31:28+0000 ttyUSB0 board_smp_init: 2 cpu
2015-07-20T18:31:28+0000 ttyUSB0
2015-07-20T18:31:28+0000 ttyUSB0
2015-07-20T18:31:28+0000 ttyUSB0
2015-07-20T18:31:28+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=5000000000
2015-07-20T18:31:28+0000 ttyUSB0
2015-07-20T18:31:29+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-07-20T18:31:29+0000 ttyUSB0 Starting next program at v0015183c
2015-07-20T18:31:29+0000 ttyUSB0 Starting K-Series Kernel
2015-07-20T18:31:29+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T18:31:29+0000 ttyUSB0 Mon Jul 20 18:25:54 2015
2015-07-20T18:31:29+0000 ttyUSB0 Starting auditd v2.0 ... started.
2015-07-20T18:31:29+0000 ttyUSB0 Interface 0 configured for IPv6.
2015-07-20T18:31:30+0000 ttyUSB0 Interface 0 configured for IPv4.
2015-07-20T18:31:30+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T18:31:31+0000 ttyUSB0 add net default: gateway :: Network is unreachable
2015-07-20T18:31:31+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2015-07-20T18:31:31+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T18:31:31+0000 ttyUSB0 Starting USB driver...
2015-07-20T18:31:31+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-07-20T18:31:31+0000 ttyUSB0
2015-07-20T18:31:31+0000 ttyUSB0
2015-07-20T18:31:31+0000 ttyUSB0
2015-07-20T18:31:31+0000 ttyUSB0
2015-07-20T18:31:31+0000 ttyUSB0 Running DES POST Test
2015-07-20T18:31:33+0000 ttyUSB0 DES POST Test Passed
2015-07-20T18:31:33+0000 ttyUSB0
2015-07-20T18:31:33+0000 ttyUSB0 Running Triple DES POST Test
2015-07-20T18:31:33+0000 ttyUSB0 Triple DES POST Test Passed
2015-07-20T18:31:33+0000 ttyUSB0
2015-07-20T18:31:33+0000 ttyUSB0 Running AES POST Test
2015-07-20T18:31:33+0000 ttyUSB0 AES POST Test Passed
2015-07-20T18:31:33+0000 ttyUSB0
2015-07-20T18:31:33+0000 ttyUSB0 Running SHA1 POST Test

```



07/20/15  
18:41:49

ttyaudit-ttyUSB0-20150720-171329.log

```
2015-07-20T18:31:34+0000 ttyUSB0 HSM Port: 05000
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0 Software Versions:
2015-07-20T18:31:34+0000 ttyUSB0 BBL 010 ABL 011 App 023
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0 CPLD Version:
2015-07-20T18:31:34+0000 ttyUSB0 1.9
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0 SCR Firmware Version:
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0 OROS-R2.99-R1.20
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0
2015-07-20T18:31:34+0000 ttyUSB0 Audit on 20/7/2015 18:25:58 00100001
2015-07-20T18:31:34+0000 ttyUSB0
```

07/2015  
18:36:39

1

ttyaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T17:50:27+0000 ttyUSB1 y
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T17:50:27+0000 ttyUSB1 BBL CRC32: 0x757574CA
2015-07-20T17:50:27+0000 ttyUSB1 Running applicationBootLoader at 0xEFFDC0000
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T17:50:27+0000 ttyUSB1 ABL CRC32: 0xE7E0FA6A
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ## ABL tamper records ##
2015-07-20T17:50:27+0000 ## ABL tamper records ##
2015-07-20T17:50:27+0000 ## ABL tamper records ##
2015-07-20T17:50:27+0000 ## ABL tamper records ##
2015-07-20T17:50:27+0000 Current Tamper Counts (decimal 0-255):
2015-07-20T17:50:27+0000 =====
2015-07-20T17:50:27+0000 vextoosTamperCount: 0
2015-07-20T17:50:27+0000 vintoosTamperCount: 6
2015-07-20T17:50:27+0000 vbboosTamperCount: 0
2015-07-20T17:50:27+0000 maxstrtempTamperCount: 0
2015-07-20T17:50:27+0000 minstrtempTamperCount: 0
2015-07-20T17:50:27+0000 meshTamperCount: 0
2015-07-20T17:50:27+0000 extampSMKTamperCount: 0
2015-07-20T17:50:27+0000 extampIMKTamperCount: 0
2015-07-20T17:50:27+0000 tempdiffTamperCount: 0
2015-07-20T17:50:27+0000 pfTamperCount: 6
2015-07-20T17:50:27+0000 restartTamperCount: 17
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 Current tamper bitmaps:
2015-07-20T17:50:27+0000 =====
2015-07-20T17:50:27+0000 currentTamper bitmap: 0x0000 0b ..... .....
```

ttysd-usb1-20150720-171329.log

```
2015-07-20T17:50:27+0000 ttyUSB1 lastTamper bitmap: 0x0080 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1
2015-07-20T17:50:27+0000 ttyUSB1 Bitmapped Change Record (most recent first):
2015-07-20T17:50:27+0000 =====
2015-07-20T17:50:27+0000 ttyUSB1 Running cryptoApplication at 0xEBF00000
2015-07-20T17:50:27+0000 ttyUSB1 Jumping to startup @ 0x001037B4
2015-07-20T17:50:27+0000 ttyUSB1 Board is P2020RDB
2015-07-20T17:50:28+0000 ttyUSB1 board_smp_init: 2 cpu
2015-07-20T17:50:28+0000 ttyUSB1
2015-07-20T17:50:28+0000 ttyUSB1 Cpu_clk=100000000, Sys_clk=100000000, CCB=500000000
2015-07-20T17:50:29+0000 ttyUSB1 System page at phys:000b000 user:0000b000 kern:0000b000
2015-07-20T17:50:29+0000 ttyUSB1 Starting next program at v0015183c
2015-07-20T17:50:29+0000 ttyUSB1 Starting K-Series Kernel
2015-07-20T17:50:29+0000 ttyUSB1 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T17:50:29+0000 ttyUSB1 Mon Jul 20 17:44:46 2015
2015-07-20T17:50:29+0000 ttyUSB1 Starting auditd v2.0 ... started.
2015-07-20T17:50:30+0000 ttyUSB1 Interface 0 configured for IPv6.
2015-07-20T17:50:30+0000 ttyUSB1 Interface 0 configured for IPv4.
2015-07-20T17:50:30+0000 ttyUSB1 route: writing to routing socket: Network is unreachable
2015-07-20T17:50:31+0000 ttyUSB1 add net default: gateway :: Network is unreachable
2015-07-20T17:50:31+0000 ttyUSB1 route: writing to routing socket: Network is unreachable
2015-07-20T17:50:31+0000 ttyUSB1 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T17:50:31+0000 ttyUSB1 Starting USB driver...
2015-07-20T17:50:31+0000 ttyUSB1 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-07-20T17:50:31+0000 ttyUSB1
2015-07-20T17:50:31+0000 ttyUSB1
```

ttysaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T17:50:33+0000 ttyUSB1
2015-07-20T17:50:33+0000 ttyUSB1 Running DES POST Test
2015-07-20T17:50:33+0000 ttyUSB1 DES POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running Triple DES POST Test
2015-07-20T17:50:33+0000 ttyUSB1 Triple DES POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running AES POST Test
2015-07-20T17:50:33+0000 ttyUSB1 AES POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running SHA1 POST Test
2015-07-20T17:50:33+0000 ttyUSB1 SHA1 POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running SHA2 POST Test
2015-07-20T17:50:33+0000 ttyUSB1 SHA2 POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running RandomGen POST Test
2015-07-20T17:50:33+0000 ttyUSB1 RandomGen POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running RSA POST Test
2015-07-20T17:50:33+0000 ttyUSB1 RSA POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running DSA POST Test
2015-07-20T17:50:33+0000 ttyUSB1 DSA POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Running ECC POST Test
2015-07-20T17:50:33+0000 ttyUSB1 ECC POST Test Passed
2015-07-20T17:50:33+0000 ttyUSB1 Audit on 20/7/2015 17:44:49 00100008
2015-07-20T17:50:33+0000 ttyUSB1
2015-07-20T17:50:33+0000 ttyUSB1 KeyPer 9860-2 Serial Number H1411006
2015-07-20T17:50:33+0000 ttyUSB1
2015-07-20T17:50:33+0000 ttyUSB1 Memory Usage:
2015-07-20T17:50:33+0000 ttyUSB1 RAM (free/total) 197Mb/256Mb
2015-07-20T17:50:33+0000 ttyUSB1 Flash (free/total) 127Mb/128Mb
2015-07-20T17:50:33+0000 ttyUSB1 black store 44b
```





ttyaudit-ttyUSB1-20150720-171329.log

```

2015-07-20T17:55:29+0000 ttyUSB1 HmcListener: Created IPv4 socket 7 on port 3000.
2015-07-20T17:55:29+0000 ttyUSB1
2015-07-20T17:55:29+0000 ttyUSB1
2015-07-20T17:55:29+0000 ttyUSB1 HmcListener: Created IPv6 socket 9 on port 3000.
2015-07-20T17:55:29+0000 ttyUSB1
2015-07-20T17:55:29+0000 ttyUSB1 Audit on 20/7/2015 17:49:45 001000003
2015-07-20T17:55:29+0000 ttyUSB1 Shutting down daemons...
2015-07-20T17:55:29+0000 ttyUSB1 AuditBuffer rx'd [-i] (3)
2015-07-20T17:55:29+0000 ttyUSB1 shutting down audit service.
2015-07-20T17:55:29+0000 ttyUSB1
2015-07-20T17:55:29+0000 ttyUSB1 HmcListener::accept(): No such process
2015-07-20T17:55:29+0000 ttyUSB1 Shutting down filesystems...
2015-07-20T17:55:31+0000 ttyUSB1
2015-07-20T17:55:31+0000 ttyUSB1 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T17:55:31+0000 ttyUSB1 BBL CRC32: 0x757574CA
2015-07-20T17:55:31+0000 ttyUSB1 Running applicationBootloader at 0xEFFDC0000
2015-07-20T17:55:31+0000 ttyUSB1
2015-07-20T17:55:31+0000 ttyUSB1 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T17:55:31+0000 ttyUSB1 ABL CRC32: 0xE7E0FA6A
2015-07-20T17:55:32+0000 ttyUSB1 #####
2015-07-20T17:55:32+0000 ttyUSB1 #####
2015-07-20T17:55:32+0000 ttyUSB1 ##### ABL tamper records  ###
2015-07-20T17:55:32+0000 ttyUSB1 #####
2015-07-20T17:55:32+0000 ttyUSB1 Current Tamper Counts (decimal 0-255):
2015-07-20T17:55:32+0000 =====
2015-07-20T17:55:32+0000 ttyUSB1 vextoolsTamperCount:    0
2015-07-20T17:55:32+0000 ttyUSB1 vintoolsTamperCount:    6
2015-07-20T17:55:32+0000 ttyUSB1 vbbootsTamperCount:     0
2015-07-20T17:55:32+0000 ttyUSB1 maxstrTempTamperCount:   0
2015-07-20T17:55:32+0000 ttyUSB1 minstTempTamperCount:   0
2015-07-20T17:55:32+0000 ttyUSB1 meshTamperCount:        0

```

ttysuidit-ttyUSB1-20150720-171329.log

```

2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 extampSMKTamperCount: 0
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 extampIMKTamperCount: 0
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 tempdiffTamperCount: 0
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 pftamperCount: 6
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 restartTamperCount: 17
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 Current tamper bitmaps:
2015-07-20T17:55:32+0000 =====
2015-07-20T17:55:32+0000 currentTamper bitmap: 0x0000 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 lastTamper bitmap: 0x0080 0b ..... 1.... ..... |EXT_POWER_DOWN
2015-07-20T17:55:32+0000 ttyUSB1
2015-07-20T17:55:32+0000 Bitmapped Change Record (most recent first):
2015-07-20T17:55:32+0000 =====
2015-07-20T17:55:32+0000 Running cryptoApplication at 0xEBF00000
2015-07-20T17:55:33+0000 ttyUSB1
2015-07-20T17:55:33+0000 Jumping to startup @ 0x001037B4
2015-07-20T17:55:33+0000 ttyUSB1
2015-07-20T17:55:33+0000 Board is P2020RDB
2015-07-20T17:55:33+0000 ttyUSB1
2015-07-20T17:55:33+0000 board_smp_init: 2 cpu
2015-07-20T17:55:33+0000 ttyUSB1
2015-07-20T17:55:33+0000 Cpu_clk=100000000, Sys_clk=100000000, CCB=500000000
2015-07-20T17:55:34+0000 ttyUSB1
2015-07-20T17:55:34+0000 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-07-20T17:55:34+0000 ttyUSB1
2015-07-20T17:55:34+0000 Starting next program at v0015183c
2015-07-20T17:55:34+0000 ttyUSB1
2015-07-20T17:55:34+0000 Starting K-Series Kernel
2015-07-20T17:55:34+0000 ttyUSB1
2015-07-20T17:55:34+0000 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T17:55:34+0000 ttyUSB1
2015-07-20T17:55:34+0000 Mon Jul 20 17:49:51 2015
2015-07-20T17:55:34+0000 ttyUSB1
2015-07-20T17:55:34+0000 Starting audiid v2.0 ... started.
2015-07-20T17:55:34+0000 ttyUSB1

```

07/20/15  
18:36:39

7

ttysd-20150720-171329.log

```
2015-07-20T17:55:34+0000 ttyUSB1 Interface 0 configured for IPv6.
2015-07-20T17:55:34+0000 ttyUSB1 Interface 0 configured for IPv4.
2015-07-20T17:55:35+0000 ttyUSB1 route: writing to routing socket: Network is unreachable
2015-07-20T17:55:35+0000 ttyUSB1 add net default: gateway :: Network is unreachable
2015-07-20T17:55:35+0000 ttyUSB1 route: writing to routing socket: Network is unreachable
2015-07-20T17:55:35+0000 ttyUSB1 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T17:55:35+0000 ttyUSB1 Starting USB driver...
2015-07-20T17:55:36+0000 ttyUSB1 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2015-07-20T17:55:36+0000 ttyUSB1
2015-07-20T17:55:36+0000 ttyUSB1
2015-07-20T17:55:37+0000 ttyUSB1 Running DES POST Test
2015-07-20T17:55:37+0000 ttyUSB1 DES POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running Triple DES POST Test
2015-07-20T17:55:37+0000 ttyUSB1 Triple DES POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running AES POST Test
2015-07-20T17:55:37+0000 ttyUSB1 AES POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running SHA1 POST Test
2015-07-20T17:55:37+0000 ttyUSB1 SHA1 POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running SHA2 POST Test
2015-07-20T17:55:37+0000 ttyUSB1 SHA2 POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running RandomGen POST Test
2015-07-20T17:55:37+0000 ttyUSB1 RandomGen POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running RSA POST Test
2015-07-20T17:55:37+0000 ttyUSB1 RSA POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running DSA POST Test
2015-07-20T17:55:37+0000 ttyUSB1 DSA POST Test Passed
2015-07-20T17:55:37+0000 ttyUSB1 Running ECC POST Test
2015-07-20T17:55:37+0000 ttyUSB1 ECC POST Test Passed
```



07/20/15  
18:36:39

ttyaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T17:55:38+0000 ttyUSB1
2015-07-20T17:55:38+0000 ttyUSB1
2015-07-20T17:55:41+0000 ttyUSB1
2015-07-20T17:55:41+0000 ttyUSB1
2015-07-20T17:55:41+0000 HmcListener: Created IPv4 socket 7 on port 3000.
2015-07-20T17:55:41+0000 ttyUSB1
2015-07-20T17:55:41+0000 ttyUSB1
2015-07-20T17:55:41+0000 HmcListener: Created IPv6 socket 8 on port 3000.
2015-07-20T17:55:41+0000 ttyUSB1
2015-07-20T17:55:41+0000 HmcListener: Created IPv6 socket 8 on port 3000.
2015-07-20T17:55:41+0000 ttyUSB1
2015-07-20T17:55:41+0000 Audit on 20/7/2015 17:49:55 00100003
2015-07-20T17:55:42+0000 ttyUSB1
2015-07-20T17:55:42+0000 Audit on 20/7/2015 17:50:55 0020006b 00400000ED62156D
2015-07-20T17:56:39+0000 ttyUSB1
2015-07-20T17:56:39+0000 Audit on 20/7/2015 17:51:16 0020006b 00400000E8E2156D
2015-07-20T17:57:00+0000 ttyUSB1
2015-07-20T17:57:00+0000 Audit on 20/7/2015 17:51:36 002000039
2015-07-20T17:57:20+0000 ttyUSB1
2015-07-20T17:57:20+0000 Audit on 20/7/2015 17:51:47 00200003b
2015-07-20T17:57:30+0000 ttyUSB1
2015-07-20T17:57:30+0000 Audit on 20/7/2015 17:52:01 00200041
2015-07-20T17:57:45+0000 ttyUSB1
2015-07-20T17:57:45+0000 HSM Status
2015-07-20T17:57:45+0000 =====
2015-07-20T17:58:23+0000 Keyper 9860-2
2015-07-20T17:58:23+0000 Serial Number H1411006
2015-07-20T17:58:23+0000 Date(dd/mm/yyyy) 20/7/2015 Time 17:52:40
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 Software Versions:
2015-07-20T17:58:23+0000 BBL 010 ABL 011 App 023
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 CPLD Version:
2015-07-20T17:58:23+0000 1.9
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 SCR Firmware Version:
2015-07-20T17:58:23+0000
```

07/20/15  
18:36:39

ttyaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 OROS-R2.99-R1.20
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 Memory Usage:
2015-07-20T17:58:23+0000 ttyUSB1 RAM (free/total) 197Mb/256Mb
2015-07-20T17:58:23+0000 ttyUSB1 Flash (free/total) 127Mb/128Mb
2015-07-20T17:58:23+0000 ttyUSB1 black store 328b
2015-07-20T17:58:23+0000 ttyUSB1 statistics 112b
2015-07-20T17:58:23+0000 ttyUSB1 other 116b
2015-07-20T17:58:23+0000 ttyUSB1 RedStore (free/total) 109Kb/128Kb
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 Network Configuration:
2015-07-20T17:58:23+0000 ttyUSB1 IPv4: enabled
2015-07-20T17:58:23+0000 ttyUSB1 IPv6: enabled
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 MAC/IP address(es): 00:E0:06:C0:E3:1B / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b31b/64
2015-07-20T17:58:23+0000 ttyUSB1 HSM Port: 05000
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 HSM Gateway(s): 0.0.0.0 ::
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2015-07-20T17:58:23+0000 ttyUSB1 capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2015-07-20T17:58:23+0000 ttyUSB1 capabilities tx=0
2015-07-20T17:58:23+0000 ttyUSB1 enabled=0
2015-07-20T17:58:23+0000 ttyUSB1 address: 00:e0:06:c0:b3:1b
2015-07-20T17:58:23+0000 ttyUSB1 media: Ethernet none
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 inet 192.168.0.2 netmask 0xfffff00 broadcast 192.168.0.255
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 inet6 2001::2e0:6ff:fec0:b31b prefixlen 64
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 inet6 fe80::2e0:6ff:fec0:b31bH\037\220@ec0 prefixlen 64 scopeid 0x2
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
```

ttyaudit-ttyUSB1-20150720-171329.log

```

2015-07-20T17:58:23+0000 ttyUSB1 Current HSM State: Secured Off-line
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1
2015-07-20T17:58:23+0000 ttyUSB1 Modes: (1=Enabled 0=Disabled)
2015-07-20T17:58:23+0000 ttyUSB1 Global Key Export 1 App Key Import 0 App Key Export 0 Asymmetric Key Gen 1
2015-07-20T17:58:23+0000 ttyUSB1 Symmetric Key Gen 1 Symmetric Key Derive 0 Signing 1 Signature Verify 1
2015-07-20T17:58:23+0000 ttyUSB1 MAC Generation 1 MAC Verification 1 Encrypt / Decrypt 1 Delete Asym Key 1
2015-07-20T17:58:23+0000 ttyUSB1 Delete Sym Key 1 Output Key Details 1 Output Key Summary 1 Suite B Algorithms 1
2015-07-20T17:58:23+0000 ttyUSB1 Non Suite B Aligs 1 Auto Online 0
2015-07-20T17:58:23+0000 ttyUSB1 Other Modes:
2015-07-20T17:58:23+0000 ttyUSB1 AES SMK FIPS Mode
2015-07-20T17:58:23+0000 ttyUSB1 Battery ok
2015-07-20T17:58:23+0000 ttyUSB1 #####
2015-07-20T17:58:23+0000 ttyUSB1 ## ABL tamper records ###
2015-07-20T17:58:23+0000 ttyUSB1 #####
2015-07-20T17:58:23+0000 ttyUSB1 Current Tamper Counts (decimal 0-255):
=====
2015-07-20T17:58:23+0000 ttyUSB1 vextoosTamperCount: 0
2015-07-20T17:58:23+0000 ttyUSB1 vintoosTamperCount: 0
2015-07-20T17:58:23+0000 ttyUSB1 vbboosTamperCount: 0
2015-07-20T17:58:23+0000 ttyUSB1 maxstrtempTamperCount: 0
2015-07-20T17:58:23+0000 ttyUSB1 minstrtempTamperCount: 0
2015-07-20T17:58:23+0000 ttyUSB1 meshTamperCount: 0
2015-07-20T17:58:24+0000 ttyUSB1 extampSMKTamperCount: 0
2015-07-20T17:58:24+0000 ttyUSB1 extampIMKTamperCount: 0
2015-07-20T17:58:24+0000 ttyUSB1 tempdiffTamperCount: 0
2015-07-20T17:58:24+0000 ttyUSB1 pfTamperCount: 0

```



```
2015-07-20T17:58:24+0000 ttyUSB1 restartTampersCount: 0
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1 Current tamper bitmaps:
2015-07-20T17:58:24+0000 ttyUSB1 =====
2015-07-20T17:58:24+0000 ttyUSB1 currentTampers bitmap: 0x0000 0b .....
2015-07-20T17:58:24+0000 ttyUSB1 LastTampers bitmap: 0x0000 0b .....
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1 Bitmapped Change Record (most recent first):
2015-07-20T17:58:24+0000 ttyUSB1 =====
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1
2015-07-20T17:58:24+0000 ttyUSB1 DRBG Instantiate Health Test On Demand Passed
2015-07-20T17:58:24+0000 ttyUSB1 DRBG Generate Health Test On Demand Passed
2015-07-20T17:58:24+0000 ttyUSB1 DRBG Reseed Health Test On Demand Passed
2015-07-20T17:58:24+0000 ttyUSB1 Audit on 20/7/2015 17:54:59 0020001c
2015-07-20T18:00:43+0000 ttyUSB1 Audit on 20/7/2015 17:56:18 0020002d 00400000E9A2156D
2015-07-20T18:02:01+0000 ttyUSB1 Audit on 20/7/2015 17:57:00 0020002d 00400000EA62156D
2015-07-20T18:02:01+0000 ttyUSB1 Audit on 20/7/2015 17:57:48 0020002d 00400000EAE2156D
2015-07-20T18:02:44+0000 ttyUSB1 Audit on 20/7/2015 17:58:28 0020002d 00400000EAA2156D
2015-07-20T18:03:32+0000 ttyUSB1 Audit on 20/7/2015 17:59:45 00200007
2015-07-20T18:05:28+0000 ttyUSB1 Audit on 20/7/2015 18:01:04 00200069 00400000ECE2156D
2015-07-20T18:06:47+0000 ttyUSB1 Audit on 20/7/2015 18:01:24 00200069 0890004AB3F3296D
2015-07-20T18:06:47+0000 ttyUSB1
2015-07-20T18:07:08+0000 ttyUSB1
2015-07-20T18:07:08+0000 ttyUSB1 TcpListener: Created IPv4 socket 11 on port 5000.
2015-07-20T18:07:10+0000 ttyUSB1
2015-07-20T18:07:10+0000 ttyUSB1 TcpListener: Created IPv6 socket 16 on port 5000.
2015-07-20T18:07:10+0000 ttyUSB1
2015-07-20T18:07:10+0000 ttyUSB1 Audit on 20/7/2015 18:01:27 00100002
2015-07-20T18:07:10+0000 ttyUSB1
```

ttyaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T18:10:11+0000 ttyUSB1
2015-07-20T18:10:11+0000 ttyUSB1
2015-07-20T18:10:11+0000 TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2015-07-20T18:10:11+0000 ttyUSB1
2015-07-20T18:10:11+0000 ttyUSB1
2015-07-20T18:10:11+0000 ttyUSB1
2015-07-20T18:10:11+0000 CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2015-07-20T18:10:11+0000 ttyUSB1
2015-07-20T18:11:19+0000 ttyUSB1
2015-07-20T18:11:19+0000 TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2015-07-20T18:11:19+0000 ttyUSB1
2015-07-20T18:11:24+0000 ttyUSB1
2015-07-20T18:11:24+0000 TcpListener: Closing connection on socket 17 from address 192.168.0.1.
2015-07-20T18:11:24+0000 ttyUSB1
2015-07-20T18:15:50+0000 ttyUSB1
2015-07-20T18:15:50+0000 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T18:15:50+0000 ttyUSB1 BBL CRC32: 0x757574CA
2015-07-20T18:15:50+0000 ttyUSB1 Running applicationBootLoader at 0xEFFDC0000
2015-07-20T18:15:50+0000 ttyUSB1
2015-07-20T18:15:50+0000 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T18:15:50+0000 ttyUSB1 ABL CRC32: 0xE7E0FA6A
2015-07-20T18:15:50+0000 ttyUSB1
2015-07-20T18:15:50+0000 #####
2015-07-20T18:15:50+0000 ## ABL tamper records ##
2015-07-20T18:15:50+0000 #####
2015-07-20T18:15:50+0000 Current Tamper Counts (decimal 0-255):
=====
2015-07-20T18:15:50+0000 vextoosTamperCount: 0
2015-07-20T18:15:50+0000 vintoosTamperCount: 6
2015-07-20T18:15:50+0000 vbboosTamperCount: 0
2015-07-20T18:15:50+0000 maxstrtempTamperCount: 0
2015-07-20T18:15:50+0000 minstrtempTamperCount: 0
2015-07-20T18:15:50+0000 meshTamperCount: 0
2015-07-20T18:15:50+0000 extampSMKTamperCount: 0
```

```
2015-07-20T18:15:50+0000 ttyUSB1 extampIMKTamperCount: 0
2015-07-20T18:15:50+0000 ttyUSB1 tempdifftamperCount: 0
2015-07-20T18:15:50+0000 ttyUSB1 pftamperCount: 6
2015-07-20T18:15:50+0000 ttyUSB1 restarttamperCount: 19
2015-07-20T18:15:50+0000 ttyUSB1 Current tamper bitmaps:
=====
2015-07-20T18:15:50+0000 ttyUSB1 currenttamper bitmap: 0x0000 0b .....
2015-07-20T18:15:50+0000 ttyUSB1 lasttamper bitmap: 0x0080 0b ..... 1... .. |EXT_POWER_DOWN
2015-07-20T18:15:50+0000 ttyUSB1 Bitmapped Change Record (most recent first):
=====
2015-07-20T18:15:50+0000 ttyUSB1 Running cryptoApplication at 0xEBF00000
2015-07-20T18:15:51+0000 ttyUSB1 Jumping to startup @ 0x001037B4
2015-07-20T18:15:51+0000 ttyUSB1 Board is P2020RDB
2015-07-20T18:15:51+0000 ttyUSB1 board_smp_init: 2 cpu
2015-07-20T18:15:51+0000 ttyUSB1 Cpu_clk=100000000, Sys_clk=100000000, CCB=500000000
2015-07-20T18:15:52+0000 ttyUSB1 System page at phys:000b0000 user:0000b000 kern:0000b000
2015-07-20T18:15:52+0000 ttyUSB1 Starting next program at v0015183c
2015-07-20T18:15:52+0000 ttyUSB1 Starting K-Series Kernel
2015-07-20T18:15:52+0000 ttyUSB1 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T18:15:52+0000 ttyUSB1 Mon Jul 20 18:10:09 2015
2015-07-20T18:15:52+0000 ttyUSB1 Starting auditd v2.0 ... started.
2015-07-20T18:15:53+0000 ttyUSB1 Interface 0 configured for IPv6.
```

ttyaudit-ttyUSB1-20150720-171329.log

2015-07-20T18:15:53+0000 ttyUSB1 Interface 0 configured for IPv4.  
2015-07-20T18:15:53+0000 ttyUSB1  
2015-07-20T18:15:54+0000 ttyUSB1 route: writing to routing socket: Network is unreachable  
2015-07-20T18:15:54+0000 ttyUSB1  
2015-07-20T18:15:54+0000 ttyUSB1 add net default: gateway ::: Network is unreachable  
2015-07-20T18:15:54+0000 ttyUSB1  
2015-07-20T18:15:54+0000 ttyUSB1 route: writing to routing socket: Network is unreachable  
2015-07-20T18:15:54+0000 ttyUSB1  
2015-07-20T18:15:54+0000 ttyUSB1 add net default: gateway 0.0.0.0: Network is unreachable  
2015-07-20T18:15:54+0000 ttyUSB1 Starting USB driver...  
2015-07-20T18:15:54+0000 ttyUSB1 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33  
2015-07-20T18:15:54+0000 ttyUSB1  
2015-07-20T18:15:54+0000 ttyUSB1  
2015-07-20T18:15:54+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running DES POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 DES POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running Triple DES POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Triple DES POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running AES POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 AES POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running SHA1 POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 SHA1 POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running SHA2 POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 SHA2 POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running RandomGen POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 RandomGen POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running RSA POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 RSA POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running DSA POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 DSA POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Running ECC POST Test  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 ECC POST Test Passed  
2015-07-20T18:15:56+0000 ttyUSB1  
2015-07-20T18:15:56+0000 ttyUSB1 Audit on 20/7/2015 18:10:12 00100008

ttyaudit-ttyUSB1-20150720-171329.log

2015-07-20T18:15:56+0000 ttyUSB1  
 2015-07-20T18:15:56+0000 ttyUSB1  
 2015-07-20T18:15:56+0000 ttyUSB1  
 2015-07-20T18:15:56+0000 ttyUSB1  
 2015-07-20T18:15:56+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1 Keyper 9860-2 Serial Number H1411006  
 2015-07-20T18:15:57+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1 Memory Usage:  
 2015-07-20T18:15:57+0000 ttyUSB1 RAM (free/total) 197Mb/256Mb  
 2015-07-20T18:15:57+0000 ttyUSB1 Flash (free/total) 127Mb/128Mb  
 2015-07-20T18:15:57+0000 ttyUSB1 black store 400b  
 2015-07-20T18:15:57+0000 ttyUSB1 statistics 112b  
 2015-07-20T18:15:57+0000 ttyUSB1 other 116b  
 2015-07-20T18:15:57+0000 ttyUSB1 RedStore (free/total) 109Kb/128Kb  
 2015-07-20T18:15:57+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1 Network Configuration:  
 2015-07-20T18:15:57+0000 ttyUSB1 IPv4: enabled  
 2015-07-20T18:15:57+0000 ttyUSB1 IPv6: enabled  
 2015-07-20T18:15:57+0000 ttyUSB1 MAC/IP address(es): 00:E0:06:C0:B3:1B / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b31b/64  
 2015-07-20T18:15:57+0000 ttyUSB1 HSM Port: 05000  
 2015-07-20T18:15:57+0000 ttyUSB1 HSM Gateway(s): 0.0.0.0 ::  
 2015-07-20T18:15:57+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1 Software Versions:  
 2015-07-20T18:15:57+0000 ttyUSB1 BBL 010 ABL 011 App 023  
 2015-07-20T18:15:57+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1 CPLD Version:  
 2015-07-20T18:15:57+0000 ttyUSB1 1.9  
 2015-07-20T18:15:57+0000 ttyUSB1  
 2015-07-20T18:15:57+0000 ttyUSB1 SCR Firmware Version:  
 2015-07-20T18:15:57+0000 ttyUSB1 OROS-R2.99-R1.20  
 2015-07-20T18:15:57+0000 ttyUSB1

```
2015-07-20T18:15:57+0000 ttyUSB1
2015-07-20T18:15:57+0000 ttyUSB1
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 HmcListener: Created IPv4 socket 10 on port 3000.
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 HmcListener: Created IPv6 socket 11 on port 3000.
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:10:13 00100003
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:11:13 0020006b 00400000E8E2156D
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:11:35 0020006b 00400000E962156D
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:12:50 0020002e 00400000EA22156D
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:12:56 00200013 00400000EA22156D
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:28:02 00200023 15400006AEB3296E
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:28:23 00200023 00400000C662156D
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Audit on 20/7/2015 18:28:41 0020001f
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Shutting down daemons...
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 AuditBuffer rx'd [-1] (3)
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 shutting down audit service.
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Terminated
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 HmcListener::accept(): No such process
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Shutting down filesystems...
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 BBL CRC32: 0x757574CA
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 Running applicationBootLoader at 0xEFFDC000
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 ABL CRC32: 0xE7E0FA6A
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 ttyUSB1
2015-07-20T18:16:00+0000 #####
2015-07-20T18:16:00+0000 #####
2015-07-20T18:16:00+0000 #####
2015-07-20T18:16:00+0000 #####
```



ttyaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T18:34:31+0000 ttyUSB1 board_smp_init: 2 cpu
2015-07-20T18:34:31+0000 ttyUSB1
2015-07-20T18:34:31+0000 ttyUSB1
2015-07-20T18:34:31+0000 ttyUSB1 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=5000000000
2015-07-20T18:34:31+0000 ttyUSB1
2015-07-20T18:34:32+0000 ttyUSB1 System page at phys:0000b000 user:0000b000 kern:0000b000
2015-07-20T18:34:32+0000 ttyUSB1 Starting next program at v0015183c
2015-07-20T18:34:32+0000 ttyUSB1 Starting K-Series Kernel
2015-07-20T18:34:32+0000 ttyUSB1 Copyright AEP Networks Ltd. All Rights Reserved.
2015-07-20T18:34:32+0000 ttyUSB1 Mon Jul 20 18:28:49 2015
2015-07-20T18:34:32+0000 ttyUSB1 Starting auditd v2.0 ... started.
2015-07-20T18:34:32+0000 ttyUSB1 Interface 0 configured for IPv6.
2015-07-20T18:34:33+0000 ttyUSB1 Interface 0 configured for IPv4.
2015-07-20T18:34:33+0000 ttyUSB1
2015-07-20T18:34:34+0000 ttyUSB1 route: writing to routing socket: Network is unreachable
2015-07-20T18:34:34+0000 ttyUSB1 add net default: gateway :: Network is unreachable
2015-07-20T18:34:34+0000 ttyUSB1 route: writing to routing socket: Network is unreachable
2015-07-20T18:34:34+0000 ttyUSB1 add net default: gateway 0.0.0.0: Network is unreachable
2015-07-20T18:34:34+0000 ttyUSB1 Starting USB driver...
2015-07-20T18:34:34+0000 ttyUSB1
2015-07-20T18:34:34+0000 ttyUSB1 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2015-07-20T18:34:34+0000 ttyUSB1
2015-07-20T18:34:34+0000 ttyUSB1
2015-07-20T18:34:34+0000 ttyUSB1
2015-07-20T18:34:34+0000 ttyUSB1 Running DES POST Test
2015-07-20T18:34:36+0000 ttyUSB1 DES POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running Triple DES POST Test
2015-07-20T18:34:36+0000 ttyUSB1 Triple DES POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running AES POST Test
2015-07-20T18:34:36+0000 ttyUSB1 AES POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running SHA1 POST Test
2015-07-20T18:34:36+0000 ttyUSB1 SHA1 POST Test Passed
```



ttyaudit-ttyUSB1-20150720-171329.log

```
2015-07-20T18:34:36+0000 ttyUSB1 Running SHA2 POST Test
2015-07-20T18:34:36+0000 ttyUSB1 SHA2 POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running RandomGen POST Test
2015-07-20T18:34:36+0000 ttyUSB1 RandomGen POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running RSA POST Test
2015-07-20T18:34:36+0000 ttyUSB1 RSA POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running DSA POST Test
2015-07-20T18:34:36+0000 ttyUSB1 DSA POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1 Running ECC POST Test
2015-07-20T18:34:36+0000 ttyUSB1 ECC POST Test Passed
2015-07-20T18:34:36+0000 ttyUSB1
2015-07-20T18:34:36+0000 ttyUSB1
2015-07-20T18:34:36+0000 ttyUSB1 Memory Usage:
2015-07-20T18:34:37+0000 ttyUSB1 RAM (free/total) 197Mb/256Mb
2015-07-20T18:34:37+0000 ttyUSB1 Flash (free/total) 127Mb/128Mb
2015-07-20T18:34:37+0000 ttyUSB1 black store 44b
2015-07-20T18:34:37+0000 ttyUSB1 statistics 112b
2015-07-20T18:34:37+0000 ttyUSB1 other 116b
2015-07-20T18:34:37+0000 ttyUSB1 RedStore (free/total) 109Kb/128Kb
2015-07-20T18:34:37+0000 ttyUSB1
2015-07-20T18:34:37+0000 ttyUSB1 Network Configuration:
2015-07-20T18:34:37+0000 ttyUSB1 IPv4: enabled
2015-07-20T18:34:37+0000 ttyUSB1 IPv6: enabled
2015-07-20T18:34:37+0000 ttyUSB1 MAC/IP address(es): 00:E0:06:C0:B3:1B / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b31b/64
2015-07-20T18:34:37+0000 ttyUSB1 HSM Port: 05000
2015-07-20T18:34:37+0000 ttyUSB1
```



**Turns Off the Laptop**

Step	Activity	Initials	Time
20.	CA unmounts HSMFD by executing cd /tmp then umount /media/HSMFD CA removes HSMFD.	AP	18:55
21.	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	AP	18:55

**Distribute HSMFDs**

Step	Activity	Initials	Time
22.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 1 for IKOS) to review, analyze and improve on procedures.	AP	18:56

**Placement of HSMs to Safe #1**

Step	Activity	Initials	Time
23.	CA, IW1, SSC1 open safe room and enter with equipment cart.	AP	18:58
24.	SSC1 opens Safe #1 shielding combination from camera.	AP	18:59
25.	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.	AP	19:00
26.	CA records placement of HSM3 in next entry field of safe log with TEB # and HSM3 serial #, printed name, date, time, and signature. CA CAREFULLY places the HSM3 into Safe #1 and IW1 initials the entry. HSM3: TEB# BB24646668 ✓ serial # H1403033 ✓	AP	19:02
27.	CA records placement of HSM4 in next entry field of safe log with TEB # and HSM4 serial #, printed name, date, time, and signature. CA CAREFULLY places the HSM4 into Safe #1 and IW1 initials the entry. HSM4: TEB# BB24646667 ✓ serial # H1411006 ✓	AP	19:03
28.	CA records placement of HSM3 and HSM4 Physical Keys in next entry field of safe log with TEB #, printed name, date, time, and signature. CA places the HSM3 and HSM4 Physical Keys into Safe #1 and IW1 initials the entry. HSM3 Physical Key: TEB# BB21907221 ✓ HSM4 Physical Key: TEB# BB21907222 ✓	AP	19:05

**Close Equipment Safe #1**

Step	Activity	Initials	Time
29.	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry. <i>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</i>	AP	19:05
30.	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.	AP	19:06
31.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	AP	19:07

**Participant Signing of IW1's Script**

Step	Activity	Initials	Time
32.	One by one, all participants come to the front of the room, confirms printed name and date. <b>Then, the participant declares that this script is a true and accurate record of the ceremony by signing on IW1's script coversheet.</b> IW records the completion time once all participants have signed the coversheet. <i>Note: If entry is pre-printed, verify the entry and sign.</i>	AP	19:08
33.	CA reviews IW1's script and signs it.	AP	19:10

**Filming Stops**

Step	Activity	Initials	Time
34.	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.	AP	19:11

**Copying and Storing the Script**

Step	Activity	Initials	Time
35.	IW1 makes at least 2 copies of his/her script: one for off-site audit bundle, one for IKOS and copies for other participants, as requested. Audit bundles each contain 1) Output of signer system – HSMFD 2) Copy of IW1's ceremony script 3) Audio-visual recording 4) Logs from the Physical Access Control and Intrusion Detection System (Range is 01/22/2015 – 07/20/2015) 5) The IW attestation (A.1 below) 6) SA attestation (A.2, A.3 below) All in a TEB labeled "HSM Acceptance Testing", 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.	AP	20:58

**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.

**Andres Pavez**



---

**Date: 20 July 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 **22 January 2015 00:00 UTC** to now.

**Connor Barthold**



---

**Date: 20 July 2015**

```
## Last commit: 2014-12-12 18:55:44 UTC by cbarthold
version 12.1X44-D35.5;
system {
    host-name srx;
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "#####"; ##
SECRET-DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "#####";
                ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "#####";
                ## SECRET-DATA
            }
        }
        user reed {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
```



```

        encrypted-password "#####";
## SECRET-DATA
    }
}
services;
syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    file messages {
        any critical;
        authorization info;
    }
    file interactive-commands {
        interactive-commands error;
    }
}
max-configurations-on-flash 5;
max-configuration-rollback 20;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
ntp {
    server 129.6.15.28;
    server 129.6.15.29;
}
}
interfaces {
    interface-range interfaces-trust {
        member ge-0/0/1;
        member fe-0/0/2;
        member fe-0/0/3;
        member fe-0/0/4;
        member fe-0/0/5;
        member fe-0/0/6;
        member fe-0/0/7;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
}
ge-0/0/0 {
    unit 0 {

```

```

        family inet {
            address 10.100.1.1/24;
        }
    }
}
ge-1/0/0 {
    unit 0 {
        family inet {
            address 192.0.35.202/26;
        }
    }
}
vlan {
    unit 0 {
        family inet {
            address 10.4.28.1/24;
        }
    }
}
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.0.35.201;
    }
}
security {
    nat {
        source {
            rule-set trust-to-untrust {
                from zone trust;
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
        rule-set wifi-to-untrust {
            from zone wifi;
            to zone untrust;
            rule source-nat-rule2 {
                match {
                    source-address 0.0.0.0/0;
                }
                then {

```

```
source-nat {
    interface;
}
}
}
}
}
}
policies {
    from-zone trust to-zone untrust {
        policy trust-to-untrust {
            match {
                source-address localnet;
                destination-address [ icann simplex1 simplex2
googledns1 googledns2 ];
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
    }
    from-zone wifi to-zone untrust {
        policy internet {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone trust {
        address-book {
            address localnet 10.4.28.0/24;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
    }
}
```

```
    }
    interfaces {
        vlan.0;
    }
}
security-zone untrust {
    address-book {
        address icann 192.0.32.0/20;
        address simplex1 216.224.218.31/32;
        address simplex2 216.224.219.32/32;
        address googledns1 8.8.8.8/32;
        address googledns2 8.8.4.4/32;
    }
    interfaces {
        ge-1/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone wifi {
    interfaces {
        ge-0/0/0.0;
    }
}
}
}
vlangs {
    vlan-trust {
        vlan-id 3;
        l3-interface vlan.0;
    }
}
}
```