

Root DNSSEC KSK Ceremony 30

Thursday August 17, 2017

Root Zone KSK Operator Key Management Facility
1920 East Maple Avenue, El Segundo, CA 90245

**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 KMF = Key Management Facility 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)

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			
IW1	Jonathan Denison / ICANN			
SSC1	Anand Mishra / ICANN			
SSC2	Jessica Castillo / ICANN			20:51:52
CO1	Arbogast Fabian / TZ			
CO2	Dmitry Burkov / RU			
CO5	Olafur Gudmundsson / IS			
CO6	Nicolas Antonieilo / UY			
CO7	Subramanian Moonesamy / MU			
RZM	Alejandro Boivar / Verisign			
RZM	John Painumkal / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Rafael Menciahca / PricewaterhouseCoopers			
AUD	Evan Higashiyama / PricewaterhouseCoopers		August 2017	
SA1	Connor Barthold / ICANN			
SA2	Josh Jenkins / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Victoria Yang / ICANN			
SW	Shaunte Anderson / PTI			
SW	Matt Larson / ICANN			
SW	LV McCoy / PTI			
EW	Gaurab Upadhaya			
EW	Rafael Lito Ibarra			
EW	Luciano Minuchin			

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: The CA leads the ceremony. Dual Occupancy is enforced. Only CAs, IWs, or SAs can enter and escort other participants to the Ceremony room. Only CA+IW can enter the safe room and escort other participants. CAs, IWs, or SAs may escort participants out of the ceremony room at the CA's discretion and only when an IW + CA or SA remain inside the ceremony. No one may leave the Ceremony room if the safe room is occupied. All participants are required to sign in and out of the ceremony room using the visitor log. The SA starts filming before the participants enter the ceremony room.

Some steps during the ceremony may require the participants to tell and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the phonetic alphabet shown below must 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 video streaming is enabled.	JD	20:00:55
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the participants list on Page 2.	JD	20:02:12

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	JD	20:02:29
4.	CA explains the use of personal electronic devices during ceremony.	JD	20:03:16
5.	CA briefly explains the purpose of the ceremony.	JD	20:04:24

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: <u>2017/08/17 20:04:52</u> All entries into this script or any logs should follow this common source of time.	JD	20:04:52

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 brings a flashlight then escorts SSC2, COs into the safe room.	JD	20:07:10
8.	SSC2, while shielding combination from camera, opens Safe #2.	JD	20:08:34
9.	SSC2 removes the existing safe log and shows the most recent page to the audit camera. IW1 provides a pre-printed safe log to the SSC2. SSC2 writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry then initials it.	JD	20:09:53

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	<p>One by one, the selected CO retrieves the required OP TEB and SO TEB (as specified on the list below) by following the steps.</p> <p>a) With the assistance of the CA (and his/her common key), the CO opens her/his safe deposit box.</p> <p>Note: Common Key is for the bottom lock. CO Key is for the top lock</p> <p>b) CO verifies the integrity of the safe deposit box, reads out its number, then removes his/her OP TEB and SO TEB</p> <p>c) CO reads out the TEB #s, then verifies its integrity.</p> <p>d) CO retains OP TEB and SO TEB (as specified below) then locks the box.</p> <p>e) CO writes date/time and signature on the safe log where the removal of their TEBs are indicated.</p> <p>f) IW1 verifies the completed safe log entries then initials it.</p> <p>Repeat these steps until all required cards listed below are removed.</p> <p>CO 1: Arbogast Fabian Box # 1791 OP TEB # BB46584450 (Retain) ✓ SO TEB # BB46584451 (Check and Return) ✓</p> <p>CO 2: Dmitry Burkov Box # 1793 OP TEB # BB46584452 (Retain) ✓ SO TEB # BB46584453 (Check and Return) ✓</p> <p>CO 5: Olafur Gudmundsson Box # 1789 OP TEB # BB46584660 (Retain) ✓ SO TEB # BB46584666 (Check and Return) ✓</p> <p>CO 6: Nicolas Antonello Box # 1073 OP TEB # BB46584458 (Retain) ✓ SO TEB # BB46584459 (Check and Return) ✓</p> <p>CO 7: Subramanian Moonesamy Box # 1792 OP TEB # BB46584460 (Retain) ✓ SO TEB # BB46584461 (Check and Return) ✓</p>	<p>go</p>	<p>20:20:57</p>

Close Credential Safe #2

Step	Activity	Initials	Time
11.	Once all relevant deposit boxes are closed and locked, SSC2 writes the date/time and signature on the safe log where "Close Safe" is indicated. IW1 verifies the safe log entry then initials it.	JP	20:21:41
12.	SSC2 returns the safe log back in the Safe #2 and locks it (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.	JP	20:22
13.	IW1, CA, SSC2, and COs leave safe room, with OP TEB and SO TEB (if applicable), closing the door behind them.	JP	20:23:09

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	JP	20:23:47
15.	SSC1, while shielding combination from camera, opens Safe #1.	JP	20:25:17
16.	SSC1 takes out the existing safe log and shows the most recent page to the audit camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry then initials it.	JP	20:26:20

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	<p>CA CAREFULLY removes HSM3 (in TEB) from the safe; Reads out the TEB # and HSM serial # then places it on the equipment cart. CA then writes the date/time and signature on the safe log where HSM removal is indicated. IW1 verifies the safe log entry then initials it.</p> <p>HSM3: TEB# BB51184611 / serial # H1403033</p> <p>CA verifies the integrity of the other HSM that will not be used, then returns it in the safe.</p> <p>HSM4: TEB# BB51184612 / serial # H1411006</p>	JD	20:28:06
18.	<p>CA removes each of the following equipment TEBs from the safe, reads out the TEB # and serial # then places it on the equipment cart. CA then writes the date/time and signature on the safe log where the removed item(s) are indicated. IW1 verifies the safe log entry then initials it.</p> <p>Laptop1 (Dell ATG6400): TEB# BB51184609 / serial # 37240147333</p> <p>OS DVD (release 20161014) + HSMFD: TEB# BB46584447</p> <p>CA verifies the integrity of the other laptop that will not be used this time and return it to the safe.</p> <p>Laptop2 (Dell ATG6400): TEB# BB24646591 / serial # 7292928457</p>	JD	20:30:39

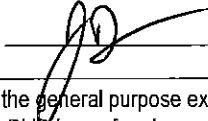
Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	<p>SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry then initials it.</p>	JD	20:31:12
20.	<p>SSC1 returns the safe log back in the Safe #1 and locks it (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.</p>	JD	20:31:54
21.	<p>CA, SSC1 and IW1 leaves the safe room with the equipment cart, closing the door behind them.</p>	JD	20:32:33

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 the TEB # and serial # while IW1 observes and matches it with the prior ceremony script in this facility. CA then places the laptop on the key ceremony table. Laptop1 (Dell ATG6400): TEB# BB51184609 / serial # 37240147333	Jo	20:35:15
2.	CA inspects the OS DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it with the prior ceremony script in this facility. CA then places the items on the key ceremony table. OS DVD (release 20161014) + HSMFD: TEB# BB46584447	Jo	20:35:56
3.	CA removes and discards the TEB from the laptop, OS DVD + HSMFD, then connects the laptop power, external display, general purpose external DVD drive. CA then boots the laptop from OS DVD (release 20161014) .	Jo	20:42:51
4.	CA sets up the laptop by following the steps below. a) Press "CTRL+ALT+F2" to get a console prompt and log in as root. b) Execute <code>system-config-display --noui</code> c) Execute <code>killall Xorg</code> d) Confirm that the external display works. e) Log in as root	Jo	20:44:04
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	Jo	20:44:35

Step	Activity	Initials	Time
6.	<p>CA inserts the new OS DVD release 20170403 into the external DVD drive, waits for it to be recognized by the OS and performs the following:</p> <p>a) Close the file system popup window</p> <p>b) Confirm the assigned drive letter by executing <code>df</code></p> <p>c) Unmount the DVD drive by executing <code>umount /dev/scd1</code></p> <p>d) Calculate the SHA-256 hash by executing <code>sha2wordlist < /dev/scd1</code></p> <p>IW1 and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.</p> <p>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.</p> <p>SHA-256: 4d127c7db1a564399c0f4e00b34d6a7611e23cdb96cd64f3a428a16319285041</p> <p>PGP Words: dreadful backwater kiwi insincere sailboat paperweight flytrap corporate python atmosphere drifter adroitness scallion disruptive Geiger impetus Athens tomorrow cobra suspicious prefer sandalwood flytrap vertigo regain cellulose ratchet Galveston bedlamp cellulose drumbeat decadence</p> <p>Note: The SHA-256 hash of the OS DVD is also published on the IANA website https://data.iana.org/ksk-ceremony/29/KC-20170403.iso.sha256</p>	JD	20:49:59
7.	CA removes the OS DVD by pressing the eject button on the external DVD drive, then places it on the ceremony table, having it visible to the audit camera and the participants.	JD	20:50:32
8.	CA repeats step 6 and 7 for the 2 nd copy of the new OS DVD release 20170403 .	JD	20:54:39
9.	<p>IW1 records the date, time then affixes his/her signature upon successful completion of the OS DVD release 20170403 acceptance testing:</p> <p>OS DVD Acceptance Test release 20170403</p> <p>Printed Name Jonathan Denison</p> <p>Date 2017/08/17</p> <p>Time <u>20:54:52</u></p> <p>Signature <u></u></p>	JD	20:54:59
10.	<p>CA disconnects the general purpose external DVD drive from the laptop, then removes the OS DVD by performing:</p> <p>a) Turn off the laptop by pressing the power switch</p> <p>b) Turn on the laptop by pressing the power switch and immediately remove the old OS DVD (release 20161014) from the laptop DVD drive</p> <p>c) Disconnect the laptop to power off</p>	JD	20:54:28
11.	CA discards all the old OS DVD (release 20161014) copies.	JD	20:57:01

Set Up Laptop

Step	Activity	Initials	Time
12.	CA boots the laptop by following the steps below. a) Connect the power supply and USB printer cable. b) Switch ON the laptop and immediately insert the new OS DVD release 20170403	JD	21:02:10
13.	CA sets up the laptop by following the steps below. a) Press "CTRL+ALT+F2" to get a console prompt and log in as root . b) Execute <code>system-config-display --noui</code> c) Execute <code>killall Xorg</code> d) Confirm that external display works. e) Log in as root	JD	21:03:58
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 <u>first device</u> "HP Laserjet xxxx" and then click the button Forward <small>Note: The xxxx is the Printer Model</small> 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	JD	21:07:31
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	JD	21:08:07
16.	CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal window, CA executes: <code>date -s "20170817 HH:MM:00"</code> where HH is two-digit Hour, MM is two digit Minutes and 00 is Zero Seconds CA executes <code>date</code> using the Terminal window to confirm the date is properly configured.	JD	21:08:53

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 OS, closes the file system popup window and formats the drive by executing <code>df</code> to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc), <code>umount /dev/sda1</code> to unmount the drive (change drive letter and partition if necessary), <code>mkfs.vfat -n HSMFD -I /dev/sda1</code> to execute a FAT32 format and label it as HSMFD. CA unplugs the FD.	jo	21:10:27
18.	CA repeats step 17 for the 2 nd blank FD	jo	21:11:17
19.	CA repeats step 17 for the 3 rd blank FD	jo	21:12:00
20.	CA repeats step 17 for the 4 th blank FD	jo	21:12:48
21.	CA repeats step 17 for the 5 th blank FD	jo	21:13:26

Connect HSMFD

Step	Activity	Initials	Time
22.	CA plugs the previous HSMFD used in the ceremony 28 into the free USB slot on the laptop and waits for OS to recognize it. CA displays the HSMFD contents to all participants then closes the file system window.	jo	21:14:40
23.	CA calculates the SHA-256 hash of the contents on the copied HSMFD by executing <code>hsmfd-hash -c</code> IW1 confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 28 annotated script (image from Ceremony 28 annotated script). SHA-256 hash: <code>cf2cecc7219eb7bfa1f176dffdc63c38dee86e510c50cf8eacc376a584b1fec</code> PGP Wordlist of the SHA-256 hash: PGP Words: stagehand Chicago tumor retraction blackjack onlooker seabird rebellion ratchet vacancy inverse therapist willow sandalwood flatfoot replica optic universe necklace travesty assume resistor ammo warranty Trojan revolver clamshell hamburger endorse disable billiard unicorn 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.	jo	21:17:23

Start Logging Terminal Session

Step	Activity	Initials	Time
24.	CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code>	jo	21:17:43
25.	CA executes <code>script script-20170817.log</code> to start a capture of terminal output.	jo	21:18:04



Start Logging HSM Output

Step	Activity	Initials	Time
26.	CA connects a serial to USB null modem cable to laptop.	jo	21:18:43
27.	CA opens a second terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal . Follow the additional steps to maximize the terminal window: a) Click the View menu and select Zoom In b) Repeat the step above as necessary and executes <code>cd /media/HSMFD</code> and executes <code>stty -F /dev/ttyUSB0 115200</code> <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.	jo	21:19:50

Power Up HSM

Step	Activity	Initials	Time
28.	CA inspects the HSM TEB for tamper evidence; reads out the TEB # and HSM serial # while IW1 observes and matches it with the prior ceremony script in this facility. HSM3: TEB# BB51184611 / serial # H1403033	jo	21:20:37
29.	CA removes and discards the TEB of the HSM, then plugs ttyUSB0 null modem serial cable to the back of the HSM.	jo	21:21:23
30.	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 the displayed HSM serial number with below. HSM3: serial # H1403033 Note: The date/time on the HSM is not used as a reference for logging and timestamp.	jo	21:22:39

Enable/Activate HSM3

Step	Activity	Initials	Time
31.	<p>One by one, CA calls each COs listed below to inspect the TEB for tamper evidence. With the help of the CA, the CO opens the TEB and hands the OP cards to the CA, then places it on the cardholder visible to everyone.</p> <p>CO 1: Arbogast Fabian OP TEB # BB46584450 107</p> <p>CO 2: Dmitry Burkov 257 OP TEB # BB46584452</p> <p>CO 5: Olafur Gudmundsson 507 OP TEB # BB46584660</p> <p>CO 6: Nicolas Antonello 607 OP TEB # BB46584458</p> <p>CO 7: Subramanian Moonesamy 707 OP TEB # BB46584460</p>		21:25:59
32.	<p>CA activates the HSM by following the steps below:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "1.Set Online", then hit ENT to confirm When "Set Online?" is displayed, then hit ENT to confirm When "Insert Card OP #?" is displayed, insert the OP card from the cardholder When "PIN?" is displayed, enter "11223344", then hit ENT When "Remove Card?" is displayed, then remove the card Repeat steps d) to f) for the 2nd and 3rd OP cards <p>Confirm the "READY" LED on the HSM is ON.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <u>1</u> of 7 2nd OP card <u>2</u> of 7 3rd OP card <u>5</u> of 7</p>		21:28:16

Check Network Connectivity Between Laptop and HSM3

Step	Activity	Initials	Time
33.	CA connects the HSM to the laptop using Ethernet cable in LAN port.	jo	21:28:59
34.	CA switches to the terminal window and tests network connectivity between laptop and HSM by executing: <code>ping 192.168.0.2</code> and looking for responses. Ctrl-C to exit program.	jo	21:29:28

Insert Copy of KSR to be Signed

Step	Activity	Initials	Time
35.	The KSR FD was transferred to the facility by the RKOS. It contains four KSRs. One is for the normal operation and three are for fallback scenarios. CA plugs the FD labeled "KSR" then waits for it to be recognized by the OS. CA points out the KSR file that will be signed on each folder, then closes the file system window.	jo	21:36:48

Execute KSR Signer for Phase D to E

Step	Activity	Initials	Time
36.	CA uses the terminal window to sign the KSR file by executing the following: <code>ksrsigner /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml</code>	jo	21:40:55
37.	The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/N): CA confirms that the HSM is online, then enters "y" to proceed.	jo	21:41:15

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
38.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room. The RZM provides identification document for the IW1 to review and retain. RZM, then reads out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. IW1 enters the RZM representative's name here: <u>ALBAINORO BOLIVAN</u>	jo	21:42:59
39.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	jo	21:43:31
40.	CA then enters "y" in response to "Is this correct y/n?" to complete the KSR signing operation. The SKR is located on <code>/media/KSR/KSK30-0-D_to_E/skr-root-2017-q4-0-d_to_e.xml</code>	jo	21:43:51

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: <div style="text-align: center;">_____</div>	JP	21:33:12
2.	IW1 Describes exception and action below.		

WHEN INSERTING THE KSR FD, IT'S POSSIBLE THE HSMFD MAY HAVE
 DISLOADED AND DISRUPTED THE SCRIPT. AS A MATTER OF PRECAUTION, CA
 CANCELLED TTYAUDIT WINDOW STARTED SECOND WINDOW FOR TTYAUDIT
 SCRIPT WINDOW (RESTARTED SCRIPT COMMAND)

* ADDITIONAL LOGS WERE PRINTED PER STEP 16 A013

- End of Root DNSSEC Script Exception -



VERISIGN™

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

August 12th, 2017

VerisignInc.com

To Whom It May Concern:

This is a letter of Verification of Employment for Alejandro A. Bolivar. Verisign, Inc. has employed Alejandro A. Bolivar full-time since September 8th, 1997, currently as a Sr. Engineer - CBO in our Product Operations organization.

Verisign is the trusted provider of Internet infrastructure services and operates the authoritative directory of all .com, .net, .cc, .tv, and .name domain names and the back-end systems for all .gov, .jobs and .edu domain names.

Verisign manages and protects the global domain name system (DNS) infrastructure for more than 113 million domain names and processes approximately 60 billion queries daily, while maintaining 100 percent operational accuracy and stability for more than a decade. Our services also help ensure that online businesses are as available as the Web itself.

As the global leader in domain names, Verisign powers the invisible navigation that takes people to where they want to go on the Internet. For more than 19 years, Verisign has operated the infrastructure for a portfolio of top-level domains that today includes .com, .net, .tv, .edu, .gov, .jobs, .name, and .cc, as well as two of the world's 13 Internet root servers. Verisign's product suite also includes Distributed Denial of Service (DDoS) Protection Services and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit Verisign.com.

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™

17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

**80ccccf481a6f5b5eff1841889b0c31cfc6ec7d4ff22def5e74a1be83b
46b8252**

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

Verisign.com

The PGP wordlist for the hash above is:

merit revolver stagehand dictator beehive hemisphere
erase finicky Zulu borderline cranky maritime puppy
article chatter Saturday southward unicorn klaxon
document uproot clergyman uncut finicky indoors
outfielder skydive Jamaica scenic Hamilton miser
enrollment

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

Starting: ksrsigner /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml (at Thu Aug 17 21:40:09 2017 UTC)

Use HSM /opt/dnssec/aep.hsmconfig?

HSM /opt/dnssec/aep.hsmconfig activated.

setenv KEYPER_LIBRARY_PATH=/opt/dnssec

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

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

HSM slot 0 included

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

HSM Information:

```
Label:          ICANNKSK
ManufacturerID: AEP Networks
Model:         Keyper 9860-2
Serial:        H1403033
```

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-07-01T00:00:00	2017-07-22T00:00:00	14796,15768	19036(Kjqmt7v)/S
2	2017-07-11T00:00:00	2017-08-01T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
3	2017-07-21T00:00:00	2017-08-11T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
4	2017-07-31T00:00:00	2017-08-21T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
5	2017-08-10T00:00:00	2017-08-31T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
6	2017-08-20T00:00:00	2017-09-10T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
7	2017-08-30T00:00:00	2017-09-20T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
8	2017-09-09T00:00:00	2017-09-30T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
9	2017-09-19T00:00:00	2017-10-10T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	15768,46809	
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	
9	2017-12-20T00:00:00	2018-01-10T00:00:00	41824,46809	

...PASSED.

SHA256 hash of KSR:

80CCCF481A6F5B5EFF1841889B0C31CFC6EC7D4FF22DEF5E74A1BE83B46B8252

>> merit revolver stagehand dictator beehive hemisphere erase finicky Zulu borderline cranky maritime puppy article chatter Saturday southward unicorn klaxon document uproot clergyman uncut finicky indoors outfielder skydive Jamaica scenic Hamilton miser enrollment <<

Reading KSK schedule "rollover(2010,2017)" from "kskschedule.json"

#	KSK Tag(CKA_LABEL)
1	19036(Kjqmt7v)/S,20326(Klajeyz)/P
2	19036(Kjqmt7v)/P,20326(Klajeyz)/S
3	19036(Kjqmt7v)/P,20326(Klajeyz)/S
4	19036(Kjqmt7v)/P,20326(Klajeyz)/S
5	19036(Kjqmt7v)/P,20326(Klajeyz)/S
6	19036(Kjqmt7v)/P,20326(Klajeyz)/S
7	19036(Kjqmt7v)/P,20326(Klajeyz)/S
8	19036(Kjqmt7v)/P,20326(Klajeyz)/S
9	19036(Kjqmt7v)/P,20326(Klajeyz)/S

Generated new SKR in /media/KSR/KSK30-0-D_to_E/skr-root-2017-q4-0-d_to_e.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	20326(Klajeyz)/S,19036(Kjqmt7v)/P
9	2017-12-20T00:00:00	2018-01-10T00:00:00	46809,41824	20326(Klajeyz)/S,19036(Kjqmt7v)/P

SHA256 hash of SKR:

C098E855190CA3DEF56B1CAA036C404E2F0127062FAFD3C3A70B39C7F277E8E0

>> slowdown narrative trauma equipment bedlamp article reform telephone vapor Hamilton befriend pedigree acne handiw ork crackdown distortion cement adviser brackish amulet cement pharmacy stapler replica repay armistice classroom re traction uproot inception trauma tobacco <<

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

Execute KSR Signer for Phase E to D

Step	Activity	Initials	Time
41.	CA uses the terminal window to sign the KSR file by executing the following: <code>ksrsigner /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml</code>	jo	21:44:44
42.	The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/N): CA confirms that the HSM is online, then enters "y" to proceed.	jo	21:44:55

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
43.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	jo	21:45:36
44.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections?"	jo	21:45:48
45.	CA then enters "y" in response to "Is this correct y/n?" to complete the KSR signing operation. The SKR is located on <code>/media/KSR/KSK30-1-E_to_D/skr-root-2017-q4-1-e_to_d.xml</code>	jo	21:46:12

Execute KSR Signer for Phase D to D

Step	Activity	Initials	Time
46.	CA uses the terminal window to sign the KSR file by executing the following: <code>ksrsigner /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d_to_d.xml</code>	jo	21:46:41
47.	The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/N): CA confirms that the HSM is online, then enters "y" to proceed.	jo	21:46:51

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
48.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	jo	21:47:34
49.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections?"	jo	21:47:43
50.	CA enters "y" in response to "Is this correct y/n?" to complete the KSR signing operation. The SKR is located on <code>/media/KSR/KSK30-2-D_to_D/skr-root-2017-q4-2-d_to_d.xml</code>	jo	21:48:03



VERISIGN™

17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

**aa23456d408436f33678fae23d81ac861782f1866f9374600f4b681d8
e5d9fec**

The PGP wordlist for the hash above is:

reward cannonball crusade hazardous crackdown Jupiter
Christmas vertigo Christmas indigo wallet tomorrow
commence inventive ribcage letterhead banjo Istanbul
unwind letterhead gremlin molasses indoors fortitude
artist disable frighten breakaway orca filament quota
unicorn

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

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

Verisign.com

```

Starting: ksrsigner /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml (at Thu Aug 17 21:44:02 2017 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
Label:          ICANNKSK
ManufacturerID: AEP Networks
Model:         Keyper 9860-2
Serial:        H1403033

```

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-07-01T00:00:00	2017-07-22T00:00:00	14796,15768	19036(Kjqmt7v)/S
2	2017-07-11T00:00:00	2017-08-01T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
3	2017-07-21T00:00:00	2017-08-11T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
4	2017-07-31T00:00:00	2017-08-21T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
5	2017-08-10T00:00:00	2017-08-31T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
6	2017-08-20T00:00:00	2017-09-10T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
7	2017-08-30T00:00:00	2017-09-20T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
8	2017-09-09T00:00:00	2017-09-30T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
9	2017-09-19T00:00:00	2017-10-10T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	15768,46809	
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	
9	2017-12-20T00:00:00	2018-01-10T00:00:00	41824,46809	

...PASSED.

SHA256 hash of KSR:

AA23456D408436F33678FAE23D81AC861782F1866F9374600F4B681D8E5D9FEC

```

>> reward cannonball crusade hazardous crackdown Jupiter Christmas vertigo Christmas indigo wallet tomorrow commence
inventive ribcage letterhead banjo Istanbul unwind letterhead gremlin molasses indoors fortitude artist disable fri
ghten breakaway orca filament quota unicorn <<

```

Reading KSK schedule "publish+(2010,2017)" from "kskschedule.json"

#	KSK Tag(CKA_LABEL)
1	19036(Kjqmt7v)/S,20326(Klajeyz)/P
2	19036(Kjqmt7v)/S,20326(Klajeyz)/P
3	19036(Kjqmt7v)/S,20326(Klajeyz)/P
4	19036(Kjqmt7v)/S,20326(Klajeyz)/P
5	19036(Kjqmt7v)/S,20326(Klajeyz)/P
6	19036(Kjqmt7v)/S,20326(Klajeyz)/P
7	19036(Kjqmt7v)/S,20326(Klajeyz)/P
8	19036(Kjqmt7v)/S,20326(Klajeyz)/P
9	19036(Kjqmt7v)/S,20326(Klajeyz)/P

Generated new SKR in /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
9	2017-12-20T00:00:00	2018-01-10T00:00:00	46809,41824	20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:

4B0A3BF8F68C47600225CA4B0C827FEDAC6CE78C79807CD13FFF1084D47C9EA4

```

>> dragnet Apollo clockwork warranty village megaton dashboard fortitude accrue caravan spellbind disable ammo Istan
bul lockup unify ribcage handiwork transit megaton jawbone intention kiwi scavenger cowbell Yucatan assume Jupiter s
teamship informant quiver Pandora <<

```

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



VERISIGN™

17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

**57f78fa5800b04e90ef37d0fbabcca5875701122851206ae1b91c7404
cb07c55**

The PGP wordlist for the hash above is:

eightball voyager payday paperweight merit armistice
adrift ultimate apple vertigo klaxon atmosphere shadow
pyramid spellbind everyday indulge hesitate Athens
candidate music backwater afflict performance beeswax
miracle soybean Dakota drainage phonetic kiwi equipment

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

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

Verisign.com

```

Starting: ksrsigner /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d_to_d.xml (at Thu Aug 17 21:46:02 2017 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
  Label:          ICANNKSK
  ManufacturerID: AEP Networks
  Model:          Keyper 9860-2
  Serial:         H1403033

```

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-07-01T00:00:00	2017-07-22T00:00:00	14796,15768	19036(Kjqmt7v)/S
2	2017-07-11T00:00:00	2017-08-01T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
3	2017-07-21T00:00:00	2017-08-11T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
4	2017-07-31T00:00:00	2017-08-21T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
5	2017-08-10T00:00:00	2017-08-31T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
6	2017-08-20T00:00:00	2017-09-10T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
7	2017-08-30T00:00:00	2017-09-20T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
8	2017-09-09T00:00:00	2017-09-30T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
9	2017-09-19T00:00:00	2017-10-10T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d_to_d.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	15768,46809	
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	
9	2017-12-20T00:00:00	2018-01-10T00:00:00	41824,46809	

...PASSED.

SHA256 hash of KSR:

57F78FA5800B04E90EF37D0FBABCCA5875701122851206AE1B91C7404CB07C55

```

>> eightball voyager payday paperweight merit armistice adrift ultimate apple vertigo klaxon atmosphere shadow pyramid
spellbind everyday indulge hesitate Athens candidate music backwater afflict performance beeswax miracle soybean
Dakota drainage phonetic kiwi equipment <<

```

Reading KSK schedule "publish+(2010,2017)" from "kskschedule.json"

- # KSK Tag(CKA_LABEL)
- 1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 2 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 3 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 4 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 5 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 6 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 7 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 8 19036(Kjqmt7v)/S,20326(Klajeyz)/P
- 9 19036(Kjqmt7v)/S,20326(Klajeyz)/P

Generated new SKR in /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d_to_d.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	20326(Klajeyz)/P,19036(Kjqmt7v)/S
9	2017-12-20T00:00:00	2018-01-10T00:00:00	46809,41824	20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:

7F5BBF9E419AA4FC42201CFC225A5F13FE96A3E4A26EE335BA41CCD1F50D96CB

```

>> lockup exodus slingshot onlooker cranky newsletter regain Wilmington crowfoot butterfat befriend Wilmington block
ade existence eyetooth barbecue woodlark monument reform tradition rebirth headwaters tissue conformist shadow decad
ence spigot scavenger vapor asteroid prefer revival <<

```

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

Execute KSR Signer for Phase C to C

Step	Activity	Initials	Time
51.	CA uses the terminal window to sign the KSR file by executing the following: <code>ksrsigner /media/KSR/KSK30-3-C_to_C/ksr-root-2017-q4-3-c_to_c.xml</code>	jo	21:48:34
52.	The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/N): CA confirms that the HSM is online, then enters "y" to proceed.	jo	21:48:46

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
53.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	jo	21:49:25
54.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections?"	jo	21:49:35
55.	CA enters "y" in response to "Is this correct y/n?" to complete the KSR signing operation. The SKR is located on <code>/media/KSR/KSK30-3-C_to_C/skr-root-2017-q4-3-c_to_c.xml</code>	jo	21:49:49

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
56.	CA prints out sufficient number of copies for participants by executing the following command on the terminal window <code>for i in \$(ls -l ksrsigner-20170817-*.log); do printlog \$i X; done</code> Note: Replace X with the number of copies for the participants.	jo	21:51:04
57.	IW1 attaches a copy of each ksrsigner log to his/her script.	jo	21:54:30



VERISIGN™

17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

**57c004641175eb804236a9ea091665c2c182720b506d4a03f527fa2b3
37e523a**

The PGP wordlist for the hash above is:

eightball recipe adrift getaway Athens impartial trouble
intention crowfoot congregate revenge undaunted Algol
bodyguard fracture repellent snapline Istanbul highchair
armistice drumbeat hazardous dogsled aggregate vapor
celebrate wallet Cherokee chisel insurgent Dupont
corrosion

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

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

Verisign.com

```

Starting: ksrsigner /media/KSR/KSK30-3-C_to_C/ksr-root-2017-q4-3-c_to_c.xml (at Thu Aug 17 21:47:56 2017 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
  Label:          ICANNKSK
  ManufacturerID: AEP Networks
  Model:          Keyper 9860-2
  Serial:         H1403033

```

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-07-01T00:00:00	2017-07-22T00:00:00	14796,15768	19036(Kjqmt7v)/S
2	2017-07-11T00:00:00	2017-08-01T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
3	2017-07-21T00:00:00	2017-08-11T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
4	2017-07-31T00:00:00	2017-08-21T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
5	2017-08-10T00:00:00	2017-08-31T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
6	2017-08-20T00:00:00	2017-09-10T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
7	2017-08-30T00:00:00	2017-09-20T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
8	2017-09-09T00:00:00	2017-09-30T00:00:00	15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S
9	2017-09-19T00:00:00	2017-10-10T00:00:00	46809,15768	20326(Klajeyz)/P,19036(Kjqmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSK30-3-C_to_C/ksr-root-2017-q4-3-c_to_c.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	15768,46809	
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	
9	2017-12-20T00:00:00	2018-01-10T00:00:00	41824,46809	

...PASSED.

SHA256 hash of KSR:

57C004641175EB804236A9EA091665C2C182720B506D4A03F527FA2B337E523A

```

>> eightball recipe adrift getaway Athens impartial trouble intention crowfoot congregate revenge undaunted Algol bo
dyguard fracture repellent snapline Istanbul highchair armistice drumbeat hazardous dogsled aggregate vapor celebrat
e wallet Cherokee chisel insurgent Dupont corrosion <<

```

Reading KSK schedule "normal(2010)" from "kskschedule.json"

```

# KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
2 19036(Kjqmt7v)/S
3 19036(Kjqmt7v)/S
4 19036(Kjqmt7v)/S
5 19036(Kjqmt7v)/S
6 19036(Kjqmt7v)/S
7 19036(Kjqmt7v)/S
8 19036(Kjqmt7v)/S
9 19036(Kjqmt7v)/S

```

Generated new SKR in /media/KSR/KSK30-3-C_to_C/skr-root-2017-q4-3-c_to_c.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2017-10-01T00:00:00	2017-10-22T00:00:00	46809,15768	19036(Kjqmt7v)/S
2	2017-10-11T00:00:00	2017-11-01T00:00:00	46809	19036(Kjqmt7v)/S
3	2017-10-21T00:00:00	2017-11-11T00:00:00	46809	19036(Kjqmt7v)/S
4	2017-10-31T00:00:00	2017-11-21T00:00:00	46809	19036(Kjqmt7v)/S
5	2017-11-10T00:00:00	2017-12-01T00:00:00	46809	19036(Kjqmt7v)/S
6	2017-11-20T00:00:00	2017-12-11T00:00:00	46809	19036(Kjqmt7v)/S
7	2017-11-30T00:00:00	2017-12-21T00:00:00	46809	19036(Kjqmt7v)/S
8	2017-12-10T00:00:00	2017-12-31T00:00:00	46809	19036(Kjqmt7v)/S
9	2017-12-20T00:00:00	2018-01-10T00:00:00	46809,41824	19036(Kjqmt7v)/S

SHA256 hash of SKR:

4EA7D9213904A03F696DA0C5D15CCD805E6720CAE190F464AC2D9585BAB181E1

```

>> drifter paragraph sugar Camelot classroom alkali ragtime customer gazelle hazardous ragtime resistor stairway fas
cinate spindle intention eyeglass graduate bison revenue tempest millionaire upshot getaway ribcage clergyman preclu
de leprosy shadow photograph minnow tolerance <<

```

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

Backup Newly Created SKR

Step	Activity	Initials	Time
58.	CA copies the contents of the KSR FD by executing the following command on the terminal window <code>cp -pR /media/KSR/*</code> Confirm overwrite by entering "y" when prompted.	JO	21:55:16
59.	CA uses the terminal window to perform the following commands: a) list the contents of the KSR FD by executing <code>ls -ltrR /media/KSR</code> b) flush the system buffers by executing <code>sync</code> c) unmount the KSR FD by executing <code>umount /media/KSR</code>	JO	21:56:22
60.	CA removes the KSR FD containing the SKR files, then gives it to the RZM representative.	JO	21:56:55

Disable/Deactivate HSM

Step	Activity	Initials	Time
61.	CA ensures to utilize the cards that were NOT used on the prior steps. CA will perform the following steps to deactivate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select " 2.Set Offline ", then hit ENT to confirm c) When " Set Offline? " is displayed, then 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 ", then hit ENT f) When " Remove Card? " is displayed, then remove the card g) Repeat steps d) to f) for the 2nd and 3rd OP cards Confirm the " READY " LED on the HSM is OFF . IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card <u>6</u> of 7 2nd OP card <u>5</u> of 7 3rd OP card <u>7</u> of 7	JO	21:59:07

Act 3. Secure Hardware and Close the Ceremony

Return HSM to TEB

Step	Activity	Initials	Time
1.	CA switches the HSM to power OFF, then disconnects the power and laptop (serial and Ethernet) connections. Note: DO NOT unplug the connections on the laptop end.	jo	22:00:19
2.	CA places the HSM into a prepared TEB, then seals it.	jo	22:01:43
3.	CA reads out the TEB # and the HSM serial #, then shows it to the participants. IW1 confirms the TEB # and HSM serial # below. HSM3: TEB# BB51184623 / serial # H1403033 CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory. CA places the HSM TEB on the equipment cart.	jo	22:02:47

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 the laptop. CA then exits out of Serial Port Activity (ttyaudit) terminal window by typing "exit", then press enter.	jo	22:03:24
5.	Terminating the logging script CA stops the logging terminal output by typing "exit", then press enter. Note: This only stops the script logging and will NOT close the terminal window.	jo	22:03:38

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA sets dotglob by executing the following command on the terminal window <code>shopt -s dotglob</code> Note: This enables copying of all files from the original HSMFD.	jo	22:04:03
7.	CA prints two copies of the hash by executing the following command on the terminal window <code>for i in \$(seq 2); do hsmfd-hash -p; done</code> Note: One copy for audit bundle and one copy for HSMFD package.	jo	22:04:32
8.	CA displays contents of HSMFD by executing the following command on the terminal window <code>ls -ltrR</code>	jo	22:05:30
9.	CA plugs a blank FD labeled HSMFD into a free USB slot on the laptop, then waits for the OS to recognize it as HSMFD_ CA closes the file system window and creates a backup of the HSMFD by executing following command on the terminal window <code>cp -pR * /media/HSMFD_</code>	jo	22:06:21
10.	CA displays the contents of HSMFD_ by executing the following command on the terminal window <code>ls -ltrR /media/HSMFD_</code>	jo	22:06:39
11.	CA matches the SHA-256 hash between the original HSMFD and the copy HSMFD by executing the following command on the terminal window <code>hsmfd-hash -m</code>	jo	22:07:12
12.	CA unmounts the HSMFD copy by executing the following command on the terminal window <code>umount /media/HSMFD_</code>	jo	22:07:21
13.	CA removes the HSMFD_ and places it on the holder.	jo	22:07:32
14.	CA repeats step 9 to 13 for the 2 nd copy.	jo	22:08:11
15.	CA repeats step 9 to 13 for the 3 rd copy.	jo	22:08:45
16.	CA repeats step 9 to 13 for the 4 th copy.	jo	22:09:28
17.	CA repeats step 9 to 13 for the 5 th copy.	jo	22:10:02

Print Logging Information

Step	Activity	Initials	Time
18.	CA prints out a hard copy of the logging information by executing the following command on the terminal window <code>enscript -2Gr -# 1 script-20170817.log</code> <code>enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20170817-*.log</code> for attachment to IW1 script. Note: Ignore the error regarding non-printable characters if prompted.	jo	22:13:07

```
# find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha2wordlist
```

SHA-256: 5f378217c62d0556dae2122c8dd32b89cf8d5167e4f9d3b512b79ab9bf2336c0

PGP Words: eyetooth consensus miser bookseller southward clergyman adult escapade surmount tomorrow atlas Chicago optic sociable briefcase matchmaker stagehand microscope drunk graduate tonic Waterloo stapler positive atlas processor pupil proximate slingshot cannonball Christmas recipe

08/17/17
22:02:58

script-20170817-2.log

```
Script started on Thu 17 Aug 2017 09:33:03 PM UTC
\033[0root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -l033[K033[K-latx
\033[00mtotal 2156
-rwxr-xr-x 1 root root 15547 Jun 9 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 40555 Jun 9 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 190 Jun 16 2010 \033[00;32mksksloDB.config.db\033[00m
-rwxr-xr-x 1 root root 2668 Jun 16 2010 \033[00;32mkskgen-20100616-211906.Log\033[0
0m
-rwxr-xr-x 1 root root 765 Jun 16 2010 \033[00;32mkskqmt7v.csv\033[00m
-rwxr-xr-x 1 root root 36864 Jun 16 2010 \033[00;32mttyaudit-ttyUSB1-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 45056 Jun 16 2010 \033[00;32mttyaudit-ttyUSB0-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 18364 Jun 16 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 4473 Jun 16 2010 \033[00;32mksksigner-20100616-214329.Log
\033[00m
-rwxr-xr-x 1 root root 196608 Jun 16 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 4096 Jun 16 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
00m
-rwxr-xr-x 1 root root 30915 Jul 8 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jul 8 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
41.3.50_ksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jul 8 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 1400 Jul 12 2010 \033[00;32mksksigner-20100712-224252.Log
\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 5506 Jul 12 2010 \033[00;32mksksigner-20100712-224426.Log
\033[00m
-rwxr-xr-x 1 root root 36885 Jul 12 2010 \033[00;32mttyaudit-ttyUSB0-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root 38221 Jul 12 2010 \033[00;32mttyaudit-ttyUSB1-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root 12956 Jul 12 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 18402 Nov 1 2010 \033[00;32mkskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jan 2 2011 \033[00;32mkskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 188 Feb 7 2011 \033[00;32mksksigner-20110207-223245.Log
\033[00m
-rwxr-xr-x 1 root root 18402 Feb 7 2011 \033[00;32mkskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5524 Feb 7 2011 \033[00;32mksksigner-20110207-223256.Log
\033[00m
-rwxr-xr-x 1 root root 13997 Feb 7 2011 \033[00;32mttyaudit-ttyUSB0-20110207-221818
.log\033[00m
-rwxr-xr-x 1 root root 20709 Feb 7 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18402 May 11 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15551 Jan 19 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18404 Jul 20 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5508 Jul 20 2011 \033[00;32mksksigner-20110720-205839.Log
\033[00m
-rwxr-xr-x 1 root root 8044 Jul 20 2011 \033[00;32mttyaudit-ttyUSB0-20110720-205811
.log\033[00m
-rwxr-xr-x 1 root root 32768 Jul 20 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18422 Sep 30 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15591 Jan 9 2012 \033[00;32mkskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18424 Feb 2 2012 \033[00;32mkskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5509 Feb 2 2012 \033[00;32mksksigner-20120202-222928.Log
\033[00m
-rwxr-xr-x 1 root root 8290 Feb 2 2012 \033[00;32mttyaudit-ttyUSB0-20120202-221813
.log\033[00m
-rwxr-xr-x 1 root root 42056 Feb 2 2012 \033[00;32mkskr-root-20120202.log\033[00m
-rwxr-xr-x 1 root root 18414 May 22 2012 \033[00;32mkskr-root-20120202.log\033[00m
-rwxr-xr-x 1 root root 15391 Jul 3 2012 \033[00;32mkskr-root-2012-q4-0.xml\033[00m
```

08/17/17
12:02:58

script-20170817-2.log

```
-rwxr-xr-x 1 root root 44497 Aug 13 2015 \033[00;32mttyaudit-ttyUSB1-20150813-220137
.log\033[00m
-rwxr-xr-x 1 root root 28755 Aug 13 2015 \033[00;32mkskr-root-20150813.log\033[00m
-rwxr-xr-x 1 root root 18314 Jan 14 2016 \033[00;32mkskr.xml.20160211235227\033[00m
-rwxr-xr-x 1 root root 15371 Jan 14 2016 \033[00;32mkskr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 11 2016 \033[00;32mkskr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5530 Feb 11 2016 \033[00;32mksrsigner-20160211-235227.log
\033[00m
-rwxr-xr-x 1 root root 12196 Feb 11 2016 \033[00;32mttyaudit-ttyUSB0-20160211-234001
.log\033[00m
-rwxr-xr-x 1 root root 6919 Feb 11 2016 \033[00;32mkskr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 17908 May 12 2016 \033[00;32mkskr.xml.20160811220932\033[00m
-rwxr-xr-x 1 root root 14301 Jul 13 2016 \033[00;32mkskr-root-2016-q4-fallback-1.xml
\033[00m
-rwxr-xr-x 1 root root 21718 Jul 13 2016 \033[00;32mkskr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18599 Jul 20 2016 \033[00;32mkskr.xml.20160811215735\033[00m
-rwxr-xr-x 1 root root 21083 Aug 11 2016 \033[00;32mkskr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5520 Aug 11 2016 \033[00;32mksrsigner-20160811-215735.log
\033[00m
-rwxr-xr-x 1 root root 17908 Aug 11 2016 \033[00;32mkskr-root-2016-q4-fallback-1.xml
\033[00m
-rwxr-xr-x 1 root root 5694 Aug 11 2016 \033[00;32mksrsigner-20160811-220932.log
\033[00m
-rwxr-xr-x 1 root root 12499 Aug 11 2016 \033[00;32mttyaudit-ttyUSB0-20160811-213430
.log\033[00m
-rwxr-xr-x 1 root root 33540 Aug 11 2016 \033[00;32mttyaudit-ttyUSB0-20160811-222510
.log\033[00m
-rwxr-xr-x 1 root root 21200 Aug 11 2016 \033[00;32mkskr-root-20160811.log\033[00m
-rwxr-xr-x 1 root root 20348 Oct 27 2016 \033[00;32mkskr.xml.201702225202\033[00m
-rwxr-xr-x 1 root root 2974 Oct 27 2016 \033[00;32mkskslotdb.db\033[00m
-rwxr-xr-x 1 root root 19586 Jan 4 2017 \033[00;32mkskr-root-2017-q2-0.xml\033[00m
drwxr-xr-x 2 root root 4096 Feb 2 2017 \033[00;32mtmp\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 \033[00;32mkskr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 \033[00;32mkskr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5494 Feb 2 2017 \033[00;32mksrsigner-20170202-225202.log
\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 \033[00;32mkeybackup-20170203-001846.log
\033[00m
-rwxr-xr-x 1 root root 2693 Feb 2 2017 \033[00;32mkskgen-20170203-001954.log\033[0
0m
-rwxr-xr-x 1 root root 817 Feb 2 2017 \033[00;32mkskslotdb.csrf\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 \033[00;32mkeybackup-20170203-003825.log
\033[00m
-rwxr-xr-x 1 root root 48066 Feb 2 2017 \033[00;32mttyaudit-ttyUSB0-20170202-223524
.log\033[00m
-rwxr-xr-x 1 root root 23999 Feb 2 2017 \033[00;32mkskr-root-20170202.log\033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:17 \033[00;32mkskr-root-20170817.log\033[00m
-rwxr-xr-x 1 root root 8192 Aug 17 21:21 \033[00;32mttyaudit-ttyUSB0-20170817-211909
.log\033[00m
drwxr-xr-x 4 root root 4096 Aug 17 21:30 \033[00;32m.. \033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:33 \033[00;32mkskr-root-20170817-2.log\033[00m
drwxr-xr-x 3 root root 16384 Aug 17 21:33 \033[00;32m.. \033[00m
\033[m\033[0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# tail\033[K; t\033[K
\033[K\033[K\033[K] ttyaud \033[00;32mttyaudit-ttyUSB0-20170817-211909.log
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000 statistics 112b
2017-08-17T21:21:28+0000 ttyUSB0
2017-08-17T21:21:28+0000 other 116b
2017-08-17T21:21:28+0000 ttyUSB0
2017-08-17T21:21:28+0000 ttyUSB0 Redstore (free/total) 109Kb/128Kb
2017-08-17T21:21:28+0000 ttyUSB0
2017-08-17T21:21:28+0000 ttyUSB0
```

```
2017-08-17T21:21:28+0000 ttyUSB0
2017-08-17T21:21:28+0000 \media/HSMFD\007[root@localhost HSMFD]# sync
\033[0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -ltr
\033[00mtotal 2164
-rwxr-xr-x 1 root root 15547 Jun 9 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 40555 Jun 9 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 190 Jun 16 2010 \033[00;32mkskslotdb.config.db\033[00m
-rwxr-xr-x 1 root root 2668 Jun 16 2010 \033[00;32mkskgen-20100616-211906.log\033[0
0m
-rwxr-xr-x 1 root root 765 Jun 16 2010 \033[00;32mkskgen7v.csrf\033[00m
-rwxr-xr-x 1 root root 36864 Jun 16 2010 \033[00;32mttyaudit-ttyUSB1-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 45056 Jun 16 2010 \033[00;32mttyaudit-ttyUSB0-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 18364 Jun 16 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 4473 Jun 16 2010 \033[00;32mksrsigner-20100616-214329.log
\033[00m
-rwxr-xr-x 1 root root 196608 Jun 16 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 4096 Jun 16 2010 \033[00;32mksrsigner-20100616-2209utc.log\033[00m
00m
-rwxr-xr-x 1 root root 30915 Jul 8 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jul 8 2010 \033[00;32mkskr-root-2010-q3-2.xml\033[00m
41.3.50.ksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jul 8 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 1400 Jul 12 2010 \033[00;32mksrsigner-20100712-224252.log
\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mkskr.xml.20100712224426\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 5506 Jul 12 2010 \033[00;32mksrsigner-20100712-224426.log
\033[00m
-rwxr-xr-x 1 root root 36885 Jul 12 2010 \033[00;32mttyaudit-ttyUSB0-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root 38221 Jul 12 2010 \033[00;32mttyaudit-ttyUSB1-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root 12956 Jul 12 2010 \033[00;32mkskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 18402 Nov 1 2010 \033[00;32mkskr.xml.20110207223256\033[00m
-rwxr-xr-x 1 root root 15547 Jan 2 2011 \033[00;32mkskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 188 Feb 7 2011 \033[00;32mksrsigner-20110207-223245.log
\033[00m
-rwxr-xr-x 1 root root 18402 Feb 7 2011 \033[00;32mkskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5524 Feb 7 2011 \033[00;32mksrsigner-20110207-223256.log
\033[00m
-rwxr-xr-x 1 root root 13997 Feb 7 2011 \033[00;32mttyaudit-ttyUSB0-20110207-221818
.log\033[00m
-rwxr-xr-x 1 root root 20799 Feb 7 2011 \033[00;32mkskr-root-20110207.log\033[00m
-rwxr-xr-x 1 root root 18402 May 11 2011 \033[00;32mkskr.xml.20110720205839\033[00m
-rwxr-xr-x 1 root root 15551 Jul 19 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18404 Jul 20 2011 \033[00;32mkskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5508 Jul 20 2011 \033[00;32mksrsigner-20110720-205839.log
\033[00m
-rwxr-xr-x 1 root root 8044 Jul 20 2011 \033[00;32mttyaudit-ttyUSB0-20110720-205011
.log\033[00m
-rwxr-xr-x 1 root root 32768 Jul 20 2011 \033[00;32mkskr-root-20110720.log\033[00m
-rwxr-xr-x 1 root root 18422 Sep 30 2011 \033[00;32mkskr.xml.20120202222928\033[00m
-rwxr-xr-x 1 root root 15591 Jan 9 2012 \033[00;32mkskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 19424 Feb 2 2012 \033[00;32mkskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5509 Feb 2 2012 \033[00;32mksrsigner-20120202-222928.log
\033[00m
-rwxr-xr-x 1 root root 8290 Feb 2 2012 \033[00;32mttyaudit-ttyUSB0-20120202-221813
.log\033[00m
-rwxr-xr-x 1 root root 42056 Feb 2 2012 \033[00;32mkskr-root-20120202.log\033[00m
-rwxr-xr-x 1 root root 18414 May 22 2012 \033[00;32mkskr.xml.20120726185458\033[00m
```


08/17/17
12:02:58

script-20170817-2.log

3

```
-rwxr-xr-x 1 root root 15391 Jul 3 2012 033[00]:32mkskr-root-2012-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18324 Jul 26 2012 033[00]:32mkskr-root-2012-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5504 Jul 26 2012 033[00]:32mksrsgner-20120726-185458.log
\033[00m
-rwxr-xr-x 1 root root 12034 Jul 26 2012 033[00]:32mttyaudit-ttyUSB0-20120726-184435
.log\033[00m
-rwxr-xr-x 1 root root 5909 Jul 26 2012 033[00]:32mkskr-root-20120726.log\033[00m
-rwxr-xr-x 1 root root 18314 Nov 12 2012 033[00]:32mkskr.xml.2013021222429\033[00m
-rwxr-xr-x 1 root root 15371 Jan 20 2013 033[00]:32mkskr-root-2013-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 12 2013 033[00]:32mkskr-root-2013-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5506 Feb 12 2013 033[00]:32mksrsgner-20130212-222429.log
\033[00m
-rwxr-xr-x 1 root root 12034 Feb 12 2013 033[00]:32mttyaudit-ttyUSB0-20130212-220521
.log\033[00m
-rwxr-xr-x 1 root root 8395 Feb 12 2013 033[00]:32mkskr-root-20130212.log\033[00m
-rwxr-xr-x 1 root root 18314 May 2 2013 033[00]:32mkskr.xml.20130807214313\033[00m
-rwxr-xr-x 1 root root 15371 Aug 5 2013 033[00]:32mkskr-root-2013-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Aug 7 2013 033[00]:32mkskr-root-2013-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5513 Aug 7 2013 033[00]:32mksrsgner-20130807-214313.log
\033[00m
-rwxr-xr-x 1 root root 8192 Aug 7 2013 033[00]:32mttyaudit-ttyUSB0-20130807-213355
.log\033[00m
-rwxr-xr-x 1 root root 5676 Aug 7 2013 033[00]:32mkskr-root-20130807.log\033[00m
-rwxr-xr-x 1 root root 18314 Oct 24 2013 033[00]:32mkskr.xml.20140213225938\033[00m
-rwxr-xr-x 1 root root 15369 Jan 14 2014 033[00]:32mkskr-root-2014-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 13 2014 033[00]:32mkskr-root-2014-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5513 Feb 13 2014 033[00]:32mksrsgner-20140213-225938.log
\033[00m
-rwxr-xr-x 1 root root 12034 Feb 13 2014 033[00]:32mttyaudit-ttyUSB0-20140213-224635
.log\033[00m
-rwxr-xr-x 1 root root 5638 Feb 13 2014 033[00]:32mkskr-root-20140213.log\033[00m
-rwxr-xr-x 1 root root 18314 Apr 17 2014 033[00]:32mkskr.xml.20140814212827\033[00m
-rwxr-xr-x 1 root root 15369 Jul 7 2014 033[00]:32mkskr-root-2014-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 0 Aug 14 2014 033[00]:32mttyaudit-ttyUSB0-20140814-211101
.log\033[00m
-rwxr-xr-x 1 root root 18314 Aug 14 2014 033[00]:32mkskr-root-2014-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5523 Aug 14 2014 033[00]:32mksrsgner-20140814-212827.log
\033[00m
-rwxr-xr-x 1 root root 12032 Aug 14 2014 033[00]:32mttyaudit-ttyUSB0-20140814-211416
.log\033[00m
-rwxr-xr-x 1 root root 5563 Aug 14 2014 033[00]:32mkskr-root-20140814.log\033[00m
-rwxr-xr-x 1 root root 18314 Nov 20 2014 033[00]:32mkskr.xml.2015012223324\033[00m
-rwxr-xr-x 1 root root 15369 Jan 13 2015 033[00]:32mkskr-root-2015-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 762 Jan 13 2015 033[00]:32mkskr-root-2015-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Jan 22 2015 033[00]:32mkskr-root-2015-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5526 Jan 22 2015 033[00]:32mksrsgner-20150122-223324.log
\033[00m
-rwxr-xr-x 1 root root 12034 Jan 22 2015 033[00]:32mttyaudit-ttyUSB0-20150122-222401
.log\033[00m
-rwxr-xr-x 1 root root 5941 Jan 22 2015 033[00]:32mkskr-root-20150122.log\033[00m
-rwxr-xr-x 1 root root 18314 Jul 28 2015 033[00]:32mkskr.xml.2015081321057\033[00m
-rwxr-xr-x 1 root root 15369 Aug 28 2015 033[00]:32mkskr-root-2015-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Aug 13 2015 033[00]:32mkskr-root-2015-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5505 Aug 13 2015 033[00]:32mksrsgner-20150813-213057.log
\033[00m
-rwxr-xr-x 1 root root 17517 Aug 13 2015 033[00]:32mttyaudit-ttyUSB0-20150813-211033
.log\033[00m
-rwxr-xr-x 1 root root 5520 Aug 13 2015 033[00]:32mksrsgner-20150814-000517.log
\033[00m
-rwxr-xr-x 1 root root 43054 Aug 13 2015 033[00]:32mttyaudit-ttyUSB0-20150813-220137
.log\033[00m
-rwxr-xr-x 1 root root 5520 Aug 13 2015 033[00]:32mksrsgner-20150814-002123.log
```

```
\033[00m
-rwxr-xr-x 1 root root 44497 Aug 13 2015 033[00]:32mttyaudit-ttyUSB1-20150813-220137
.log\033[00m
-rwxr-xr-x 1 root root 28755 Aug 13 2015 033[00]:32mkskr-root-20150813.log\033[00m
-rwxr-xr-x 1 root root 18314 Jan 14 2016 033[00]:32mkskr.xml.20160211235227\033[00m
-rwxr-xr-x 1 root root 15371 Jan 14 2016 033[00]:32mkskr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 11 2016 033[00]:32mkskr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5530 Feb 11 2016 033[00]:32mksrsgner-20160211-235227.log
\033[00m
-rwxr-xr-x 1 root root 12196 Feb 11 2016 033[00]:32mttyaudit-ttyUSB0-20160211-234001
.log\033[00m
-rwxr-xr-x 1 root root 6919 Feb 11 2016 033[00]:32mkskr-root-20160211.log\033[00m
-rwxr-xr-x 1 root root 17908 May 12 2016 033[00]:32mkskr.xml.20160811220932\033[00m
-rwxr-xr-x 1 root root 14301 Jul 13 2016 033[00]:32mkskr-root-2016-q4-fallback-1.xml
\033[00m
-rwxr-xr-x 1 root root 21718 Jul 13 2016 033[00]:32mkskr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18599 Jul 20 2016 033[00]:32mkskr.xml.20160811215735\033[00m
-rwxr-xr-x 1 root root 21083 Aug 11 2016 033[00]:32mkskr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5520 Aug 11 2016 033[00]:32mksrsgner-20160811-215735.log
\033[00m
-rwxr-xr-x 1 root root 17908 Aug 11 2016 033[00]:32mkskr-root-2016-q4-fallback-1.xml
\033[00m
-rwxr-xr-x 1 root root 5694 Aug 11 2016 033[00]:32mksrsgner-20160811-220932.log
\033[00m
-rwxr-xr-x 1 root root 12499 Aug 11 2016 033[00]:32mttyaudit-ttyUSB0-20160811-213430
.log\033[00m
-rwxr-xr-x 1 root root 33540 Aug 11 2016 033[00]:32mttyaudit-ttyUSB0-20160811-222510
.log\033[00m
-rwxr-xr-x 1 root root 21200 Aug 11 2016 033[00]:32mkskr-root-20160811.log\033[00m
-rwxr-xr-x 1 root root 20348 Oct 27 2016 033[00]:32mkskr.xml.20170202225202\033[00m
-rwxr-xr-x 1 root root 2974 Oct 27 2016 033[00]:32mkskr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 19556 Jan 4 2017 033[00]:32mkskr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 4096 Feb 2 2017 033[00]:32mkskr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 033[00]:32mkskr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 033[00]:32mkskr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5494 Feb 2 2017 033[00]:32mksrsgner-20170202-225202.log
\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 033[00]:32mkskr-root-20170203-001846.log
\033[00m
-rwxr-xr-x 1 root root 2693 Feb 2 2017 033[00]:32mkskr-root-20170203-001954.log\033[00m
-rwxr-xr-x 1 root root 817 Feb 2 2017 033[00]:32mkskr-root-20170203-003825.log
-rwxr-xr-x 1 root root 357 Feb 2 2017 033[00]:32mkskr-root-20170203-003825.log
\033[00m
-rwxr-xr-x 1 root root 48066 Feb 2 2017 033[00]:32mttyaudit-ttyUSB0-20170202-223524
.log\033[00m
-rwxr-xr-x 1 root root 23999 Feb 2 2017 033[00]:32mkskr-root-20170202.log\033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:17 2017 033[00]:32mkskr-root-20170817.log\033[00m
-rwxr-xr-x 1 root root 8192 Aug 17 21:21 2017 033[00]:32mttyaudit-ttyUSB0-20170817-211909
.log\033[00m
-rwxr-xr-x 1 root root 4096 Aug 17 21:30 033[00]:32mkskr-root-20170817-2.log\033[00m
-rwxr-xr-x 1 root root 16384 Aug 17 21:33 033[00]:32mkskr-root-20170817-2.log\033[00m
-rwxr-xr-x 1 root root 8192 Aug 17 21:33 033[00]:32mkskr-root-20170817-2.log\033[00m
\033[m\033[0]:root@localhost:/media/HSMFD\007[root@localhost HSMFD]# 033[Kksrsi\007gne
xtMedia/KSR/KSK\00730-0-D_to_E/krsr-root-2017-q4-0-d
Starting: krsrsgner /media/KSR/KSK30-0-D_to_E/krsr-root-2017-q4-0-d
g 17 21:40:09 2017 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to hsmconfig in the affirmative! (y/N): y
HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
```

08/17/17
12:02:58

script-20170817-2.log

4

```
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper 9860-2
Serial: H1403033
```

```
Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-07-01T00:00:00 2017-07-22T00:00:00 14796,15768 19036(KJgmt7v)/S
2 2017-07-11T00:00:00 2017-08-01T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
4 2017-07-31T00:00:00 2017-08-21T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
5 2017-08-10T00:00:00 2017-08-31T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
6 2017-08-20T00:00:00 2017-09-10T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
7 2017-08-30T00:00:00 2017-09-20T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
8 2017-09-09T00:00:00 2017-09-30T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
9 2017-09-19T00:00:00 2017-10-10T00:00:00 46809,15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
...VALIDATED.
```

```
Validate and Process KSR /media/KSR/KSK30-0-D_to_E/skr-root-2017-q4-0-d_to_e.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 15768,46809
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809
9 2017-12-20T00:00:00 2018-01-10T00:00:00 41824,46809
...PASSED.
```

```
SHA256 hash of KSR:
80CCCF481A6F5BEFF1841889B0C31FC6EC7D4FF22DEF5E74A1BE83B46B8252
>> merit revolver stagenhand dictator beehive hemisphere erase finicky Zulu borderline
cranky maritime puppy article chatter Saturday southward unicorn klaxon document uproo
t clergyman uncut finicky indoors outfielder skydive Jamaica scenic Hamilton miser enr
ollment <<
Is this correct (Y/N)? Y
```

```
Reading KSK schedule "rolllover(2010,2017)" from "kkskschedule.json"
# KSK Tag(CKA_LABEL)
1 19036(KJgmt7v)/S,20326(KLajeyz)/P
2 19036(KJgmt7v)/P,20326(KLajeyz)/S
3 19036(KJgmt7v)/P,20326(KLajeyz)/S
4 19036(KJgmt7v)/P,20326(KLajeyz)/S
5 19036(KJgmt7v)/P,20326(KLajeyz)/S
6 19036(KJgmt7v)/P,20326(KLajeyz)/S
7 19036(KJgmt7v)/P,20326(KLajeyz)/S
8 19036(KJgmt7v)/P,20326(KLajeyz)/S
```

```
9 19036(KJgmt7v)/P,20326(KLajeyz)/S
Generated new SKR in /media/KSR/KSK30-0-D_to_E/skr-root-2017-q4-0-d_to_e.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 46809,15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 20326(KLajeyz)/S,19036(KJgmt7v)/P
9 2017-12-20T00:00:00 2018-01-10T00:00:00 46809,41824 20326(KLajeyz)/S,19036(KJgmt7v)/P
```

```
SHA256 hash of SKR:
C098E85190CA3DEF5B1CA036C404E2F0127062FAFD3C3A70B39C7F277E9E0
>> slowdown narrative trauma equipment bedlamp article reform telephone vapor Hamilton
befriend pedigre acme handiwork crackdown distortion cement adviser brackish amulet
cement pharmacy stapler replica repay armistice classroom retraction uproot inception
trauma tobacco <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

```
***** Log output in ./ksrsigner-20170817-214009.log *****
\033[0;root@localhost:~/media/HSMFD\007[root@localhost HSMFD]# ksrsl\007gner /media/KSR
/KSK30\toE.to.D\007k\007sr-root-2017-q4-1-e_
Starting: ksrsigner /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml (at Thu Au
g 17 21:44:02 2017 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative! (Y/N): Y
```

```
HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper 9860-2
Serial: H1403033
```

```
Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-07-01T00:00:00 2017-07-22T00:00:00 14796,15768 19036(KJgmt7v)/S
2 2017-07-11T00:00:00 2017-08-01T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
4 2017-07-31T00:00:00 2017-08-21T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
5 2017-08-10T00:00:00 2017-08-31T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
6 2017-08-20T00:00:00 2017-09-10T00:00:00 15768 20326(KLajeyz)/P,19036(KJgmt7v)/S
```

08/17/17
22:02:58

script-20170817-2.log

```

7v)/S
7 2017-08-30T00:00:00 2017-09-20T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
8 2017-09-09T00:00:00 2017-09-30T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
9 2017-09-19T00:00:00 2017-10-10T00:00:00 46809,15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
...VALIDATED.

```

```

Validate and Process KSR /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 15768,46809
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809
9 2017-12-20T00:00:00 2018-01-10T00:00:00 41824,46809
...PASSED.

```

```

SHA256 hash of KSR:
AA23456d40843678FAE23D81AC861782F1866F9374600F4B681D8E5D9FEC
>> reward cannonball crusade hazardous crackdown Jupiter Christmas vertigo Christmas i
ndigo wallet tomorrow commence inventive ribcage letterhead banjo Istanbul unwind lett
erhead greenlin molasses indoors fortitude artist disable frighten breakaway orca filam
ent quota unicorn <<
Is this correct (y/N)? y

```

```

Reading KSK schedule "publish+(2010,2017)" from "kkskschedule.json"
# KSK Tag(CKA_LABEL)
1 19036(KJgmt7v)/S,20326(KLaJeyz)/P
2 19036(KJgmt7v)/S,20326(KLaJeyz)/P
3 19036(KJgmt7v)/S,20326(KLaJeyz)/P
4 19036(KJgmt7v)/S,20326(KLaJeyz)/P
5 19036(KJgmt7v)/S,20326(KLaJeyz)/P
6 19036(KJgmt7v)/S,20326(KLaJeyz)/P
7 19036(KJgmt7v)/S,20326(KLaJeyz)/P
8 19036(KJgmt7v)/S,20326(KLaJeyz)/P
9 19036(KJgmt7v)/S,20326(KLaJeyz)/P
Generated new SKR in /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 46809,15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
9 2017-12-20T00:00:00 2018-01-10T00:00:00 46809,41824 20326(KLaJeyz)/P,19036(KJgmt
7v)/S

```

```

SHA256 hash of SKR:
4B0A3BF9F68C47600225CA4B0C827FEDAC6CE78C79807CD13FFF1084D47C9EAM
>> dragnet Apollo clockwork warranty village megaton dashboard fortitude accrue carava
n spellbind disable ammo Istanbul lockup unify ribcage handiwork transit megaton jawbo
ne intention kiwi scavenger cowbell Yucatan assume Jupiter steamship informant quiver
Pandora <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

```

```

***** Log output in /ksr/signer-20170817-214402.log *****
\033[0;root@localhost:~/media/HSMFD\007[root@localhost HSMFD]# ksrsi\007gner /media/KSK
\0638RMRKSK30-2-D_to_D/ksr-root-2017-q4-2-d
Starting: karsigner /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d
g 17 21:46:02 2017 UTC
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

```

```

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper 9860-2
Serial: H1403033

```

```

Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-07-01T00:00:00 2017-07-22T00:00:00 14796,15768 19036(KJgmt7v)/S
2 2017-07-11T00:00:00 2017-08-01T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
4 2017-07-31T00:00:00 2017-08-21T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
5 2017-08-10T00:00:00 2017-08-31T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
6 2017-08-20T00:00:00 2017-09-10T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
7 2017-08-30T00:00:00 2017-09-20T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
8 2017-09-09T00:00:00 2017-09-30T00:00:00 15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
9 2017-09-19T00:00:00 2017-10-10T00:00:00 46809,15768 20326(KLaJeyz)/P,19036(KJgmt
7v)/S
...VALIDATED.

```

```

Validate and Process KSR /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d_to_d.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 15768,46809
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809
9 2017-12-20T00:00:00 2018-01-10T00:00:00 41824,46809
...PASSED.

```

08/17/17
22:02:58

```
SHA256 hash of KSR:
57F78FA5800B04E90E37D0FBABCC5875701122851206AE1B91C7404CB07C55
>> eightball voyager payday paperweight merit armistice adrift ultimate apple vertigo
klixon atmosphere shadow pyramid spellbind everyday indulge hesitate Athens candidate
music backwater afflict performance beeswax miracle soybean Dakota drainage phonetic k
lwi equipment <<
Is this correct (Y/N)? Y
```

```
Reading KSK schedule "publish+(2010,2017)" from "kkskschedule.json"
# KSK Tag(CKA_LABEL)
1 19036(KJgmt7v)/S,20326(Klajeyz)/P
2 19036(KJgmt7v)/S,20326(Klajeyz)/P
3 19036(KJgmt7v)/S,20326(Klajeyz)/P
4 19036(KJgmt7v)/S,20326(Klajeyz)/P
5 19036(KJgmt7v)/S,20326(Klajeyz)/P
6 19036(KJgmt7v)/S,20326(Klajeyz)/P
7 19036(KJgmt7v)/S,20326(Klajeyz)/P
8 19036(KJgmt7v)/S,20326(Klajeyz)/P
9 19036(KJgmt7v)/S,20326(Klajeyz)/P
Generated new SKR in /media/KSR/KSK30-2-D_to_d/skr-root-2017-q4-2-d_to_c.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 46809,15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
9 2017-12-20T00:00:00 2018-01-10T00:00:00 46809,41824 20326(Klajeyz)/P,19036(KJgmt
7v)/S
```

```
SHA256 hash of KSR:
7F5BF9E419AA4FC42201CF225A5F13FE96A3E4A26EE335BA1CCD1F50D96CB
>> lockup exodus slingshot onlooker cranky newsletter regain willington crowfoot butte
riat befriend willington blockade existence eyetooth barbecue woodlark monument reform
tradition rebirth headwaters tissue conformist shadow decadence spigot scavenger vapo
r asteroid prefer revival <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

***** Log output in ./ksrsigner-20170817-214602.log *****
\KSK30\Media\to_c\ksr-root-2017-q4-3-c_
Starting: ksrsigner /media/KSR/KSK30-3-c_to_c\ksr-root-2017-q4-3-c_to_c.xml (at Thu Au
g 17 21:47:56 2017 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
```

script-20170817-2.log

```
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper 9860-2
Serial: HI403033
Validating last SKR with HSM...
```

```
# Inception Expiration ZSK Tags
1 2017-07-01T00:00:00 2017-07-22T00:00:00 14796,15768 KSK Tag(CKA_LABEL)
2 2017-07-11T00:00:00 2017-08-01T00:00:00 15768 19036(KJgmt7v)/S
3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
4 2017-07-31T00:00:00 2017-08-21T00:00:00 15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
5 2017-08-10T00:00:00 2017-08-31T00:00:00 15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
6 2017-08-20T00:00:00 2017-09-10T00:00:00 15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
7 2017-08-30T00:00:00 2017-09-20T00:00:00 15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
8 2017-09-09T00:00:00 2017-09-30T00:00:00 15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
9 2017-09-19T00:00:00 2017-10-10T00:00:00 46809,15768 20326(Klajeyz)/P,19036(KJgmt
7v)/S
...VALIDATED.
```

```
Validate and Process KSR /media/KSR/KSK30-3-c_to_c\ksr-root-2017-q4-3-c_to_c.xml...
# Inception Expiration ZSK Tags
1 2017-10-01T00:00:00 2017-10-22T00:00:00 15768,46809 KSK Tag(CKA_LABEL)
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809 19036(KJgmt7v)/S
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
9 2017-12-20T00:00:00 2018-01-10T00:00:00 41824,46809 20326(Klajeyz)/P,19036(KJgmt
7v)/S
...PASSED.
```

```
SHA256 hash of KSR:
57C004641175EB804236A9EA091665C2C182720B506D4A03F527FA2B37B523A
>> eightball recipe adrift getaway Athens impartial trouble intention crowfoot congrog
ate revenge undaunted Algor bodyguard fracture repellent snapline Istanbul highchair a
rmistice drumbeat hazardous dogsled aggregate vapor celebrate wallet Cherokee chisel i
nsurgent Dupont corrosion <<
Is this correct (Y/N)? Y
```

```
Reading KSK schedule "normal(2010)" from "kkskschedule.json"
# KSK Tag(CKA_LABEL)
1 19036(KJgmt7v)/S
2 19036(KJgmt7v)/S
3 19036(KJgmt7v)/S
4 19036(KJgmt7v)/S
5 19036(KJgmt7v)/S
6 19036(KJgmt7v)/S
7 19036(KJgmt7v)/S
8 19036(KJgmt7v)/S
9 19036(KJgmt7v)/S
Generated new SKR in /media/KSR/KSK30-3-c_to_c\skr-root-2017-q4-3-c_to_c.xml
# Inception Expiration ZSK Tags
1 2017-10-01T00:00:00 2017-10-22T00:00:00 46809,15768 KSK Tag(CKA_LABEL)
19036(KJgmt7v)/S
```

08/17/17
22:02:58

script-20170817-2.log

7

```
2 2017-10-11T00:00:00 2017-11-01T00:00:00 46809 19036(Kjgmt7v)/S
3 2017-10-21T00:00:00 2017-11-11T00:00:00 46809 19036(Kjgmt7v)/S
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 19036(Kjgmt7v)/S
5 2017-11-10T00:00:00 2017-11-21T00:00:00 46809 19036(Kjgmt7v)/S
6 2017-11-20T00:00:00 2017-12-01T00:00:00 46809 19036(Kjgmt7v)/S
7 2017-11-30T00:00:00 2017-12-11T00:00:00 46809 19036(Kjgmt7v)/S
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 19036(Kjgmt7v)/S
9 2017-12-20T00:00:00 2018-01-10T00:00:00 46809,41,824 19036(Kjgmt7v)/S

SHA256 hash of SKR:
4EA7D9213904A03F696DA0C5D15CDD805B6720CAE190F4642CD9585BA81E181E1
>> drifter paragraph sugar Camelot classroom alkali ragtime customer gazelle hazardous
ragtime resistor stairway fascinate spindie intention eyeglass graduate bison revenue
tempest millionaire upshot getaway ribcage clergyman preclude leprosy shadow photogra
ph minnow tolerance <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

***** Log output in ./krsigner-20170817-214756.log *****
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# krsigner /media/KSR/KSK
30e3c2mb_Q9R8SfA08BfQ09326e483a[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033
[C\033[C\033[C\033[C\033[K
\033[K\033[A\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033
\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033
$! krsigner-20170817-*.log; do pA033[Krintlog
[ 1 pages * 18 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 18 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 18 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 18 copy ] sent to printer
2 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -pR /media/KSR/* *
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -la
\033[00mtotal 2244
drwxr-xr-x 7 root root 16384 Aug 17 21:54 \033[00;34m.\033[00m
drwxr-xr-x 4 root root 4096 Aug 17 21:30 \033[00;34m.. \033[00m
-rwxr-xr-x 1 root root 762 Jan 13 2015 \033[00;32mhash_ksr20.txt\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 \033[00;32mkeybackup-20170203-001846.log
\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 \033[00;32mkeybackup-20170203-003825.log
\033[00m
-rwxr-xr-x 1 root root 765 Jun 16 2010 \033[00;32mkjgmt7v.csr\033[00m
-rwxr-xr-x 1 root root 817 Feb 2 2017 \033[00;32mkjgmt7v.csr\033[00m
4096 Aug 17 21:43 \033[00;32mksr30-0-D_to_E\033[00m
drwxr-xr-x 2 root root 4096 Aug 17 21:45 \033[00;34mKSR30-0-D_to_D\033[00m
drwxr-xr-x 2 root root 4096 Aug 17 21:47 \033[00;34mKSR30-2-D_to_D\033[00m
drwxr-xr-x 2 root root 4096 Aug 17 21:49 \033[00;34mKSR30-3-C_to_C\033[00m
-rwxr-xr-x 1 root root 2668 Jun 16 2010 \033[00;32mksken-20100616-211906.log\033[0
0m
-rwxr-xr-x 1 root root 2693 Feb 2 2017 \033[00;32mksken-20170203-001954.log\033[0
0m
-rwxr-xr-x 1 root root 190 Jun 16 2010 \033[00;32mKSRslotDB.config.db\033[00m
2974 Jun 27 2016 \033[00;32mKSRslotDB.db\033[00m
-rwxr-xr-x 1 root root 15547 Jun 9 2010 \033[00;32mksr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jul 8 2010 \033[00;32mksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jul 2 2011 \033[00;32mksr-root-2011-q3-0.xml\033[00m
-rwxr-xr-x 1 root root 15551 Jun 19 2011 \033[00;32mksr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15591 Jan 9 2012 \033[00;32mksr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 15591 Jan 3 2012 \033[00;32mksr-root-2012-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15371 Jan 20 2013 \033[00;32mksr-root-2013-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 15371 Jan 5 2013 \033[00;32mksr-root-2013-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15371 Aug 5 2013 \033[00;32mksr-root-2013-q4-0.xml\033[00m

-rwxr-xr-x 1 root root 15369 Jan 14 2014 \033[00;32mksr-root-2014-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 15369 Jul 7 2014 \033[00;32mksr-root-2014-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15369 Jan 13 2015 \033[00;32mksr-root-2015-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 15369 Jul 28 2015 \033[00;32mksr-root-2015-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15371 Jan 14 2016 \033[00;32mksr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 21718 Jul 13 2016 \033[00;32mksr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 14301 Jul 13 2016 \033[00;32mksr-root-2016-q4-failback-1.xml
\033[00m
-rwxr-xr-x 1 root root 19556 Jan 4 2017 \033[00;32mksr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 4473 Jun 16 2010 \033[00;32mksrsigner-20100616-214329.log
\033[00m
-rwxr-xr-x 1 root root 1400 Jul 12 2010 \033[00;32mksrsigner-20100712-224252.log
\033[00m
-rwxr-xr-x 1 root root 5506 Jul 12 2010 \033[00;32mksrsigner-20100712-224426.log
\033[00m
-rwxr-xr-x 1 root root 188 Feb 7 2011 \033[00;32mksrsigner-20110207-223245.log
\033[00m
-rwxr-xr-x 1 root root 5524 Feb 7 2011 \033[00;32mksrsigner-20110207-223256.log
\033[00m
-rwxr-xr-x 1 root root 5508 Jul 20 2011 \033[00;32mksrsigner-20110720-205839.log
\033[00m
-rwxr-xr-x 1 root root 5509 Feb 2 2012 \033[00;32mksrsigner-20120202-222928.log
\033[00m
-rwxr-xr-x 1 root root 5504 Jul 26 2012 \033[00;32mksrsigner-20120726-185458.log
\033[00m
-rwxr-xr-x 1 root root 5506 Feb 12 2013 \033[00;32mksrsigner-20130212-222429.log
\033[00m
-rwxr-xr-x 1 root root 5513 Aug 7 2013 \033[00;32mksrsigner-20130807-214313.log
\033[00m
-rwxr-xr-x 1 root root 5513 Feb 13 2014 \033[00;32mksrsigner-20140213-225938.log
\033[00m
-rwxr-xr-x 1 root root 5523 Aug 14 2014 \033[00;32mksrsigner-20140814-212827.log
\033[00m
-rwxr-xr-x 1 root root 5526 Jan 22 2015 \033[00;32mksrsigner-20150122-223324.log
\033[00m
-rwxr-xr-x 1 root root 5505 Aug 13 2015 \033[00;32mksrsigner-20150813-213057.log
\033[00m
-rwxr-xr-x 1 root root 5520 Aug 13 2015 \033[00;32mksrsigner-20150814-000517.log
\033[00m
-rwxr-xr-x 1 root root 5520 Aug 13 2015 \033[00;32mksrsigner-20150814-002123.log
\033[00m
-rwxr-xr-x 1 root root 5530 Feb 11 2016 \033[00;32mksrsigner-20160211-225227.log
\033[00m
-rwxr-xr-x 1 root root 5520 Aug 11 2016 \033[00;32mksrsigner-20160811-215735.log
\033[00m
-rwxr-xr-x 1 root root 5694 Aug 11 2016 \033[00;32mksrsigner-20160811-220932.log
\033[00m
-rwxr-xr-x 1 root root 5494 Feb 2 2017 \033[00;32mksrsigner-20170202-225202.log
\033[00m
-rwxr-xr-x 1 root root 6645 Aug 17 21:43 \033[00;32mksrsigner-20170817-214009.log
\033[00m
-rwxr-xr-x 1 root root 6648 Aug 17 21:45 \033[00;32mksrsigner-20170817-214402.log
\033[00m
-rwxr-xr-x 1 root root 6662 Aug 17 21:47 \033[00;32mksrsigner-20170817-214602.log
\033[00m
-rwxr-xr-x 1 root root 6355 Aug 17 21:49 \033[00;32mksrsigner-20170817-214756.log
\033[00m
-rwxr-xr-x 1 root root 4096 Jun 16 2010 \033[00;32mksrsigner-20100616-2209utcc.log\033[
00m
-rwxr-xr-x 1 root root 196608 Jun 16 2010 \033[00;32mksrsigner-20100616.log\033[00m
-rwxr-xr-x 1 root root 12956 Jul 12 2010 \033[00;32mksrsigner-20100712.log\033[00m
-rwxr-xr-x 1 root root 20709 Feb 7 2011 \033[00;32mksrsigner-20110207.log\033[00m
```

08/17/17
21:02:58

script-20170817-2.log

```
-rwxr-xr-x 1 root root 32768 Jul 20 2011 \033[00;32mscript-20110720.log\033[00m
-rwxr-xr-x 1 root root 42056 Feb 2 2012 \033[00;32mscript-20120202.log\033[00m
-rwxr-xr-x 1 root root 5909 Jul 26 2012 \033[00;32mscript-20120726.log\033[00m
-rwxr-xr-x 1 root root 8365 Feb 12 2013 \033[00;32mscript-20130212.log\033[00m
-rwxr-xr-x 1 root root 5676 Aug 7 2013 \033[00;32mscript-20130807.log\033[00m
-rwxr-xr-x 1 root root 5638 Feb 13 2014 \033[00;32mscript-20140213.log\033[00m
-rwxr-xr-x 1 root root 5563 Aug 14 2014 \033[00;32mscript-20140814.log\033[00m
-rwxr-xr-x 1 root root 5941 Jan 22 2015 \033[00;32mscript-20150122.log\033[00m
-rwxr-xr-x 1 root root 28755 Aug 13 2015 \033[00;32mscript-20150813.log\033[00m
-rwxr-xr-x 1 root root 6919 Feb 11 2016 \033[00;32mscript-20160211.log\033[00m
-rwxr-xr-x 1 root root 21200 Aug 11 2016 \033[00;32mscript-20160811.log\033[00m
-rwxr-xr-x 1 root root 23999 Feb 2 2017 \033[00;32mscript-20170202.log\033[00m
-rwxr-xr-x 1 root root 40960 Aug 17 21:49 \033[00;32mscript-20170817-2.log\033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:17 \033[00;32mscript-20170817.log\033[00m
-rwxr-xr-x 1 root root 18364 Jun 16 2010 \033[00;32mskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mskr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 18402 Feb 7 2011 \033[00;32mskr-root-2011-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18404 Jul 20 2011 \033[00;32mskr-root-2011-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18424 Feb 2 2012 \033[00;32mskr-root-2012-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18324 Jul 26 2012 \033[00;32mskr-root-2012-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 12 2013 \033[00;32mskr-root-2013-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Aug 7 2013 \033[00;32mskr-root-2013-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 13 2014 \033[00;32mskr-root-2014-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Aug 14 2014 \033[00;32mskr-root-2014-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Jan 22 2015 \033[00;32mskr-root-2015-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Aug 13 2015 \033[00;32mskr-root-2015-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Feb 11 2016 \033[00;32mskr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 21083 Aug 11 2016 \033[00;32mskr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 17908 Aug 11 2016 \033[00;32mskr-root-2016-q4-fallback\x033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 \033[00;32mskr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mskr.xml.20100712224426\033[00m
-rwxr-xr-x 1 root root 18402 Nov 1 2010 \033[00;32mskr.xml.20110207232556\033[00m
-rwxr-xr-x 1 root root 18402 May 11 2011 \033[00;32mskr.xml.20110720205939\033[00m
-rwxr-xr-x 1 root root 18422 Sep 30 2011 \033[00;32mskr.xml.2012022222324\033[00m
-rwxr-xr-x 1 root root 18414 May 22 2012 \033[00;32mskr.xml.20120726185458\033[00m
-rwxr-xr-x 1 root root 18314 Nov 12 2012 \033[00;32mskr.xml.20130212222429\033[00m
-rwxr-xr-x 1 root root 18314 May 2 2013 \033[00;32mskr.xml.20130807214313\033[00m
-rwxr-xr-x 1 root root 18314 Oct 24 2013 \033[00;32mskr.xml.20140213225938\033[00m
-rwxr-xr-x 1 root root 18314 Apr 17 2014 \033[00;32mskr.xml.20140814212827\033[00m
-rwxr-xr-x 1 root root 18314 Jul 28 2014 \033[00;32mskr.xml.20150122223324\033[00m
-rwxr-xr-x 1 root root 18314 Jul 28 2015 \033[00;32mskr.xml.20150813213057\033[00m
-rwxr-xr-x 1 root root 18314 Jan 14 2016 \033[00;32mskr.xml.201602112355227\033[00m
-rwxr-xr-x 1 root root 18599 Jul 20 2016 \033[00;32mskr.xml.20160811215735\033[00m
-rwxr-xr-x 1 root root 17908 May 12 2016 \033[00;32mskr.xml.20160811220932\033[00m
-rwxr-xr-x 1 root root 20348 Oct 27 2016 \033[00;32mskr.xml.20170202225202\033[00m
-rwxr-xr-x 2 root root 4096 Aug 17 21:49 \033[00;32mtmp\033[00m
-rwxr-xr-x 1 root root 45056 Jun 16 2010 \033[00;32mttyaudit-ttyUSB0-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 36885 Jul 12 2010 \033[00;32mttyaudit-ttyUSB0-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root 13997 Feb 7 2011 \033[00;32mttyaudit-ttyUSB0-20110207-221918
.log\033[00m
-rwxr-xr-x 1 root root 8044 Jul 20 2011 \033[00;32mttyaudit-ttyUSB0-20110720-205011
.log\033[00m
-rwxr-xr-x 1 root root 8290 Feb 2 2012 \033[00;32mttyaudit-ttyUSB0-20120202-221813
.log\033[00m
-rwxr-xr-x 1 root root 12034 Jul 26 2012 \033[00;32mttyaudit-ttyUSB0-20120726-184435
.log\033[00m
-rwxr-xr-x 1 root root 12034 Feb 12 2013 \033[00;32mttyaudit-ttyUSB0-20130212-220521
.log\033[00m
-rwxr-xr-x 1 root root 8192 Aug 7 2013 \033[00;32mttyaudit-ttyUSB0-20130807-213355
.log\033[00m
-rwxr-xr-x 1 root root 12034 Feb 13 2014 \033[00;32mttyaudit-ttyUSB0-20140213-224635
.log\033[00m
-rwxr-xr-x 1 root root 0 Aug 14 2014 \033[00;32mttyaudit-ttyUSB0-20140814-211101
.log\033[00m
-rwxr-xr-x 1 root root 12032 Aug 14 2014 \033[00;32mttyaudit-ttyUSB0-20140814-211416
.log\033[00m
-rwxr-xr-x 1 root root 12034 Jan 22 2015 \033[00;32mttyaudit-ttyUSB0-20150122-222401
.log\033[00m
-rwxr-xr-x 1 root root 17517 Aug 13 2015 \033[00;32mttyaudit-ttyUSB0-20150813-211033
.log\033[00m
-rwxr-xr-x 1 root root 43054 Aug 13 2015 \033[00;32mttyaudit-ttyUSB0-20150813-220137
.log\033[00m
-rwxr-xr-x 1 root root 12196 Feb 11 2016 \033[00;32mttyaudit-ttyUSB0-20160211-234001
.log\033[00m
-rwxr-xr-x 1 root root 12499 Aug 11 2016 \033[00;32mttyaudit-ttyUSB0-20160811-213430
.log\033[00m
-rwxr-xr-x 1 root root 33540 Aug 11 2016 \033[00;32mttyaudit-ttyUSB0-20160811-222510
.log\033[00m
-rwxr-xr-x 1 root root 48066 Feb 2 2017 \033[00;32mttyaudit-ttyUSB0-20170202-223524
.log\033[00m
-rwxr-xr-x 1 root root 8192 Aug 17 21:21 \033[00;32mttyaudit-ttyUSB0-20170817-211909
.log\033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:35 \033[00;32mttyaudit-ttyUSB0-20170817-213501
.log\033[00m
-rwxr-xr-x 1 root root 36864 Jun 16 2010 \033[00;32mttyaudit-ttyUSB1-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 38221 Jul 12 2010 \033[00;32mttyaudit-ttyUSB1-20100712-212549
.log\033[00m
-rwxr-xr-x 1 root root 44497 Aug 13 2015 \033[00;32mttyaudit-ttyUSB1-20150813-220137
.log\033[00m
-rwxr-xr-x 1 root root 15547 Jul 8 2010 \033[00;32mksr_1_20100708144111_14165_198.
41.3.50_ksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 40555 Jun 9 2010 \033[00;32mksr-20100517-172720.log\033[00m
-rwxr-xr-x 1 root root 30915 Jul 8 2010 \033[00;32mksr-20100708-144111.log\033[00m
\033[m\033[0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -ltr
\033[00mtotal 2252
-rwxr-xr-x 1 root root 15547 Jun 9 2010 \033[00;32mksr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 40555 Jun 9 2010 \033[00;32mksr-20100517-172720.log\033[00m
-rwxr-xr-x 1 root root 190 Jun 16 2010 \033[00;32mksr_lotDB_config.db\033[00m
-rwxr-xr-x 1 root root 2668 Jun 16 2010 \033[00;32mksr_kgen-20100616-211906.log\033[0
0m
-rwxr-xr-x 1 root root 765 Jun 16 2010 \033[00;32mkjgmt7v.csr\033[00m
-rwxr-xr-x 1 root root 36864 Jun 16 2010 \033[00;32mttyaudit-ttyUSB1-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 45056 Jun 16 2010 \033[00;32mttyaudit-ttyUSB0-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root 18364 Jun 16 2010 \033[00;32mksr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root 4473 Jun 16 2010 \033[00;32mksrsigner-20100616-214329.log
\033[00m
-rwxr-xr-x 1 root root 196808 Jun 16 2010 \033[00;32mscript-20100616.log\033[00m
-rwxr-xr-x 1 root root 4096 Jun 16 2010 \033[00;32mscript-20100616-2209utc.log\033[
00m
-rwxr-xr-x 1 root root 30915 Jul 8 2010 \033[00;32mksr-20100708-144111.log\033[00m
-rwxr-xr-x 1 root root 15847 Jul 8 2010 \033[00;32mksr_1_20100708144111_14165_198.
41.3.50_ksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 15847 Jul 8 2010 \033[00;32mksr-root-2010-q4-1.xml\033[00m
-rwxr-xr-x 1 root root 1400 Jul 12 2010 \033[00;32mksrsigner-20100712-224252.log
\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mksr.xml.20100712224426\033[00m
-rwxr-xr-x 1 root root 18364 Jul 12 2010 \033[00;32mksr-root-2010-q4-1.xml\033[00m
```

08/17/17
22:02:58

script-20170817-2.log

-rwxr-xr-x 1 root root 5506 Jul 12 2010 \033[00;32mksrsgn-20100712-224426.log	-rwxr-xr-x 1 root root 12034 Feb 13 2014 \033[00;32mttyaudit-ttyUSB0-20140213-224635
\033[00m	.log\033[00m
-rwxr-xr-x 1 root root 36885 Jul 12 2010 \033[00;32mttyaudit-ttyUSB0-20100712-212549	-rwxr-xr-x 1 root root 5638 Feb 13 2014 \033[00;32mscript-20140213.log\033[00m
.log\033[00m	18314 Apr 17 2014 \033[00;32mksr.xml.20140814212827\033[00m
-rwxr-xr-x 1 root root 38221 Jul 12 2010 \033[00;32mttyaudit-ttyUSB1-20100712-212549	-rwxr-xr-x 1 root root 15369 Jul 7 2014 \033[00;32mksr-root-2014-q4-0.xml\033[00m
.log\033[00m	-rwxr-xr-x 1 root root 0 Aug 14 2014 \033[00;32mttyaudit-ttyUSB0-20140814-211101
-rwxr-xr-x 1 root root 12956 Jul 12 2010 \033[00;32mscript-20100712.log\033[00m	.log\033[00m
-rwxr-xr-x 1 root root 18402 Nov 1 2010 \033[00;32mksr.xml.20110720223256\033[00m	-rwxr-xr-x 1 root root 18314 Aug 14 2014 \033[00;32mksr-root-2014-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15547 Jan 2 2011 \033[00;32mksr-root-2011-q2-0.xml\033[00m	-rwxr-xr-x 1 root root 5523 Aug 14 2014 \033[00;32mksrsgn-20140814-212827.log
-rwxr-xr-x 1 root root 198 Feb 7 2011 \033[00;32mksrsgn-20110207-223245.log	\033[00m
\033[00m	-rwxr-xr-x 1 root root 12032 Aug 14 2014 \033[00;32mttyaudit-ttyUSB0-20140814-2111416
-rwxr-xr-x 1 root root 18402 Feb 7 2011 \033[00;32mksr-root-2011-q2-0.xml\033[00m	.log\033[00m
-rwxr-xr-x 1 root root 5524 Feb 7 2011 \033[00;32mksrsgn-20110207-223256.log	-rwxr-xr-x 1 root root 5563 Aug 14 2014 \033[00;32mscript-20140814.log\033[00m
\033[00m	18314 Nov 20 2014 \033[00;32mksr.xml.20150122223324\033[00m
-rwxr-xr-x 1 root root 13997 Feb 7 2011 \033[00;32mttyaudit-ttyUSB0-20110207-221818	-rwxr-xr-x 1 root root 15369 Jan 13 2015 \033[00;32mksr-root-2015-q2-0.xml\033[00m
.log\033[00m	-rwxr-xr-x 1 root root 762 Jan 13 2015 \033[00;32mksr_kst20.txt\033[00m
-rwxr-xr-x 1 root root 20709 Feb 7 2011 \033[00;32mscript-20110207.log\033[00m	-rwxr-xr-x 1 root root 18314 Jan 22 2015 \033[00;32mksr-root-2015-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18402 May 11 2011 \033[00;32mksr.xml.20110720205839\033[00m	-rwxr-xr-x 1 root root 5526 Jan 22 2015 \033[00;32mksrsgn-20150122-22324.log
-rwxr-xr-x 1 root root 15551 Jul 19 2011 \033[00;32mksr-root-2011-q4-0.xml\033[00m	\033[00m
-rwxr-xr-x 1 root root 18404 Jul 20 2011 \033[00;32mksr-root-2011-q4-0.xml\033[00m	-rwxr-xr-x 1 root root 12034 Jan 22 2015 \033[00;32mttyaudit-ttyUSB0-20150122-222401
-rwxr-xr-x 1 root root 5508 Jul 20 2011 \033[00;32mksrsgn-20110720-205839.log	.log\033[00m
\033[00m	-rwxr-xr-x 1 root root 5941 Jan 22 2015 \033[00;32mscript-20150122.log\033[00m
-rwxr-xr-x 1 root root 8044 Jul 20 2011 \033[00;32mttyaudit-ttyUSB0-20110720-205011	-rwxr-xr-x 1 root root 18314 Jul 28 2015 \033[00;32mksr.xml.20150813213057\033[00m
.log\033[00m	-rwxr-xr-x 1 root root 15369 Jul 28 2015 \033[00;32mksr-root-2015-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 32768 Jul 20 2011 \033[00;32mscript-20110720.log\033[00m	-rwxr-xr-x 1 root root 18314 Aug 13 2015 \033[00;32mksr-root-2015-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 18422 Sep 30 2011 \033[00;32mksr.xml.201202222928\033[00m	-rwxr-xr-x 1 root root 5505 Aug 13 2015 \033[00;32mksrsgn-20150813-213057.log
-rwxr-xr-x 1 root root 15591 Jan 9 2012 \033[00;32mksr-root-2012-q2-0.xml\033[00m	\033[00m
-rwxr-xr-x 1 root root 18424 Feb 2 2012 \033[00;32mksr-root-2012-q2-0.xml\033[00m	-rwxr-xr-x 1 root root 17517 Aug 13 2015 \033[00;32mttyaudit-ttyUSB0-20150813-211033
-rwxr-xr-x 1 root root 5509 Feb 2 2012 \033[00;32mksrsgn-20120202-222928.log	.log\033[00m
\033[00m	-rwxr-xr-x 1 root root 5520 Aug 13 2015 \033[00;32mksrsgn-20150814-000517.log
-rwxr-xr-x 1 root root 8290 Feb 2 2012 \033[00;32mttyaudit-ttyUSB0-20120202-221813	\033[00m
.log\033[00m	-rwxr-xr-x 1 root root 43054 Aug 13 2015 \033[00;32mttyaudit-ttyUSB0-20150813-220137
-rwxr-xr-x 1 root root 42056 Feb 2 2012 \033[00;32mscript-20120202.log\033[00m	.log\033[00m
-rwxr-xr-x 1 root root 18414 May 22 2012 \033[00;32mksr.xml.20120726165458\033[00m	-rwxr-xr-x 1 root root 5520 Aug 13 2015 \033[00;32mksrsgn-20150814-002123.log
-rwxr-xr-x 1 root root 15391 Jul 3 2012 \033[00;32mksr-root-2012-q4-0.xml\033[00m	\033[00m
-rwxr-xr-x 1 root root 18324 Jul 26 2012 \033[00;32mksr-root-2012-q4-0.xml\033[00m	-rwxr-xr-x 1 root root 44497 Aug 13 2015 \033[00;32mttyaudit-ttyUSB1-20150813-220137
-rwxr-xr-x 1 root root 5504 Jul 26 2012 \033[00;32mksrsgn-20120726-185458.log	.log\033[00m
\033[00m	-rwxr-xr-x 1 root root 28755 Aug 13 2015 \033[00;32mscript-20150813.log\033[00m
-rwxr-xr-x 1 root root 12034 Jul 26 2012 \033[00;32mttyaudit-ttyUSB0-20120726-184435	-rwxr-xr-x 1 root root 18314 Jan 14 2016 \033[00;32mksr.xml.20160211235227\033[00m
.log\033[00m	-rwxr-xr-x 1 root root 15371 Jan 14 2016 \033[00;32mksr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5909 Jul 26 2012 \033[00;32mscript-20120726.log\033[00m	-rwxr-xr-x 1 root root 18314 Feb 11 2016 \033[00;32mksr-root-2016-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 18314 Nov 12 2012 \033[00;32mksr.xml.2013021222429\033[00m	-rwxr-xr-x 1 root root 5530 Feb 11 2016 \033[00;32mksrsgn-20160211-235227.log
-rwxr-xr-x 1 root root 15371 Jan 20 2013 \033[00;32mksr-root-2013-q2-0.xml\033[00m	\033[00m
-rwxr-xr-x 1 root root 18314 Feb 12 2013 \033[00;32mksr-root-2013-q2-0.xml\033[00m	-rwxr-xr-x 1 root root 12196 Feb 11 2016 \033[00;32mttyaudit-ttyUSB0-20160211-234001
-rwxr-xr-x 1 root root 5506 Feb 12 2013 \033[00;32mksrsgn-20130212-222429.log	.log\033[00m
\033[00m	-rwxr-xr-x 1 root root 6919 Feb 11 2016 \033[00;32mscript-20160211.log\033[00m
-rwxr-xr-x 1 root root 12034 Feb 12 2013 \033[00;32mttyaudit-ttyUSB0-20130212-220521	-rwxr-xr-x 1 root root 17908 May 12 2016 \033[00;32mksr.xml.20160811220932\033[00m
.log\033[00m	-rwxr-xr-x 1 root root 14301 Jul 13 2016 \033[00;32mksr-root-2016-q4-fallback-1.xml
-rwxr-xr-x 1 root root 8385 Feb 12 2013 \033[00;32mscript-20130212.log\033[00m	\033[00m
-rwxr-xr-x 1 root root 18314 May 2 2013 \033[00;32mksr.xml.20130807214313\033[00m	-rwxr-xr-x 1 root root 21718 Jul 13 2016 \033[00;32mksr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 15371 Aug 5 2013 \033[00;32mksr-root-2013-q4-0.xml\033[00m	-rwxr-xr-x 1 root root 18599 Jul 20 2016 \033[00;32mksr.xml.20160811215735\033[00m
-rwxr-xr-x 1 root root 18314 Aug 7 2013 \033[00;32mksr-root-2013-q4-0.xml\033[00m	-rwxr-xr-x 1 root root 21083 Aug 11 2016 \033[00;32mksr-root-2016-q4-0.xml\033[00m
-rwxr-xr-x 1 root root 5513 Aug 7 2013 \033[00;32mksrsgn-20130807-214313.log	-rwxr-xr-x 1 root root 5520 Aug 11 2016 \033[00;32mksrsgn-20160811-215735.log
\033[00m	\033[00m
-rwxr-xr-x 1 root root 8192 Aug 7 2013 \033[00;32mttyaudit-ttyUSB0-20130807-213955	-rwxr-xr-x 1 root root 17908 Aug 11 2016 \033[00;32mksr-root-2016-q4-fallback-1.xml
.log\033[00m	\033[00m
-rwxr-xr-x 1 root root 5676 Aug 7 2013 \033[00;32mscript-20130807.log\033[00m	-rwxr-xr-x 1 root root 5694 Aug 11 2016 \033[00;32mksrsgn-20160811-220932.log
-rwxr-xr-x 1 root root 18314 Oct 24 2013 \033[00;32mksr.xml.20140213225938\033[00m	\033[00m
-rwxr-xr-x 1 root root 15369 Jan 14 2014 \033[00;32mksr-root-2014-q2-0.xml\033[00m	-rwxr-xr-x 1 root root 12499 Aug 11 2016 \033[00;32mttyaudit-ttyUSB0-20160811-213430
-rwxr-xr-x 1 root root 18314 Feb 13 2014 \033[00;32mksr-root-2014-q2-0.xml\033[00m	.log\033[00m
-rwxr-xr-x 1 root root 5513 Feb 13 2014 \033[00;32mksrsgn-20140213-225938.log	-rwxr-xr-x 1 root root 33540 Aug 11 2016 \033[00;32mttyaudit-ttyUSB0-20160811-222510
\033[00m	.log\033[00m

08/17/17
22:02:58

script-20170817-2.log

```

-rwxr-xr-x 1 root root 21200 Aug 11 2016 \033[00;32mscript-20160811.log\033[00m
-rwxr-xr-x 1 root root 20348 Oct 27 2016 \033[00;32mkr.xml.20170202225202\033[00m
-rwxr-xr-x 1 root root 2974 Oct 27 2016 \033[00;32mkslotdb.db\033[00m
-rwxr-xr-x 1 root root 19556 Jan 4 2017 \033[00;32mkr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 \033[00;32mkr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb 2 2017 \033[00;32mkr-root-2017-q2-0.xml\033[00m
-rwxr-xr-x 1 root root 5494 Feb 2 2017 \033[00;32mksigner-20170202-225202.log\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 \033[00;32mkeybackup-20170203-001846.log\033[00m
-rwxr-xr-x 1 root root 2693 Feb 2 2017 \033[00;32mksngen-20170203-001954.log\033[00m
-rwxr-xr-x 1 root root 817 Feb 2 2017 \033[00;32mklajeyz.csr\033[00m
-rwxr-xr-x 1 root root 357 Feb 2 2017 \033[00;32mkeybackup-20170203-003825.log\033[00m
-rwxr-xr-x 1 root root 48066 Feb 2 2017 \033[00;32mttyaudit-ttyUSB0-20170202-223524.log\033[00m
-rwxr-xr-x 1 root root 23999 Feb 2 2017 \033[00;32mscript-20170202.log\033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:17 \033[00;32mscript-20170817.log\033[00m
-rwxr-xr-x 1 root root 8192 Aug 17 21:21 \033[00;32mttyaudit-ttyUSB0-20170817-211909.log\033[00m
-rwxr-xr-x 4 root root 4096 Aug 17 21:30 \033[00;34m..033[00m
-rwxr-xr-x 1 root root 0 Aug 17 21:35 \033[00;32mttyaudit-ttyUSB0-20170817-213501.log\033[00m
-rwxr-xr-x 1 root root 6645 Aug 17 21:43 \033[00;32mksigner-20170817-214009.log\033[00m
-rwxr-xr-x 2 root root 4096 Aug 17 21:43 \033[00;34mKSK30-0-D_to_F\033[00m
-rwxr-xr-x 1 root root 6648 Aug 17 21:45 \033[00;32mksigner-20170817-214402.log\033[00m
-rwxr-xr-x 2 root root 4096 Aug 17 21:45 \033[00;34mKSK30-1-E_to_D\033[00m
-rwxr-xr-x 1 root root 6662 Aug 17 21:47 \033[00;32mksigner-20170817-214602.log\033[00m
-rwxr-xr-x 2 root root 4096 Aug 17 21:47 \033[00;34mKSK30-2-D_to_D\033[00m
-rwxr-xr-x 1 root root 4096 Aug 17 21:49 \033[00;34mtmp\033[00m
-rwxr-xr-x 1 root root 6355 Aug 17 21:49 \033[00;32mksigner-20170817-214756.log\033[00m
-rwxr-xr-x 2 root root 4096 Aug 17 21:49 \033[00;34mKSK30-3-C_to_C\033[00m
-rwxr-xr-x 7 root root 16384 Aug 17 21:54 \033[00;34m..033[00m
-rwxr-xr-x 1 root root 49152 Aug 17 21:54 \033[00;32mscript-20170817-2.log\033[00m
\033[m\033[0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -la033[KtrR /,m
\033[Km033[K033[Kmedia/KSR
\033[00m/media/KSR:
total 16
drwxr-xr-x 2 root root 4096 Aug 17 21:45 \033[00;34mKSK30-0-D_to_F\033[00m
drwxr-xr-x 2 root root 4096 Aug 17 21:45 \033[00;34mKSK30-1-E_to_D\033[00m
drwxr-xr-x 2 root root 4096 Aug 17 21:47 \033[00;34mKSK30-2-D_to_D\033[00m
drwxr-xr-x 2 root root 4096 Aug 17 21:49 \033[00;34mKSK30-3-C_to_C\033[00m
/media/KSR/KSK30-0-D_to_E:
total 104
-rwxr-xr-x 1 root root 24419 Aug 15 23:30 \033[00;32mkr.xml.20170817214009\033[00m
-rwxr-xr-x 1 root root 19556 Aug 15 23:30 \033[00;32mkr-root-2017-q4-0-d_to_e.xml\033[00m
-rwxr-xr-x 1 root root 1344 Aug 15 23:30 \033[00;32mkschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Aug 17 21:43 \033[00;32mkr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Aug 17 21:43 \033[00;32mkr-root-2017-q4-0-d_to_e.xml\033[00m
total 104
-rwxr-xr-x 1 root root 24419 Aug 15 23:30 \033[00;32mkr.xml.20170817214402\033[00m
-rwxr-xr-x 1 root root 19556 Aug 15 23:30 \033[00;32mkr-root-2017-q4-1-e_to_d.xml\033[00m

```

```

\033[00m
-rwxr-xr-x 1 root root 1344 Aug 15 23:30 \033[00;32mkschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Aug 17 21:45 \033[00;32mkr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Aug 17 21:45 \033[00;32mkr-root-2017-q4-1-e_to_d.xml\033[00m
/media/KSR/KSK30-2-D_to_D:
total 104
-rwxr-xr-x 1 root root 24419 Aug 15 23:30 \033[00;32mkr.xml.20170817214602\033[00m
-rwxr-xr-x 1 root root 19556 Aug 15 23:30 \033[00;32mkr-root-2017-q4-2-d_to_d.xml\033[00m
-rwxr-xr-x 1 root root 1344 Aug 15 23:30 \033[00;32mkschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Aug 17 21:47 \033[00;32mkr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Aug 17 21:47 \033[00;32mkr-root-2017-q4-2-d_to_d.xml\033[00m
/media/KSR/KSK30-3-C_to_C:
total 86
-rwxr-xr-x 1 root root 24419 Aug 15 23:30 \033[00;32mkr.xml.20170817214756\033[00m
-rwxr-xr-x 1 root root 19556 Aug 15 23:30 \033[00;32mkr-root-2017-q4-3-c_to_c.xml\033[00m
-rwxr-xr-x 1 root root 1148 Aug 15 23:30 \033[00;32mkschedule.json\033[00m
-rwxr-xr-x 1 root root 20347 Aug 17 21:49 \033[00;32mkr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Aug 17 21:49 \033[00;32mkr-root-2017-q4-3-c_to_c.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]# exit
exit
Script done on Thu 17 Aug 2017 10:02:58 PM UTC

```


08/17/17
21:21:28

tiyandhi-ttyUSB0-20170817-211909.log

```
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0 lastTampers bitmap: 0x0080 0b ..... 1.... .... |EXT_POWER_DOWN
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2017-08-17T21:21:21+0000 =====
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0
2017-08-17T21:21:21+0000 ttyUSB0 Running cryptoApplication at 0x8EF00000
2017-08-17T21:21:22+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2017-08-17T21:21:22+0000 ttyUSB0 Board is P2020RDB
2017-08-17T21:21:22+0000 ttyUSB0 board_smp_init: 2 cpu
2017-08-17T21:21:22+0000 ttyUSB0
2017-08-17T21:21:22+0000 ttyUSB0
2017-08-17T21:21:22+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=500000000
2017-08-17T21:21:22+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2017-08-17T21:21:23+0000 ttyUSB0 Starting next program at v0015183c
2017-08-17T21:21:23+0000 ttyUSB0 Starting K-Series Kernel
2017-08-17T21:21:23+0000 ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2017-08-17T21:21:23+0000 ttyUSB0 Thu Aug 17 20:39:17 2017
2017-08-17T21:21:23+0000 ttyUSB0 Starting audited v2.0 ... started.
2017-08-17T21:21:23+0000 ttyUSB0 Interface 0 configured for IPv6.
2017-08-17T21:21:24+0000 ttyUSB0 Interface 0 configured for IPv4.
2017-08-17T21:21:24+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2017-08-17T21:21:25+0000 ttyUSB0 add net default: gateway :: Network is unreachable
2017-08-17T21:21:25+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2017-08-17T21:21:25+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2017-08-17T21:21:25+0000 ttyUSB0 Starting USB driver...
2017-08-17T21:21:25+0000 ttyUSB0 9860 v2.3 Keyper Application - Nov 8 2013 13:17:33
2017-08-17T21:21:25+0000 ttyUSB0
2017-08-17T21:21:25+0000 ttyUSB0
```

```

2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running DES POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 DES POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running Triple DES POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Triple DES POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running AES POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 AES POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running SHA1 POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 SHA1 POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running SHA2 POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 SHA2 POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running RandomGen POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 RandomGen POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running RSA POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 RSA POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running DSA POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 DSA POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Running ECC POST Test
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 ECC POST Test Passed
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Audit on 17/8/2017 20:39:20 00100008
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Keyper 9860-2 Serial Number H1403033
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Memory Usage:
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 RAM (free/total) 197Mb/256Mb
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 Flash (free/total) 127Mb/128Mb
2017-08-17T21:21:26+0000 ttyUSB0
2017-08-17T21:21:26+0000 ttyUSB0 black store 472b

```

2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000
2017-08-17T21:21:28+0000

ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
RedStore (free/total)

statistics 112b
other 116b
109Kb/128Kb

08/17/17
22:02:32

ttysaudit-ttyUSB0-20170817-213501.log

2017-08-17T21:40:42+0000 ttyUSB0
2017-08-17T21:40:42+0000 ttyUSB0
2017-08-17T21:40:42+0000 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17T21:40:42+0000 ttyUSB0
2017-08-17T21:43:08+0000 ttyUSB0
2017-08-17T21:43:08+0000 ttyUSB0
2017-08-17T21:43:08+0000 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2017-08-17T21:43:08+0000 ttyUSB0
2017-08-17T21:44:17+0000 ttyUSB0
2017-08-17T21:44:17+0000 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17T21:44:17+0000 ttyUSB0
2017-08-17T21:44:17+0000 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2017-08-17T21:45:31+0000 ttyUSB0
2017-08-17T21:45:31+0000 ttyUSB0
2017-08-17T21:45:31+0000 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17T21:46:14+0000 ttyUSB0
2017-08-17T21:46:14+0000 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2017-08-17T21:46:14+0000 ttyUSB0
2017-08-17T21:47:17+0000 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17T21:47:17+0000 ttyUSB0
2017-08-17T21:47:17+0000 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2017-08-17T21:47:17+0000 ttyUSB0
2017-08-17T21:48:07+0000 ttyUSB0
2017-08-17T21:48:07+0000 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17T21:48:07+0000 ttyUSB0
2017-08-17T21:48:07+0000 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2017-08-17T21:49:06+0000 ttyUSB0
2017-08-17T21:49:06+0000 Audit on 17/8/2017 21:15:10 00200069 0A4000009DC6296E
2017-08-17T21:49:06+0000 ttyUSB0
2017-08-17T21:49:06+0000 Audit on 17/8/2017 21:15:39 00200069 0A4000009D86296E
2017-08-17T21:49:06+0000 ttyUSB0
2017-08-17T21:49:06+0000 Audit on 17/8/2017 21:16:10 00200069 0A400000B7C6296E
2017-08-17T21:57:17+0000 ttyUSB0
2017-08-17T21:57:17+0000 TcpListener: Closed IPv4 socket 14 on port 5000.
2017-08-17T21:58:17+0000 ttyUSB0
2017-08-17T21:58:22+0000 ttyUSB0
2017-08-17T21:58:22+0000 TcpListener: Closed IPv6 socket 15 on port 5000.
2017-08-17T21:58:22+0000 ttyUSB0
2017-08-17T21:58:22+0000 Audit on 17/8/2017 21:16:15 00100003
2017-08-17T21:58:22+0000 ttyUSB0

Place HSMFD and OS DVD into the TEB

Step	Activity	Initials	Time
19.	CA unmounts the HSMFD by executing the following commands on the terminal window <code>cd /tmp</code> <code>umount /media/HSMFD</code> CA removes the HSMFD, then places it on the holder.	jo	22:13:47
20.	CA performs the following steps to turn off the laptop. a) Turn off the laptop by pressing the power switch. b) Turn on the laptop by pressing the power switch and immediately removes the OS DVD from the laptop DVD drive. c) Disconnect power from the laptop.	jo	22:14:32
21.	CA places (2) HSMFDs, (2) OS DVD and (1) paper with printed HSMFD hash into a prepared TEB, then seals it. CA reads out the TEB #, then shows it to IW1 and participants to confirm. OS DVD (release 20170403) + HSMFD: TEB# BB46584481	jo	22:16:32
22.	CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory. CA places the OS DVD and HSMFD TEB on the equipment cart.	jo	22:16:55

Distribute HSMFDs






Step	Activity	Initials	Time
23.	CA distributes the remaining HSMFDs: Two for IW1 (for audit bundles) Two for both RKOS (for SKR exchange with RZM and for process review)	jo	22:17:26

Returning Laptop to TEB

Step	Activity	Initials	Time
24.	CA disconnects all connections to the laptop including printer, display and network, then places it into a prepared TEB, then seals it. CA reads out the TEB #, then shows it to IW1 and participants to confirm. Laptop1 (Dell ATG6400): TEB# BB51184625 / serial # 37240147333	jo	22:18:58
25.	CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory. CA places the laptop TEB on the equipment cart.	jo	22:19:17

Return OP Card to TEB

Step	Activity	Initials	Time
26.	<p>One by one, CA calls each COs listed below to the ceremony table to perform the following steps.</p> <ul style="list-style-type: none"> a) CA takes OP TEB and plastic case prepared for the CO. b) CO takes his/her OP card from the cardholder and places it inside the plastic case. c) CO gives the plastic case containing the OP card to the CA. d) CA places the plastic case into the prepared TEB, reads out the TEB # and description and then seals it. e) CA initials the TEB with a ballpoint pen, then IW1 keeps the sealing strips for later inventory. f) IW1 inspects the TEB, confirms the TEB # with the list below and then initials it with a ballpoint pen. g) CA gives the TEB containing the OP card to the CO. h) CO inspects the TEB, verifies its content, then initials it with a ballpoint pen. i) CO writes the date/time and signature on the table of IW1's script, then IW1 initials the entry. j) CO returns to his/her seat with the TEB and careful not to poke or puncture the TEB. k) Repeat steps for all the remaining COs on the list. <p>CO 1: Arbogast Fabian ✓ 187 OP TEB # BB46584476</p> <p>CO 2: Dmitry Burkov ✓ 227 OP TEB # BB46584477</p> <p>CO 5: Olafur Gudmundsson ✓ OP TEB # BB46584478</p> <p>CO 6: Nicolas Antonello ✓ OP TEB # BB46584479</p> <p>CO 7: Subramanian Moonesamy ✓ OP TEB # BB46584480</p>	<p>JP</p>	<p>22:24:00</p>

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584476	Arbogast Fabian		17 August 2017	22:21 UTC	22:21
CO 2	OP 2 of 7	BB46584477	Dmitry Burkov		17 August 2017	22:24 UTC	22
CO 5	OP 5 of 7	BB46584478	Ólafur Guðmundsson		17 August 2017	22:25 UTC	22
CO 6	OP 6 of 7	BB46584479	Nicolas Antonello		17 August 2017	22:27 UTC	22
CO 7	OP 7 of 7	BB46584480	Subramanian Moonesamy		17 August 2017	22:28 UTC	22

Returning Equipment to Safe #1

Step	Activity	Initials	Time
27.	CA, IW1, SSC1 enters the safe room with the equipment cart.	jo	22:29:58
28.	SSC1, while shielding the combination from the camera, opens Safe #1.	jo	22:31:09
29.	SSC1 removes the safe log and writes the date/time and signature on the safe log where the Open Safe is indicated. IW1 verifies the safe log entry and then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	jo	22:32:00
30.	CA CAREFULLY removes the HSM TEB from the cart, reads out the TEB # and the HSM serial #, then CAREFULLY places it inside Safe #1. CA writes the date/time and signature on the safe log where "HSM return" is indicated. IW1 verifies the safe log entry and initials it. HSM3: TEB# BB51184623 / serial # H1403033	jo	22:32:58
31.	CA removes each of the following TEBs from the equipment cart; reads out the TEB # and serial # (if applicable), then places it inside the Safe #1. CA writes the date/time and signature on the safe log where the returned item is indicated. IW1 verifies the safe log entry and initials it. Laptop1 (Dell ATG6400): TEB# BB51184625 / serial # 37240147333 OS DVD (release 20170403) + HSMFD: TEB# BB46584481	jo	22:34:16

Close Equipment Safe #1

Step	Activity	Initials	Time
32.	SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry and then initials it.	jo	22:34:41
33.	SSC1 returns the safe log back to Safe #1 and locks it (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.	jo	22:35:19
34.	CA, SSC1 and IW1 leaves the safe room with the equipment cart closing the door behind them.	jo	22:35:46

Open Credential Safe #2

Step	Activity	Initials	Time
35.	CA and IW1 brings a flashlight, then escorts SSC2, COs with their OP Card and SO Cards (if available) in TEBs into the safe room.	jo	22:36:13
36.	SSC2, while shielding combination from the camera, opens Safe #2.	jo	22:37:26
37.	SSC2 removes the safe log and writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry and then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	jo	22:38:09

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
38.	<p>One by one, the selected CO returns the TEBs of OP and SO cards (as specified on the list below) by following the steps below.</p> <ul style="list-style-type: none"> a) CO reads out their OP card TEB # and SO card TEB # (as specified on the list) and verifies its integrity b) With the assistance of the CA (and his/her common key), the CO opens his/her safe deposit box. <p>Note: Common Key is for the bottom lock. CO Key is for the top lock</p> <ul style="list-style-type: none"> c) CO reads out the safe deposit box number, verifies its integrity, places his/her TEBs inside it and then locks it. d) CO writes the date/time and signature on the safe log that indicates return of the cards. e) IW1 verifies the completed safe log entries and then initials it. <p>Repeat these steps until all the required cards listed below are returned.</p> <p>CO 1: Arbogast Fabian ✓ Box # 1791 OP TEB # BB46584476</p> <p>CO 2: Dmitry Burkov ✓ Box # 1793 OP TEB # BB46584477</p> <p>CO 5: Olafur Gudmundsson ✓ Box # 1789 OP TEB # BB46584478</p> <p>CO 6: Nicolas Antoniello ✓ Box # 1073 OP TEB # BB46584479</p> <p>CO 7: Subramanian Moonesamy ✓ Box # 1792 OP TEB # BB46584480</p>	<p style="text-align: center;">JD</p>	<p style="text-align: center;">22:44:39</p>

Close Credential Safe #2

Step	Activity	Initials	Time
39.	Once all relevant deposit boxes are closed and locked, SSC2 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry and then initials it.	jo	22:45:57
40.	SSC2 returns the safe log back to Safe #2 and then locks it (spin dial must go 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.	jo	22:46:00
41.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	jo	22:46:27

Participant Signing of IW1's Script

Step	Activity	Initials	Time
42.	CA reads the exceptions that may have occurred during the ceremony.	jo	22:47:17
43.	CA calls each attendee on the participants list to proceed to the ceremony table to confirm their printed name and date. Each attendee will sign IW1's participants list declaring that this script is a true and accurate record of the ceremony. IW1 records the completion time once all participants have signed the participants list.	jo	22:51:54
44.	CA reviews IW1's script and signs the participants list.	jo	22:53:26

Stop Online Streaming

Step	Activity	Initials	Time
45.	CA acknowledges the participation of the online participants and then notifies the SA to stop the online streaming.	jo	22:53:50


Post Ceremony Information

Step	Activity	Initials	Time
46.	CA informs onsite participants about post ceremony activities.	jo	22:58:00

Sign Out of Ceremony Room and Stop Video Recording

Step	Activity	Initials	Time
47.	RKOS ensures that all participants sign out of the Ceremony Room log and are then escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.	jo	23:04:30
48.	CA notifies the SA to stop video recording.	jo	23:05:01

Bundle Audit Materials

Step	Activity	Initials	Time
49.	<p>IW1 makes (1) copy of his/her script for off-site audit bundle.</p> <p>Each Audit bundle contains:</p> <ul style="list-style-type: none"> 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 System and Intrusion Detection System (Range is 02/02/2017 – 08/17/2017) e) IW1 attestation (Section A.1) f) SA attestation (Sections A.2 and A.3) <p>All TEBs are labeled "Root DNSSEC KSK Ceremony 30", dated and signed by IW1 and CA. An off-site audit bundle is delivered to an off-site storage. The CA holds the ultimate responsibility to finalize the audit bundle collection</p>		<p>2017/08/18</p> <p>00:42:00</p>

All remaining participants sign out of ceremony room log and leave.

Audit Bundle Checklist:

1. Output of Signer System (CA)

One electronic copy (physical flash drive) of the HSMFD in each audit bundle. Each bundle is placed inside a tamper-evident bag that is 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 is for the original audit bundle and the other as a duplicate.

4. Logs from the Physical Access Control System (PACS) and Intrusion Detection System (IDS) (SA1)

One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PACS and IDS configuration review, the list of enrolled users, the event log and configuration audit log files are contained in each audit bundle. Each audit bundle is placed in a tamper-evident bag that is 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 System 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. Ensure 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.

Jonathan Denison



Date: 18 August 2017

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 **2 February 2017 00:00 UTC** to now.

Connor Barthold



Date: 18 August 2017

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: 18 August 2017

```
cbarthold@sr> show configuration { no-more
## Last commit: 2017-01-12 22:30:47 UTC by jjenkins
version 12.1X46-D35.1;
system {
  host-name sr;
  domain-name sks.lax.dns.icann.org;
  location {
    country-code US;
    postal-code 90245;
    building Equinix-LA3;
    floor 1;
    rack 1;
  }
  ports {
    console {
      log-out-on-disconnect;
      type vt100;
    }
  }
  root-authentication {
    encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
  }
  name-server {
    8.8.8.8;
    8.8.4.4;
  }
  login {
    user bmartin {
      full-name "Brian Martin";
      uid 2005;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECR
ET-DATA
      }
    }
    user cbarthold {
      full-name "Connor A. Barthold";
      uid 2004;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECR
ET-DATA
      }
    }
    user jjenkins {
      full-name "Josh Jenkins";
      uid 2007;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX " ## SECR
ET-DATA
      }
    }
    user rquinn {
      full-name "Reed Quinn";
      uid 2003;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX " ## SECR
ET-DATA
      }
    }
  }
  services {
    ssh {
      root-login deny;
    }
    netconf {
      ssh;
    }
  }
  syslog {
    archive size 100k files 3;
    user * {
      any emergency;
    }
    file messages {
      any critical;
      authorization info;
    }
    file interactive-commands {
      interactive-commands error;
    }
  }
  max-configurations-on-flash 5;
  max-configuration-rollback 20;
  license {
    autoupdate {
      url https://ae1.juniper.net/junos/key_retrieval;
```



```

    }
  }
  ntp {
    server 129.6.15.28;
    server 129.6.15.29;
  }
}
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";
  /* Not available at KMF-West */
  disable;
}
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 192.0.35.202/26;
    }
  }
}
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 10.4.28.193/26;
    }
  }
  unit 1 {
    family inet {
      address 10.4.28.129/26;
    }
  }
  unit 2 {
    family inet {
      address 10.4.28.1/25;
    }
  }
}
routing-options {
  static {
    route 0.0.0.0/0 next-hop 192.0.35.201;
    route 10.4.29.0/24 next-hop st0.1;
    route 152.194.1.148/32 next-hop 192.0.35.201;
  }
}
policy-options {
  prefix-list resolver-servers {
    8.8.4.4/32;
    8.8.8.8/32;
  }
  prefix-list local-prefixes {
    10.4.28.0/24;
  }
  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 "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
    }
    gateway Gateway-to-KMF-East {
      ike-policy ike-policy-KMF;
      address 152.194.1.148;
      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-East {
  bind-interface st0.1;
  ike {
    gateway Gateway-to-KMF-East;
    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 vldco {
  policy access-to-video {
    match {
      source-address IMS;
      destination-address kmf_west_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_east_acs kmf_east_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 allow-access-access {
  match {
    source-address kmf_west_access;
    destination-address kmf_east_access;
    application any;
  }
  then {
    permit;
  }
}
}
from-zone ipsec to-zone access {
  policy allow-ipsec-to-access {
    match {
      source-address [ kmf_east_acs kmf_east_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 allow-access-access {
  match {
    source-address kmf_east_access;
    destination-address kmf_west_access;
    application any;
  }
  then {
    permit;
  }
}
}
}

```

```
from-zone video to-zone ipsec {
  policy allow-video-to-ipsec {
    match {
      source-address VSS;
      destination-address kmf_east_vss;
      application any;
    }
    then {
      permit;
      log {
        session-close;
      }
    }
  }
}
policy allow-access-video {
  match {
    source-address kmf_west_video;
    destination-address kmf_east_video;
    application any;
  }
  then {
    permit;
  }
}
}
from-zone guest to-zone untrust {
  policy allow-guest-to-untrust {
    match {
      source-address kmf_west_guest;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
}
from-zone wifi to-zone untrust {
  policy allow-wifi-to-untrust {
    match {
      source-address kmf_west_wifi;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
}
from-zone ipsec to-zone video {
  policy allow-ipsec-to-video {
    match {
      source-address kmf_east_vss;
      destination-address VSS;
      application any;
    }
    then {
      permit;
      log {
        session-close;
      }
    }
  }
}
policy allow-icmp {
  match {
    source-address any;
    destination-address any;
    application any;
  }
  then {
    permit;
  }
}
}
policy allow-access-video {
  match {
    source-address kmf_east_video;
    destination-address kmf_west_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;
    }
}
}
from-zone video to-zone video {
    policy allow-ntp {
        match {
            source-address any;
            destination-address video-ntp-server;
            application Junos-ntp;
        }
        then {
            permit;
        }
    }
}
default-policy {
    deny-all;
}
}
zones {
    security-zone access {
        address-book {
            address ACS 10.4.28.203/32;
            address ACC 10.4.28.202/32;
            address IDP 10.4.28.201/32;
            address EVM 10.4.28.200/32;
            address IMS 10.4.28.204/32;
            address E1 10.4.28.210/32;
            address E3 10.4.28.212/32;
            address E4 10.4.28.213/32;
            address kmf_west_access 10.4.28.192/26;
            address localnet 10.4.28.0/24;
            address-set iris-scanners {
                address E1;
                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_west_video 10.4.28.128/26;
        address VSS 10.4.28.150/32;
        address C1 10.4.28.151/32;
    }
}

```

```

address C2 10.4.28.152/32;
address C3 10.4.28.153/32;
address video-ntp-server 10.28.4.129/32;
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 10.4.28.20/32;
    address VCC 10.4.28.22/32;
    address kmf_west_guest 10.4.28.0/25;
  }
  interfaces {
    vlan.2 {
      host-inbound-traffic {
        system-services {
          ping;
        }
      }
    }
  }
}
}
security-zone ipsec {
  address-book {
    address kmf_east_access 10.4.29.192/26;
    address kmf_east_video 10.4.29.128/26;
    address kmf_east_acs 10.4.29.204/32;
    address kmf_east_acc 10.4.29.202/32;
    address kmf_east_ldp 10.4.29.201/32;
    address kmf_east_evm 10.4.29.200/32;
    address kmf_east_ims 10.4.29.203/32;
    address kmf_east_E1 10.4.29.210/32;
    address kmf_east_E2 10.4.29.211/32;
    address kmf_east_E3 10.4.29.212/32;
    address kmf_east_E4 10.4.29.213/32;
    address kmf_east_vss 10.4.29.150/32;
    address kmf_east_C1 10.4.29.151/32;
    address kmf_east_C2 10.4.29.152/32;
    address kmf_east_C3 10.4.29.153/32;
  }
  interfaces {
    st0.1 {
      host-inbound-traffic {
        system-services {
          ping;
          lke;
          ssh;
        }
      }
    }
  }
}
}
security-zone wifi {
  address-book {
    address kmf_west_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-exceede
d ];
    }
    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-ispsec-esp {
    from {
        protocol esp;
    }
    then accept;
}
term allow-ispsec-udp {
    from {
        protocol udp;
        port 500;
    }
    then accept;
}
term allow-ssh {
    from {
        source-address {
            152.194.1.148/32;
            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;
    }
  }
}
```