Root DNSSEC KSK Ceremony 27

Thursday October 27, 2016

Root Zone KSK Operator Key Management Facility
18155 Technology Drive, Culpeper, VA 22701-3805

This ceremony is executed under the
DNSSEC Practice Statement for the Root Zone KSK Operator Version 4th Edition (2016-10-01)

Abbreviations

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

Participants

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

Title	Printed Name	Signature	Date	Time
CA	Kim Davies / PTI		2016/10/27	22:00
IW1	Patrick Jones / ICANN			
SSC1	James Cole / ICANN			
SSC2	Joe Catapano / ICANN			
CO1	Frederico Neves / BR			
CO3	Olaf Kolkman / NL			
CO4	Robert Seastrom / US			
CO5	Christopher Griffiths / US			
CO7	Alain Aina / TG			
RZM	Alejandro Bolivar / Verisign			
RZM	Andrew Kim / Verisign			
RZM	John Painumkal / Verisign			
AUD	Eugene Jeong / PricewaterhouseCoopers			
AUD	Richard Stark / PricewaterhouseCoopers			
SA1	Connor Barthold / ICANN			
SA2	Reed Quinn / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Richard Lamb / ICANN			
SW	Edward Lewis / ICANN			
SW	Matt Larson / ICANN			
SW	Derek Ellison / ICANN			
EW	Joseph Abley			

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

Note: Dual Occupancy is enforced. CA leads the ceremony. Only CAs, IWs, or SAs can enter the 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 inside the safe room. Participants must sign in and out of the ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before the completion of the ceremony. The SA starts filming before the participants enter the room.

Some steps during the ceremony require the participants to tell and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the phonetic alphabet shown below will be used:

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

Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.	PA	17:02
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.	PA	1704

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	PA	1704
4.	CA explains the use of personal electronics devices during ceremony.	PA	1705
5.	CA briefly explains the purpose of the ceremony.	PA	1707

Verify Time and Date

Step	Activity	Initials	Time
6.	IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2016/10/27 1707:39 All entries into this script or any logs should follow this common source of time.	PA	17:07

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.	PA	17:09
8.	SSC2, while shielding combination from camera, opens Safe #2.	PA	17:10
9.	SSC2 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC2. SSC2 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in the safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PA	17:11

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	One by one, the selected CO retrieves the required OP cards and SO cards following the steps shown below. a) With the assistance of CA (and his/her common key), opens her/his safe deposit box. **Note: Common Key is the bottom lock and CO Key is the top lock** b) Retains OP TEB and SO TEB then locks the safe deposit box. c) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below. d) Makes an entry in the safe log indicating OP TEB and SO TEB removal with box #, printed name, date, time and signature. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** Repeat these steps until all required cards are removed. IW1 initials this entry when all COs have finished.		
	CO 1: Frederico Neves ✓ **Box # 1238** ✓ **OP TEB # BB46584314 (Retain)** ✓ **SO TEB # BB21820443 (Retain)** ✓	PJ	17:14
	CO 3: Olaf Kolkman **Box # 1239** ✓ **OP TEB # BB46584302 (Retain)** ✓ **SO TEB # BB21907253 (Retain)** ✓	PJ	17:16
	CO 4: Robert Seastrom **Box # 1260** ✓ **OP TEB # BB46584303 (Retain)** ✓ **SO TEB # BB21907203 (Retain)** ✓	PJ	17:18
	CO 5: Christopher Griffiths **Box # 1240** ✓ **OP TEB # BB46584541 (Retain)** ✓ **SO TEB # BB21907206 (Retain)** ✓	PJ	17:20
	CO 7: Alain Aina **Box # 1242** ✓ **OP TEB # BB46584319 (Retain)** ✓ **SO TEB # BB21907212 (Retain)** ✓	PJ	17:22

Close Credential Safe #2

Step	Activity	Initials	Time
11.	Once all relevant deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PS	1724
12.	SSC2 puts log in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	PS	17:24
13.	IW1, CA, SSC2, and Cos leave safe room, with OP cards and SO cards (if applicable) in TEBs, closing the door behind them.	PS	17:25

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	PS	1726
15.	SSC1, while shielding combination from camera, opens Safe #1.	PS	1727
16.	SSC1 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in the safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PS	1727

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	**CA CAREFULLY removes HSM1, HSM2, HSM3 and HSM4 (in TEB)** from the safe and completes the entry on the safe log indicating HSMs Removal, TEB # and serial number, printed name, date, time, and signature. CA then places the items on the equipment cart. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** **HSM1: TEB# BB24706804 / serial # K6002016** **HSM2: TEB# BB24646744 / serial # K6002013** **HSM3: TEB# BB24646616 / serial # H1403032** **HSM4: TEB# BB24646658 / serial # H1411011**	PD	1730
18.	CA takes out the items listed below from the safe and completes the entry on the safe log indicating each item, TEB#, serial number if available. Printed name, date, time and signature. CA then places the items on the equipment cart. IW1 initials each entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** **Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997** **O/S DVD (release 20160503) + HSMFD: TEB# BB46584299** Verify the integrity of the other Laptop that will not be used this time and return it to the safe. **Laptop1 (Dell ATG6400): TEB# BB24646657 / serial # 41593712005**	PD	1732

Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	SSC1 makes an entry including printed name, date, time and signature on the safe log indicating, "Close safe". IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PD	17:33
20.	SSC1 puts log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	PD	17:34
21.	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.	PD	17:34

Act 2. OS/DVD Acceptance Test, Confirm and Sign the Key Signing Requests

OS/DVD Acceptance Test

Step	Activity	Initials	Time
1.	CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. **Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997**	PB	1737
2.	CA inspects the O/S DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. **O/S DVD (release 20160503) + HSMFD: TEB# BB46584299**	PB	17:38
3.	CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on the key ceremony table; discards TEBs; connects laptop power, external display, general purpose external DVD drive and boots laptop from **O/S DVD (release 20160503).**	PB	~~17:41~~ 17:43
4.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes `system-config-display --noui` c) CA executes `killall Xorg` d) CA confirms that external display works. e) CA logs in as root	PB	17:45
5.	CA opens a terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal** Follow the additional steps to maximize the terminal window: a) Click the **View** menu and select **Zoom** In b) Repeat the step above as necessary	PB	1746

Step	Activity	Initials	Time

6.	CA inserts the new O/S DVD **release 20161014** into the external DVD drive, waits for it to be recognized by the O/S and performs the following:
	a) Close the file system popup window
	b) Confirm the assigned drive letter by executing
	`df`
	c) Unmount the DVD drive by executing
	`umount /dev/scd1`
	d) Calculate the SHA256 hash by executing
	`sha256sum /dev/scd1`
	`SHA256 hash for release 20161014:`
	991f7be8cfbc3b4bdb6f5e5f84092486755a08a3c36712e37a26ccd808631692
	IW1 and participants confirm that the result matches the above, which also matches the one published on:
	https://data.iana.org/ksk-ceremony/27/KC-20161014.iso.sha256
		PJ
		
		PJ
			1747
			
			1750 1754

7.	CA removes the O/S DVD by pressing the eject button on the external DVD drive and places it on the ceremony table visible from the audit camera and the participants.	PJ	1751
8.	CA repeats step 6 and 7 for the 2nd copy of the new O/S DVD **release 20161014**.	PJ	17:54
9.	IW1 records the date, time then affixes his/her signature upon successful completion of the O/S DVD release 20161014 acceptance testing: **O/S DVD Acceptance Test release 20161014** **Printed Name** **Patrick Jones** **Date** **2016/10/27** **Time** 17:55.18 **Signature** Patrick Jones	PJ	17:55
10.	CA disconnects the general purpose external DVD drive from the laptop, then removes the O/S DVD by performing: a) Turn off the laptop by pressing the power switch b) Turn on the laptop by pressing the power switch and immediately remove the old O/S DVD **(release 20160503)** from the laptop DVD drive c) Disconnect the laptop power to power off the laptop	PJ	17:57
11.	CA discards all the old O/S DVD **(release 20160503)** copies.	PJ	17:58

Set Up Laptop

Step	Activity	Initials	Time
12.	CA connects the laptop power, printer and boots the laptop using the new **O/S DVD release 20161014**.	PS	1803
13.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes `system-config-display --noui` c) CA executes `killall Xorg` d) CA confirms that external display works. e) CA logs in as root	PS	1804
14.	CA confirms that the printer is connected then configures printer as default and prints test page by going to **System > Administration > Printing** And follow the steps below: a) Click the **New Printer** icon (left side), leave everything default and then click the button **Forward** b) Under "Select Connection" choose the first device "**HP Laserjet xxxx**" and then click the button **Forward** (Note: The xxxx is the Printer Model) c) Select **HP** and click the button **Forward** d) Under "Models" scroll up and select **"Laserjet"**, and then click the button **Forward** e) Click the button **Apply** to finish f) Under "Local Printers" from the left menu, select "**printer**" g) Click the button **"Make Default Printer**" and "**Print Test Page"** h) Close the printer setup windows	PS	1806
15.	CA opens a terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal** Follow the additional steps to maximize the terminal window: c) Click the **View** menu and select **Zoom In** d) Repeat the step above as necessary	PS	1807
16.	CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal windows, CA executes: `cp /usr/share/zoneinfo/UTC /etc/localtime` When "`cp: overwrite `/etc/localtime'?`" is displayed, type "`y`" and press enter. then `date -s "20161027 HH:MM:00"` where **HH** is two-digit Hour, **MM** is two digit Minutes and **00** is Zero Seconds CA executes `date` using the Terminal window to confirm the date is properly configured.	PS	1808

Root DNSSEC Script Exception

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

Instructions: Initial each step that has been completed below. Note time.

Note Exception Time

Step	Activity	Initials	Time
1.	IW1 notes date and time of key ceremony exception and signs here: 2016/10/27 18:17.42	PJ	18:17.42
2.	IW1 Describes exception and action below.		

Steps 17-23. Issue identified with HSMFD - NJB Flash Drives were not preformatted so exact Commands could not be executed in order as written in Script. Instead the drives were formatted & then verified that they were formatted correctly.

PJ.

– End of Root DNSSEC Script Exception –

Format and label blank FD

Step	Activity	Initials	Time

17.	CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system popup window and formats the drive by executing
	`df`
	to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc),
	`umount /dev/sda1`
	to unmounts the drive (change drive letter and partition if necessary),
	`mkfs.vfat -n HSMFD -I /dev/sda1`
	to execute a FAT32 format and label it as HSMFD.
	CA unplugs the FD.
		PD	1814

18.	CA repeats step 17 for the 2nd blank FD	PD	1814
19.	CA repeats step 17 for the 3rd blank FD	PD	1814
20.	CA repeats step 17 for the 4th blank FD	PD	1815
21.	CA repeats step 17 for the 5th blank FD	PD	1816
22.	CA repeats step 17 for the 6th blank FD	PD	1814
23.	CA repeats step 17 for the 7th blank FD	PD	1817

note issue with HSMFD

03 was tried first

Connect HSMFD

Step	Activity	Initials	Time
24.	CA plugs the previous HSMFD used in the **ceremony 25** into the free USB slot on the laptop and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.	PD	1820.

25.	Calculate the sha256 hash of the contents on the copied HSMFD.
	`find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum`
	IW1 confirms that the result matches the sha256 hash of the HSMFD that is on the annotated script from the **Ceremony 25**.
	Previous hash should read as below (image from Ceremony 25 annotated script).
	`800faf1265dc41a79cfa35135118fd59edbdfc21b4b6ed887fb484166d3df629`
	Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash written on the ceremony script.
		PD	1822

Start Logging Terminal Session

Step	Activity	Initials	Time
26.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`	PJ	1822
27.	CA executes `script script-20161027.log` to start a capture of terminal output.	PJ	1822

Start Logging HSM Output

Step	Activity	Initials	Time
28.	CA connects a serial to USB null modem cable to laptop.	PJ	1823

29.	CA opens a second terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal.**
	Follow the additional steps to maximize the terminal window:
	a) Click the **View** menu and select **Zoom In**
	b) Repeat the step above as necessary
	and executes
	`cd /media/HSMFD`
	and executes
	`stty -F /dev/ttyUSB0 115200`
	`ttyaudit /dev/ttyUSB0`
	to start logging HSM serial port outputs. Note: **DO NOT** unplug USB serial port from laptop as this causes logging to stop.
		PJ	1824

Power Up HSM3

Step	Activity	Initials	Time
30.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. ✓ **HSM3: TEB# BB24646616 / serial # H1403032** ✓	PJ	1825
31.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	PJ	1826
32.	CA switches to the ttyaudit terminal window and connects power to HSM and switches the power ON. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) **HSM3: serial # H1403032** ✓ **Note: The HSM date and time was set from the factory and will not be used as a reference**	PJ	1827

Enable/Activate HSM3

Step	Activity	Initials	Time
33.	One by one, CA calls each COs listed below to inspect the TEB for tamper evidence, opens the TEB and hands the OP cards to the CA who then places the cards in cardholder visible to all. **CO 1: Frederico Neves** ✓ **OP TEB # BB46584314** **CO 3: Olaf Kolkman** ✓ **OP TEB # BB46584302** **CO 4: Robert Seastrom** ✓ **OP TEB # BB46584303** **CO 5: Christopher Griffiths** ✓ **OP TEB # BB46584541** **CO 7: Alain Aina** ✓ **OP TEB # BB46584319**	PJ PJ PJ PJ PJ	1828 1829 1830 1830 1831
34.	CA will perform the following steps to activate the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"1.Set Online"** hit **ENT** to confirm c) When **"Set Online?"** is displayed, hit **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When **"Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card Confirm the **"READY"** led on the **HSM** is **ON.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 7 of 7 2nd OP card 4 of 7 3rd OP card 5 of 7	PJ	1834

Check Network Connectivity Between Laptop and HSM3

Step	Activity	Initials	Time
35.	CA connects HSM to laptop using Ethernet cable in **LAN** port.	PS	1835
36.	CA switches to the terminal window and tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` and looking for responses. Ctrl-C to exit program.	PS	1835

Insert Copy of KSR to be signed

Step	Activity	Initials	Time
37.	The KSRs are downloaded to the KSRFDs and transferred to the facility by the RKOS. CA plugs FD labeled **"KSR"** with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA shows the KSR file contents by performing: a) Double click the ksr-root-2017-q1-0.xml file ✓ b) Select **DISPLAY** on the pop-up menu ✓ c) Maximize the window to show the contents ✓ Note: DO NOT save any changes on the file.	PS	1836
38.	CA closes the KSR contents window and the file system window.	PS	1837

Execute KSR signer

Step	Activity	Initials	Time
39.	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2017-q1-0.xml`	PS	1838
40.	The KSR signer will ask whether the HSM is activated or not as below. `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters "y" to proceed to verification. Note: DO NOT enter "y" for the "Is this correct y/n?" yet.	PS	1838

VERISIGN

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

VerisignInc.com

October 13th, 2016

To Whom It May Concern:

This is a letter of Verification of Employment for John G. Painumkal. Verisign, Inc. has employed John G. Painumkal full-time since May 5th, 2008, currently as a Sr. Engineer - CBO in our DNS Operations organization.

Verisign is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day our identity protection and registry services allow companies and consumers all over the world to engage in trusted communications and commerce.

For over 10 years, Verisign Internet Infrastructure has been at the very heart of the Internet, enabling key transactions and protecting valuable data. Verisign facilitates as many as 31 billion authoritative Domain Name System (DNS) queries a day, and has been providing this service since 1998 with 100% availability. Over the years the Verisign Internet Infrastructure has scaled quickly and dramatically, and has the capacity to scale just as dramatically in the coming years, as the world moves to Internet-based transactions. Verisign's Network Intelligence and Availability team helps protect against distributed denial of service or DDoS attacks through an in-the-cloud monitoring and mitigation services. Verisign's iDefense Security Intelligence Services help identify and track vulnerabilities, malicious code, threats, and helps provide comprehensive intelligence to enable customers to proactively manage risk.

Should you have further questions, please contact me at the number below.

Sincerely,

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

VERISIGN

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

Verisigninc.com

October 27, 2016

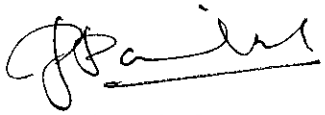
The SHA256 hash of the 2017 Q1 KSR file is:

1c470a168e72b56dcd8ba6bbc716783ae35ef8f42931e18e3c9e34e5df2c71a8

The PGP wordlist for the hash above is:

befriend determine allow bodyguard orca holiness scorecard hazardous spindle Medusa rematch publisher soybean bodyguard island corrosion tissue finicky Vulcan Virginia breakup company tempest microwave cobra onlooker choking travesty talon Chicago hamlet paramount

Attested on behalf of VeriSign by:



John G. Painumkal
Sr. Engineer
Cryptographic Business Operations
VeriSign, Inc.

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
41.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to identify him/herself, present identification document for IW1 to retain, then reads out the SHA256 hash in PGP wordlist format for the KSR previously sent to Root Zone KSK Operator. IW1 enters the RZM representative's name here: John G. Painumkal	PJ	1840
42.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?	PJ	1841
43.	CA then enters "`y`" in response to "`Is this correct y/n?`" to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in `/media/KSR/skr-root-2017-q1-0.xml`	PJ	1841

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

Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2010-q4-1.xml (at Mon Jul 12 22:44:26 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper Pro 0405
    Serial:          K6002018

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-07-01T00:00:00 2010-07-15T23:59:59 55138,41248  19036
2  2010-07-11T00:00:00 2010-07-25T23:59:59 41248         19036
3  2010-07-21T00:00:00 2010-08-04T23:59:59 41248         19036
4  2010-07-31T00:00:00 2010-08-14T23:59:59 41248         19036
5  2010-08-10T00:00:00 2010-08-24T23:59:59 41248         19036
6  2010-08-20T00:00:00 2010-09-03T23:59:59 41248         19036
7  2010-08-30T00:00:00 2010-09-13T23:59:59 41248         19036
8  2010-09-09T00:00:00 2010-09-24T00:00:00 41248         19036
9  2010-09-20T00:00:00 2010-10-05T23:59:59 40288,41248   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2010-q4-1.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59 40288,41248
2  2010-10-11T00:00:00 2010-10-25T23:59:59 40288
3  2010-10-21T00:00:00 2010-11-04T23:59:59 40288
4  2010-10-31T00:00:00 2010-11-14T23:59:59 40288
5  2010-11-10T00:00:00 2010-11-24T23:59:59 40288
6  2010-11-20T00:00:00 2010-12-04T23:59:59 40288
7  2010-11-30T00:00:00 2010-12-14T23:59:59 40288
8  2010-12-10T00:00:00 2010-12-25T00:00:00 40288
9  2010-12-21T00:00:00 2011-01-05T23:59:59 21639,40288
...PASSED.

SHA256 hash of KSR:
A17E539793B2611112C4F591A06AF4FBC2221DDDD71794BC72D5AEE910C72543
>> ratchet insurgent dwelling mosquito playhouse pioneer fallout Babylon atlas reproduce vapor miracle
ragtime hamburger upshot Wichita snapshot candidate Belfast tambourine stopwatch bookseller Pluto
pyramid highchair specialist robust ultimate assume retraction bombast decimal <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2010-q4-1.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59 40288,41248  19036
2  2010-10-11T00:00:00 2010-10-25T23:59:59 40288         19036
3  2010-10-21T00:00:00 2010-11-04T23:59:59 40288         19036
4  2010-10-31T00:00:00 2010-11-14T23:59:59 40288         19036
5  2010-11-10T00:00:00 2010-11-24T23:59:59 40288         19036
6  2010-11-20T00:00:00 2010-12-04T23:59:59 40288         19036
7  2010-11-30T00:00:00 2010-12-14T23:59:59 40288         19036
8  2010-12-10T00:00:00 2010-12-25T00:00:00 40288         19036
9  2010-12-21T00:00:00 2011-01-05T23:59:59 40288,21639   19036

SHA256 hash of SKR:
00CC341B7B3BAEE2E62B1AA6A58DEF07F02E4950E959E6A6ACBD7CEFF2741257
>> aardvark revolver choking bravado kickoff councilman robust tomorrow tracker Cherokee beehive
paragon reindeer microscope uncut amusement unearth coherence deckhand embezzle treadmill examine
tracker paragon ribcage quantity kiwi unravel uproot hydraulic atlas Eskimo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20100712-224426.log **********
```

Figure 1

```
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2017-q1-0.xml (at Thu Oct 27 18:38:03 2
016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2016-10-01T00:00:00 2016-10-15T23:59:59  46551,39291   19036
2  2016-10-11T00:00:00 2016-10-25T23:59:59  46551,39291   19036
3  2016-10-21T00:00:00 2016-11-04T23:59:59  46551,39291   19036
4  2016-10-31T00:00:00 2016-11-14T23:59:59  39291         19036
5  2016-11-10T00:00:00 2016-11-24T23:59:59  39291         19036
6  2016-11-20T00:00:00 2016-12-04T23:59:59  39291         19036
7  2016-11-30T00:00:00 2016-12-14T23:59:59  39291         19036
8  2016-12-10T00:00:00 2016-12-25T23:59:59  39291         19036
9  2016-12-21T00:00:00 2017-01-05T23:59:59  61045,39291   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2017-q1-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-01-01T00:00:00 2017-01-22T00:00:00  61045,39291
2  2017-01-11T00:00:00 2017-02-01T00:00:00  61045
3  2017-01-21T00:00:00 2017-02-11T00:00:00  61045
4  2017-01-31T00:00:00 2017-02-21T00:00:00  61045
5  2017-02-10T00:00:00 2017-03-03T00:00:00  61045
6  2017-02-20T00:00:00 2017-03-13T00:00:00  61045
7  2017-03-02T00:00:00 2017-03-23T00:00:00  61045
8  2017-03-12T00:00:00 2017-04-02T00:00:00  61045
9  2017-03-21T00:00:00 2017-04-11T00:00:00  61045,14796
...PASSED.

SHA256 hash of KSR:
1C470A168E72B56DCD8BA6BBC716783AE35EF8F42931E18E3C9E34E5DF2C71A8
>> befriend determine allow bodyguard orca holiness scorecard hazardous spindle Medusa
rematch publisher soybean bodyguard island corrosion tissue finicky Vulcan Virginia bre
akup company tempest microwave cobra onlooker choking travesty talon Chicago hamlet par
amount <<

Generated new SKR in /media/KSR/skr-root-2017-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-01-01T00:00:00 2017-01-22T00:00:00  61045,39291   19036
```

```
2  2017-01-11T00:00:00 2017-02-01T00:00:00  61045          19036
3  2017-01-21T00:00:00 2017-02-11T00:00:00  61045          19036
4  2017-01-31T00:00:00 2017-02-21T00:00:00  61045          19036
5  2017-02-10T00:00:00 2017-03-03T00:00:00  61045          19036
6  2017-02-20T00:00:00 2017-03-13T00:00:00  61045          19036
7  2017-03-02T00:00:00 2017-03-23T00:00:00  61045          19036
8  2017-03-12T00:00:00 2017-04-02T00:00:00  61045          19036
9  2017-03-21T00:00:00 2017-04-11T00:00:00  14796,61045    19036

SHA256 hash of SKR:
0475E10C848902105B2B06580F6990D17285FDDD96AA8DD535967A1423A97312
>> adrift impartial tempest article mural matchmaker accrue autopsy erase Cherokee affl
ict everyday artist guitarist peachy scavenger highchair leprosy willow tambourine pref
er pedigree optic specialist chopper monument keyboard belowground blowtorch passenger
hockey backwater <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
44.	CA prints out a sufficient number of copies for participants using `for i in $(seq X); do printlog ksrsigner-20161027-*.log; done` where ksrsigner-**20161027-***.log is replaced by log output file displayed by program. This generates **X** copies and hands copies to participants.	PJ	1844
45.	IW1 attaches a copy to his/her script.	PJ	1844

Backup Newly Created SKR

Step	Activity	Initials	Time
46.	CA copies the contents of the KSR FD by running `cp -p /media/KSR/* .` for posting back to RZM. Confirm overwrite by entering "y" when prompted.	PJ	1846

47.	CA lists contents of KSR FD which should now have an SKR by running
	`ls -ltr /media/KSR`
	flushes the system buffers:
	`sync`
	then unmounts the KSR FD using
	`umount /media/KSR`
		PJ	1847

48.	CA removes the FD **KSR** containing SKR and gives it to the RZM representative.	PJ	1847

Act 3. New KSK Generation and Backup

Generate New Key

Step	Activity	Initials	Time
1.	On the laptop terminal window, CA executes: **kskgen** to generate the new KSK inside the HSM and the Certificate Signing Request (CSR). 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. If **"slot"** is asked type **0.** **Note: Displayed output should be similar to Figure 2.**	PS	1849

```
Starting: kskgen (at Fri Oct 14 22:31:14 2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1411008

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

SHA256 DS resource record and hash:
. IN DS 16340 8 2 7659C176FB54F512331A9DA7A24005E3E7CA2904CAA574648B02B00FC89FB70E
>> inverse examine snapline impetus watchword equation vapor backwater chisel Bradbury quadrant
paragraph rebirth Dakota adult torpedo transit revenue breakup alkali spellbind paperweight indoors
getaway obtuse aftermath ruffled atmosphere spaniel opulent seabird Atlantic <<

Created CSR file "Klaavzo.csr":
O: Public Technical Identifiers
OU: Cryptographic Business Operations
CN: Root Zone KSK 2016-10-14T22:31:25+00:00
1.3.6.1.4.1.1000.53: . IN DS 16340 8 2
7659C176FB54F512331A9DA7A24005E3E7CA2904CAA574648B02B00FC89FB70E

Klaavzo.csr SHA256 thumbprint and hash:
61B8E6C3518A54FCEBC95623FD377A52C1AC47615 7F5B8753B2C700C51C0FE85
>> fallout provincial tracker replica drunken maverick eating Wilmington trouble retrospect egghead
cannonball willow consensus keyboard enrollment snapline penetrate dashboard frequency eightball
visitor select impartial clockwork Chicago guidance article drunken recipe woodlark leprosy <<

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

Figure 2

```
Starting: kskgen (at Thu Oct 27 18:49:20 2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

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

SHA256 DS resource record and hash:
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
>> tapeworm hazardous crumpled provincial alone midsummer Belfast corporate revenge fas
cinate alone asteroid kiwi glossary stagnate Jupiter endorse typewriter merit Dakota pu
ppy pyramid frighten confidence eightball autopsy crowfoot consensus soybean warranty t
umor microscope <<

Created CSR file "Klajeyz.csr":
O: Public Technical Identifiers
OU: Cryptographic Business Operations
CN: Root Zone KSK 2016-10-27T18:50:19+00:00
1.3.6.1.4.1.1000.53: . IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC6834
57104237C7F8EC8D

Klajeyz.csr SHA256 thumbprint and hash:
3674086DE75997F47F27302774630C31A6C43D81F5FA43D107A43DECB1C63755
>> Christmas hydraulic aimless hazardous transit examine preshrunk Virginia lockup cele
brate chairlift celebrate indoors Galveston ammo company rematch reproduce commence inv
entive vapor whimsical crucial scavenger ahead Pandora commence unicorn sailboat respon
sive clamshell equipment <<

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

Print Copies of the Key Generation log

Step	Activity	Initials	Time
2.	CA prints out hard copies of the kskgen log output file by executing `printlog kskgen-20161027-*.log X` for attachment to IW1 script and copies for the participants. This generates **X** copies and hands copies to participants. CA explains the status of the new KSK.	PJ	1851

Record Keypair Label

Step	Activity	Initials	Time
3.	IW1 records the keypair label here Klajeyz	PJ	1856

Verify the New Key

Step	Activity	Initials	Time
4.	CA checks the new Key by executing `keybackup -l -P 123456` then confirm the new keypair label on the previous step is listed.	PJ	1857

Verify CSR

Step	Activity	Initials	Time
5.	CA checks the integrity of the CSR by executing a) CA executes `displaycsr XXXX.csr` Where **XXXX** is replaced with the Keypair label indicated on Step 3. b) Hit SPACE bar until the end of display, then hit "q" to end. **Note: Displayed output should be similar to Figure 3.**	PJ	1858

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: O=Public Technical Identifiers, OU=Cryptographic Business Operations, CN=Root Zone
KSK 2016-10-14T22:31:25+00:00/1.3.6.1.4.1.1000.53=. IN DS 16340 8 2
7659C176FB54F512331A9DA7A24005E3E7CA2904CAA574648B02B00FC89FB70E
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e8:ec:74:d8:66:db:eb:aa:b1:e0:a0:af:c1:97:
                    [...]
                    da:0d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
        7c:65:b3:bd:ed:51:96:ec:f3:89:03:e2:91:e5:a1:9d:a3:52:
        [...]
```

Figure 3

Disable/Deactivate HSM3

Step	Activity	Initials	Time
6.	CA makes sure to utilize the cards that were NOT used to activate the HSM are used to deactivate the HSM. CA will perform the following steps to deactivate the HSM: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"2.Set Offline"** hit **ENT** to confirm c) When **"Set Offline?"** is displayed, hit **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** hit **ENT** f) When **"Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP cards Confirm the **"READY"** led on the HSM is **OFF.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 1 of 7 2nd OP card 3 of 7 3rd OP card 7 of 7	PS	1900

Ceremony Break

Step	Activity	Initials	Time
7.	CA initiates the ceremony break and requests the TCRs to leave the TEBs with SO cards on the ceremony table visible to the audit cameras.	PS	1902
8.	CA divides the participants that require ceremony break in groups and must ensure the following: • At least (1) CA and (1) IW should remain in front of the ceremony table when each group is escorted for ceremony break. • At least (2) Crypto Officers and (1) Auditor should remain in the ceremony room when each group is escorted for ceremony break • Audit Cameras are never obstructed CA, IW or SA will escort each group of participants out of the ceremony room for ceremony break.	PS	1903
9.	Once all the groups have returned to the ceremony room, CA ensures that all participants are present, then distributes the TEBs with SO cards to the TCRs for the ceremony to resume.	PS	1934

Create Temporary CO Cards

Step	Activity	Initials	Time
10.	One by one, CA calls each COs listed below to inspect their TEB for tamper evidence, opens the TEB and hands the SO cards to the CA who then places the cards in cardholder visible to all.		
	CO 1: Frederico Neves ✓ **SO TEB # BB21820443**	PS	1935
	CO 3: Olaf Kolkman ✓ **SO TEB # BB21907253**	PS	1936
	CO 4: Robert Seastrom ✓ **SO TEB # BB21907203**	PS	1936
	CO 5: Christopher Griffiths ✓ **SO TEB # BB21907206**	PS	1937
	CO 7: Alain Aina ✓ **SO TEB # BB21907212**	PS	1937
	Note: There are two sets of SO cards that cannot be mixed. Cards on the same set cannot work with the other set and vice-versa.		

Create Temporary CO Cards

Step	Activity	Initials	Time
11.	CA makes sure to utilize **3 SO** cards from the same set to make **Crypto Officer (CO)** cards: a) Utilize the HSM's keyboard and scroll through menu using **<>** key b) Select **"7.Role Mgmt"** hit **ENT** to confirm c) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder d) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** e) When **"Remove Card?"** is displayed, remove card f) Repeat steps c) to e) for the 2nd and 3rd SO cards g) Select **"1.Issue Cards"** hit **ENT** to confirm h) Select **"1.Issue CO Cards"** hit **ENT** to confirm i) When **"Issue CO Cards?"** is displayed, hit **ENT** to confirm j) When **"Num Cards?"** is displayed, enter **"2"** and hit **ENT** to confirm k) When **"Num Req Cards?"** is displayed, enter **"2"** and hit **ENT** to confirm l) When **"Insert Card #?"** is displayed, insert the proper sequence of **CO** card from the cardholder m) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** n) When **"Remove Card?"** is displayed, remove card o) Repeat steps l) to n) for the 2nd CO card p) When **"CO Cards Issued"** is displayed, hit **ENT** to confirm q) Hit **CLR twice** to return to the main menu **"Secured"** IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card 1 of 7 2nd SO card 3 of 7 3rd SO card 4 of 7	PJ PJ PJ	1440 1443

Backup New KSK

Step	Activity	Initials	Time
12.	CA will use the **2 CO cards** to backup the New KSK into **Application Key (APP. Key)** cards: a) Utilize the HSM's keyboard and scroll through menu using **<>** key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Insert Card CO #?"** is displayed, insert the CO card from the cardholder d) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** e) When **"Remove Card?"** is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select **"3.App Keys"** hit **ENT** to confirm h) Select **"1.Backup"** hit **ENT** to confirm i) When **"Backup?"** is displayed, hit **ENT** to confirm j) When **"Which Media?"** is displayed, select **"2.Backup to Card"** and hit **ENT** to confirm k) Using **<>** key, select **"2.Specify key"** hit **ENT** to confirm l) Using **<>** key until the new key generate above is display on the top of the list, then hit **"A"** to select the new key and hit **ENT** to confirm m) When **"Insert B/U Card?"** is displayed insert the proper APP. Key card from the cardholder n) When **"Remove Card?"** is displayed, remove card o) When **"Backup Success"** is displayed, hit **ENT** to confirm p) Repeat steps h) to o) for the 2nd, 3rd, and 4th backup copy q) Hit **CLR twice** to return to the main menu **"Secured"** **Note: As the backup cards are created, the CA writes the Keypair label on the card, then places it on the cardholder.**	PS PS PS	1944 1947 1950

Return HSM3 to TEB

Step	Activity	Initials	Time
13.	CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.	PS	1953
14.	CA places the HSM into a prepared TEB and seals it.	PS	1954
15.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM3: TEB# BB24646656 / serial # H1403032** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	PS	1955

Power Up HSM4

Step	Activity	Initials	Time
16.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM4: TEB# BB24646658 / serial # H1411011**	PS	1957
17.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	PS	1957
18.	CA switches to the ttyaudit terminal window and connects power to HSM and switches the power ON. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) **HSM4: serial # H1411011** **Note: The HSM date and time was set from the factory and will not be used as a reference**	PS	1958

Import New KSK to HSM4

Step	Activity	Initials	Time
19.	CA will use the **2 CO cards** to import the new KSK using **Application Key (APP. Key)** cards: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Insert Card CO #?"** is displayed, insert the CO card from the cardholder d) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** e) When **"Remove Card?"** is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select **"3.App Keys"** hit **ENT** to confirm h) Select **"2.Restore"** hit **ENT** to confirm i) When **"Restore?"** is displayed, hit **ENT** to confirm j) When **"Which Media?"** is displayed, select **"2. From Card"** and hit **ENT** to confirm k) When **"Insert Card #?"** is displayed, insert any APP Key card from the cardholder l) When **"Remove Card?"** is displayed, remove card m) When **"Restore Complete"** is displayed, hit **ENT** to confirm n) Hit **CLR twice** to return to the main menu **"Secured"** As the cards are used, the CA places it in the cardholder.	PS	2000

Enable/Activate HSM4

Step	Activity	Initials	Time
20.	CA will perform the following steps to activate the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"1.Set Online"** hit **ENT** to confirm c) When **"Set Online?"** is displayed, hit **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When **"Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card Confirm the **"READY"** led on the **HSM** is **ON.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 1 of 7 2nd OP card 5 of 7 3rd OP card 4 of 7	PS PS	2002 2003

Check Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
21.	CA connects HSM to laptop using Ethernet cable in **LAN** port.	PS	2004
22.	CA switches to the terminal window and tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` and looking for responses. Ctrl-C to exit program.	PS	2004

Verify New Key

Step	Activity	Initials	Time
23.	CA checks the new Key by executing `keybackup -l -P 123456` then confirms the new keypair label on step 3. is listed.	PS	2005

Generate and Verify CSR

Step	Activity	Initials	Time
24.	CA change directory by executing `cd /tmp` ✓ then `kskgen XXXX` ✓ where **XXXX** is replaced by the Keypair label generated in the step **3.** 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. If **"slot"** is asked type **0.**	PS	2005
25.	CA checks the integrity of the CSR by executing a) CA executes **`displaycsr XXXX.csr`** Where **XXXX** is replaced with the Keypair label indicated on Step 3. b) Verify the DS resource record matches with the printed copies from Step 2. c) Hit SPACE bar until the end of display, then hit "q" to end.	PS	2007
26.	CA return to the working directory by executing `cd /media/HSMFD`	PS	2008

Disable/Deactivate HSM4

Step	Activity	Initials	Time
27.	CA will perform the following steps to deactivate the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"2.Set Offline"** hit **ENT** to confirm ✓ c) When **"Set Offline?"** is displayed, hit **ENT** to confirm ✓ d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** hit **ENT** ✓ f) When **"Remove Card?"** is displayed, remove card ✓ g) Repeat steps d) to f) for the 2nd and 3rd OP cards ✓✓ Confirm the **"READY"** led on the HSM is **OFF.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 1 of 7 2nd OP card 7 of 7 3rd OP card 5 of 7 * Note card 5 had an issue in shutting down HSM	PJ PJ	2009 2012

Clear and Destroy CO Cards

Step	Activity	Initials	Time
28.	CA makes sure to utilize **3 SO cards** from the **same set** that were NOT used before to clear **Crypto Officer (CO)** cards: a) Utilize the HSM's keyboard and scroll through menu using **<>** key b) Select **"7.Role Mgmt"** hit **ENT** to confirm c) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder 1 d) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** ✓ e) When **"Remove Card?"** is displayed, remove card ✓ f) Repeat steps c) to e) for the 2nd and 3rd SO card 3 ✓ 5 ✓ g) Select **"4.Clear RoleCard"** hit **ENT** to confirm ✓ h) When **"Clear Card?"** is displayed, hit **ENT** to confirm ✓ i) When **"Num Cards?"** is displayed, enter **"2"** and hit **ENT** to confirm ✓ j) When **"Insert Card #?"** is displayed, take the proper sequence of the **CO** card form the cardholder, show the **CO** card to the audit camera, then insert the **CO** into the HSM's card reader ✓ k) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** l) When **"Remove Card?"** is displayed, remove card m) Repeat steps j) to l) for the 2nd CO cards ✓ n) Hit **CLR** to return to the main menu **"Secured"** IW1 records the used cards below. Set # 2 1st SO card 1 of 7 2nd SO card 3 of 7 3rd SO card 5 of 7 CA uses the shredder to destroy the cleared CO cards.	PJ PJ PJ	2014 2015 2016

Return HSM4 to TEB

Step	Activity	Initials	Time
29.	CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.	PS	2018
30.	CA places the HSM into a prepared TEB and seals it.	PS	2019
31.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM4: TEB# BB24646654 / serial # H1411011** ✓ CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	PS	2020

Act 4. Secure Hardware, Key Deletion and Zeroization the Old HSMs

Restart Serial Port Activity

Step	Activity	Initials	Time
1.	CA switches to the ttyaudit terminal window and disconnects the USB serial adaptor from laptop. CA then re-connects the serial to USB null modem cable to the laptop.	PS	2022
2.	CA executes the following to start logging of the HSM serial port outputs. `ttyaudit /dev/ttyUSB0` Note: **DO NOT** unplug the USB serial port from the laptop as this will cause logging to stop.	PS	2022

Power Up HSM1

Step	Activity	Initials	Time
3.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM1: TEB# BB24706804 / serial # K6002016**	PS	2023
4.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	PS	2024
5.	CA connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp). **HSM1: serial # K6002016** **Note: The HSM date and time was set from the factory.**	PS	2025

HSM1: List KSK

Step	Activity	Initials	Time
6.	CA utilizes **3 SO cards** from the **same set** to list the KSK stored in the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"4.Output Key Summary"** hit **ENT** to confirm i) When **"Key Summary?"** is displayed, hit **ENT** to confirm j) Select **"5.Output Key Details"** hit **ENT** to confirm k) When **"List Key?"** is displayed, hit **ENT** to confirm l) Hit **CLR** to return to the previous menu CA matches the displayed KSK label `Kjqmt7v` in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card 7 of 7 2nd SO card 4 of 7 3rd SO card 5 of 7	PS PS	2026 2028

HSM1: Delete KSK

Step	Activity	Initials	Time
7.	CA utilizes **3 SO cards** from the **same set** to delete the KSK in the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"2.App Keys"** hit **ENT** to confirm i) Select **"7.Erase App Keys"** hit **ENT** to confirm j) When **"Erase App Keys?"** is displayed, hit **ENT** to confirm k) When **"Done"** is displayed, hit **ENT** to confirm l) Select **"4.Output Key Summary"** hit **ENT** to confirm m) When **"Key Summary?"** is displayed, hit **ENT** to confirm n) Select **"5.Output Key Details"** hit **ENT** to confirm o) When **"List Key?"** is displayed, hit **ENT** to confirm p) Hit **CLR** to return to the previous menu CA confirms there is not a key displayed in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 2 1st SO card 7 of 7 2nd SO card 4 of 7 3rd SO card 3 of 7	PJ PJ	2029 2031

HSM1: Zeroisation

Step	Activity	Initials	Time
8.	CA utilizes **3 SO cards** from the **same set** to place the HSM on "**Initialized**" state. This will zeroise the HSM and erase all keys (AAK, SMK, APP), settings and configuration: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"4.HSM Mgmt"** hit **ENT** to confirm c) When **"HSM Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"A.Go Initialised"** hit **ENT** to confirm i) When **"Go Initialised?"** is displayed, hit **ENT** to confirm j) Wait until **"Done"** is displayed. It may take a few minutes for HSM to restart after erasing all keys. When this operation is complete the HSM will reboot and after self test the HSM display should say **"Important Read Manual"** indicating the HSM is in the initialized state. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 2 1st SO card 7 of 7 2nd SO card 4 of 7 3rd SO card 3 of 7	PJ PJ	2033 2034

Return HSM1 to TEB

Step	Activity	Initials	Time
9.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected.	PJ	2034
10.	CA places the HSM into a prepared TEB and seals it.	PJ	2036
11.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM1: TEB# BB24646647 / serial # K6002016** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	PJ	2036

Power Up HSM2

Step	Activity	Initials	Time
12.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM2: TEB# BB24646674 / serial # K6002013**	PJ	2037
13.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	PJ	2038
14.	CA connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) **HSM2: serial # K6002013** **Note: The HSM date and time was set from the factory.**	PJ	2039

HSM2: List the KSK

Step	Activity	Initials	Time
15.	CA utilizes **3 SO cards** from the **same set** to list the KSK in the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When **"Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"4.Output Key Summary"** hit **ENT** to confirm i) When **"Key Summary?"** is displayed, hit **ENT** to confirm j) Select **"5.Output Key Details"** hit **ENT** to confirm k) When **"List Key?"** is displayed, hit **ENT** to confirm l) Hit **CLR** to return to the previous menu CA matches displayed KSK keypair label `Kjqmt7v` in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card 7 of 7 2nd SO card 3 of 7 3rd SO card 1 of 7	PJ PJ	2040 2041

HSM2: Delete the KSK

Step	Activity	Initials	Time
16.	CA utilizes **3 SO cards** from the **same set** to delete the KSK in the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?**" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"2.App Keys"** hit **ENT** to confirm i) Select **"7.Erase App Keys"** hit **ENT** to confirm j) When **"Erase App Keys?"** is displayed, hit **ENT** to confirm k) When **"Done"** is displayed, hit **ENT** to confirm l) Select **"4.Output Key Summary"** hit **ENT** to confirm m) When **"Key Summary?"** is displayed, hit **ENT** to confirm n) Select **"5.Output Key Details"** hit **ENT** to confirm o) When **"List Key?"** is displayed, hit **ENT** to confirm p) Hit **CLR** to return to the previous menu CA confirms there is not a key displayed in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 2 1st SO card 4 of 7 2nd SO card 7 of 7 3rd SO card 5 of 7	PJ PJ	2042 2044

HSM2: Zeroisation

Step	Activity	Initials	Time
17.	CA utilizes **3 SO cards** from the **same set** to place the HSM on "**Initialized**" state. This will zeroise the HSM and erase all keys (AAK, SMK, APP), settings and configuration: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"4.HSM Mgmt"** hit **ENT** to confirm c) When **"HSM Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"A.Go Initialised"** hit **ENT** to confirm i) When **"Go Initialised?"** is displayed, hit **ENT** to confirm j) Wait until **"Done"** is displayed. It may take a few minutes for HSM to restart after erasing all keys. When this operation is complete the HSM will reboot and after self test the HSM display should say **"Important Read Manual"** indicating the HSM is in the initialized state. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card 1 of 7 2nd SO card 5 of 7 3rd SO card 4 of 7	PJ PJ	2045 2046

Act 5. Secure Hardware and Close the Ceremony

Return HSM2 to TEB

Step	Activity	Initials	Time
1.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected.	PJ	2048
2.	CA places the HSM into a prepared TEB and seals it.	PJ	2049
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM2: TEB# BB24646652 / serial # K6002013** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	PJ	2050

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
4.	**Closing ttyaudit terminal window** CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of **ttyaudit terminal window** by typing "exit".	PJ	2050
5.	**Terminating the logging script** CA stops logging terminal output by entering "exit" in the other terminal window. This only stops the script logging and will **NOT** close window.	PJ	2051

KSK 27

```
# find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum
1c668e831efca9059d4cdc69c7be1a0f2b042e84cd833566de040ba950894538  -
```

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA sets dotglob by executing `shopt -s dotglob` This allows copying everything in the original HSMFD.	PS	2051
7.	CA calculates the sha256hash of the contents on the original HSMFD. `find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum`	PS	2051
8.	CA copy and paste the sha256hash and paste it on Text Editor by going to **Applications > Accessories > Text Editor**	PS	2052
9.	CA prints five copies of the hash, then writes "**KSK 27**" on all the pages One for the audit bundle and the other for the HSMFD packages.	PS	2053
10.	CA displays contents of HSMFD by executing `ls -ltr`	PS	2055
11.	CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the O/S (as HSMFD_); and copies the contents of the HSMFD to the blank drive for backup by executing `cp -Rp * /media/HSMFD_`	PS	2055
12.	CA displays contents of HSMFD_ by executing `ls -ltr /media/HSMFD_`	PS	2056
13.	Calculate the sha256hash of the contents on the copied HSMFD. `find -P /media/HSMFD_ -type f -print0 | sort -z | xargs -0 cat | sha256sum` Confirm that it matches the sha256hash of the original HSMFD by using the text editor to copy and paste the hash for comparison.	PS	2056
14.	CA unmounts new FD using `umount /media/HSMFD_`	PS	2056
15.	CA removes **HSMFD_** and places it on the table.	PS	2056
16.	CA repeats step 11 to 15 for the 2nd copy.	PS	2057
17.	CA repeats step 11 to 15 for the 3rd copy.	PS	2057
18.	CA repeats step 11 to 15 for the 4th copy.	PS	2058
19.	CA repeats step 11 to 15 for the 5th copy.	PS	2059
20.	CA repeats step 11 to 15 for the 6th copy.	PS	2100
21.	CA repeats step 11 to 15 for the 7th copy.	PS	2101

```
Script started on Thu 27 Oct 2016 06:22:54 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=1.06 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.365 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.526 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.365 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.365/0.581/1.068/0.288 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner Kjqmt7v /media
/KSR/ksr-root-2017-q1-0.xml
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2017-q1-0.xml (at Thu Oct 27 18:38:03
2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:          ICANNKSK
    ManufacturerID: AEP Networks
    Model:          Keyper 9860-2
    Serial:         H1403032

Validating last SKR with HSM...
#  Inception           Expiration           ZSK Tags     KSK Tag(CKA_LABEL)
1  2016-10-01T00:00:00 2016-10-15T23:59:59  46551,39291  19036
2  2016-10-11T00:00:00 2016-10-25T23:59:59  46551,39291  19036
3  2016-10-21T00:00:00 2016-11-04T23:59:59  46551,39291  19036
4  2016-10-31T00:00:00 2016-11-14T23:59:59  39291        19036
5  2016-11-10T00:00:00 2016-11-24T23:59:59  39291        19036
6  2016-11-20T00:00:00 2016-12-04T23:59:59  39291        19036
7  2016-11-30T00:00:00 2016-12-14T23:59:59  39291        19036
8  2016-12-10T00:00:00 2016-12-25T23:59:59  39291        19036
9  2016-12-21T00:00:00 2017-01-05T23:59:59  61045,39291  19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2017-q1-0.xml...
#  Inception           Expiration           ZSK Tags     KSK Tag(CKA_LABEL)
1  2017-01-01T00:00:00 2017-01-22T00:00:00  61045,39291
2  2017-01-11T00:00:00 2017-02-01T00:00:00  61045
3  2017-01-21T00:00:00 2017-02-11T00:00:00  61045
4  2017-01-31T00:00:00 2017-02-21T00:00:00  61045
5  2017-02-10T00:00:00 2017-03-03T00:00:00  61045
6  2017-02-20T00:00:00 2017-03-13T00:00:00  61045
7  2017-03-02T00:00:00 2017-03-23T00:00:00  61045
8  2017-03-12T00:00:00 2017-04-02T00:00:00  61045
9  2017-03-21T00:00:00 2017-04-11T00:00:00  61045,14796
...PASSED.

SHA256 hash of KSR:
1C470A168E72B56DCD8BA6BBC716783AE35EF8F42931E18E3C9E34E5DF2C71A8
>> befriend determine allow bodyguard orca holiness scorecard hazardous spindle Medusa
 rematch publisher soybean bodyguard island corrosion tissue finicky Vulcan Virginia b
reakup company tempest microwave cobra onlooker choking travesty talon Chicago hamlet
paramount <<
```

```
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2017-q1-0.xml
#  Inception           Expiration           ZSK Tags     KSK Tag(CKA_LABEL)
1  2017-01-01T00:00:00 2017-01-22T00:00:00  61045,39291  19036
2  2017-01-11T00:00:00 2017-02-01T00:00:00  61045        19036
3  2017-01-21T00:00:00 2017-02-11T00:00:00  61045        19036
4  2017-01-31T00:00:00 2017-02-21T00:00:00  61045        19036
5  2017-02-10T00:00:00 2017-03-03T00:00:00  61045        19036
6  2017-02-20T00:00:00 2017-03-13T00:00:00  61045        19036
7  2017-03-02T00:00:00 2017-03-23T00:00:00  61045        19036
8  2017-03-12T00:00:00 2017-04-02T00:00:00  61045        19036
9  2017-03-21T00:00:00 2017-04-11T00:00:00  14796,61045  19036

SHA256 hash of SKR:
0475E10C848902105B2B06580F6990D17285FDDD96AA8DD535967A1423A97312
>> adrift impartial tempest article mural matchmaker accrue autopsy erase Cherokee af
lict everyday artist guitarist peachy scavenger highchair leprosy willow tambourine p
efer pedigree optic specialist chopper monument keyboard belowground blowtorch passen
er hockey backwater <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20161027-183803.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# for i in $(seq 14); dep
\0d3ðħK033[K033[Ko prin\007tlog ksrsigner-20161027-*.log
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
[ 2 pages * 1 copy ] sent to printer
3 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -p /media/KSR/* .
cp: overwrite './skr.xml'? y
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -ltr /media/KSR
\033[00mtotal 84
-rwxr-xr-x 1 root root 19557 Oct 24 22:05 \033[00;32mksr-root-2017-q1-0.xml\033[00m
-rwxr-xr-x 1 root root 21083 Oct 24 22:05 \033[00;32mskr.xml.20161027183803\033[00m
-rwxr-xr-x 1 root root 20348 Oct 27 18:41 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 20348 Oct 27 18:41 \033[00;32mskr-root-2017-q1-0.xml\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# sync
```

```
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/KSR
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# kskgen
Starting: kskgen (at Thu Oct 27 18:49:20 2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

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

SHA256 DS resource record and hash:
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
>> tapeworm hazardous crumpled provincial alone midsummer Belfast corporate revenge fa
scinate alone asteroid kiwi glossary stagnate Jupiter endorse typewriter merit Dakota
puppy pyramid frighten confidence eightball autopsy crowfoot consensus soybean warrant
y tumor microscope <<

Created CSR file "Klajeyz.csr":
O: Public Technical Identifiers
OU: Cryptographic Business Operations
CN: Root Zone KSK 2016-10-27T18:50:19+00:00
1.3.6.1.4.1.1000.53: . IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683
457104237C7F8EC8D

Klajeyz.csr SHA256 thumbprint and hash:
3674086DE75997F47F27302774630C31A6C43D81F5FA43D107A43DECB1C63755
>> Christmas hydraulic aimless hazardous transit examine preshrunk Virginia lockup cel
ebrate chairlift celebrate indoors Galveston ammo company rematch reproduce commence i
nventive vapor whimsical crucial scavenger ahead Pandora commence unicorn sailboat res
ponsive clamshell equipment <<

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

********** Log output in ./kskgen-20161027-184920.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# printlog kskge\007n-2016
1027-184920.log 24
[ 1 pages * 24 copy ] sent to printer
3 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# printlog kskgen-20161027
-184920.log 24
[ 1 pages * 24 copy ] sent to printer
3 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# keyback\033[Kup -l -P 12
3456
Starting: keybackup -l -P 123456 (at Thu Oct 27 18:57:05 2016 UTC)
2 public keys:
label:Klajeyz
label:Kjqmt7v
2 private keys:
label:Klajeyz
label:Kjqmt7v

********** Log output in ./keybackup-20161027-185705.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# displaycsr Klajeyz.csr
[illegible]
    Data:
        Version: 0 (0x0)
        Subject: O=Public Technical Identifiers, OU=Cryptographic Business Operations
 CN=Root Zone KSK 2016-10-27T18:50:19+00:00/1.3.6.1.4.1.1000.53=. IN DS 20326 8 2 E06
44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ac:ff:b4:09:bc:c9:39:f8:31:f7:a1:e5:ec:88:
                    f7:a5:92:55:ec:53:04:0b:e4:32:02:73:90:a4:ce:
                    89:6d:6f:90:86:f3:c5:e1:77:fb:fe:11:81:63:aa:
                    ec:7a:f1:46:2c:47:94:59:44:c4:e2:c0:26:be:5e:
                    98:bb:cd:ed:25:97:82:72:e1:e3:e0:79:c5:09:4d:
                    57:3f:0e:83:c9:2f:02:b3:2d:35:13:b1:55:0b:82:
                    69:29:c8:0d:d0:f9:2c:ac:96:6d:17:76:9f:d5:86:
                    7b:64:7c:3f:38:02:9a:bd:c4:81:52:eb:8f:20:71:
                    59:ec:c5:d2:32:c7:c1:53:7c:79:f4:b7:ac:28:ff:
                    11:68:2f:21:68:1b:f6:d6:ab:a5:55:03:2b:f6:f9:
                    f0:36:be:b2:aa:a5:b3:77:8d:6e:eb:fb:a6:bf:9e:
                    a1:91:be:4a:b0:ca:ea:75:9e:2f:77:3a:1f:90:29:
                    c7:3e:cb:8d:57:35:b9:32:1d:b0:85:f1:b8:e2:d8:
\033[K                  03:8f:e2:94:19:92:54:8c:ee:0d:67:dd:45:47:e1:
                    1d:d6:3a:f9:c9:fc:1c:54:66:fb:68:4c:f0:09:d7:
                    19:7c:2c:f7:9e:79:2a:b5:01:e6:a8:a1:ca:51:9a:
                    f2:cb:9b:5f:63:67:e9:4c:0d:47:50:24:51:35:7b:
                    e1:b5
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
        80:8a:21:20:14:8a:5f:d8:91:e4:81:ac:e8:07:dd:e9:47:32:
        ed:ba:2e:a5:06:47:7e:a5:66:a9:2f:aa:b3:1a:df:f6:44:b1:
        44:8f:2c:4f:76:63:06:10:e7:52:d7:40:f2:2d:c8:b3:d5:7a:
        ad:4f:74:38:c8:39:68:54:e7:21:ba:c1:5a:af:29:39:8d:11:
        66:5a:54:f3:f0:15:d2:db:6a:e5:3e:cc:e3:c2:d6:c5:60:2b:
        6a:1a:04:73:d6:0e:a5:10:cc:26:9e:bc:27:12:a2:14:84:95:
        6c:03:cb:60:8d:ac:d9:74:41:b4:c5:20:1f:9d:f0:37:5c:8b:
        5c:9f:17:4c:e0:3a:79:db:c1:58:75:6d:b0:af:60:85:8f:fe:
        bf:f6:93:21:49:cc:55:e2:49:fc:8d:15:89:d4:2d:48:1d:d2:
        ee:52:11:7e:d2:74:89:ba:34:fd:54:c3:f7:d2:90:bc:9e:a9:
        95:cb:6a:41:9d:2a:eb:54:0d:3b:65:57:9f:ce:19:29:64:7f:
        1c:a6:fb:49:f9:15:2f:af:0a:dc:88:03:be:34:cd:fd:db:67:
        76:dc:59:61:98:25:30:94:f9:72:f4:ce:4c:61:3c:b7:d4:30:
        26:b1:78:fa:20:ab:83:04:e1:dd:31:58:24:e7:98:8a:d3:01:
\033[K      1b:bb:80:d7
\033[K[illegible]491\033]0;root@localhost:/media/HSMFD\007[root@localhost H
MFD]# displaycsr Klajeyz.csr
[illegible]
    Data:
        Version: 0 (0x0)
        Subject: O=Public Technical Identifiers, OU=Cryptographic Business Operations
 CN=Root Zone KSK 2016-10-27T18:50:19+00:00/1.3.6.1.4.1.1000.53=. IN DS 20326 8 2 E06
44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
```

```
                    00:ac:ff:b4:09:bc:c9:39:f8:31:f7:a1:e5:ec:88:
                    f7:a5:92:55:ec:53:04:0b:e4:32:02:73:90:a4:ce:
                    89:6d:6f:90:86:f3:c5:e1:77:fb:fe:11:81:63:aa:
                    ec:7a:f1:46:2c:47:94:59:44:c4:e2:c0:26:be:5e:
                    98:bb:cd:ed:25:97:82:72:e1:e3:e0:79:c5:09:4d:
                    57:3f:0e:83:c9:2f:02:b3:2d:35:13:b1:55:0b:82:
                    69:29:c8:0d:d0:f9:2c:ac:96:6d:17:76:9f:d5:86:
                    7b:64:7c:3f:38:02:9a:bd:c4:81:52:eb:8f:20:71:
                    59:ec:c5:d2:32:c7:c1:53:7c:79:f4:b7:ac:28:ff:
                    11:68:2f:21:68:1b:f6:d6:ab:a5:55:03:2b:f6:f9:
                    f0:36:be:b2:aa:a5:b3:77:8d:6e:eb:fb:a6:bf:9e:
                    a1:91:be:4a:b0:ca:ea:75:9e:2f:77:3a:1f:90:29:
                    c7:3e:cb:8d:57:35:b9:32:1d:b0:85:f1:b8:e2:d8:
\033[?1049l\033>\033[?1049l\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=1.70 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.358 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.529 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.361 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.358/0.738/1.704/0.561 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# keybackup -l -P 123456
Starting: keybackup -l -P 123456 (at Thu Oct 27 20:05:01 2016 UTC)
2 public keys:
label:Klajeyz
label:Kjqmt7v
2 private keys:
label:Klajeyz
label:Kjqmt7v

********** Log output in ./keybackup-20161027-200501.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cd /t\033[Kmp
\033]0;root@localhost:/tmp\007[root@localhost tmp]# kskgen Klajeyz\033[K033[Kz
Starting: kskgen Klajeyz (at Thu Oct 27 20:05:57 2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:          ICANNKSK
    ManufacturerID: AEP Networks
    Model:          Keyper 9860-2
    Serial:         H1411011

Looking for RSA keypair labeled "Klajeyz"...
Found keypair labeled "Klajeyz"
SHA256 DS resource record and hash:
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
>> tapeworm hazardous crumpled provincial alone midsummer Belfast corporate revenge fascinate alone asteroid kiwi glossary stagnate Jupiter endorse typewriter merit Dakota puppy pyramid frighten confidence eightball autopsy crowfoot consensus soybean warranty tumor microscope <<

Created CSR file "Klajeyz.csr":
O: Public Technical Identifiers
OU: Cryptographic Business Operations
CN: Root Zone KSK 2016-10-27T20:06:06+00:00
1.3.6.1.4.1.1000.53: . IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC68457104237C7F8EC8D

Klajeyz.csr SHA256 thumbprint and hash:
5C0C3BB122C2C1DD2945641334CEC7AA0130FA36ADBADA8C60A86D94F2A2ED30
>> escape article clockwork photograph blockade repellent snapline tambourine breakup detector flytrap barbecue choking sardonic soybean pedigree absurd commando wallet congregate ringbolt puberty surmount megaton facial paramount goggles molecule uproot Pacific tunnel commando <<

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

********** Log output in ./kskgen-20161027-200557.log **********
\033]0;root@localhost:/tmp\007[root@localhost tmp]# displ\007aycsr Klajeyz.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: O=Public Technical Identifiers, OU=Cryptographic Business Operations, CN=Root Zone KSK 2016-10-27T20:06:06+00:00/1.3.6.1.4.1.1000.53=. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ac:ff:b4:09:bc:c9:39:f8:31:f7:a1:e5:ec:88:
                    f7:a5:92:55:ec:53:04:0b:e4:32:02:73:90:a4:ce:
                    89:6d:6f:90:86:f3:c5:e1:77:fb:fe:11:81:63:aa:
                    ec:7a:f1:46:2c:47:94:59:44:c4:e2:c0:26:be:5e:
                    98:bb:cd:ed:25:97:82:72:e1:e3:e0:79:c5:09:4d:
                    57:3f:0e:83:c9:2f:02:b3:2d:35:13:b1:55:0b:82:
                    69:29:c8:0d:d0:f9:2c:ac:96:6d:17:76:9f:d5:86:
                    7b:64:7c:3f:38:02:9a:bd:c4:81:52:eb:8f:20:71:
                    59:ec:c5:d2:32:c7:c1:53:7c:79:f4:b7:ac:28:ff:
                    11:68:2f:21:68:1b:f6:d6:ab:a5:55:03:2b:f6:f9:
                    f0:36:be:b2:aa:a5:b3:77:8d:6e:eb:fb:a6:bf:9e:
                    a1:91:be:4a:b0:ca:ea:75:9e:2f:77:3a:1f:90:29:
                    c7:3e:cb:8d:57:35:b9:32:1d:b0:85:f1:b8:e2:d8:
\033[?1049l\033>\033[?1049l\033]0;root@localhost:/tmp\007[root@localhost tmp]# cd media/HSMFD
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit

Script done on Thu 27 Oct 2016 08:50:59 PM UTC
```

```
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0 H1403032 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0 BBL CRC32: 0x757574CA
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0 H1403032 011403 ABL 011 : Tamper Challenge Response Key
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:52+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2016-10-27T18:26:52+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 ####################################
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 ###     ABL tamper records       ###
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 ####################################
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 ====================================
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 vextoosTamperCount:     0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 vintoosTamperCount:     45
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 vbboosTamperCount:      0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 maxstrtempTamperCount:  0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 minstrtempTamperCount:  0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 meshTamperCount:        0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 extampSMKTamperCount:   0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 extampIMKTamperCount:   0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 tempdiffTamperCount:    0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 pfTamperCount:          45
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 restartTamperCount:     143
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 Current tamper bitmaps:
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 ======================
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
```

```
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0 ========================================
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:53+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0 Board is P2020RDB
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0 board_smp_init: 2 cpu
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:54+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2016-10-27T18:26:54+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 Starting next program at v0015183c
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 Starting K-Series Kernel
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 Thu Oct 27 17:54:17 2016
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 Starting auditd v2.0 ... started.
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:55+0000        ttyUSB0 Interface 0 configured for IPv6.
2016-10-27T18:26:55+0000        ttyUSB0
2016-10-27T18:26:56+0000        ttyUSB0 Interface 0 configured for IPv4.
2016-10-27T18:26:56+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0 Starting USB driver...
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0
2016-10-27T18:26:57+0000        ttyUSB0
```

```
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running DES POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 DES POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running Triple DES POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Triple DES POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running AES POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 AES POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running SHA1 POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 SHA1 POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running SHA2 POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 SHA2 POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running RandomGen POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 RandomGen POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running RSA POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 RSA POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running DSA POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 DSA POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 Running ECC POST Test
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:58+0000        ttyUSB0 ECC POST Test Passed
2016-10-27T18:26:58+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0 Audit on 27/10/2016 17:54:20 00100008
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0 Keyper 9860-2  Serial Number H1403032
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:26:59+0000        ttyUSB0 Memory Usage:
2016-10-27T18:26:59+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 RAM (free/total)        197Mb/256Mb
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0    black store          440b
```

```
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0    statistics           112b
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0    other                116b
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 RedStore (free/total)   109Kb/128Kb
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 Network Configuration:
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 IPv4: enabled
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 IPv6: enabled
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B2:3D / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b23d/64
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 HSM Port: 05000
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 Software Versions:
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 BBL 010 ABL 011 App 023
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 CPLD Version:
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 1.9
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 SCR Firmware Version:
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 OROS-R2.99-R1.20
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:27:00+0000        ttyUSB0 Audit on 27/10/2016 17:54:21 00100003
2016-10-27T18:27:00+0000        ttyUSB0
2016-10-27T18:33:26+0000        ttyUSB0 Audit on 27/10/2016 18:00:47 00200069 0880004A7BB3296D
2016-10-27T18:33:26+0000        ttyUSB0
2016-10-27T18:33:50+0000        ttyUSB0 Audit on 27/10/2016 18:01:11 00200069 0880004A83B3296D
2016-10-27T18:33:50+0000        ttyUSB0
```

```
2016-10-27T18:34:16+0000        ttyUSB0 Audit on 27/10/2016 18:01:38 00200069 0880004A7B33296D
2016-10-27T18:34:16+0000        ttyUSB0
2016-10-27T18:34:18+0000        ttyUSB0
2016-10-27T18:34:18+0000        ttyUSB0
2016-10-27T18:34:18+0000        ttyUSB0 TcpListener: Created IPv4 socket 15 on port 5000.
2016-10-27T18:34:18+0000        ttyUSB0
2016-10-27T18:34:18+0000        ttyUSB0
2016-10-27T18:34:18+0000        ttyUSB0
2016-10-27T18:34:18+0000        ttyUSB0 TcpListener: Created IPv6 socket 16 on port 5000.
2016-10-27T18:34:18+0000        ttyUSB0
2016-10-27T18:34:19+0000        ttyUSB0 Audit on 27/10/2016 18:01:40 00100002
2016-10-27T18:34:19+0000        ttyUSB0
2016-10-27T18:38:46+0000        ttyUSB0
2016-10-27T18:38:46+0000        ttyUSB0
2016-10-27T18:38:46+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-10-27T18:38:46+0000        ttyUSB0
2016-10-27T18:41:53+0000        ttyUSB0
2016-10-27T18:41:53+0000        ttyUSB0
2016-10-27T18:41:53+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-10-27T18:41:53+0000        ttyUSB0
2016-10-27T18:50:14+0000        ttyUSB0
2016-10-27T18:50:14+0000        ttyUSB0
2016-10-27T18:50:14+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-10-27T18:50:14+0000        ttyUSB0
2016-10-27T18:50:19+0000        ttyUSB0
2016-10-27T18:50:19+0000        ttyUSB0
2016-10-27T18:50:19+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-10-27T18:50:19+0000        ttyUSB0
2016-10-27T18:57:05+0000        ttyUSB0
2016-10-27T18:57:05+0000        ttyUSB0
2016-10-27T18:57:05+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-10-27T18:57:05+0000        ttyUSB0
2016-10-27T18:57:05+0000        ttyUSB0
2016-10-27T18:57:05+0000        ttyUSB0
2016-10-27T18:57:05+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-10-27T18:57:05+0000        ttyUSB0
2016-10-27T18:59:43+0000        ttyUSB0 Audit on 27/10/2016 18:27:04 00200069 00800002714F156D
2016-10-27T18:59:43+0000        ttyUSB0
2016-10-27T19:00:08+0000        ttyUSB0 Audit on 27/10/2016 18:27:30 00200069 0880004A7AB3296D
2016-10-27T19:00:08+0000        ttyUSB0
2016-10-27T19:00:39+0000        ttyUSB0 Audit on 27/10/2016 18:27:58 00200069 0880004A7BB3296D
2016-10-27T19:00:39+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0 TcpListener: Closed IPv4 socket 15 on port 5000.
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0 TcpListener: Closed IPv6 socket 16 on port 5000.
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:00:45+0000        ttyUSB0 Audit on 27/10/2016 18:28:06 00100003
2016-10-27T19:00:45+0000        ttyUSB0
2016-10-27T19:39:32+0000        ttyUSB0 Audit on 27/10/2016 19:06:54 00200023 00400000C322156D
2016-10-27T19:39:32+0000        ttyUSB0
2016-10-27T19:39:54+0000        ttyUSB0 Audit on 27/10/2016 19:07:15 00200023 00400000C862156D
```

```
2016-10-27T19:39:54+0000        ttyUSB0
2016-10-27T19:40:12+0000        ttyUSB0 Audit on 27/10/2016 19:07:34 00200023 00400000F922156D
2016-10-27T19:40:12+0000        ttyUSB0
2016-10-27T19:41:27+0000        ttyUSB0 Audit on 27/10/2016 19:08:49 0020002c 47800001BE2D2972
2016-10-27T19:41:27+0000        ttyUSB0
2016-10-27T19:42:18+0000        ttyUSB0 Audit on 27/10/2016 19:09:40 0020002c 478000017EED2972
2016-10-27T19:42:18+0000        ttyUSB0
2016-10-27T19:42:40+0000        ttyUSB0 Audit on 27/10/2016 19:10:01 00200077 478000017EED2972
2016-10-27T19:42:40+0000        ttyUSB0
2016-10-27T19:44:30+0000        ttyUSB0 Audit on 27/10/2016 19:11:52 0020006b 47800001BE2D2972
2016-10-27T19:44:30+0000        ttyUSB0
2016-10-27T19:44:52+0000        ttyUSB0 Audit on 27/10/2016 19:12:13 0020006b 478000017EED2972
2016-10-27T19:44:52+0000        ttyUSB0
2016-10-27T19:46:53+0000        ttyUSB0 Audit on 27/10/2016 19:14:14 0020002e 47800001806D2972
2016-10-27T19:46:53+0000        ttyUSB0
2016-10-27T19:46:58+0000        ttyUSB0 Audit on 27/10/2016 19:14:20 00200013 47800001806D2972
2016-10-27T19:46:58+0000        ttyUSB0
2016-10-27T19:48:38+0000        ttyUSB0 Audit on 27/10/2016 19:16:00 0020002e 47800001BDED2972
2016-10-27T19:48:38+0000        ttyUSB0
2016-10-27T19:48:44+0000        ttyUSB0 Audit on 27/10/2016 19:16:05 00200013 47800001BDED2972
2016-10-27T19:48:44+0000        ttyUSB0
2016-10-27T19:49:19+0000        ttyUSB0 Audit on 27/10/2016 19:16:40 0020002e 4780000180AD2972
2016-10-27T19:49:19+0000        ttyUSB0
2016-10-27T19:49:24+0000        ttyUSB0 Audit on 27/10/2016 19:16:46 00200013 4780000180AD2972
2016-10-27T19:49:24+0000        ttyUSB0
2016-10-27T19:50:04+0000        ttyUSB0 Audit on 27/10/2016 19:17:24 0020002e 47800001BEAD2972
2016-10-27T19:50:04+0000        ttyUSB0
2016-10-27T19:50:10+0000        ttyUSB0 Audit on 27/10/2016 19:17:31 00200013 47800001BEAD2972
2016-10-27T19:50:10+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0 H1411011 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0 BBL CRC32: 0x757574CA
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0 H1411011 011403 ABL 011 : Tamper Challenge Response Key
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:14+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2016-10-27T19:58:14+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 ####################################
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 ###     ABL tamper records       ###
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 ####################################
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 ====================================
2016-10-27T19:58:15+0000        ttyUSB0
```

```
2016-10-27T19:58:15+0000        ttyUSB0 vextoosTamperCount:     0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 vintoosTamperCount:     13
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 vbboosTamperCount:      0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 maxstrtempTamperCount:  0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 minstrtempTamperCount:  0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 meshTamperCount:        0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 extampSMKTamperCount:   0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 extampIMKTamperCount:   0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 tempdiffTamperCount:    0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 pfTamperCount:          13
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 restartTamperCount:     27
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 Current tamper bitmaps:
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 ======================
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 lastTamper bitmap:      0x0000 0b .... .... .... ....
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0 ==========================================
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:15+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 Board is P2020RDB
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 board_smp_init: 2 cpu
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
```

```
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 Starting next program at v0015183c
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:16+0000        ttyUSB0 Starting K-Series Kernel
2016-10-27T19:58:16+0000        ttyUSB0
2016-10-27T19:58:17+0000        ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2016-10-27T19:58:17+0000        ttyUSB0
2016-10-27T19:58:17+0000        ttyUSB0 Thu Oct 27 19:26:44 2016
2016-10-27T19:58:17+0000        ttyUSB0
2016-10-27T19:58:17+0000        ttyUSB0 Starting auditd v2.0 ... started.
2016-10-27T19:58:17+0000        ttyUSB0
2016-10-27T19:58:17+0000        ttyUSB0 Interface 0 configured for IPv6.
2016-10-27T19:58:17+0000        ttyUSB0
2016-10-27T19:58:18+0000        ttyUSB0 Interface 0 configured for IPv4.
2016-10-27T19:58:18+0000        ttyUSB0
2016-10-27T19:58:18+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2016-10-27T19:58:18+0000        ttyUSB0
2016-10-27T19:58:18+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2016-10-27T19:58:18+0000        ttyUSB0
2016-10-27T19:58:18+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2016-10-27T19:58:18+0000        ttyUSB0
2016-10-27T19:58:18+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2016-10-27T19:58:18+0000        ttyUSB0
2016-10-27T19:58:18+0000        ttyUSB0 Starting USB driver...
2016-10-27T19:58:18+0000        ttyUSB0
2016-10-27T19:58:19+0000        ttyUSB0 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2016-10-27T19:58:19+0000        ttyUSB0
2016-10-27T19:58:19+0000        ttyUSB0
2016-10-27T19:58:19+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running DES POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 DES POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running Triple DES POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Triple DES POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running AES POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 AES POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running SHA1 POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 SHA1 POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running SHA2 POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 SHA2 POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running RandomGen POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 RandomGen POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
```

```
2016-10-27T19:58:20+0000        ttyUSB0 Running RSA POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 RSA POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running DSA POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 DSA POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 Running ECC POST Test
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:20+0000        ttyUSB0 ECC POST Test Passed
2016-10-27T19:58:20+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 Audit on 27/10/2016 19:26:47 00100008
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 Keyper 9860-2  Serial Number H1411011
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 Memory Usage:
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 RAM (free/total)        197Mb/256Mb
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0    black store          440b
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0    statistics           112b
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0    other                116b
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 RedStore (free/total)   109Kb/128Kb
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 Network Configuration:
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 IPv4: enabled
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 IPv6: enabled
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B3:2A / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b32a/64
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 HSM Port: 05000
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 Software Versions:
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 BEL 010 ABL 011 App 023
```

```
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 CPLD Version:
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 1.9
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:21+0000        ttyUSB0 SCR Firmware Version:
2016-10-27T19:58:21+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0 OROS-R2.99-R1.20
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:58:22+0000        ttyUSB0 Audit on 27/10/2016 19:26:48 00100003
2016-10-27T19:58:22+0000        ttyUSB0
2016-10-27T19:59:36+0000        ttyUSB0 Audit on 27/10/2016 19:28:03 0020006b 47800001BE2D2972
2016-10-27T19:59:36+0000        ttyUSB0
2016-10-27T19:59:59+0000        ttyUSB0 Audit on 27/10/2016 19:28:26 0020006b 478000017EED2972
2016-10-27T19:59:59+0000        ttyUSB0
2016-10-27T20:00:47+0000        ttyUSB0 Audit on 27/10/2016 19:29:14 00200016 Klajeyz
2016-10-27T20:00:47+0000        ttyUSB0
2016-10-27T20:00:50+0000        ttyUSB0 Audit on 27/10/2016 19:29:14 00200015 47800001806D2972
2016-10-27T20:00:50+0000        ttyUSB0
2016-10-27T20:00:50+0000        ttyUSB0 Audit on 27/10/2016 19:29:17 00200018
2016-10-27T20:00:50+0000        ttyUSB0
2016-10-27T20:02:33+0000        ttyUSB0 Audit on 27/10/2016 19:31:00 00200069 00800002714F156D
2016-10-27T20:02:33+0000        ttyUSB0
2016-10-27T20:02:52+0000        ttyUSB0 Audit on 27/10/2016 19:31:19 0020006a 0880004A7B33296D
2016-10-27T20:02:52+0000        ttyUSB0
2016-10-27T20:03:22+0000        ttyUSB0 Audit on 27/10/2016 19:31:48 00200069 0880004A7B33296D
2016-10-27T20:03:22+0000        ttyUSB0
2016-10-27T20:03:41+0000        ttyUSB0 Audit on 27/10/2016 19:32:07 00200069 0880004A83B3296D
2016-10-27T20:03:41+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0 TcpListener: Created IPv4 socket 15 on port 5000.
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0 TcpListener: Created IPv6 socket 16 on port 5000.
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:03:43+0000        ttyUSB0 Audit on 27/10/2016 19:32:10 00100002
2016-10-27T20:03:43+0000        ttyUSB0
2016-10-27T20:05:01+0000        ttyUSB0
2016-10-27T20:05:01+0000        ttyUSB0
```

```
2016-10-27T20:05:01+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-10-27T20:05:01+0000        ttyUSB0
2016-10-27T20:05:01+0000        ttyUSB0
2016-10-27T20:05:01+0000        ttyUSB0
2016-10-27T20:05:01+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-10-27T20:05:01+0000        ttyUSB0
2016-10-27T20:06:06+0000        ttyUSB0
2016-10-27T20:06:06+0000        ttyUSB0
2016-10-27T20:06:06+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-10-27T20:06:06+0000        ttyUSB0
2016-10-27T20:06:06+0000        ttyUSB0
2016-10-27T20:06:06+0000        ttyUSB0
2016-10-27T20:06:06+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-10-27T20:06:06+0000        ttyUSB0
2016-10-27T20:09:31+0000        ttyUSB0 Audit on 27/10/2016 19:37:57 00200069 00800002714F156D
2016-10-27T20:09:31+0000        ttyUSB0
2016-10-27T20:09:50+0000        ttyUSB0 Audit on 27/10/2016 19:38:16 00200069 0880004A7BB3296D
2016-10-27T20:09:50+0000        ttyUSB0
2016-10-27T20:10:55+0000        ttyUSB0 Audit on 27/10/2016 19:39:21 0020006a
2016-10-27T20:10:55+0000        ttyUSB0
2016-10-27T20:11:17+0000        ttyUSB0 Audit on 27/10/2016 19:39:43 00200069 0880004A7B33296D
2016-10-27T20:11:17+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0 TcpListener: Closed IPv4 socket 15 on port 5000.
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0 TcpListener: Closed IPv6 socket 16 on port 5000.
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:11:21+0000        ttyUSB0 Audit on 27/10/2016 19:39:48 00100003
2016-10-27T20:11:21+0000        ttyUSB0
2016-10-27T20:13:22+0000        ttyUSB0 Audit on 27/10/2016 19:41:48 00200023 00800002784F156D
2016-10-27T20:13:22+0000        ttyUSB0
2016-10-27T20:13:42+0000        ttyUSB0 Audit on 27/10/2016 19:42:08 00200023 00800002948F156D
2016-10-27T20:13:42+0000        ttyUSB0
2016-10-27T20:14:02+0000        ttyUSB0 Audit on 27/10/2016 19:42:28 00200023 008000029ECF156D
2016-10-27T20:14:02+0000        ttyUSB0
2016-10-27T20:15:26+0000        ttyUSB0 Audit on 27/10/2016 19:43:53 00200070 47800001BE2D2972
2016-10-27T20:15:26+0000        ttyUSB0
2016-10-27T20:16:03+0000        ttyUSB0 Audit on 27/10/2016 19:44:27 00200070 478000017EED2972
2016-10-27T20:16:03+0000        ttyUSB0
```

```
2016-10-27T20:24:46+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2016-10-27T20:24:46+0000        ttyUSB0
2016-10-27T20:24:46+0000        ttyUSB0
2016-10-27T20:24:46+0000        ttyUSB0 Battery OK!
2016-10-27T20:24:46+0000        ttyUSB0
2016-10-27T20:24:47+0000        ttyUSB0
2016-10-27T20:24:47+0000        ttyUSB0 No Tamper Counts in BBRAM!
2016-10-27T20:24:47+0000        ttyUSB0
2016-10-27T20:24:47+0000        ttyUSB0  Loading Application (APP)
2016-10-27T20:24:47+0000        ttyUSB0
2016-10-27T20:24:48+0000        ttyUSB0  Starting loaded code.
2016-10-27T20:24:48+0000        ttyUSB0
2016-10-27T20:24:49+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2016-10-27T20:24:49+0000        ttyUSB0
2016-10-27T20:24:50+0000        ttyUSB0 wdog started
2016-10-27T20:24:50+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running DES POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 DES POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running Triple DES POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Triple DES POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running AES POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 AES POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running SHA1 POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 SHA1 POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running SHA2 POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 SHA2 POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running RSA POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 RSA POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running DSA POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 DSA POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 Running RandomGen POST Test
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:53+0000        ttyUSB0 RandomGen POST Test Passed
2016-10-27T20:24:53+0000        ttyUSB0
2016-10-27T20:24:54+0000        ttyUSB0 Additional RandomGen POST Test Passed
```

```
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 27/10/2016 at 18:38:10
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0  0x100008
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 App Details Response:
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Part Number: Keyper Pro 0405
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 Serial Number: Serial K6002016
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 App Build Number: App 020
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 ABL Build Number: ABL 029
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:54+0000	ttyUSB0 AL Build Number: AL 02A
2016-10-27T20:24:54+0000	ttyUSB0
2016-10-27T20:24:55+0000	ttyUSB0 CS Build Number: CS 029
2016-10-27T20:24:55+0000	ttyUSB0
```

```
2016-10-27T20:24:55+0000        ttyUSB0 Total Private Memory 4173377
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0 Free Private Memory 4173377
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0 Total Dynamic Memory 14569472
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0 Free Dynamic Memory 14569472
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0 Date and Time: 18:38:10 on 27/10/2016
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0 Created socket 1 on port 3000.
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0 27/10/2016 at 18:38:11
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:24:55+0000        ttyUSB0  0x100003
2016-10-27T20:24:55+0000        ttyUSB0
2016-10-27T20:26:50+0000        ttyUSB0
2016-10-27T20:26:50+0000        ttyUSB0
2016-10-27T20:26:50+0000        ttyUSB0 27/10/2016 at 18:40:07
2016-10-27T20:26:50+0000        ttyUSB0
2016-10-27T20:26:50+0000        ttyUSB0  0x200023 00800002780F156D
2016-10-27T20:26:50+0000        ttyUSB0
2016-10-27T20:27:10+0000        ttyUSB0
2016-10-27T20:27:10+0000        ttyUSB0
2016-10-27T20:27:10+0000        ttyUSB0 27/10/2016 at 18:40:26
2016-10-27T20:27:10+0000        ttyUSB0
2016-10-27T20:27:10+0000        ttyUSB0  0x200023 00400000F922156D
2016-10-27T20:27:10+0000        ttyUSB0
2016-10-27T20:27:28+0000        ttyUSB0
2016-10-27T20:27:28+0000        ttyUSB0
2016-10-27T20:27:28+0000        ttyUSB0 27/10/2016 at 18:40:44
2016-10-27T20:27:28+0000        ttyUSB0
2016-10-27T20:27:28+0000        ttyUSB0  0x200023 00800002788F156D
2016-10-27T20:27:28+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0 Dumping HSM Key Summary
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0 ========================
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0 RSA,2048,Private,1
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0 ====================
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:27:44+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
```

```
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0 Dumping HSM Key Details
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0 ========================
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0 Kjqmt7v,RSA,FIPS,2048,wt,svednvu
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0 ====================
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:28:00+0000        ttyUSB0
2016-10-27T20:29:54+0000        ttyUSB0
2016-10-27T20:29:54+0000        ttyUSB0
2016-10-27T20:29:54+0000        ttyUSB0 27/10/2016 at 18:43:10
2016-10-27T20:29:54+0000        ttyUSB0
2016-10-27T20:29:54+0000        ttyUSB0  0x200023 00800000294CF156D
2016-10-27T20:29:54+0000        ttyUSB0
2016-10-27T20:30:12+0000        ttyUSB0
2016-10-27T20:30:12+0000        ttyUSB0
2016-10-27T20:30:12+0000        ttyUSB0 27/10/2016 at 18:43:28
2016-10-27T20:30:12+0000        ttyUSB0
2016-10-27T20:30:12+0000        ttyUSB0  0x200023 00800002A48F156D
2016-10-27T20:30:12+0000        ttyUSB0
2016-10-27T20:30:32+0000        ttyUSB0
2016-10-27T20:30:32+0000        ttyUSB0
2016-10-27T20:30:32+0000        ttyUSB0 27/10/2016 at 18:43:48
2016-10-27T20:30:32+0000        ttyUSB0
2016-10-27T20:30:32+0000        ttyUSB0  0x200023 00800002948F156D
2016-10-27T20:30:32+0000        ttyUSB0
2016-10-27T20:30:56+0000        ttyUSB0
2016-10-27T20:30:56+0000        ttyUSB0
2016-10-27T20:30:56+0000        ttyUSB0 27/10/2016 at 18:44:12
2016-10-27T20:30:56+0000        ttyUSB0
2016-10-27T20:30:56+0000        ttyUSB0  0x200068
2016-10-27T20:30:56+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0 Dumping HSM Key Summary
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0 ========================
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0 ====================
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:09+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
```

```
2016-10-27T20:31:20+0000        ttyUSB0 Dumping HSM Key Details
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0 ========================
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0 ==================
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:31:20+0000        ttyUSB0
2016-10-27T20:32:19+0000        ttyUSB0
2016-10-27T20:32:19+0000        ttyUSB0
2016-10-27T20:32:19+0000        ttyUSB0 27/10/2016 at 18:45:36
2016-10-27T20:32:19+0000        ttyUSB0
2016-10-27T20:32:19+0000        ttyUSB0  0x200023 0080000294CF156D
2016-10-27T20:32:19+0000        ttyUSB0
2016-10-27T20:32:39+0000        ttyUSB0
2016-10-27T20:32:39+0000        ttyUSB0
2016-10-27T20:32:39+0000        ttyUSB0 27/10/2016 at 18:45:55
2016-10-27T20:32:39+0000        ttyUSB0
2016-10-27T20:32:39+0000        ttyUSB0  0x200023 00800002A48F156D
2016-10-27T20:32:39+0000        ttyUSB0
2016-10-27T20:32:57+0000        ttyUSB0
2016-10-27T20:32:57+0000        ttyUSB0
2016-10-27T20:32:57+0000        ttyUSB0 27/10/2016 at 18:46:14
2016-10-27T20:32:57+0000        ttyUSB0
2016-10-27T20:32:57+0000        ttyUSB0  0x200023 00800002948F156D
2016-10-27T20:32:57+0000        ttyUSB0
2016-10-27T20:33:20+0000        ttyUSB0
2016-10-27T20:33:20+0000        ttyUSB0
2016-10-27T20:33:20+0000        ttyUSB0 27/10/2016 at 18:46:36
2016-10-27T20:33:20+0000        ttyUSB0
2016-10-27T20:33:20+0000        ttyUSB0  0x20001f
2016-10-27T20:33:20+0000        ttyUSB0
2016-10-27T20:33:37+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2016-10-27T20:33:37+0000        ttyUSB0
2016-10-27T20:33:38+0000        ttyUSB0
2016-10-27T20:33:38+0000        ttyUSB0 Battery OK!
2016-10-27T20:33:38+0000        ttyUSB0
2016-10-27T20:33:39+0000        ttyUSB0
2016-10-27T20:33:39+0000        ttyUSB0 No Tamper Counts in BBRAM!
2016-10-27T20:33:39+0000        ttyUSB0
2016-10-27T20:33:39+0000        ttyUSB0  Loading Application (APP)
2016-10-27T20:33:39+0000        ttyUSB0
2016-10-27T20:33:40+0000        ttyUSB0  Starting loaded code.
2016-10-27T20:33:40+0000        ttyUSB0
2016-10-27T20:33:40+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2016-10-27T20:33:40+0000        ttyUSB0
2016-10-27T20:33:42+0000        ttyUSB0 wdog started
2016-10-27T20:33:42+0000        ttyUSB0
2016-10-27T20:33:47+0000        ttyUSB0
2016-10-27T20:33:47+0000        ttyUSB0
2016-10-27T20:33:47+0000        ttyUSB0 Running DES POST Test
2016-10-27T20:33:47+0000        ttyUSB0
2016-10-27T20:33:47+0000        ttyUSB0 DES POST Test Passed
```

```
2016-10-27T20:33:47+0000	ttyUSB0
2016-10-27T20:33:47+0000	ttyUSB0 Running Triple DES POST Test
2016-10-27T20:33:47+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Triple DES POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running AES POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 AES POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running SHA1 POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 SHA1 POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running SHA2 POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 SHA2 POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running RandomGen SHA1 POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Randomgen SHA1 POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running RSA POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 RSA POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running DSA POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 DSA POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Running RandomGen POST Test
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 App Details Response:
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
```

```
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:48+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:48+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Part Number: Keyper Pro 0405
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Serial Number: Serial K6002016
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 App Build Number: App 020
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 ABL Build Number: ABL 029
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 AL Build Number: AL 02A
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 CS Build Number: CS 029
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Total Private Memory 4174428
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Free Private Memory 4174428
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Total Dynamic Memory 14569472
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Free Dynamic Memory 14569472
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Date and Time: 18:47:04 on 27/10/2016
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 Created socket 1 on port 3000.
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0 27/10/2016 at 18:47:05
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:33:49+0000	ttyUSB0  0x100001
2016-10-27T20:33:49+0000	ttyUSB0
2016-10-27T20:38:45+0000	ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2016-10-27T20:38:45+0000	ttyUSB0
2016-10-27T20:38:46+0000	ttyUSB0
2016-10-27T20:38:46+0000	ttyUSB0 Battery OK!
2016-10-27T20:38:46+0000	ttyUSB0
2016-10-27T20:38:46+0000	ttyUSB0
2016-10-27T20:38:47+0000	ttyUSB0 No Tamper Counts in BBRAM!
2016-10-27T20:38:47+0000	ttyUSB0
2016-10-27T20:38:47+0000	ttyUSB0  Loading Application (APP)
```

```
2016-10-27T20:38:47+0000        ttyUSB0
2016-10-27T20:38:48+0000        ttyUSB0  Starting loaded code.
2016-10-27T20:38:48+0000        ttyUSB0
2016-10-27T20:38:48+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2016-10-27T20:38:48+0000        ttyUSB0
2016-10-27T20:38:50+0000        ttyUSB0 wdog started
2016-10-27T20:38:50+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running DES POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 DES POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running Triple DES POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Triple DES POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running AES POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 AES POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running SHA1 POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 SHA1 POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running SHA2 POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 SHA2 POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running RSA POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 RSA POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running DSA POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 DSA POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Running RandomGen POST Test
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 RandomGen POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0 28/10/2014 at 18:39:52
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:53+0000        ttyUSB0  0x100008
2016-10-27T20:38:53+0000        ttyUSB0
2016-10-27T20:38:54+0000        ttyUSB0
2016-10-27T20:38:54+0000        ttyUSB0
2016-10-27T20:38:54+0000        ttyUSB0
2016-10-27T20:38:54+0000        ttyUSB0
```

```
2016-10-27T20:38:54+0000          ttyUSB0 App Details Response:
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Part Number: Keyper Pro 0405
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Serial Number: Serial K6002013
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 App Build Number: App 020
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 ABL Build Number: ABL 029
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 AL Build Number: AL 02A
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 CS Build Number: CS 029
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Total Private Memory 4173377
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Free Private Memory 4173377
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:54+0000          ttyUSB0 Total Dynamic Memory 14569472
2016-10-27T20:38:54+0000          ttyUSB0
2016-10-27T20:38:55+0000          ttyUSB0 Free Dynamic Memory 14569472
2016-10-27T20:38:55+0000          ttyUSB0
2016-10-27T20:38:55+0000          ttyUSB0 Date and Time: 18:39:52 on 28/10/2014
```

```
2016-10-27T20:38:55+0000        ttyUSB0
2016-10-27T20:38:55+0000        ttyUSB0 Created socket 1 on port 3000.
2016-10-27T20:38:55+0000        ttyUSB0
2016-10-27T20:38:55+0000        ttyUSB0
2016-10-27T20:38:55+0000        ttyUSB0
2016-10-27T20:38:55+0000        ttyUSB0 28/10/2014 at 18:39:53
2016-10-27T20:38:55+0000        ttyUSB0
2016-10-27T20:38:55+0000        ttyUSB0  0x100003
2016-10-27T20:38:55+0000        ttyUSB0
2016-10-27T20:40:18+0000        ttyUSB0
2016-10-27T20:40:18+0000        ttyUSB0
2016-10-27T20:40:18+0000        ttyUSB0 28/10/2014 at 18:41:17
2016-10-27T20:40:18+0000        ttyUSB0
2016-10-27T20:40:18+0000        ttyUSB0  0x200023 00800002780F156D
2016-10-27T20:40:18+0000        ttyUSB0
2016-10-27T20:40:40+0000        ttyUSB0
2016-10-27T20:40:40+0000        ttyUSB0
2016-10-27T20:40:40+0000        ttyUSB0 28/10/2014 at 18:41:38
2016-10-27T20:40:40+0000        ttyUSB0
2016-10-27T20:40:40+0000        ttyUSB0  0x200023 00400000C862156D
2016-10-27T20:40:40+0000        ttyUSB0
2016-10-27T20:41:06+0000        ttyUSB0
2016-10-27T20:41:06+0000        ttyUSB0
2016-10-27T20:41:06+0000        ttyUSB0 28/10/2014 at 18:42:04
2016-10-27T20:41:06+0000        ttyUSB0
2016-10-27T20:41:06+0000        ttyUSB0  0x200023 00400000C322156D
2016-10-27T20:41:06+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0 Dumping HSM Key Summary
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0 ========================
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0 RSA,2048,Private,1
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0 ==================
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:25+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0 Dumping HSM Key Details
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0 ======================
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0 Kjqmt7v,RSA,FIPS,2048,wt,svedmvu
2016-10-27T20:41:34+0000        ttyUSB0
```

```
2016-10-27T20:41:34+0000        ttyUSB0 ==================
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:41:34+0000        ttyUSB0
2016-10-27T20:42:47+0000        ttyUSB0
2016-10-27T20:42:47+0000        ttyUSB0
2016-10-27T20:42:47+0000        ttyUSB0 28/10/2014 at 18:43:45
2016-10-27T20:42:47+0000        ttyUSB0
2016-10-27T20:42:47+0000        ttyUSB0  0x200023 00800002A48F156D
2016-10-27T20:42:47+0000        ttyUSB0
2016-10-27T20:43:04+0000        ttyUSB0
2016-10-27T20:43:04+0000        ttyUSB0
2016-10-27T20:43:04+0000        ttyUSB0 28/10/2014 at 18:44:02
2016-10-27T20:43:04+0000        ttyUSB0
2016-10-27T20:43:04+0000        ttyUSB0  0x200023 0080000294CF156D
2016-10-27T20:43:04+0000        ttyUSB0
2016-10-27T20:43:24+0000        ttyUSB0
2016-10-27T20:43:24+0000        ttyUSB0
2016-10-27T20:43:24+0000        ttyUSB0 28/10/2014 at 18:44:22
2016-10-27T20:43:24+0000        ttyUSB0
2016-10-27T20:43:24+0000        ttyUSB0  0x200023 008000029ECF156D
2016-10-27T20:43:24+0000        ttyUSB0
2016-10-27T20:43:47+0000        ttyUSB0
2016-10-27T20:43:47+0000        ttyUSB0
2016-10-27T20:43:47+0000        ttyUSB0 28/10/2014 at 18:44:45
2016-10-27T20:43:47+0000        ttyUSB0
2016-10-27T20:43:47+0000        ttyUSB0  0x200068
2016-10-27T20:43:47+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0 Dumping HSM Key Summary
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0 ==========================
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0 ==================
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:13+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0 Dumping HSM Key Details
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0 ========================
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0 ==================
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:44:24+0000        ttyUSB0
```

```
2016-10-27T20:44:24+0000        ttyUSB0
2016-10-27T20:45:33+0000        ttyUSB0
2016-10-27T20:45:33+0000        ttyUSB0
2016-10-27T20:45:33+0000        ttyUSB0 28/10/2014 at 18:46:31
2016-10-27T20:45:33+0000        ttyUSB0
2016-10-27T20:45:33+0000        ttyUSB0  0x200023 00400000C322156D
2016-10-27T20:45:33+0000        ttyUSB0
2016-10-27T20:45:52+0000        ttyUSB0
2016-10-27T20:45:52+0000        ttyUSB0
2016-10-27T20:45:52+0000        ttyUSB0 28/10/2014 at 18:46:50
2016-10-27T20:45:52+0000        ttyUSB0
2016-10-27T20:45:52+0000        ttyUSB0  0x200023 00800002788F156D
2016-10-27T20:45:52+0000        ttyUSB0
2016-10-27T20:46:14+0000        ttyUSB0
2016-10-27T20:46:14+0000        ttyUSB0
2016-10-27T20:46:14+0000        ttyUSB0 28/10/2014 at 18:47:12
2016-10-27T20:46:14+0000        ttyUSB0
2016-10-27T20:46:14+0000        ttyUSB0  0x200023 00400000F922156D
2016-10-27T20:46:14+0000        ttyUSB0
2016-10-27T20:46:32+0000        ttyUSB0
2016-10-27T20:46:32+0000        ttyUSB0
2016-10-27T20:46:32+0000        ttyUSB0 28/10/2014 at 18:47:30
2016-10-27T20:46:32+0000        ttyUSB0
2016-10-27T20:46:32+0000        ttyUSB0  0x20001f
2016-10-27T20:46:32+0000        ttyUSB0
2016-10-27T20:47:40+0000        ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
2016-10-27T20:47:40+0000        ttyUSB0
2016-10-27T20:47:41+0000        ttyUSB0
2016-10-27T20:47:41+0000        ttyUSB0 Battery OK!
2016-10-27T20:47:41+0000        ttyUSB0
2016-10-27T20:47:41+0000        ttyUSB0
2016-10-27T20:47:42+0000        ttyUSB0 No Tamper Counts in BBRAM!
2016-10-27T20:47:42+0000        ttyUSB0
2016-10-27T20:47:42+0000        ttyUSB0  Loading Application (APP)
2016-10-27T20:47:42+0000        ttyUSB0
2016-10-27T20:47:43+0000        ttyUSB0  Starting loaded code.
2016-10-27T20:47:43+0000        ttyUSB0
2016-10-27T20:47:43+0000        ttyUSB0 \000Application - Feb 25 2010 11:08:02
2016-10-27T20:47:43+0000        ttyUSB0
2016-10-27T20:47:45+0000        ttyUSB0 wdog started
2016-10-27T20:47:45+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 Running DES POST Test
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 DES POST Test Passed
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 Running Triple DES POST Test
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 Triple DES POST Test Passed
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 Running AES POST Test
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 AES POST Test Passed
2016-10-27T20:47:50+0000        ttyUSB0
```

```
2016-10-27T20:47:50+0000        ttyUSB0 Running SHA1 POST Test
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:50+0000        ttyUSB0 SHA1 POST Test Passed
2016-10-27T20:47:50+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Running SHA2 POST Test
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 SHA2 POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Running RandomGen SHA1 POST Test
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Randomgen SHA1 POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Running RSA POST Test
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 RSA POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Running DSA POST Test
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 DSA POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Running RandomGen POST Test
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 App Details Response:
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:51+0000        ttyUSB0 Additional RandomGen POST Test Passed
```

```
2016-10-27T20:47:51+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Additional RandomGen POST Test Passed
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Part Number: Keyper Pro 0405
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Serial Number: Serial K6002013
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 App Build Number: App 020
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 ABL Build Number: ABL 029
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 AL Build Number: AL 02A
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 CS Build Number: CS 029
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Total Private Memory 4174428
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Free Private Memory 4174428
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Total Dynamic Memory 14569472
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Free Dynamic Memory 14569472
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Date and Time: 18:48:49 on 28/10/2014
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 Created socket 1 on port 3000.
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0 28/10/2014 at 18:48:50
2016-10-27T20:47:52+0000        ttyUSB0
2016-10-27T20:47:52+0000        ttyUSB0  0x100001
2016-10-27T20:47:52+0000        ttyUSB0
```

Print Logging Information

Step	Activity	Initials	Time

22.	CA prints out a hard copy of logging information by executing
	`enscript -2Gr -# 1 script-20161027.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20161027-*.log`
	for attachment to IW1 script.
	Note: Ignore the error regarding non-printable characters if prompted.
		PJ	2102

Return HSMFD and O/S DVD to TEB

Step	Activity	Initials	Time

23.	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
	CA removes HSMFD.
		PJ	2105

24.	CA performs the following to turn off the laptop. a) CA turns off the laptop by pressing the power switch b) CA turns on the laptop by pressing the power switch and immediately removes the O/S DVD from the laptop DVD drive c) CA turns off the laptop again by pressing the power switch	PJ	2106
25.	CA places **TWO** HSMFDs and two OS/DVD, paper with printed hash in prepared TEB; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **O/S DVD (release 20161014) + HSMFD: TEB# BB46584601** ✓	PJ	2107
26.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	PJ	2108

Pack APP. Key Backup Cards to TEB

Step	Activity	Initials	Time
27.	CA performs the following to secure the APP Key backups for this KSK facility. a) CA places **TWO** APP Key cards into the plastic case. ✓ b) CA places the plastic case, **ONE** HSMFD and **ONE** printed copy of the HSMFD HASH inside the TEB then seals it. ✓ c) CA and IW initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. d) CA reads out the TEB # and shows it to all participants to compare with the TEB # below. e) CA then places the TEB on the equipment cart. **APP. Key: TEB # BB46584645** ✓	PJ	2109

Pack APP. Key Backups Cards to TEB

Step	Activity	Initials	Time
28.	CA calls the RKOS to the front of the room one at a time and repeat steps below to secure the APP Key backups for the West Coast KSK facility. a) CA places **ONE** APP Key card into the plastic case. b) CA places the plastic case, **ONE** HSMFD and **ONE** printed copy of the HSMFD HASH inside the TEB then seals it. c) CA and IW initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. d) CA reads out the TEB # and shows it to all participants for comparison with the TEB # below. e) CA hands the TEB containing **ONE** APP Key card to the RKOS. RKOS inspects the TEB then returns to his seat being careful not to poke or puncture the it. **RKOS: Alberto Duero – APP Key Bundle Courier** **APP. Key TEB # BB46584642** **RKOS: Andres Pavez – APP Key Bundle Courier** **APP. Key TEB # BB46584643**	PJ PJ	2112 2114

Distribute HSMFDs

Step	Activity	Initials	Time
29.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles), to RKOS (1 to post SKR to RZM), and to review, analyze and improve on procedures.	PJ	2115

Returning Laptop to TEB

Step	Activity	Initials	Time
30.	CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. **Laptop2 (Dell ATG6400): TEB# BB24646655 / serial # 35063364997**	PJ	2116
31.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.	PJ	2116

Return OP and SO Cards to TEB

Step	Activity	Initials	Time
32.	CA calls each COs to the front of the room one at a time and repeats the steps below. a) CA takes the two TEBs prepared for the CO and reads out the TEB # and description while showing each bag. b) CO places his/her OP card into the plastic case. c) CO places his/her SO cards into the plastic case. d) CA places each plastic case into the proper TEBs, seals and initials TEB using a ballpoint pen. e) IW1 inspects each TEB, confirms description in the table on the next page and initials TEB using a ballpoint pen. IW1 keeps sealing strips for later inventory. f) CA hands each TEBs containing the OP and the SO cards to the CO. CO inspects and verifies TEB # and contents, then initials his/her TEB using a ballpoint pen. g) CO enters completion time and signs for each TEB in the table below in IW1's script. IW1 initials table entry. h) CO returns to his/her seat with the TEBs, being careful not to poke or puncture TEBs. **CO 1: Frederico Neves** **OP TEB # BB46584591** ✓ **SO TEB # BB46584592** ✓ **CO 3: Olaf Kolkman** ✓ **OP TEB # BB46584593** ✓ **SO TEB # BB46584594** ✓ **CO 4: Robert Seastrom** ✓ **OP TEB # BB46584595** ✓ **SO TEB # BB46584596** ✓ **CO 5: Christopher Griffiths** ✓ **OP TEB # BB46584597** ✓ **SO TEB # BB46584598** ✓ **CO 7: Alain Aina** ✓ **OP TEB # BB46584599** ✓ **SO TEB # BB46584600** ✓	PJ	2130

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584591	Frederico Neves	Frederico Neves	20161027	2120	PJ
CO 1	SO 1 of 7	BB46584592	Frederico Neves	Frederico Neves	20161027	2120	PJ
CO 3	OP 3 of 7	BB46584593	Olaf Kolkman		27 oct 2016	21:23	PJ
CO 3	SO 3 of 7	BB46584594	Olaf Kolkman		27 oct 2016	21:23	PJ
CO 4	OP 4 of 7	BB46584595	Robert Seastrom		27-OCT-2016	21:25	PJ
CO 4	SO 4 of 7	BB46584596	Robert Seastrom		27-OCT-2016	21:25	PJ
CO 5	OP 5 of 7	BB46584597	Christopher Griffiths		27 oct 2016	21:28	PJ
CO 5	SO 5 of 7	BB46584598	Christopher Griffiths		27 oct 2016	21:28	PJ
CO 7	OP 7 of 7	BB46584599	Alain Aina		27 oct 2016	21:30	PJ
CO 7	SO 7 of 7	BB46584600	Alain Aina		27 Oct 2016	21:30	PJ

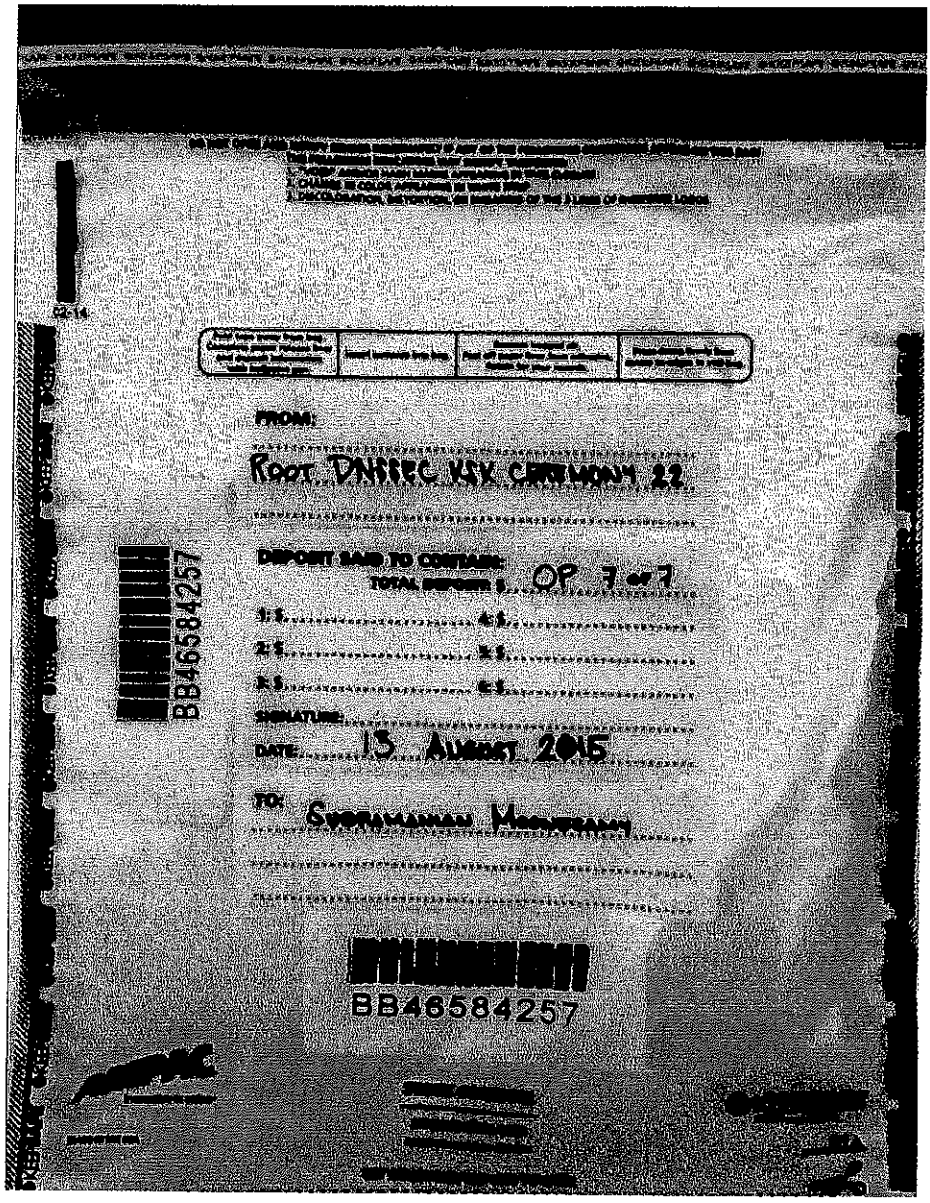

FROM:
ROOT DNSSEC KSK CEREMONY 27
DEPOSIT SAID TO CONTAIN:
OP 7 of 7
DATE: 13 AUGUST 2015
TO:
BB46584257
BB46584257

Figure 4

Returning Equipment to Safe #1

Step	Activity	Initials	Time
33.	CA, IW1, SSC1 open safe room and enter with the equipment cart.	PS	2131
34.	SSC1 opens Safe #1 shielding combination from camera.	PS	2132
35.	SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PS	2133
36.	CA records return of **HSM1, HSM2, HSM3 and HSM4** in the next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA **CAREFULLY** places the HSMs into Safe #1 and IW1 initials the entry. **HSM1: TEB# BB24646647** ✓ **HSM2: TEB# BB24646652** ✓ **HSM3: TEB# BB24646656** ✓ **HSM4: TEB# BB24646654** ✓	PS	2135
37.	CA records return of **laptop** in the next entry field of the safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry. **Laptop2 (Dell ATG6400): TEB# BB24646655** ✓	PS	2136
38.	CA records return of **O/S DVD + HSMFD** in the next entry field of the safe log with TEB #, printed name, date, time, and signature; places the **O/S DVD + HSMFD** into Safe #1 and IW1 initials the entry. **O/S DVD (release 20161014) + HSMFD: TEB# BB46584601** ✓	PS	2136
39.	CA records return of **APP Key** in the next entry field of the safe log with TEB #, printed name, date, time, and signature; then places the **APP Key** into Safe #1 and IW1 initials the entry. **APP Key: TEB# BB46584645** ✓	PS	2137

Close Equipment Safe #1

Step	Activity	Initials	Time
40.	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PS	2137
41.	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). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	PS	2138
42.	IW1, CA, and SSC1 return to ceremony room with the equipment cart closing the door behind them.	PS	2139

Open Credential Safe #2

Step	Activity	Initials	Time
43.	CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP and SO cards (if applicable) in TEBs with them.	PS	2140
44.	SSC2 opens Safe #2 while shielding combination from camera.	PS	2141
45.	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PS	2142

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
46.	One by one, each COs along with the CA (using his/her common key): a) Open his/her respective safe deposit box and read out box number inside Safe #2. **# Common Key is bottom lock and CO Key is top lock** b) CO makes an entry into the safe log indicating the return of OP card and SO cards (if applicable) including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB #s and card type to his/her script. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** c) CO shows each TEB to the camera, then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA. Repeat the steps above until all cards are returned to the deposit box. **CO 1: Frederico Neves** **Box # 1238** ✓ **OP TEB # BB46584591** ✓ **SO TEB # BB46584592** ✓ **CO 3: Olaf Kolkman** **Box # 1239** ✓ **OP TEB # BB46584593** ✓ **SO TEB # BB46584594** ✓ **CO 4: Robert Seastrom** **Box # 1260** ✓ **OP TEB # BB46584595** ✓ **SO TEB # BB46584596** ✓ **CO 5: Christopher Griffiths** **Box # 1240** ✓ **OP TEB # BB46584597** ✓ **SO TEB # BB46584598** ✓ **CO 7: Alain Aina** **Box # 1242** ✓ **OP TEB # BB46584599** ✓ **SO TEB # BB46584600** ✓	PB	2152

Close Credential Safe #2

Step	Activity	Initials	Time
47.	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "Close safe" into the safe log. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PA	2152
48.	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise, then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	PA	2152
49.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	PA	2157

Participant Signing of IW1's Script

Step	Activity	Initials	Time
50.	One by one, all participants come to the front of the room, confirms the printed name and date, **then, signs IW1's coversheet declaring that this script is a true and an accurate record of the ceremony.** IW1 records the completion time once all participants have signed the coversheet. **Note: If entry is pre-printed, verify the entry and sign.**	PA	2159
51.	CA reviews IW1's script and signs it.	PA	2159

Stop Online Streaming

Step	Activity	Initials	Time
52.	CA acknowledges the participation of online participants and confirms with SA to stop online streaming.	PA	2200

Sign Out of Ceremony Room

Step	Activity	Initials	Time
53.	RKOS ensures that all participants sign out of Ceremony Room log and are escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.	PA	2216

Stop Video Recording

Step	Activity	Initials	Time
54.	CA confirms with SA to stop video recording.	PA	2220

Bundle Audit Materials

Step	Activity	Initials	Time
55.	IW1 makes at least 1 copy of his/her script for off-site audit bundle. Audit bundles each contain: a) Output of signer system – HSMFD b) Copy of IW1's key ceremony script c) Audio-visual recording d) Logs from the Physical Access Control and Intrusion Detection System (Range is **05/12/2016 – 10/27/2016**) e) The IW1 attestation (A.1 below) f) SA attestation (A.2, A.3 below) All in a TEB labeled **"Root DNSSEC KSK Ceremony 27"**, 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.**	PJ	2322

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 IW1's notes and the IW1's attestation. See Appendix A.1.

3. Audio-visual recordings from the key ceremony (SA1)
One set for the original audit bundle and the other for duplicate.

4. Logs from the Physical Access Control (PAC) and Intrusion Detection System (IDS) (SA1)
One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC and IDS configuration review, the list of 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 SA1 and the IW1.

IW1 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 (SA1)
SA1's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix A.2.

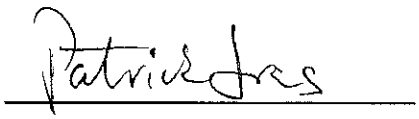
6. Configuration review of the Firewall System (SA1)
SA1's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3. Make sure the scrambled passwords are eliminated from the configuration before publishing it.

7. Other items
If applicable.

A.1 Key Ceremony Script (by IW1)

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.

Patrick Jones



Date: 27 October 2016

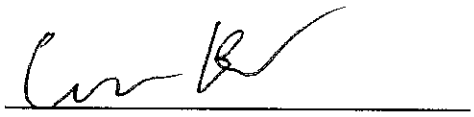
A.2 Access Control System Configuration Review (by SA1)

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 **12 May 2016 00:00 UTC** to now.

Connor Barthold



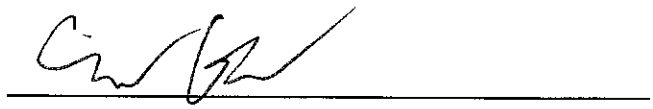
Date: 27 October 2016

A.3 Firewall Configuration Review (by SA1)

I have reviewed the firewall configuration from the other KMF and not found any discrepancies or anything else out of the ordinary.

Enclosed is the configuration extract from the firewall unit.

Connor Barthold



Date: 27 October 2016

```
cbarthold@srx> show configuration | no-more
## Last commit: 2016-06-16 19:37:52 UTC by rquinn
version 12.1X46-D35.1;
system {
    host-name srx;
    domain-name ksk.cjr.dns.icann.org;
    location {
        country-code US;
        postal-code 22701;
        building Terramark-Admin;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }I
    }
    root-authentication {
        encrypted-password "XXXXXXXX"; ## SECRET-DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        inactive: user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
```

```
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
        source-address 10.4.29.1;
    }
}
chassis {
    config-button no-rescue no-clear;
}
interfaces {
    interface-range access {
        member-range ge-0/0/0 to ge-0/0/8;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-access;
                }
            }
```

```
    }
}
interface-range video {
    member-range ge-0/0/9 to ge-0/0/12;
    unit 0 {
        family ethernet-switching {
            vlan {
                members vlan-video;
            }
        }
    }
}
interface-range wifi {
    member ge-0/0/13;
    unit 0 {
        family inet {
            address 10.100.1.1/24;
        }
    }
}
interface-range guest {
    member ge-0/0/14;
    member ge-0/0/15;
    unit 0 {
        family ethernet-switching {
            vlan {
                members vlan-guest;
            }
        }
    }
}
ge-0/0/0 {
    description "Access Control Server";
}
ge-0/0/1 {
    description "Access Control Client Custom Solution";
}
ge-0/0/2 {
    description "Intrusion Detection Panel";
}
ge-0/0/3 {
    description "Environment Monitoring";
}
ge-0/0/4 {
    description "Monitoring Server";
}
ge-0/0/5 {
    description "IRIS Enrollment";
}
ge-0/0/6 {
```

```
    description "Iris Scanner T2";
}
ge-0/0/7 {
    description "Iris Scanner T3";
}
ge-0/0/8 {
    description "Iris Scanner T4";
}
ge-0/0/9 {
    description "Video Surveillance Server";
}
ge-0/0/10 {
    description "Camera 1";
}
ge-0/0/11 {
    description "Camera 2";
}
ge-0/0/12 {
    description "Camera 3";
}
ge-0/0/13 {
    description "Wifi Connection";
}
ge-0/0/14 {
    description "Streaming Laptop";
}
ge-0/0/15 {
    description "Audio Camera Client";
}
ge-1/0/0 {
    unit 0 {
        family inet {
            address 152.194.1.148/28;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            filter {
                input route-engine-filter;
            }
        }
    }
}
st0 {
    unit 1 {
        description "IPSec KMF-West";
        family inet;
    }
```

```
    }
    vlan {
        unit 0 {
            family inet {
                address 10.4.29.193/26;
            }
        }
        unit 1 {
            family inet {
                address 10.4.29.129/26;
            }
        }
        unit 2 {
            family inet {
                address 10.4.29.1/25;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 152.194.1.145;
        route 10.4.28.0/24 next-hop st0.1;
        route 192.0.35.202/32 next-hop 152.194.1.145;
    }
}
policy-options {
    prefix-list resolver-servers {
        8.8.4.4/32;
        8.8.8.8/32;
    }
    prefix-list local-prefixes {
        10.4.29.0/24;
    }
    prefix-list ntp-servers {
        129.6.15.28/32;
        129.6.15.29/32;
    }
}
security {
    ike {
        policy ike-policy-KMF {
            pre-shared-key ascii-text "XXXXXXXX"; ## SECRET-DATA
        }
        gateway Gateway-to-KMF-West {
            ike-policy ike-policy-KMF;
            address 192.0.35.202;
            external-interface ge-1/0/0;
        }
    }
```

```
ipsec {
    traceoptions {
        flag all;
    }
    proposal IPSecProposal {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 7200;
    }
    policy defaultPolicy {
        perfect-forward-secrecy {
            keys group5;
        }
        proposals IPSecProposal;
    }
    vpn vpn-to-KMF-West {
        bind-interface st0.1;
        ike {
            gateway Gateway-to-KMF-West;
            ipsec-policy defaultPolicy;
        }
        establish-tunnels immediately;
    }
}
screen {
    ids-option external-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
    }
}
nat {
    source {
        rule-set internal-to-external {
            from zone [ access guest wifi ];
```

```
            to zone untrust;
            rule source-nat-rule {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
policies {
    from-zone access to-zone untrust {
        policy allow-mail {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address [ icann-dns google-dns ];
                application [ junos-dns-udp junos-dns-tcp ];
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-simplex {
            match {
                source-address IDP;
                destination-address simplex;
                application any;
            }
            then {
                permit;
```

```
            log {
                session-close;
            }
        }
    }
}
from-zone access to-zone video {
    policy access-to-video {
        match {
            source-address IMS;
            destination-address kmf_east_video;
            application junos-icmp-all;
        }
        then {
            permit;
        }
    }
}
from-zone access to-zone ipsec {
    policy allow-access-to-ipsec {
        match {
            source-address [ ACS ACC ];
            destination-address [ kmf_west_acs kmf_west_acc ];
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy temp-allow-access-access {
        match {
            source-address kmf_east_access;
            destination-address kmf_west_access;
            application any;
        }
        then {
            permit;
```

```
        }
    }
}
from-zone ipsec to-zone access {
    policy allow-ipsec-to-access {
        match {
            source-address [ kmf_west_acs kmf_west_acc ];
            destination-address [ ACS ACC ];
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy temp-allow-access-access {
        match {
            source-address kmf_west_access;
            destination-address kmf_east_access;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone video to-zone ipsec {
    policy allow-video-to-ipsec {
        match {
            source-address VSS;
            destination-address kmf_west_vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
```

```
        }
    }
    policy temp-allow-access-video {
        match {
            source-address kmf_east_video;
            destination-address kmf_west_video;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone guest to-zone untrust {
    policy allow-guest-to-untrust {
        match {
            source-address kmf_east_guest;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone wifi to-zone untrust {
    policy allow-wifi-to-untrust {
        match {
            source-address kmf_east_wifi;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ipsec to-zone video {
    policy allow-ipsec-to-video {
        match {
            source-address kmf_west_vss;
            destination-address VSS;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
```

```
        }
        policy temp-allow-access-video {
            match {
                source-address kmf_west_video;
                destination-address kmf_east_video;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone access to-zone access {
        policy allow-access {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    default-policy {
        deny-all;
    }
}
zones {
    security-zone access {
        address-book {
            address ACS 10.4.29.203/32;
            address ACC 10.4.29.202/32;
            address IDP 10.4.29.201/32;
            address EVM 10.4.29.200/32;
            address IMS 10.4.29.204/32;
            address E1 10.4.29.210/32;
            address E2 10.4.29.211/32;
            address E3 10.4.29.212/32;
            address E4 10.4.29.213/32;
            address kmf_east_access 10.4.29.192/26;
            address localnet 10.4.29.0/24;
            address-set iris-scanners {
                address E1;
                address E2;
                address E3;
                address E4;
            }
        }
        interfaces {
```

```
        vlan.0 {
            host-inbound-traffic {
                system-services {
                    ping;
                    ntp;
                }
            }
        }
    }
}
security-zone untrust {
    address-book {
        address icann 192.0.32.0/20;
        address icann-dns 192.0.42.53/32;
        address googledns1 8.8.8.8/32;
        address googledns2 8.8.4.4/32;
        address simplex1 216.224.218.31/32;
        address simplex2 216.224.218.32/32;
        address simplex3 216.224.218.33/32;
        address simplex4 216.224.218.34/32;
        address-set google-dns {
            address googledns1;
            address googledns2;
        }
        address-set simplex {
            address simplex1;
            address simplex2;
            address simplex3;
            address simplex4;
        }
    }
    screen external-screen;
    interfaces {
        ge-1/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ping;
                    ssh;
                }
            }
        }
    }
}
security-zone video {
    address-book {
        address kmf_east_video 10.4.29.128/26;
        address VSS 10.4.29.150/32;
        address C1 10.4.29.151/32;
        address C2 10.4.29.152/32;
        address C3 10.4.29.153/32;
```

```
        address-set cameras {
            address C1;
            address C2;
            address C3;
        }
    }
    interfaces {
        vlan.1 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone guest {
    address-book {
        address STR 10.4.29.20/32;
        address VCC 10.4.29.22/32;
        address kmf_east_guest 10.4.29.0/25;
    }
    interfaces {
        vlan.2 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone ipsec {
    address-book {
        address kmf_west_access 10.4.28.192/26;
        address kmf_west_video 10.4.28.128/26;
        address kmf_west_acs 10.4.28.204/32;
        address kmf_west_acc 10.4.28.202/32;
        address kmf_west_idp 10.4.28.201/32;
        address kmf_west_evm 10.4.28.200/32;
        address kmf_west_ims 10.4.28.203/32;
        address kmf_west_E1 10.4.28.210/32;
        address kmf_west_E3 10.4.28.212/32;
        address kmf_west_E4 10.4.28.213/32;
        address kmf_west_vss 10.4.28.150/32;
        address kmf_west_C1 10.4.28.151/32;
        address kmf_west_C2 10.4.28.152/32;
        address kmf_west_C3 10.4.28.153/32;
    }
    interfaces {
```

```
                st0.1 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                            ike;
                            ssh;
                        }
                    }
                }
            }
        }
        security-zone wifi {
            address-book {
                address kmf_east_wifi 10.100.1.0/24;
            }
            interfaces {
                ge-0/0/13.0 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
    }
}
firewall {
    family inet {
        filter route-engine-filter {
            term deny-icmp-redirects {
                from {
                    protocol icmp;
                    icmp-type redirect;
                }
                then {
                    discard;
                }
            }
            term allow-icmp {
                from {
                    protocol icmp;
                    icmp-type [ echo-request echo-reply unreachable
time-exceeded ];
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
```

```
term allow-traceroute {
    from {
        protocol udp;
        port 33434-33534;
    }
    then {
        policer small-bw-limit;
        accept;
    }
}
term allow-dns {
    from {
        source-prefix-list {
            resolver-servers;
        }
        protocol udp;
        source-port domain;
    }
    then {
        policer small-bw-limit;
        accept;
    }
}
term allow-ntp {
    from {
        source-prefix-list {
            local-prefixes;
            ntp-servers;
        }
        protocol udp;
        port ntp;
    }
    then {
        policer small-bw-limit;
        accept;
    }
}
term allow-establish {
    from {
        protocol tcp;
        tcp-established;
    }
    then accept;
}
term allow-ipsec-esp {
    from {
        protocol esp;
    }
    then accept;
}
```

```
            term allow-ipsec-udp {
                from {
                    protocol udp;
                    port 500;
                }
                then accept;
            }
            term temp-allow-ssh {
                from {
                    source-address {
                        192.0.35.202/32;
                        10.4.29.0/24;
                        10.4.28.0/24;
                    }
                    protocol tcp;
                    destination-port ssh;
                }
                then accept;
            }
            term LAST {
                then {
                    discard;
                }
            }
        }
    }
    policer small-bw-limit {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 15k;
        }
        then discard;
    }
}
poe {
    interface all;
}
vlans {
    vlan-access {
        vlan-id 3;
        l3-interface vlan.0;
    }
    vlan-guest {
        vlan-id 5;
        l3-interface vlan.2;
    }
    vlan-video {
        vlan-id 4;
        l3-interface vlan.1;
    }
```

```
}

cbarthold@srx>
```