Root DNSSEC KSK Ceremony 29

Thursday April 27, 2017

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

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

Abbreviations

AUD =	Third Party Auditor	**CA =**	Ceremony Administrator	**CO =**	Crypto Officer
EW =	External Witness	**FD =**	Flash Drive	**HSM =**	Hardware Security Module
IW =	Internal Witness	**KSR =**	Key Signing Request	**OP =**	Operator
PTI =	Public Technical Identifiers	**RKOS =**	RZ KSK Operations Security	**RZM =**	Root Zone Maintainer
SA =	System Administrator	**SKR =**	Signed Key Response	**SO =**	Security Officer
SSC =	Safe Security Controller	**SW =**	Staff Witness		

TEB = Tamper Evident Bag (AMPAC, item #GCS1013,item #GCS0912 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20

Participants

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

Title	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		27 April 2017	20:07
IW1	Shauna Royston / ICANN			
SSC1	James Cole / ICANN			
SSC2	Derek Ellison / ICANN			
CO3	Olaf Kolkman / NL			
CO4	Robert Seastrom / US			
CO5	Christopher Griffiths / US			
CO6	Gaurab Upadhaya / NP			
CO7	Alain Aina / TG			
RZM	Alejandro Bolivar / Verisign			
RZM	Alex Brown / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Fonkam Teda / PricewaterhouseCoopers			
AUD	Eugene Jeong / PricewaterhouseCoopers			
SA1	Connor Barthold / ICANN			
SA2	Reed Quinn / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Matt Larson / ICANN			
SW	Kim Davies / PTI			
SW	LV McCoy / PTI			
EW	Dustin Phillips			
EW	Timothy McGinnis			
EW	Joseph Abley			
EW	Ashley Heineman			
EW	Sascha Sporschill			
EW	Anne Wang			

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

Note: Dual Occupancy is enforced. CA leads the ceremony. Only CAs, IWs, or SAs can enter the ceremony room and/or escort other participants. Only CA+IW can enter safe room and/or escort other participants. CAs, SAs or IWs may let individuals out of the ceremony room but only when CA+IW remain in the ceremony room. No one may leave when CA+IW are inside the safe room. Participants must sign in and out of the ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before the completion of the ceremony. The SA starts filming before the participants enter the room.

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

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

Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.	SR	17:00
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the participants list on Page 2.	SR	17:01

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	SR	17:02
4.	CA explains the use of personal electronic devices during ceremony.	SR	17:03
5.	CA briefly explains the purpose of the ceremony.	SR	17:04

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: 27 APR 2017 17:04 All entries into this script or any logs should follow this common source of time.	SR	17:04

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 brings a flashlight then escorts SSC2, COs into the safe room.	SR	17:06
8.	SSC2, while shielding combination from camera, opens Safe #2.	SR	17:07
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.	SR	17:09

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	One by one, the selected CO retrieves the required OP TEB and SO TEB (as specified on the list below) by following the steps. a) With the assistance of the CA (and his/her common key), the CO opens her/his safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock** b) CO verifies the integrity of the safe deposit box, reads out its number, then removes his/her OP TEB and SO TEB c) CO reads out the TEB #s, then verifies its integrity. d) CO retains OP TEB and SO TEB (as specified below) then locks the box. e) CO writes date/time and signature on the safe log where the removal of their TEBs are indicated. f) IW1 verifies the completed safe log entries then initials it. Repeat these steps until all required cards listed below are removed. **CO 3: Olaf Kolkman** **Box # 1239** OP TEB # **BB46584593 (Retain)** ✓ SO TEB # **BB46584594 (Check and Return)** ✓ **CO 4: Robert Seastrom** **Box # 1260** OP TEB # **BB46584595 (Retain)** ✓ SO TEB # **BB46584596 (Check and Return)** ✓ **CO 5: Christopher Griffiths** **Box # 1240** OP TEB # **BB46584597 (Retain)** ✓ SO TEB # **BB46584598 (Check and Return)** ✓ **CO 6: Gaurab Upadhaya** **Box # 1261** OP TEB # **BB46584298 (Retain)** ✓ SO TEB # **BB21907207 (Check and Return)** ✓ **CO 7: Alain Aina** **Box # 1242** OP TEB # **BB46584599 (Retain)** ✓ SO TEB # **BB46584600 (Check and Return)** ✓	SR	17:23 17

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.	SR	17:23
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.	SR	17:24
13.	IW1, CA, SSC2, and COs leave safe room, with OP TEB and SO TEB (if applicable), closing the door behind them.	SR	17:25

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	SR	17:26
15.	SSC1, while shielding combination from camera, opens Safe #1.	SR	17:28
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.	SR	17:29

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	**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. **HSM3: TEB# BB24646656 / serial # H1403032** CA verifies the integrity of the other HSM that will not be used, then returns it in the safe. **HSM4: TEB# BB24646654 / serial # H1411011**	SR	17:32
18.	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. **Laptop1 (Dell ATG6400): TEB# BB24646657 / serial # 41593712005** **OS DVD (release 20161014) + HSMFD: TEB# BB46584601** CA verifies the integrity of the other laptop that will not be used this time and return it to the safe. **Laptop2 (Dell ATG6400): TEB# BB24646655 / serial # 35063364997**	SR	17:35

Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	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.	SR	17:36
20.	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.	SR	17:36
21.	CA, SSC1 and IW1 leaves the safe room with the equipment cart, closing the door behind them.	SR	17:37

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# BB24646657 / serial # 41593712005**	SR	17:39
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# BB46584601**	SR	17:40
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).**	SR	17:46
4.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. ✓ b) CA executes `system-config-display --noui` ✓ c) CA executes `killall Xorg` ✓ d) CA confirms that external display works. ✓ e) CA logs in as root	SR	17:47
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	SR	17:48

Step	Activity	Initials	Time

6.	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:
	a) Close the file system popup window
	b) Confirm the assigned drive letter by executing
	`df`
	c) Unmount the DVD drive by executing
	`umount /dev/sdl`
	d) Calculate the SHA-256 hash by executing
	`sha2wordlist < /dev/sdl`
	
	IW1 and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.
	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.
	SHA-256:
	4d127c7db1a564399c0f4e00b34d6a7611e23cdb96cd64f3a428a16319285041
	
	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
	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
		SR	17:53

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.	SR	17:54
8.	CA repeats step 6 and 7 for the 2nd copy of the new OS DVD **release 20170403**.	SR	17:58
9.	IW1 records the date, time then affixes his/her signature upon successful completion of the OS DVD release **20170403** acceptance testing: **OS DVD Acceptance Test release 20170403** **Printed Name** **Shauna Royston** **Date** **2017/04/27** **Time** 17:59 **Signature** Shauna Royston	SR	17:59
10.	CA disconnects the general purpose external DVD drive from the laptop, then removes the OS DVD by performing: a) Turn off the laptop by pressing the power switch b) Turn on the laptop by pressing the power switch and immediately remove the old OS DVD **(release 20161014)** from the laptop DVD drive c) Disconnect the laptop to power off	SR	18:00
11.	CA discards all the old OS DVD **(release 20161014)** copies.	SR	18:01

Set Up Laptop

Step	Activity	Initials	Time
12.	CA connects the laptop power, printer and boots the laptop using the new **OS DVD release 20170403**.	SR	18:04
13.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes `system-config-display --noui` c) CA executes `killall Xorg` d) CA confirms that external display works. e) CA logs in as root	SR	18:06
14.	CA confirms that the printer is connected then configures printer as default and prints test page by going to **System > Administration > Printing** And follow the steps below: a) Click the **New Printer** icon (left side), leave everything default and then click the button **Forward** b) Under "Select Connection" choose the first device "**HP Laserjet xxxx**" and then click the button **Forward** **Note:** The xxxx is the Printer Model c) Select **HP** and click the button **Forward** d) Under "Models" scroll up and select **"Laserjet"**, and then click the button **Forward** e) Click the button **Apply** to finish f) Under "Local Printers" from the left menu, select "**printer**" g) Click the button **"Make Default Printer"** and **"Print Test Page"** h) Close the printer setup windows	SR	18:08
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	SR	18:08
16.	CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal window, CA executes: `date -s "20170427 HH:MM:00"` where **HH** is two-digit Hour, **MM** is two digit Minutes and **00** is Zero Seconds CA executes `date` using the Terminal window to confirm the date is properly configured.	SR	18:09

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
	`df`
	to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc),
	`umount /dev/sda1`
	to unmount the drive (change drive letter and partition if necessary),
	`mkfs.vfat -n HSMFD -I /dev/sda1`
	to execute a FAT32 format and label it as HSMFD.
	CA unplugs the FD.
		SR	18:11

18.	CA repeats step 17 for the 2nd blank FD	SR	18:11
19.	CA repeats step 17 for the 3rd blank FD	SR	18:12
20.	CA repeats step 17 for the 4th blank FD	SR	18:13
21.	CA repeats step 17 for the 5th blank FD	SR	18:13

Connect HSMFD

Step	Activity	Initials	Time
22.	CA plugs the previous HSMFD used in the **ceremony 27** 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.	SR	18:15

23.	CA calculates the SHA-256 hash of the contents on the copied HSMFD by executing
	`hsmfd-hash -c`
	IW1 confirms that the result matches the SHA-256 hash of the HSMFD from the **Ceremony 27** annotated script (image from Ceremony 27 annotated script).
	
	SHA-256 hash:
	`1c668e831efca9059d4cdc69c7be1a0f2b042e84cd833566de040ba950894538`
	
	PGP Wordlist of the SHA-256 hash:
	`PGP Words: befriend gossamer orca Jamaica berserk Wilmington revenge almighty quadrant disbelief sweatband guitarist soybean racketeer beehive atmosphere briefcase alkali buzzard Jupiter spindle Jamaica chopper gossamer tactics alkali alone passenger drumbeat matchmaker crusade consulting`
	
	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.
		SR	18:17

Start Logging Terminal Session

Step	Activity	Initials	Time
24.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`	SR	18:18
25.	CA executes `script script-20170427.log` to start a capture of terminal output.	SR	18:18

Start Logging HSM Output

Step	Activity	Initials	Time
26.	CA connects a serial to USB null modem cable to laptop.	SR	18:19

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
	`cd /media/HSMFD`
	and executes
	`stty -F /dev/ttyUSB0 115200`
	`ttyaudit /dev/ttyUSB0`
	to start logging HSM serial port outputs. Note: **DO NOT** unplug USB serial port from laptop as this causes logging to stop.
		SR	18:20

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# BB24646656 / serial # H1403032**	SR	18:22
29.	CA removes and discards the TEB of the HSM, then plugs ttyUSB0 null modem serial cable to the back of the HSM.	SR	18:23
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 # H1403032** **Note: The date/time on the HSM is not used as a reference for logging and timestamp.**	SR	18:24

Enable/Activate HSM3

Step	Activity	Initials	Time
31.	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. **CO 3: Olaf Kolkman** OP TEB # **BB46584593** **CO 4: Robert Seastrom** OP TEB # **BB46584595** **CO 5: Christopher Griffiths** OP TEB # **BB46584597** **CO 6: Gaurab Upadhaya** OP TEB # **BB46584298** **CO 7: Alain Aina** OP TEB # **BB46584599**	SR	18:31
32.	CA activates the **HSM** by following the steps below: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, then hit **ENT** to confirm c) When **"Set Online?"** 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 **ON.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card 3 of 7 2nd OP card 4 of 7 3rd OP card 5 of 7	SR	18:34

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.	SR	18:35
34.	CA switches to the terminal window and tests network connectivity between laptop and HSM by executing: `ping 192.168.0.2` and looking for responses. Ctrl-C to exit program.	SR	18:36

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 three KSRs. One is for the normal operation and two 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.	SR	18:37

Execute KSR Signer for Phase C to D

Step	Activity	Initials	Time
36.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK29-0-C_to_D/ksr-root-2017-q3-0-c_to_d.xml`	SR	18:39
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.	SR	18:39

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: ALEJANDRO BOLIVAR	SR	18:42
39.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	SR	18:43
40.	CA then enters "`y`" in response to "`Is this correct y/n?`" to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK29-0-C_to_D/skr-root-2017-q3-0-c_to_d.xml`	SR	18:44

VERISIGN

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

Verisigninc.com

April 26th, 2017

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

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

VerisignInc.com

27 April, 2017

The SHA256 hash of the 2017 Q3 KSR file is:

1b8539fbcd3e684b86868fa64bb4ad150fa41686123866a92008eb43942f74f0

The PGP wordlist for the hash above is:

beeswax leprosy classroom Wichita spindle cumbersome
frighten disable necklace letterhead payday paragon
dragnet politeness ringbolt bifocals artist Pandora
backward letterhead atlas consulting framework passenger
bison antenna trouble decimal Pluto combustion indoors
upcoming

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

VERISIGN

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

VerisignInc.com

27 April, 2017

The SHA256 hash of the 2017 Q3 KSR file is:

4bd72ada163b305e8f723ff8de343cb2c0439bfef7d92e7834e51370a636b116

The PGP wordlist for the hash above is:

dragnet stethoscope brickyard surrender backward
councilman chairlift finicky payday holiness cowbell
warranty tactics confidence cobra pioneer slowdown
decimal puppy yesteryear virus supportive buzzard indigo
choking travesty Aztec hesitate rematch congregate
sailboat bodyguard

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

VERISIGN

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

VerisignInc.com

27 April, 2017

The SHA256 hash of the 2017 Q3 KSR file is:

60284f8d207a2d7f673d6dfe72b5f95af07bfed1ace74c53c1d66721e065ef71

The PGP wordlist for the hash above is:

facial cellulose dropper microscope bison infancy button integrate freedom crucifix goggles yesteryear highchair positive waffle existence unearth inferno woodlark scavenger ribcage truncated drainage enterprise snapline speculate freedom Camelot tapeworm glossary uncut hideaway

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

Execute KSR Signer for Phase D to C

Step	Activity	Initials	Time
41.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK29-1-D_to_C/ksr-root-2017-q3-1-d_to_c.xml`	SKR	18:45
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.	SKR	18:45

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.	SKR	18:46
44.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	SKR	18:46
45.	CA then enters "`y`" in response to "`Is this correct y/n?`" to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK29-1-D_to_C/skr-root-2017-q3-1-d_to_c.xml`	SKR	18:47

Execute KSR Signer for Phase C to C

Step	Activity	Initials	Time
46.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK29-2-C_to_C/ksr-root-2017-q3-2-C_to_c.xml`	SR	18:49
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.	SR	18:49

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.	SR	18:50
49.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	SR	18:50
50.	CA enters "`y`" in response to "`Is this correct y/n?`" to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK29-2-C_to_C/skr-root-2017-q3-2-c_to_c.xml`	SR	18:50

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
51.	CA prints out sufficient number of copies for participants by executing the following command on the terminal window `for i in $(ls -1 ksrsigner-20170427-*.log); do printlog $i X; done` **Note**: Replace **X** with the number of copies for the participants.	SR	18:58
52.	IW1 attaches a copy of each ksrsigner log to his/her script.	SR	18:58

```
Starting: ksrsigner /media/KSR/KSK29-0-C_to_D/ksr-root-2017-q3-0-c_to_d.xml (at Thu Apr 27 18:38:53 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:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-04-01T00:00:00 2017-04-22T00:00:00  14796,61045   19036(Kjqmt7v)/S
2  2017-04-11T00:00:00 2017-05-02T00:00:00  14796         19036(Kjqmt7v)/S
3  2017-04-21T00:00:00 2017-05-12T00:00:00  14796         19036(Kjqmt7v)/S
4  2017-05-01T00:00:00 2017-05-22T00:00:00  14796         19036(Kjqmt7v)/S
5  2017-05-11T00:00:00 2017-06-01T00:00:00  14796         19036(Kjqmt7v)/S
6  2017-05-21T00:00:00 2017-06-11T00:00:00  14796         19036(Kjqmt7v)/S
7  2017-05-31T00:00:00 2017-06-21T00:00:00  14796         19036(Kjqmt7v)/S
8  2017-06-10T00:00:00 2017-07-01T00:00:00  14796         19036(Kjqmt7v)/S
9  2017-06-20T00:00:00 2017-07-11T00:00:00  14796,15768   19036(Kjqmt7v)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK29-0-C_to_D/ksr-root-2017-q3-0-c_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-07-01T00:00:00 2017-07-22T00:00:00  15768,14796
2  2017-07-11T00:00:00 2017-08-01T00:00:00  15768
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768
9  2017-09-19T00:00:00 2017-10-10T00:00:00  15768,46809
...PASSED.

SHA256 hash of KSR:
1B8539FBCD3E684B86868FA64BB4AD150FA41686123866A92008EB43942F74F0
>> beeswax leprosy classroom Wichita spindle cumbersome frighten disable necklace letterhead payday paragon dragnet
politeness ringbolt bifocals artist Pandora backward letterhead atlas consulting framework passenger bison antenna t
rouble decimal Pluto combustion indoors upcoming <<

Reading KSK schedule "publish(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
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/KSK29-0-C_to_D/skr-root-2017-q3-0-c_to_d.xml
#  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

SHA256 hash of SKR:
B6D3E6EE92B48003B20AB53848B4CD5CA19D698DF868B56D27FCAA8043146C42
>> Scotland sociable tracker universe physique politeness merit aggregate sawdust Apollo scorecard consulting deadbo
lt politeness spindle fascinate ratchet Ohio gazelle microscope Vulcan gravity scorecard hazardous brackish Wilmingt
on reward intention crucial belowground glucose December <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK29-1-D_to_C/ksr-root-2017-q3-1-d_to_c.xml (at Thu Apr 27 18:45:19 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:         H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-04-01T00:00:00 2017-04-22T00:00:00  14796,61045   19036(Kjqmt7v)/S
2  2017-04-11T00:00:00 2017-05-02T00:00:00  14796         19036(Kjqmt7v)/S
3  2017-04-21T00:00:00 2017-05-12T00:00:00  14796         19036(Kjqmt7v)/S
4  2017-05-01T00:00:00 2017-05-22T00:00:00  14796         19036(Kjqmt7v)/S
5  2017-05-11T00:00:00 2017-06-01T00:00:00  14796         19036(Kjqmt7v)/S
6  2017-05-21T00:00:00 2017-06-11T00:00:00  14796         19036(Kjqmt7v)/S
7  2017-05-31T00:00:00 2017-06-21T00:00:00  14796         19036(Kjqmt7v)/S
8  2017-06-10T00:00:00 2017-07-01T00:00:00  14796         19036(Kjqmt7v)/S
9  2017-06-20T00:00:00 2017-07-11T00:00:00  14796,15768   19036(Kjqmt7v)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK29-1-D_to_C/ksr-root-2017-q3-1-d_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-07-01T00:00:00 2017-07-22T00:00:00  15768,14796
2  2017-07-11T00:00:00 2017-08-01T00:00:00  15768
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768
9  2017-09-19T00:00:00 2017-10-10T00:00:00  15768,46809
...PASSED.

SHA256 hash of KSR:
4BD72ADA163B305E8F723FF8DE343CB2C0439BFEF7D92E7834E51370A636B116
>> dragnet stethoscope brickyard surrender backward councilman chairlift finicky payday holiness cowbell warranty ta
ctics confidence cobra pioneer slowdown decimal puppy yesteryear virus supportive buzzard indigo choking travesty Az
tec hesitate rematch congregate sailboat bodyguard <<

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/KSK29-1-D_to_C/skr-root-2017-q3-1-d_to_c.xml
#  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         19036(Kjqmt7v)/S
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768         19036(Kjqmt7v)/S
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768         19036(Kjqmt7v)/S
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768         19036(Kjqmt7v)/S
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768         19036(Kjqmt7v)/S
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768         19036(Kjqmt7v)/S
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768         19036(Kjqmt7v)/S
9  2017-09-19T00:00:00 2017-10-10T00:00:00  46809,15768   19036(Kjqmt7v)/S

SHA256 hash of SKR:
D74AD012038310A1CB18225C47A3143A41FD1CE5A8A931AA75DD733550E659E2
>> stopwatch direction stagnate backwater acme Jamaica assume outfielder spheroid borderline blockade fascinate dash
board pandemic baboon corrosion cranky Wyoming befriend travesty retouch passenger chatter pedigree indulge tambouri
ne hockey conformist drumbeat trombonist endow tomorrow <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK29-2-C_to_C/ksr-root-2017-q3-2-c_to_c.xml (at Thu Apr 27 18:49:12 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:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-04-01T00:00:00 2017-04-22T00:00:00  14796,61045   19036(Kjqmt7v)/S
2  2017-04-11T00:00:00 2017-05-02T00:00:00  14796         19036(Kjqmt7v)/S
3  2017-04-21T00:00:00 2017-05-12T00:00:00  14796         19036(Kjqmt7v)/S
4  2017-05-01T00:00:00 2017-05-22T00:00:00  14796         19036(Kjqmt7v)/S
5  2017-05-11T00:00:00 2017-06-01T00:00:00  14796         19036(Kjqmt7v)/S
6  2017-05-21T00:00:00 2017-06-11T00:00:00  14796         19036(Kjqmt7v)/S
7  2017-05-31T00:00:00 2017-06-21T00:00:00  14796         19036(Kjqmt7v)/S
8  2017-06-10T00:00:00 2017-07-01T00:00:00  14796         19036(Kjqmt7v)/S
9  2017-06-20T00:00:00 2017-07-11T00:00:00  14796,15768   19036(Kjqmt7v)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK29-2-C_to_C/ksr-root-2017-q3-2-c_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-07-01T00:00:00 2017-07-22T00:00:00  15768,14796
2  2017-07-11T00:00:00 2017-08-01T00:00:00  15768
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768
9  2017-09-19T00:00:00 2017-10-10T00:00:00  15768,46809
...PASSED.

SHA256 hash of KSR:
60284F8D207A2D7F673D6DFE72B5F95AF07BFED1ACE74C53C1D66721E065EF71
>> facial cellulose dropper microscope bison infancy button integrate freedom crucifix goggles yesteryear highchair
positive waffle existence unearth inferno woodlark scavenger ribcage truncated drainage enterprise snapline speculat
e freedom Camelot tapeworm glossary uncut hideaway <<

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/KSK29-2-C_to_C/skr-root-2017-q3-2-c_to_c.xml
#  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         19036(Kjqmt7v)/S
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768         19036(Kjqmt7v)/S
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768         19036(Kjqmt7v)/S
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768         19036(Kjqmt7v)/S
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768         19036(Kjqmt7v)/S
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768         19036(Kjqmt7v)/S
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768         19036(Kjqmt7v)/S
9  2017-09-19T00:00:00 2017-10-10T00:00:00  46809,15768   19036(Kjqmt7v)/S

SHA256 hash of SKR:
57178A11DAC10D60D2C570EE50DA4B393E48A3C582E82BE58417A2F9BCAB34CB
>> eightball bookseller Oakland Babylon surmount recover ancient fortitude standard resistor guidance universe drumb
eat surrender dragnet corporate concert dictator reform resistor miser typewriter briefcase travesty mural bookselle
r rebirth Waterloo showgirl Pegasus choking revival <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Backup Newly Created SKR

Step	Activity	Initials	Time
53.	CA copies the contents of the KSR FD by executing the following command on the terminal window `cp -pR /media/KSR/* .` Confirm overwrite by entering "y" when prompted.	SKR	18:59

54.	CA uses the terminal window to perform the following commands:
	a) list the contents of the KSR FD by executing
	`ls -ltrR /media/KSR`
	b) flush the system buffers by executing
	`sync`
	c) unmount the KSR FD by executing
	`umount /media/KSR`
		SKR	19:00

55.	CA removes the **KSR** FD containing the SKR files, then gives it to the RZM representative.	SKR	19:00

Disable/Deactivate HSM

Step	Activity	Initials	Time
56.	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 6 of 7 2nd OP card 7 of 7 3rd OP card 3 of 7	SKR	19:03

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.**	SR	19:04
2.	CA places the HSM into a prepared TEB, then seals it.	SR	19:05
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# BB51184621 / serial # H1403032** 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.	SR	19:07

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
4.	**Closing ttyaudit terminal window** CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from the laptop. CA then exits out of Serial Port Activity **(ttyaudit) terminal window** by typing "exit", then press enter.	SR	19:08
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.	SR	19:09

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA sets dotglob by executing the following command on the terminal window `shopt -s dotglob` **Note:** This enables copying of all files from the original HSMFD.	SR	19:09
7.	CA prints two copies of the hash by executing the following command on the terminal window `for i in $(seq 2); do hsmfd-hash -p; done` **Note:** One copy for audit bundle and one copy for HSMFD package.	SR	19:11
8.	CA displays contents of HSMFD by executing the following command on the terminal window `ls -ltrR`	SR	19:11
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 `cp -pR * /media/HSMFD_`	SR	19:13
10.	CA displays the contents of HSMFD_ by executing the following command on the terminal window `ls -ltrR /media/HSMFD_`	SR	19:13
11.	CA matches the SHA-256 hash between the original HSMFD and the copy HSMFD by executing the following command on the terminal window `hsmfd-hash -m`	SR	19:14
12.	CA unmounts the HSMFD copy by executing the following command on the terminal window `umount /media/HSMFD_`	SR	19:14
13.	CA removes the **HSMFD_** and places it on the holder.	SR	19:15
14.	CA repeats step 9 to 13 for the 2nd copy.	SR	19:16
15.	CA repeats step 9 to 13 for the 3rd copy.	SR	19:17
16.	CA repeats step 9 to 13 for the 4th copy.	SR	19:18
17.	CA repeats step 9 to 13 for the 5th copy.	SR	19:18

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
	`enscript -2Gr -# 1 script-20170427.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20170427-*.log`
	for attachment to IW1 script.
	Note: Ignore the error regarding non-printable characters if prompted.
		SR	19:21

HSMFD SHA-256 HASH 2017/04/27

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

SHA-256:     fad7dfd411fa6e48d18fe4ede0004724312a16ec596558f66b66d13d637c638e
PGP Words:  wallet stethoscope talon souvenir Athens whimsical goldfish dictator stairw
ay midsummer tonic unify tapeworm adroitness dashboard Capricorn chatter chambermaid ba
ckward unicorn endow glossary endorse vocalist glitter gossamer stairway crucifix flatf
oot informant flatfoot microwave
```

```
Script started on Thu 27 Apr 2017 06:18:26 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=1.34 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.360 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.526 ms

--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.360/0.745/1.349/0.432 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/KSR/KRK
\033]0;root@localhost:/media/HSMFD\007033[K033[KSK29\007-0-C_to_D/ks\007r-root-2017-q3-0-c_to_
Starting: ksrsigner /media/KSR/KSK29-0-C_to_D/ksr-root-2017-q3-0-c_to_d.xml (at Thu Ap
r 27 18:38:53 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:         H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-04-01T00:00:00 2017-04-22T00:00:00  14796,61045   19036(Kjqmt7v)/S
2  2017-04-11T00:00:00 2017-05-02T00:00:00  14796         19036(Kjqmt7v)/S
3  2017-04-21T00:00:00 2017-05-12T00:00:00  14796         19036(Kjqmt7v)/S
4  2017-05-01T00:00:00 2017-05-22T00:00:00  14796         19036(Kjqmt7v)/S
5  2017-05-11T00:00:00 2017-06-01T00:00:00  14796         19036(Kjqmt7v)/S
6  2017-05-21T00:00:00 2017-06-11T00:00:00  14796         19036(Kjqmt7v)/S
7  2017-05-31T00:00:00 2017-06-21T00:00:00  14796         19036(Kjqmt7v)/S
8  2017-06-10T00:00:00 2017-07-01T00:00:00  14796         19036(Kjqmt7v)/S
9  2017-06-20T00:00:00 2017-07-11T00:00:00  14796,15768   19036(Kjqmt7v)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK29-0-C_to_D/ksr-root-2017-q3-0-c_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-07-01T00:00:00 2017-07-22T00:00:00  15768,14796
2  2017-07-11T00:00:00 2017-08-01T00:00:00  15768
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768
9  2017-09-19T00:00:00 2017-10-10T00:00:00  15768,46809
...PASSED.

SHA256 hash of KSR:
1B8539FBCD3E684B86868FA64BB4AD150FA41686123866A92008EB43942F74F0
>> beeswax leprosy classroom Wichita spindle cumbersome frighten disable necklace lett
erhead payday paragon dragnet politeness ringbolt bifocals artist Pandora backward let
terhead atlas consulting framework passenger bison antenna trouble decimal Pluto combu
stion indoors upcoming <<
Is this correct (y/N)? y

Reading KSK schedule "publish(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
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/KSK29-0-C_to_D/skr-root-2017-q3-0-c_to_d.xml
#  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(Kjqmt
7v)/S
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2017-09-19T00:00:00 2017-10-10T00:00:00  46809,15768   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
B6D3E6EE92B48003B20AB53848B4CD5CA19D698DF868B56D27FCAA8043146C42
>> Scotland sociable tracker universe physique politeness merit aggregate sawdust Apol
lo scorecard consulting deadbolt politeness spindle fascinate ratchet Ohio gazelle mic
roscope Vulcan gravity scorecard hazardous brackish Wilmington reward intention crucia
l belowground glucose December <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20170427-183853.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/KSR/KSK
\033]0;root@localhost:/media/HSMFD\007[K29-1-D_to_C/ksr-root-2017-q3-1-d_to_
Starting: ksrsigner /media/KSR/KSK29-1-D_to_C/ksr-root-2017-q3-1-d_to_c.xml (at Thu Ap
r 27 18:45:19 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:         H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
```

```
1  2017-04-01T00:00:00 2017-04-22T00:00:00  14796,61045   19036(Kjqmt7v)/S
2  2017-04-11T00:00:00 2017-05-02T00:00:00  14796         19036(Kjqmt7v)/S
3  2017-04-21T00:00:00 2017-05-12T00:00:00  14796         19036(Kjqmt7v)/S
4  2017-05-01T00:00:00 2017-05-22T00:00:00  14796         19036(Kjqmt7v)/S
5  2017-05-11T00:00:00 2017-06-01T00:00:00  14796         19036(Kjqmt7v)/S
6  2017-05-21T00:00:00 2017-06-11T00:00:00  14796         19036(Kjqmt7v)/S
7  2017-05-31T00:00:00 2017-06-21T00:00:00  14796         19036(Kjqmt7v)/S
8  2017-06-10T00:00:00 2017-07-01T00:00:00  14796         19036(Kjqmt7v)/S
9  2017-06-20T00:00:00 2017-07-11T00:00:00  14796,15768   19036(Kjqmt7v)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK29-1-D_to_C/ksr-root-2017-q3-1-d_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-07-01T00:00:00 2017-07-22T00:00:00  15768,14796
2  2017-07-11T00:00:00 2017-08-01T00:00:00  15768
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768
9  2017-09-19T00:00:00 2017-10-10T00:00:00  15768,46809
...PASSED.

SHA256 hash of KSR:
4BD72ADA163B305E8F723FF8DE343CB2C0439BFEF7D92E7834E51370A636B116
>> dragnet stethoscope brickyard surrender backward councilman chairlift finicky payda
y holiness cowbell warranty tactics confidence cobra pioneer slowdown decimal puppy ye
steryear virus supportive buzzard indigo choking travesty Aztec hesitate rematch congr
egate sailboat bodyguard <<
Is this correct (y/N)? y

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/KSK29-1-D_to_C/skr-root-2017-q3-1-d_to_c.xml
#  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         19036(Kjqmt7v)/S
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768         19036(Kjqmt7v)/S
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768         19036(Kjqmt7v)/S
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768         19036(Kjqmt7v)/S
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768         19036(Kjqmt7v)/S
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768         19036(Kjqmt7v)/S
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768         19036(Kjqmt7v)/S
9  2017-09-19T00:00:00 2017-10-10T00:00:00  46809,15768   19036(Kjqmt7v)/S

SHA256 hash of SKR:
D74AD012038310A1CB18225C47A3143A41FD1CE5A8A931AA75DD733550E659E2
>> stopwatch direction stagnate backwater acme Jamaica assume outfielder spheroid bord
erline blockade fascinate dashboard pandemic baboon corrosion cranky Wyoming befriend
travesty retouch passenger chatter pedigree indulge tambourine hockey conformist drumb
eat trombonist endow tomorrow <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20170427-184519.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/KSR/KSK
\00229-2-C_to_C/ksr-root-2017-q3-2-c_to_
Starting: ksrsigner /media/KSR/KSK29-2-C_to_C/ksr-root-2017-q3-2-c_to_c.xml (at Thu Ap
r 27 18:49:12 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:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-04-01T00:00:00 2017-04-22T00:00:00  14796,61045   19036(Kjqmt7v)/S
2  2017-04-11T00:00:00 2017-05-02T00:00:00  14796         19036(Kjqmt7v)/S
3  2017-04-21T00:00:00 2017-05-12T00:00:00  14796         19036(Kjqmt7v)/S
4  2017-05-01T00:00:00 2017-05-22T00:00:00  14796         19036(Kjqmt7v)/S
5  2017-05-11T00:00:00 2017-06-01T00:00:00  14796         19036(Kjqmt7v)/S
6  2017-05-21T00:00:00 2017-06-11T00:00:00  14796         19036(Kjqmt7v)/S
7  2017-05-31T00:00:00 2017-06-21T00:00:00  14796         19036(Kjqmt7v)/S
8  2017-06-10T00:00:00 2017-07-01T00:00:00  14796         19036(Kjqmt7v)/S
9  2017-06-20T00:00:00 2017-07-11T00:00:00  14796,15768   19036(Kjqmt7v)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK29-2-C_to_C/ksr-root-2017-q3-2-c_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2017-07-01T00:00:00 2017-07-22T00:00:00  15768,14796
2  2017-07-11T00:00:00 2017-08-01T00:00:00  15768
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768
9  2017-09-19T00:00:00 2017-10-10T00:00:00  15768,46809
...PASSED.

SHA256 hash of KSR:
60284F8D207A2D7F673D6DFE72B5F95AF07BFED1ACE74C53C1D66721E065EF71
>> facial cellulose dropper microscope bison infancy button integrate freedom crucifix
 goggles yesteryear highchair positive waffle existence unearth inferno woodlark scave
nger ribcage truncated drainage enterprise snapline speculate freedom Camelot tapeworm
 glossary uncut hideaway <<
Is this correct (y/N)? y

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/KSK29-2-C_to_C/skr-root-2017-q3-2-c_to_c.xml
#  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         19036(Kjqmt7v)/S
3  2017-07-21T00:00:00 2017-08-11T00:00:00  15768         19036(Kjqmt7v)/S
4  2017-07-31T00:00:00 2017-08-21T00:00:00  15768         19036(Kjqmt7v)/S
5  2017-08-10T00:00:00 2017-08-31T00:00:00  15768         19036(Kjqmt7v)/S
6  2017-08-20T00:00:00 2017-09-10T00:00:00  15768         19036(Kjqmt7v)/S
7  2017-08-30T00:00:00 2017-09-20T00:00:00  15768         19036(Kjqmt7v)/S
8  2017-09-09T00:00:00 2017-09-30T00:00:00  15768         19036(Kjqmt7v)/S
9  2017-09-19T00:00:00 2017-10-10T00:00:00  46809,15768   19036(Kjqmt7v)/S

SHA256 hash of SKR:
57178A11DAC10D60D2C570EE50DA4B393E48A3C582E82BE58417A2F9BCAB34CB
>> eightball bookseller Oakland Babylon surmount recover ancient fortitude standard re
sistor guidance universe drumbeat surrender dragnet corporate concert dictator reform
resistor miser typewriter briefcase travesty mural bookseller rebirth Waterloo showgir
l Pegasus choking revival <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20170427-184912.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# for i in $(ls -1 ksrsign
ê#;2@ð@427-*.log); do printlog ¥033[K$i
[ 1 pages * 14 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 14 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 14 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 -ltrR /media/KSR
\033[00m/media/KSR:
total 12
drwxr-xr-x 2 root root 4096 Apr 27 18:44 \033[00;34mKSK29-0-C_to_D\033[00m
drwxr-xr-x 2 root root 4096 Apr 27 18:46 \033[00;34mKSK29-1-D_to_C\033[00m
drwxr-xr-x 2 root root 4096 Apr 27 18:50 \033[00;34mKSK29-2-C_to_C\033[00m

/media/KSR/KSK29-0-C_to_D:
total 92
-rwxr-xr-x 1 root root 20347 Apr 20 22:19 \033[00;32mskr.xml.20170427183853\033[00m
-rwxr-xr-x 1 root root 19556 Apr 20 22:19 \033[00;32mksr-root-2017-q3-0-c_to_d.xml\033
[00m
-rwxr-xr-x 1 root root   540 Apr 20 22:19 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24419 Apr 27 18:44 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24419 Apr 27 18:44 \033[00;32mskr-root-2017-q3-0-c_to_d.xml\033
[00m

/media/KSR/KSK29-1-D_to_C:
total 84
-rwxr-xr-x 1 root root 20347 Apr 20 22:19 \033[00;32mskr.xml.20170427184519\033[00m
-rwxr-xr-x 1 root root 19556 Apr 20 22:19 \033[00;32mksr-root-2017-q3-1-d_to_c.xml\033
[00m
-rwxr-xr-x 1 root root   454 Apr 20 22:19 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 20347 Apr 27 18:46 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Apr 27 18:46 \033[00;32mskr-root-2017-q3-1-d_to_c.xml\033
[00m

/media/KSR/KSK29-2-C_to_C:
total 84
-rwxr-xr-x 1 root root 20347 Apr 20 22:19 \033[00;32mskr.xml.20170427184912\033[00m
-rwxr-xr-x 1 root root 19556 Apr 20 22:19 \033[00;32mksr-root-2017-q3-2-c_to_c.xml\033
[00m
-rwxr-xr-x 1 root root   454 Apr 20 22:19 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 20347 Apr 27 18:50 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Apr 27 18:50 \033[00;32mskr-root-2017-q3-2-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[K
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit

Script done on Thu 27 Apr 2017 07:09:04 PM UTC
```

```
2017-04-27T18:23:42+0000        ttyUSB0 þ
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 H1403032 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 BBL CRC32: 0x757574CA
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 H1403032 011403 ABL 011 : Tamper Challenge Response Key
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ####################################
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ###     ABL tamper records       ###
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ####################################
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ====================================
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 vextoosTamperCount:     0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 vintoosTamperCount:     46
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 vbboosTamperCount:      0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 maxstrtempTamperCount:  0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 minstrtempTamperCount:  0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 meshTamperCount:        0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 extampSMKTamperCount:   0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 extampIMKTamperCount:   0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 tempdiffTamperCount:    0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 pfTamperCount:          46
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 restartTamperCount:     146
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 Current tamper bitmaps:
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ======================
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
```

```
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0 ============================================
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:42+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0 Board is P2020RDB
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0 board_smp_init: 2 cpu
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:43+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2017-04-27T18:23:43+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0 Starting next program at v0015183c
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0 Starting K-Series Kernel
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:44+0000        ttyUSB0 Thu Apr 27 17:41:31 2017
2017-04-27T18:23:44+0000        ttyUSB0
2017-04-27T18:23:45+0000        ttyUSB0 Starting auditd v2.0 ... started.
2017-04-27T18:23:45+0000        ttyUSB0
2017-04-27T18:23:45+0000        ttyUSB0 Interface 0 configured for IPv6.
2017-04-27T18:23:45+0000        ttyUSB0
2017-04-27T18:23:45+0000        ttyUSB0 Interface 0 configured for IPv4.
2017-04-27T18:23:45+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0 Starting USB driver...
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0
2017-04-27T18:23:46+0000        ttyUSB0
```

```
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running DES POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 DES POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running Triple DES POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Triple DES POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running AES POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 AES POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running SHA1 POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 SHA1 POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running SHA2 POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 SHA2 POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running RandomGen POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 RandomGen POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running RSA POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 RSA POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running DSA POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 DSA POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Running ECC POST Test
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 ECC POST Test Passed
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0 Audit on 27/4/2017 17:41:34 00100008
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:48+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 Keyper 9860-2  Serial Number H1403032
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 Memory Usage:
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 RAM (free/total)        197Mb/256Mb
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0    black store          512b
```

```
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0    statistics           112b
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0    other                116b
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 RedStore (free/total)   109Kb/128Kb
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 Network Configuration:
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 IPv4: enabled
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 IPv6: enabled
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B2:3D / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b23d/64
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 HSM Port: 05000
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 Software Versions:
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 BBL 010 ABL 011 App 023
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 CPLD Version:
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 1.9
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 SCR Firmware Version:
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 OROS-R2.99-R1.20
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:23:49+0000        ttyUSB0 Audit on 27/4/2017 17:41:35 00100003
2017-04-27T18:23:49+0000        ttyUSB0
2017-04-27T18:33:13+0000        ttyUSB0 Audit on 27/4/2017 17:50:59 00200069 0880004A7AB3296D
2017-04-27T18:33:13+0000        ttyUSB0
2017-04-27T18:33:42+0000        ttyUSB0 Audit on 27/4/2017 17:51:29 00200069 0880004A83B3296D
2017-04-27T18:33:42+0000        ttyUSB0
```

```
2017-04-27T18:34:08+0000        ttyUSB0 Audit on 27/4/2017 17:51:54 00200069 0880004A7B33296D
2017-04-27T18:34:08+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0 TcpListener: Created IPv4 socket 15 on port 5000.
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0 TcpListener: Created IPv6 socket 16 on port 5000.
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:34:11+0000        ttyUSB0 Audit on 27/4/2017 17:51:57 00100002
2017-04-27T18:34:11+0000        ttyUSB0
2017-04-27T18:39:21+0000        ttyUSB0
2017-04-27T18:39:21+0000        ttyUSB0
2017-04-27T18:39:21+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2017-04-27T18:39:21+0000        ttyUSB0
2017-04-27T18:44:08+0000        ttyUSB0
2017-04-27T18:44:08+0000        ttyUSB0
2017-04-27T18:44:08+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2017-04-27T18:44:08+0000        ttyUSB0
2017-04-27T18:45:32+0000        ttyUSB0
2017-04-27T18:45:32+0000        ttyUSB0
2017-04-27T18:45:32+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2017-04-27T18:45:32+0000        ttyUSB0
2017-04-27T18:46:50+0000        ttyUSB0
2017-04-27T18:46:50+0000        ttyUSB0
2017-04-27T18:46:50+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2017-04-27T18:46:50+0000        ttyUSB0
2017-04-27T18:49:26+0000        ttyUSB0
2017-04-27T18:49:26+0000        ttyUSB0
2017-04-27T18:49:26+0000        ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2017-04-27T18:49:26+0000        ttyUSB0
2017-04-27T18:50:41+0000        ttyUSB0
2017-04-27T18:50:41+0000        ttyUSB0
2017-04-27T18:50:41+0000        ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2017-04-27T18:50:41+0000        ttyUSB0
2017-04-27T19:01:34+0000        ttyUSB0 Audit on 27/4/2017 18:19:20 00200069 0880004A7B73296D
2017-04-27T19:01:34+0000        ttyUSB0
2017-04-27T19:02:00+0000        ttyUSB0 Audit on 27/4/2017 18:19:46 00200069 0880004A7BB3296D
2017-04-27T19:02:00+0000        ttyUSB0
2017-04-27T19:02:30+0000        ttyUSB0 Audit on 27/4/2017 18:20:16 00200069 0880004A7AB3296D
2017-04-27T19:02:30+0000        ttyUSB0
2017-04-27T19:02:36+0000        ttyUSB0
2017-04-27T19:02:36+0000        ttyUSB0
2017-04-27T19:02:36+0000        ttyUSB0 TcpListener: Closed IPv4 socket 15 on port 5000.
2017-04-27T19:02:36+0000        ttyUSB0
2017-04-27T19:02:36+0000        ttyUSB0
2017-04-27T19:02:36+0000        ttyUSB0
2017-04-27T19:02:36+0000        ttyUSB0 TcpListener: Closed IPv6 socket 16 on port 5000.
2017-04-27T19:02:36+0000        ttyUSB0
2017-04-27T19:02:37+0000        ttyUSB0 Audit on 27/4/2017 18:20:23 00100003
2017-04-27T19:02:37+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
	`cd /tmp`
	`umount /media/HSMFD`
	CA removes the HSMFD, then places it on the holder.
		SR	19:22

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.	SR	19:23
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 confirms. **OS DVD (release 20170403) + HSMFD: TEB# BB46584512**	SR	19:25
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.	SR	19:26

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)	SR	19:27

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# BB51184616 / serial # 41593712005**	SA	19:29
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.	SR	19:30

Return OP Card to TEB

Step	Activity	Initials	Time
26.	One by one, CA calls each COs listed below to the ceremony table to perform the following steps. 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. **CO 3: Olaf Kolkman** **OP TEB # BB46584464** **CO 4: Robert Seastrom** **OP TEB # BB46584465** **CO 5: Christopher Griffiths** **OP TEB # BB46584466** **CO 6: Gaurab Upadhaya** **OP TEB # BB46584467** **CO 7: Alain Aina** **OP TEB # BB46584468**	SR	19:44

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 3	OP 3 of 7	BB46584464	Olaf Kolkman		27 April 2017	1954 UTC	SR
CO 4	OP 4 of 7	BB46584465	Robert Seastrom		27 April 2017	1937 UTC	SR
CO 5	OP 5 of 7	BB46584466	Christopher Griffiths		27 April 2017	1939 UTC	SR
CO 6	OP 6 of 7	BB46584467	Gaurab Upadhaya		27 April 2017	1941 UTC	SR
CO 7	OP 7 of 7	BB46584468	Alain Aina		27 April 2017	19:43 UTC	SR

Returning Equipment to Safe #1

Step	Activity	Initials	Time
27.	CA, IW1, SSC1 enters the safe room with the equipment cart.	SR	19:45
28.	SSC1, while shielding the combination from the camera, opens Safe #1.	SR	19:46
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.**	SR	19:46
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# BB51184621 / serial # H1403032**	SR	19:48
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# BB51184616 / serial # 41593712005** **OS DVD (release 20170403) + HSMFD: TEB# BB46584512**	SR	19:49

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.	SR	19:50
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.	SR	19:50
34.	CA, SSC1 and IW1 leaves the safe room with the equipment cart closing the door behind them.	SR	19:51

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.	SR	19:52
36.	SSC2, while shielding combination from the camera, opens Safe #2.	SR	19:53
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.**	SR	19:54

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
38.	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. 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. **Note: Common Key is for the bottom lock. CO Key is for the top lock** 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. Repeat these steps until all the required cards listed below are returned. **CO 3: Olaf Kolkman** **Box # 1239** **OP TEB # BB46584464** **CO 4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584465** **CO 5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46584466** **CO 6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB46584467** **CO 7: Alain Aina** **Box # 1242** **OP TEB # BB46584468**	AR	20:01

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.	SR	20:02
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.	SR	20:02
41.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	SR	20:03

Participant Signing of IW1's Script

Step	Activity	Initials	Time
42.	CA reads the exceptions that may have occurred during the ceremony.	SR	20:03
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.	SR	20:07
44.	CA reviews IW1's script and signs the participants list.	SR	20:11

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.	SR	20:12

Sign Out of Ceremony Room

Step	Activity	Initials	Time
46.	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.	SR	20:32

Stop Video Recording

Step	Activity	Initials	Time
47.	CA notifies the SA to stop video recording.	SR	20:32

Bundle Audit Materials

Step	Activity	Initials	Time
48.	IW1 makes (1) copy of his/her script for off-site audit bundle. Each Audit bundle contains: ✓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 **10/27/2016 – 04/27/2017**) ✓e) IW1 attestation (Section A.1) ✓f) SA attestation (Sections A.2 and A.3) All TEBs are labeled **"Root DNSSEC KSK Ceremony 29"**, 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**	SR	21:37

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.

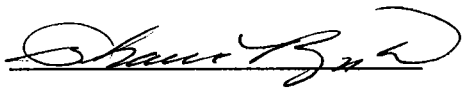
6. Configuration review of the Firewall System (SA1)
SA1's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

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.

Shauna Royston



Date: 27 April 2017

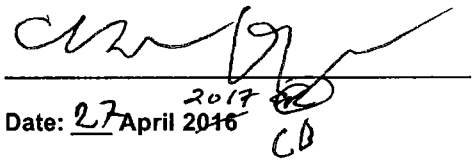
A.2 Access Control System Configuration Review (by SA1)

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 **27 October 2016 00:00 UTC** to now.

Connor Barthold



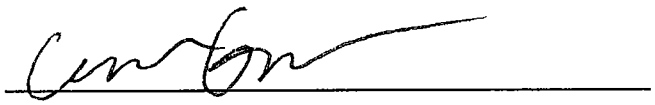
Date: 27 ~~April 2016~~ 2017 CB

A.3 Firewall Configuration Review (by SA1)

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

Enclosed is the configuration extract from the firewall unit.

Connor Barthold



Date: 27 **April** ~~**2016**~~ 2017 BR CB

```
version 12.1X46-D35.1;
system {
    host-name srx;
    domain-name ksk.cjr.dns.icann.org;
    location {
        country-code US;
        postal-code 22701;
        building Terramark-Admin;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "$1$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-
DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        inactive: user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "$1$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ##
SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "$1$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ##
SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "$1$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ##
SECRET-DATA
            }
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
        source-address 10.4.29.1;
    }
}
chassis {
    config-button no-rescue no-clear;
}
interfaces {
    interface-range access {
        member-range ge-0/0/0 to ge-0/0/8;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-access;
                }
            }
        }
    }
    interface-range video {
        member-range ge-0/0/9 to ge-0/0/12;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-video;
                }
            }
        }
    }
    interface-range wifi {
        member ge-0/0/13;
        unit 0 {
            family inet {
                address 10.100.1.1/24;
            }
        }
    }
    interface-range guest {
        member ge-0/0/14;
        member ge-0/0/15;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-guest;
                }
            }
        }
    }
    ge-0/0/0 {
        description "Access Control Server";
    }
    ge-0/0/1 {
        description "Access Control Client Custom Solution";
    }
    ge-0/0/2 {
        description "Intrusion Detection Panel";
    }
    ge-0/0/3 {
        description "Environment Monitoring";
    }
    ge-0/0/4 {
        description "Monitoring Server";
    }
    ge-0/0/5 {
        description "IRIS Enrollment";
    }
    ge-0/0/6 {
        description "Iris Scanner T2";
    }
    ge-0/0/7 {
        description "Iris Scanner T3";
    }
    ge-0/0/8 {
        description "Iris Scanner T4";
    }
    ge-0/0/9 {
        description "Video Surveillance Server";
    }
    ge-0/0/10 {
        description "Camera 1";
    }
    ge-0/0/11 {
        description "Camera 2";
    }
    ge-0/0/12 {
        description "Camera 3";
    }
    ge-0/0/13 {
        description "Wifi Connection";
    }
    ge-0/0/14 {
        description "Streaming Laptop";
    }
    ge-0/0/15 {
        description "Audio Camera Client";
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 152.194.1.148/28;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input route-engine-filter;
                }
            }
        }
    }
    st0 {
        unit 1 {
            description "IPSec KMF-West";
            family inet;
        }
    }
    vlan {
        unit 0 {
            family inet {
                address 10.4.29.193/26;
            }
```

```
        }
        unit 1 {
            family inet {
                address 10.4.29.129/26;
            }
        }
        unit 2 {
            family inet {
                address 10.4.29.1/25;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 152.194.1.145;
        route 10.4.28.0/24 next-hop st0.1;
        route 192.0.35.202/32 next-hop 152.194.1.145;
    }
}
policy-options {
    prefix-list resolver-servers {
        8.8.4.4/32;
        8.8.8.8/32;
    }
    prefix-list local-prefixes {
        10.4.29.0/24;
    }
    prefix-list ntp-servers {
        129.6.15.28/32;
        129.6.15.29/32;
    }
}
security {
    ike {
        policy ike-policy-KMF {
            pre-shared-key ascii-text "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ##
SECRET-DATA
        }
        gateway Gateway-to-KMF-West {
            ike-policy ike-policy-KMF;
            address 192.0.35.202;
            external-interface ge-1/0/0;
        }
    }
    ipsec {
        traceoptions {
            flag all;
        }
        proposal IPSecProposal {
            protocol esp;
            authentication-algorithm hmac-sha-256-128;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 7200;
        }
        policy defaultPolicy {
            perfect-forward-secrecy {
                keys group5;
            }
            proposals IPSecProposal;
        }
        vpn vpn-to-KMF-West {
            bind-interface st0.1;
            ike {
                gateway Gateway-to-KMF-West;
                ipsec-policy defaultPolicy;
            }
            establish-tunnels immediately;
        }
    }
    screen {
        ids-option external-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
                land;
            }
        }
    }
    nat {
        source {
            rule-set internal-to-external {
                from zone [ access guest wifi ];
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
}
policies {
    from-zone access to-zone untrust {
        policy allow-mail {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address [ icann-dns google-dns ];
                application [ junos-dns-udp junos-dns-tcp ];
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-simplex {
            match {
                source-address IDP;
                destination-address simplex;
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
    }
    from-zone access to-zone video {
        policy access-to-video {
            match {
                source-address IMS;
                destination-address kmf_east_video;
                application junos-icmp-all;
            }
            then {
                permit;
            }
        }
    }
    from-zone access to-zone ipsec {
        policy allow-access-to-ipsec {
            match {
                source-address [ ACS ACC ];
                destination-address [ kmf_west_acs kmf_west_acc ];
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-icmp {
            match {
                source-address any;
                destination-address any;
                application junos-icmp-ping;
            }
            then {
                permit;
            }
        }
        policy allow-access-access {
            match {
                source-address kmf_east_access;
                destination-address kmf_west_access;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone ipsec to-zone access {
        policy allow-ipsec-to-access {
            match {
                source-address [ kmf_west_acs kmf_west_acc ];
                destination-address [ ACS ACC ];
                application any;
            }
            then {
                permit;
                log {
```

```
            session-close;
          }
        }
      }
      policy allow-icmp {
        match {
          source-address any;
          destination-address any;
          application junos-icmp-ping;
        }
        then {
          permit;
        }
      }
      policy allow-access-access {
        match {
          source-address kmf_west_access;
          destination-address kmf_east_access;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone video to-zone ipsec {
      policy allow-video-to-ipsec {
        match {
          source-address VSS;
          destination-address kmf_west_vss;
          application any;
        }
        then {
          permit;
          log {
            session-close;
          }
        }
      }
      policy allow-access-video {
        match {
          source-address kmf_east_video;
          destination-address kmf_west_video;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone guest to-zone untrust {
      policy allow-guest-to-untrust {
        match {
          source-address kmf_east_guest;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone wifi to-zone untrust {
      policy allow-wifi-to-untrust {
        match {
          source-address kmf_east_wifi;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone ipsec to-zone video {
      policy allow-ipsec-to-video {
        match {
          source-address kmf_west_vss;
          destination-address VSS;
          application any;
        }
        then {
          permit;
          log {
            session-close;
          }
        }
      }
      policy allow-access-video {
        match {
          source-address kmf_west_video;
          destination-address kmf_east_video;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone access to-zone access {
      policy allow-access {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    default-policy {
      deny-all;
    }
  }
  zones {
    security-zone access {
      address-book {
        address ACS 10.4.29.203/32;
        address ACC 10.4.29.202/32;
        address IDP 10.4.29.201/32;
        address EVM 10.4.29.200/32;
        address IMS 10.4.29.204/32;
        address E1 10.4.29.210/32;
        address E2 10.4.29.211/32;
        address E3 10.4.29.212/32;
        address E4 10.4.29.213/32;
        address kmf_east_access 10.4.29.192/26;
        address localnet 10.4.29.0/24;
        address-set iris-scanners {
          address E1;
          address E2;
          address E3;
          address E4;
        }
      }
      interfaces {
        vlan.0 {
          host-inbound-traffic {
            system-services {
              ping;
              ntp;
            }
          }
        }
      }
    }
    security-zone untrust {
      address-book {
        address icann 192.0.32.0/20;
        address icann-dns 192.0.42.53/32;
        address googledns1 8.8.8.8/32;
        address googledns2 8.8.4.4/32;
        address simplex1 216.224.218.31/32;
        address simplex2 216.224.218.32/32;
        address simplex3 216.224.218.33/32;
        address simplex4 216.224.218.34/32;
        address-set google-dns {
          address googledns1;
          address googledns2;
        }
        address-set simplex {
          address simplex1;
          address simplex2;
          address simplex3;
          address simplex4;
        }
      }
      screen external-screen;
      interfaces {
        ge-1/0/0.0 {
          host-inbound-traffic {
            system-services {
              ping;
              ssh;
            }
          }
        }
      }
    }
    security-zone video {
      address-book {
        address kmf_east_video 10.4.29.128/26;
        address VSS 10.4.29.150/32;
        address C1 10.4.29.151/32;
        address C2 10.4.29.152/32;
        address C3 10.4.29.153/32;
        address-set cameras {
          address C1;
          address C2;
          address C3;
        }
      }
      interfaces {
        vlan.1 {
          host-inbound-traffic {
            system-services {
              ping;
            }
          }
        }
      }
    }
    security-zone guest {
      address-book {
        address STR 10.4.29.20/32;
        address VCC 10.4.29.22/32;
        address kmf_east_guest 10.4.29.0/25;
```

```
        }
        interfaces {
            vlan.2 {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
            }
        }
    }
    security-zone ipsec {
        address-book {
            address kmf_west_access 10.4.28.192/26;
            address kmf_west_video 10.4.28.128/26;
            address kmf_west_acs 10.4.28.204/32;
            address kmf_west_acc 10.4.28.202/32;
            address kmf_west_idp 10.4.28.201/32;
            address kmf_west_evm 10.4.28.200/32;
            address kmf_west_ims 10.4.28.203/32;
            address kmf_west_E1 10.4.28.210/32;
            address kmf_west_E3 10.4.28.212/32;
            address kmf_west_E4 10.4.28.213/32;
            address kmf_west_vss 10.4.28.150/32;
            address kmf_west_C1 10.4.28.151/32;
            address kmf_west_C2 10.4.28.152/32;
            address kmf_west_C3 10.4.28.153/32;
        }
        interfaces {
            st0.1 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        ike;
                        ssh;
                    }
                }
            }
        }
    }
    security-zone wifi {
        address-book {
            address kmf_east_wifi 10.100.1.0/24;
        }
        interfaces {
            ge-0/0/13.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
            }
        }
    }
}
firewall {
    family inet {
        filter route-engine-filter {
            term deny-icmp-redirects {
                from {
                    protocol icmp;
                    icmp-type redirect;
                }
                then {
                    discard;
                }
            }
            term allow-icmp {
                from {
                    protocol icmp;
                    icmp-type [ echo-request echo-reply unreachable time-exceeded ];
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-traceroute {
                from {
                    protocol udp;
                    port 33434-33534;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-dns {
                from {
                    source-prefix-list {
                        resolver-servers;
                    }
                    protocol udp;
                    source-port domain;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-ntp {
                from {
                    source-prefix-list {
                        local-prefixes;
                        ntp-servers;
                    }
                    protocol udp;
                    port ntp;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-establish {
                from {
                    protocol tcp;
                    tcp-established;
                }
                then accept;
            }
            term allow-ipsec-esp {
                from {
                    protocol esp;
                }
                then accept;
            }
            term allow-ipsec-udp {
                from {
                    protocol udp;
                    port 500;
                }
                then accept;
            }
            term allow-ssh {
                from {
                    source-address {
                        192.0.35.202/32;
                        10.4.29.0/24;
                        10.4.28.0/24;
                    }
                    protocol tcp;
                    destination-port ssh;
                }
                then accept;
            }
            term LAST {
                then {
                    discard;
                }
            }
        }
    }
    policer small-bw-limit {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 15k;
        }
        then discard;
    }
}
poe {
    interface all;
}
vlans {
    vlan-access {
        vlan-id 3;
        l3-interface vlan.0;
    }
    vlan-guest {
        vlan-id 5;
        l3-interface vlan.2;
    }
    vlan-video {
        vlan-id 4;
        l3-interface vlan.1;
    }
}
```