



Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 25

Thursday May 12, 2016

ICANN KSK Facility@Terremark NCR
18155 Technology Drive, Culpeper, VA 22701-3805

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



Abbreviations

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

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			
IW1	Jonathan Denison / ICANN			21:00
SSC1	James Cole / ICANN			
SSC2	Grace Abuhamad / ICANN			
CO2	Anne-Marie Eklund Lowinder / SE			
CO3	Olaf Kolkman / NL			
CO4	Robert Seastrom / US			
CO5	Christopher Griffiths / US			
CO6	Gaurab Upadhaya / NP			
RZM	Alejandro Bolivar / Verisign			
RZM	Duane Wessels / Verisign			
RZM	John Painumkal / Verisign			
RZM	James Simonetti / Verisign			
AUD	Ryan Ung / PricewaterhouseCoopers		12 May 2016	
AUD	Timothy Chang / PricewaterhouseCoopers			
SA1	Connor Barthold / ICANN			
SA2	Reed Quinn / ICANN			
SA3	Brian Martin / ICANN			
CA3 IKOS	Alberto Duero / ICANN			
IW2 / IKOS	Andres Pavez / ICANN			
CA3	Edward Lewis / ICANN			
CA4	Richard Lamb / ICANN			
Staff Witness	Derek Ellison / ICANN			
				21:16

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



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

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

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



ICANN DNSSEC Script Exception

Abbreviations

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

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

Note Exception Time

Step	Activity	Initials	Time
1.	IW1 notes date and time of key ceremony exception and signs here: <u>17:03 2016/05/12</u>	<i>jh</i>	17:03
2.	IW1 Describes exception and action below.	<i>jp</i>	17:04

ACT 1, STEP 2 PUNY DUELO STANDING IN FOR FRANCISCO ALIAS
AS CA

– End of DNSSEC Script Exception –



Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.	JD	17:01
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.	JD	17:04

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	JD	17:05
4.	CA explains the use of personal electronics devices during ceremony.	JD	17:06
5.	CA briefly explains the purpose of the ceremony.	JD	17:09

Verify Time and Date

Step	Activity	Initials	Time
6.	<p>IW1 enters UTC date (year/month/day) and time using a reasonably accurate wall clock visible to all in the Ceremony Room:</p> <p>Date and time: <u>2016/09/12 17:10</u></p> <p>All entries into this script or any logs should follow this common source of time.</p>	JD	17:10

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.	JD	17:12
8.	SSC2, while shielding combination from camera, opens Safe #2.	JD	17:14
9.	<p>SSC2 takes out the existing safe log and shows the most current page to the camera.</p> <p>IW1 provides a blank pre-printed safe log to the SSC2.</p> <p>SSC2 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p>	JD	17:16

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	<p>One by one, the selected COs retrieves required OP cards and SO cards (if applicable) following the steps shown below.</p> <ul style="list-style-type: none"> a) With the assistance of CA (and his/her common key), opens her/his safe deposit box. # Common Key is bottom lock and CO Key is top lock b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below. c) Retains OP TEB and SO TEB (if applicable) and locks box. d) Makes an entry in safe log indicating OP TEB and SO TEB removal (if applicable) with box #, printed name, date, time and signature. <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>Repeat these steps until all required cards are removed. IW1 initials this entry when all COs have finished.</p> <p>CO 2: Anne-Marie Eklund Lowinder Box # 1259 OP TEB # BB46584315 (Retain) SO TEB # BB21907211 (Check and return)</p> <p>CO 3: Olaf Kolkman Box # 1239 OP TEB # BB46584316 (Retain) SO TEB # BB21907253 (Check and return)</p> <p>CO 4: Robert Seastrom Box # 1260 OP TEB # BB46584267 (Retain) SO TEB # BB21907203 (Check and return)</p> <p>CO 5: Christopher Griffiths Box # 1240 OP TEB # BB46584317 (Retain) SO TEB # BB21907206 (Check and return)</p> <p>CO 6: Gaurab Upadhaya Box # 1261 OP TEB # BB21907210 (Retain) SO TEB # BB21907207 (Check and return)</p>	<p style="text-align: center;">JD</p>	<p style="text-align: center;">17:28</p>



Close Credential Safe #2

Step	Activity	Initials	Time
11.	Once all safe deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	JP	17:29
12.	SSC2 puts log in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and card reader indicator is green.	JP	17:30
13.	IW1, CA, SSC2, and COs leave safe room, with OP cards and SO cards (if applicable) in TEBs, closing the door behind them.	JP	17:31

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	JP	17:34
15.	SSC1, while shielding combination from camera, opens Safe #1.	JP	17:35
16.	SSC1 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	JP	17:37

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	<p>CA CAREFULLY removes HSM4 (in TEB) from the safe and completes the entry on the safe log indicating HSM Removal, TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>HSM4: TEB# BB24646675 / serial # H1411011</p> <p>Verify the integrity of the other HSMs that will not be used and return them to the safe.</p> <p>HSM1: TEB# BB24706804 / serial # K6002016</p> <p>HSM2: TEB# BB24646674 / serial # K6002013</p> <p>HSM3: TEB# BB24646616 / serial # H1403032</p>	jo	17:42
18.	<p>CA takes out the items listed below from the safe and completes the entry on the safe log indicating each item, TEB#, serial number if available. Printed name, date, time and signature. CA places the item on the equipment cart. IW1 initials this entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>Laptop1 (Dell ATG6400): TEB# BB24646672 / serial # 41593712005</p> <p>O/S DVD (Rev600) + HSMFD: TEB# BB46584320</p> <p>Verify the integrity of the other Laptop that will not be used this time and return it to the safe.</p> <p>Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997</p>	jo	17:47

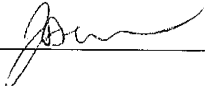
Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	<p>SSC1 makes an entry including printed name, date, time and signature on the safe log indicating, "Close safe". IW1 initials this entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p>	jo	17:48
20.	<p>SSC1 puts log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise).</p> <p>CA and IW1 verify that the safe is locked and door indicator light is green.</p>	jo	17:51
21.	<p>CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.</p>	jo	17:52

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

OS/DVD Acceptance Test

Step	Activity	Initials	Time
1.	CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. Laptop1 (Dell ATG6400): TEB# BB24646672 / serial # 41593712005	JP	17:54
2.	CA inspects the O/S DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. O/S DVD (Rev600) + HSMFD: TEB# BB46584320	JP	17:55
3.	CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on the key ceremony table; discards TEBs; connects laptop power, external display, printer, general purpose external DVD drive and boots laptop from O/S DVD (Rev600) .	JP	18:02
4.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes <code>system-config-display --noui</code> c) CA executes <code>killall Xorg</code> d) CA confirms that external display works. e) CA logs in as root	JP	18:04
5.	CA opens a terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal Follow the additional steps to maximize the terminal window: a) Click the <u>V</u> iew menu and select Zoom In b) Repeat the step above as necessary	JP	18:05
6.	CA inserts the new O/S DVD release 20160503 into the external DVD drive, waits for it to be recognized by the O/S and performs the following: a) Close the file system popup window b) Confirm the assigned drive letter by executing <code>df</code> c) Unmount the DVD drive by executing <code>umount /dev/scd1</code> d) Calculate the SHA256 hash by executing <code>sha256sum /dev/scd1</code> SHA256 hash for release 20160503: 6cabb3c146aa13fbc9a9d61488b2c6f8c7e9e723a89b8574b0288578a65cc0f5 IW1 and participants confirm that the result matches the above, which also matches the one published on: https://data.iana.org/ksk-ceremony/25/KC-20160503.iso.sha256	JP	18:11

Step	Activity	Initials	Time
7.	CA removes the O/S DVD by pressing the eject button on the external DVD drive and places it on the ceremony table visible from the audit camera and the participants.	JD	18:12
8.	CA repeats step 6 and 7 for the 2 nd copy of the new O/S DVD release 20160503.	JD	18:18
9.	<p>IW1 records the date, time then affixes his/her signature upon successful completion of the O/S DVD release 20160503 acceptance testing:</p> <p>O/S DVD Acceptance Test release 20160503 Printed Name Jonathan Denison Date 2016/05/12</p> <p>Time <u>18:18</u></p> <p>Signature </p>	JD	18:18
10.	<p>CA disconnects the general purpose external DVD drive from the laptop, then removes the O/S DVD by performing:</p> <ul style="list-style-type: none"> a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch and immediately remove the old O/S DVD (Rev600) from the laptop DVD drive c) Turns off the laptop again by pressing the power switch 	JD	18:20
11.	CA discards all the old O/S DVD (Rev600) copies.	JD	18:27

Set Up Laptop

Step	Activity	Initials	Time
12.	CA boots laptop using the new O/S DVD release 20160503.	jp	18:26
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 <code>system-config-display --noui</code> c) CA executes <code>killall Xorg</code> d) CA confirms that external display works. e) CA logs in as root	jp	18:27
14.	CA confirms that the printer is connected then configures printer as default and prints test page by going to System > Administration > Printing And follow the steps below: a) Click the New Printer icon (left side), leave everything default and then click the button Forward b) Under "Select Connection" choose the <u>first device</u> " HP Laserjet xxxx " and then click the button Forward (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 "	jp	18:31
15.	CA opens a terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal Follow the additional steps to maximize the terminal window: c) Click the View menu and select Zoom In d) Repeat the step above as necessary	jp	18:32
16.	CA checks and fixes the date and time on the laptop while referencing the laptop wall clock. On the laptop terminal windows, CA executes: <code>cp /usr/share/zoneinfo/UTC /etc/localtime</code> When " <code>cp: overwrite '/etc/localtime' ?</code> " is displayed, type " y " and press enter. then <code>date -s "20160512 HH:MM:00"</code> where HH is two digit Hour, MM is two digit Minutes and 00 is Zero Seconds CA executes <code>date</code> using the Terminal window to confirm the date is properly configured.	jp	18:34

Format and label blank FD

Step	Activity	Initials	Time
17.	CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system popup window and formats the drive by executing <code>df</code> to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc), <code>umount /dev/sda1</code> to unmounts the drive (change drive letter and partition if necessary), <code>mkfs.vfat -n HSMFD -I /dev/sda1</code> to execute a FAT32 format and label it as HSMFD. CA unplugs the FD.	JD	18:36
18.	CA repeats step 17 for the 2 nd blank FD	JD	18:38
19.	CA repeats step 17 for the 3 rd blank FD	JD	18:39
20.	CA repeats step 17 for the 4 th blank FD	JD	18:39
21.	CA repeats step 17 for the 5 th blank FD	JD	18:40

Connect HSMFD

Step	Activity	Initials	Time
22.	CA plugs the previous HSMFD used in the ceremony 23 into the free USB slot on the laptop and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.	JD	18:42
23.	Calculate the sha256 hash of the contents on the copied HSMFD. <code>find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum</code> IW1 confirms that the result matches the sha256 hash of the HSMFD that is on the annotated script from the Ceremony 23 . Previous hash should read as below (image from Ceremony 23 annotated script). f6a5b2a1026f59cc694abe9faf8b7956c64760ff674464ed69dfd6e4c0141e21 Note: The CA should assign some attendees to confirm the hash displayed on the TV screen and the rest will confirm the hash written on the ceremony script.	JD	18:45

Start Logging Terminal Session

Step	Activity	Initials	Time
24.	CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code>	JD	18:45
25.	CA executes <code>script script-20160512.log</code> to start a capture of terminal output.	JD	18:46



Start Logging HSM Output

Step	Activity	Initials	Time
26.	CA connects a serial to USB null modem cable to laptop.	JD	18:46
27.	CA opens a second terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal . Follow the additional steps to maximize the terminal window: a) Click the View menu and select Zoom In b) Repeat the step above as necessary and executes <code>cd /media/HSMFD</code> and executes <code>stty -F /dev/ttyUSB0 115200</code> <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.	JD	18:48

Power Up HSM

Step	Activity	Initials	Time
28.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. HSM4: TEB# BB24646675 / serial # H1411011	JD	18:50
29.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	JD	18:51
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 displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) HSM4: serial # H1411011 Note: The HSM date and time was set from the factory.	JD	18:52



Enable/Activate HSM

Step	Activity	Initials	Time
31.	<p>One by one, CA calls each COs listed below to inspect the TEB for tamper evidence, opens the TEB and hands the OP cards to the CA who places the cards in cardholder visible to all.</p> <p>CO 2: Anne-Marie Eklund Lowinder OP TEB # BB46584315</p> <p>CO 3: Olaf Kolkman OP TEB # BB46584316</p> <p>CO 4: Robert Seastrom OP TEB # BB46584267</p> <p>CO 5: Christopher Griffiths OP TEB # BB46584317</p> <p>CO 6: Gaurab Upadhaya OP TEB # BB21907210</p>	JP	18:58
32.	<p>CA will perform the following steps to activate the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "1.Set Online" hit ENT to confirm c) When "Set Online?" is displayed, hit ENT to confirm d) When "Insert Card OP #?" is displayed, insert the OP card from the cardholder e) When "PIN?" is displayed, enter "11223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card <p>Confirm the "READY" led on the HSM is ON.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <u>2</u> of 7 2nd OP card <u>5</u> of 7 3rd OP card <u>3</u> of 7</p>	JP	19:01

Check Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
33.	CA connects HSM to laptop using Ethernet cable in LAN port.	JP	19:01
34.	CA switches to the terminal window and tests network connectivity between laptop and HSM by entering ping 192.168.0.2 and looking for responses. Ctrl-C to exit program.	JP	19:02



Insert 1st KSR to be signed

Step	Activity	Initials	Time
35.	The KSRs are downloaded to the KSRFD and transferred to the facility by the IKOS. CA plugs FD labeled "KSR2048" with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA shows the KSR file contents by: a) Double click file b) Select DISPLAY on the pop-up menu c) Maximize the window to show the contents Note: DO NOT save any changes on the file.	jo	19:05
36.	CA closes the KSR contents window and the file system window.	jo	19:05

Execute KSR signer

Step	Activity	Initials	Time
37.	CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR2048/ksr-root-2016-q3-0.xml</code>	jo	19:06
38.	The KSR signer will ask whether the HSM is activated or not as below. Activate HSM prior to accepting in the affirmative!! (y/N): CA confirms that the HSM is online and then enters "y" to proceed to verification. Note: DO NOT enter "y" for the "Is this correct y/n?" yet.	jo	19:07

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
39.	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to identify him/herself, present identification document for IW1 to retain and read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN. IW1 enters RZM representative's name here: <u>JOHN G. PANUMKAL</u>	jo	19:09
40.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?	jo	19:11
41.	CA then enters "y" in response to "Is this correct y/n?" to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in <code>/media/KSR2048/skr-root-2016-q3-0.xml</code>	jo	19:13



VERISIGN™

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

May 9th, 2016

VerisignInc.com

To Whom It May Concern:

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

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

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

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

Sincerely,

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



VERISIGN™

May 12, 2016

The SHA256 hash of the 2016 Q3 KSR file is:

**89a144a441ed218c00cdb001182fa490716795c6a4fecb6549ca2856a
4a982ad**

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

VerisignInc.com

The PGP wordlist for the hash above is:

nightbird outfielder crumpled Pandora cranky unify
blackjack megaton aardvark sandalwood ruffled adviser
beaming combustion regain millionaire hamlet graduate
preclude responsive regain yesteryear spheroid glossary
deckhand revenue breadline escapade regain passenger
miser perceptive

Attested on behalf of VeriSign by:

John Painumkal
Cryptographic Engineer IV
Cryptographic Business Operations
VeriSign, Inc.



ICANN Root DNSSEC KSK Ceremony 25

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

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

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

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

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

SHA256 hash of KSR:
A17E539793B261112C4F591A06AF4FBC2221DDDD71794BC72D5AEE910C72543
>> ratchet insurgent dwelling mosquito playhouse pioneer fallout Babylon atlas reproduce vapor miracle
ragtime hamburger upshot Wichita snapshot candidate Belfast tambourine stopwatch bookseller Pluto
pyramid highchair specialist robust ultimate assume retraction bombast decimal <<
Is this correct (y/N)? y

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

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

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

Figure 1



Print Copies of the Operation for Participants

Step	Activity	Initials	Time
42.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog krsigner-20160512-*.log; done</code> where krsigner-20160512-*.log is replaced by log output file displayed by program. This example generates X copies and hands copies to participants.	jo	19:17
43.	IW1 attaches a copy to his/her script and writes "KSR 2048"	jo	19:17

Backup Newly Created SKR

Step	Activity	Initials	Time
44.	CA copies the contents of the KSR FD by running <code>cp -p /media/KSR2048/* .</code> for posting back to RZM. Confirm overwrite by entering "y" when prompted.	jo	19:18
45.	CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR2048</code> flushes the system buffers: <code>sync</code> and then unmounts the KSR FD using <code>umount /media/KSR2048</code>	jo	19:19
46.	CA removes the FD KSR2048 containing SKR and gives it to the RZM representative.	jo	19:20

Insert 2nd KSR to be signed

Step	Activity	Initials	Time
47.	CA plugs FD labeled "KSR1024FB" with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA shows the KSR file contents by: a) Double click file b) Select DISPLAY on the pop-up menu c) Maximize the window to show the contents Note: DO NOT save any changes on the file.	jo	19:22
48.	CA closes the KSR contents window and the file system window.	jo	19:22

KSR 2048

Starting: ksrsigner Kjqmt7v /media/KSR2048/ksr-root-2016-q3-0.xml (at Thu May 12 19:06:19 2016 UTC)

Use HSM /opt/dnssec/aep.hsmconfig?

HSM /opt/dnssec/aep.hsmconfig activated.

setenv KEYPER_LIBRARY_PATH=/opt/dnssec

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

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

HSM slot 0 included

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

HSM Information:

Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper 9860-2
Serial: H1411011

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2016-04-01T00:00:00	2016-04-15T23:59:59	54549,60615	19036
2	2016-04-11T00:00:00	2016-04-25T23:59:59	60615	19036
3	2016-04-21T00:00:00	2016-05-05T23:59:59	60615	19036
4	2016-05-01T00:00:00	2016-05-15T23:59:59	60615	19036
5	2016-05-11T00:00:00	2016-05-25T23:59:59	60615	19036
6	2016-05-21T00:00:00	2016-06-04T23:59:59	60615	19036
7	2016-05-31T00:00:00	2016-06-14T23:59:59	60615	19036
8	2016-06-10T00:00:00	2016-06-24T23:59:59	60615	19036
9	2016-06-20T00:00:00	2016-07-05T23:59:59	46551,60615	19036

...VALIDATED.

Validate and Process KSR /media/KSR2048/ksr-root-2016-q3-0.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2016-07-01T00:00:00	2016-07-15T23:59:59	60615,46551	
2	2016-07-11T00:00:00	2016-07-25T23:59:59	46551	
3	2016-07-21T00:00:00	2016-08-04T23:59:59	46551	
4	2016-07-31T00:00:00	2016-08-14T23:59:59	46551	
5	2016-08-10T00:00:00	2016-08-24T23:59:59	46551	
6	2016-08-20T00:00:00	2016-09-03T23:59:59	46551	
7	2016-08-30T00:00:00	2016-09-13T23:59:59	46551	
8	2016-09-09T00:00:00	2016-09-24T23:59:59	46551	
9	2016-09-20T00:00:00	2016-10-05T23:59:59	39291,46551	

...PASSED.

SHA256 hash of KSR:

89A144A441ED218C00CDB001182FA490716795C6A4FECB6549CA2856A4A982AD

>> nightbird outfielder crumpled Pandora cranky unify blackjack megaton aardvark sandal wood ruffled adviser beaming combustion regain millionaire hamlet graduate preclude res pensive regain yesteryear spheroid glossary deckhand revenue breadline escapade regain passenger miser perceptive <<

Generated new SKR in /media/KSR2048/skr-root-2016-q3-0.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2016-07-01T00:00:00	2016-07-15T23:59:59	46551,60615	19036

2	2016-07-11T00:00:00	2016-07-25T23:59:59	46551	19036
3	2016-07-21T00:00:00	2016-08-04T23:59:59	46551	19036
4	2016-07-31T00:00:00	2016-08-14T23:59:59	46551	19036
5	2016-08-10T00:00:00	2016-08-24T23:59:59	46551	19036
6	2016-08-20T00:00:00	2016-09-03T23:59:59	46551	19036
7	2016-08-30T00:00:00	2016-09-13T23:59:59	46551	19036
8	2016-09-09T00:00:00	2016-09-24T23:59:59	46551	19036
9	2016-09-20T00:00:00	2016-10-05T23:59:59	46551,39291	19036

SHA256 hash of SKR:

FE137AB39140D5D79F9C7B3018A7B995E5341385A41E11AEE6FBE30843F3D561

>> woodlark barbecue keyboard pocketful pheasant Dakota sterling stethoscope quota October kickoff commando beaming paragraph sentence Montana topmost confidence Aztec leprosy regain Burlington Athens performance tracker Wichita tissue antenna crucial vertigo sterling frequency <<

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



Execute KSR signer

Step	Activity	Initials	Time
49.	CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR1024FB/ksr-root-2016-q3-fallback-1.xml</code>	JD	19:23
50.	The KSR signer will ask whether the HSM is activated or not as below. Activate HSM prior to accepting in the affirmative!! (y/N) : CA confirms that the HSM is online and then enters "y" to proceed to verification. Note: DO NOT enter "y" for the "Is this correct y/n?" yet.	JD	19:24

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
51.	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN.	JD	19:25
52.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?	JD	19:25
53.	CA then enters "y" in response to "Is this correct y/n?" to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in <code>/media/KSR1024FB/skr-root-2016-q3-fallback-1.xml</code>	JD	19:26

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
54.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog \$(ls -tr ksrsigner-20160512-*.log tail -n 1); done</code> This example generates X copies and hands copies to participants.	JD	19:30
55.	IW1 attaches a copy to his/her script and writes "KSR 1024 FallBack"	JD	19:30



VERISIGN™

May 12, 2016

The SHA256 hash of the 2016 Q3 fallback KSR file is:

**a12289b4292265658f403785cae5856d1c90e588afd959c5f9dc008c8
f6303da**

The PGP wordlist for the hash above is:

ratchet candidate nightbird politeness breakup candidate
fracture glossary payday Dakota clamshell leprosy
spellbind travesty music hazardous befriend millionaire
topmost maritime rocker supportive endow resistor waffle
sympathy aardvark megaton payday Galveston acme surrender

Attested on behalf of VeriSign by:

John Painumkal
Cryptographic Engineer IV
Cryptographic Business Operations
VeriSign, Inc.

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

VerisignInc.com

KSR 1024 FALLBACK

Starting: ksr signer Kjqmt7v /media/KSR1024FB/ksr-root-2016-q3-fallback-1.xml (at Thu May 12 19:23:25 2016 UTC)

Use HSM /opt/dnssec/aep.hsmconfig?

HSM /opt/dnssec/aep.hsmconfig activated.

setenv KEYPER_LIBRARY_PATH=/opt/dnssec

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

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

HSM slot 0 included

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

HSM Information:

Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper 9860-2
Serial: H1411011

Validating last SKR with HSM...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2016-04-01T00:00:00	2016-04-15T23:59:59	54549,60615	19036
2	2016-04-11T00:00:00	2016-04-25T23:59:59	60615	19036
3	2016-04-21T00:00:00	2016-05-05T23:59:59	60615	19036
4	2016-05-01T00:00:00	2016-05-15T23:59:59	60615	19036
5	2016-05-11T00:00:00	2016-05-25T23:59:59	60615	19036
6	2016-05-21T00:00:00	2016-06-04T23:59:59	60615	19036
7	2016-05-31T00:00:00	2016-06-14T23:59:59	60615	19036
8	2016-06-10T00:00:00	2016-06-24T23:59:59	60615	19036
9	2016-06-20T00:00:00	2016-07-05T23:59:59	46551,60615	19036

...VALIDATED.

Validate and Process KSR /media/KSR1024FB/ksr-root-2016-q3-fallback-1.xml...

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2016-07-01T00:00:00	2016-07-15T23:59:59	60615,46551	
2	2016-07-11T00:00:00	2016-07-25T23:59:59	46551	
3	2016-07-21T00:00:00	2016-08-04T23:59:59	46551	
4	2016-07-31T00:00:00	2016-08-14T23:59:59	46551	
5	2016-08-10T00:00:00	2016-08-24T23:59:59	46551	
6	2016-08-20T00:00:00	2016-09-03T23:59:59	46551	
7	2016-08-30T00:00:00	2016-09-13T23:59:59	46551	
8	2016-09-09T00:00:00	2016-09-24T23:59:59	46551	
9	2016-09-20T00:00:00	2016-10-05T23:59:59	46551	

...PASSED.

SHA256 hash of KSR:

A12289B4292265658F403785CAE5856D1C90E588AFD959C5F9DC008C8F6303DA

>> ratchet candidate nightbird politeness breakup candidate fracture glossary payday Da kota clamshell leprosy spellbind travesty music hazardous befriend millionaire topmost maritime rocker supportive endow resistor waffle sympathy aardvark megaton payday Galve ston acme surrender <<

Generated new SKR in /media/KSR1024FB/ksr-root-2016-q3-fallback-1.xml

#	Inception	Expiration	ZSK Tags	KSK Tag(CKA_LABEL)
1	2016-07-01T00:00:00	2016-07-15T23:59:59	46551,60615	19036

2	2016-07-11T00:00:00	2016-07-25T23:59:59	46551	19036
3	2016-07-21T00:00:00	2016-08-04T23:59:59	46551	19036
4	2016-07-31T00:00:00	2016-08-14T23:59:59	46551	19036
5	2016-08-10T00:00:00	2016-08-24T23:59:59	46551	19036
6	2016-08-20T00:00:00	2016-09-03T23:59:59	46551	19036
7	2016-08-30T00:00:00	2016-09-13T23:59:59	46551	19036
8	2016-09-09T00:00:00	2016-09-24T23:59:59	46551	19036
9	2016-09-20T00:00:00	2016-10-05T23:59:59	46551	19036

SHA256 hash of SKR:

14D771445AA6E51E553856D5EA8C38248DA9B0FF68AE5C3475E6D3350FE93DAA

>> baboon stethoscope hamlet designing enlist paragon topmost Burlington edict consulting egghead specialist Trojan megaton classic Capricorn optic passenger ruffled Yucatan frighten performance escape confidence indulge trombonist stapler conformist artist ultimate commence pedigree <<

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



Backup Newly Created SKR

Step	Activity	Initials	Time
56.	CA copies the contents of the KSR FD by running <code>cp -p /media/KSR1024FB/* .</code> for posting back to RZM. Confirm overwrite by entering "y" when prompted.	jo	19:31
57.	CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR1024FB</code> flushes the system buffers: <code>sync</code> and then unmounts the KSR FD using <code>umount /media/KSR1024FB</code>	jo	19:32
58.	CA removes the FD KSR1024FB containing SKR and gives it to the RZM representative.	jo	19:33

Disable/Deactivate HSM

Step	Activity	Initials	Time
59.	CA makes sure to utilize the cards that were NOT used to activate the HSM are used to deactivate the HSM. CA will perform the following steps to deactivate the HSM: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select " 2.Set Offline " hit ENT to confirm c) When " Set Offline? " is displayed, hit ENT to confirm d) When " Insert Card OP #? " is displayed, insert the OP card from the cardholder e) When " PIN? " is displayed, enter " 11223344 " hit ENT f) When " Remove Card? " is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP cards Confirm the " READY " led on the HSM is OFF . IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card <u>4</u> of 7 2nd OP card <u>6</u> of 7 3rd OP card <u>3</u> of 7	jo	19:36



Act 3. Secure Hardware and Close the Ceremony

Return HSM to a TEB

Step	Activity	Initials	Time
1.	CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.	JD	19:37
2.	CA places the HSM into a prepared TEB and seals it.	JD	19:39
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM4: TEB# BB24646658/ serial # H1411011 IW1 and CA initials the TEB and keeps the sealing strip for later inventory. CA places item on equipment cart.	JD	19:41

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
4.	Closing ttyaudit terminal window CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of ttyaudit terminal window by typing "exit".	JD	19:41
5.	Terminating the logging script CA stops logging terminal output by entering "exit" in the other terminal window. This only stops the script logging and will NOT close window.	JD	19:42



Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA set dotglob by executing <code>shopt -s dotglob</code> This allows copying everything in the original HSMFD.	JD	19:42
7.	CA calculates the sha256hash of the contents on the original HSMFD. <code>find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum</code>	JD	19:43
8.	CA copy and paste the sha256hash and paste it on Text Editor by going to Applications > Accessories > Text Editor	JD	19:44
9.	CA prints two copies of the hash. One for the audit bundle and the other for the HSMFD package then writes "KSK 25" on the printed copies.	JD	19:45
10.	CA displays contents of HSMFD by executing <code>ls -ltr</code>	JD	19:47
11.	CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the O/S (as HSMFD_); and copies the contents of the HSMFD to the blank drive for backup by executing <code>cp -Rp * /media/HSMFD_</code>	JD	19:49
12.	CA displays contents of HSMFD_ by executing <code>ls -ltr /media/HSMFD_</code>	JD	19:49
13.	Calculate the sha256hash of the contents on the copied HSMFD. <code>find -P /media/HSMFD_ -type f -print0 sort -z xargs -0 cat sha256sum</code> Confirm that it matches the sha256hash of the original HSMFD by using the text editor to copy and paste the hash for comparison.	JD	19:51
14.	CA unmounts new FD using <code>umount /media/HSMFD_</code>	JD	19:51
15.	CA removes HSMFD_ and places it on the table.	JD	19:51
16.	CA repeats step 11 to 15 for the 2 nd copy	JD	19:53
17.	CA repeats step 11 to 15 for the 3 rd copy	JD	19:55
18.	CA repeats step 11 to 15 for the 4 th copy	JD	19:56
19.	CA repeats step 11 to 15 for the 5 th copy	JD	19:57

Print Logging Information

Step	Activity	Initials	Time
20.	CA prints out a hard copy of logging information by executing <code>enscript -2Gr -# 1 script-20160512.log</code> <code>enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20160512-*.log</code> for attachment to IW1 script. Note: ignore the error regarding non-printable characters if prompted.	JD	19:59

800faf1265dc41a79cfa35135118fd59edbdffc21b4b6ed887fb484166d3df629

05/12/16
19:41:24

ttyaudit-ttyUSB0-20160512-184752.log

```
2016-05-12T18:51:31+0000 ttyUSB0
2016-05-12T18:51:31+0000 ttyUSB0 H1411011 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2016-05-12T18:51:31+0000 ttyUSB0
2016-05-12T18:51:31+0000 ttyUSB0 BBL CRC32: 0x757574CA
2016-05-12T18:51:31+0000 ttyUSB0
2016-05-12T18:51:31+0000 ttyUSB0 Running applicationBootLoader at 0xEFDCC0000
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 H1411011 011403 ABL 011 : Tamper Challenge Response Key
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 ABL CRC32: 0xE7E0FAGA
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 #####
2016-05-12T18:51:32+0000 ttyUSB0 ## ABL tamper records ##
2016-05-12T18:51:32+0000 ttyUSB0 #####
2016-05-12T18:51:32+0000 ttyUSB0 Current Tamper Counts (decimal 0-255):
2016-05-12T18:51:32+0000 =====
2016-05-12T18:51:32+0000 ttyUSB0 vextoosTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 vintoosTamperCount: 12
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 vbboosTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 maxstrtempTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 minstrtempTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 meshTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 extampSNKTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 extampINKTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 tempdiffTamperCount: 0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 pf7TamperCount: 12
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 restartTamperCount: 25
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 Current tamper bitmaps:
2016-05-12T18:51:32+0000 ttyUSB0
2016-05-12T18:51:32+0000 ttyUSB0 =====
2016-05-12T18:51:32+0000 ttyUSB0 currentTamper bitmap: 0x0000 0b .....
2016-05-12T18:51:32+0000
```


05/12/16
19:41:24

ttyaudit-ttyUSB0-20160512-184752.log

```
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 Running DES POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 DES POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running Triple DES POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 Triple DES POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running AES POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 AES POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running SHA1 POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 SHA1 POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running SHA2 POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 SHA2 POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running RandomGen POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 RandomGen POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running RSA POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 RSA POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running DSA POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 DSA POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Running ECC POST Test
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 ECC POST Test Passed
2016-05-12T18:51:37+0000 ttyUSB0 Audit on 12/5/2016 18:27:58 00100008
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 Keyper 9860-2 Serial Number Hi411011
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 Memory Usage:
2016-05-12T18:51:37+0000 ttyUSB0 RAM (free/total) 197Mb/256Mb
2016-05-12T18:51:37+0000 ttyUSB0 Flash (free/total) 127Mb/128Mb
2016-05-12T18:51:37+0000 ttyUSB0
2016-05-12T18:51:37+0000 ttyUSB0 black store 450b
```


05/12/16
19:41:24

ttyaudit-ttyUSB0-20160512-184752.log

```
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 statistics 112b
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 other 116b
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 RedStore (free/total) 109Kb/128Kb
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 Network Configuration:
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 IPv4: enabled
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 IPv6: enabled
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B3:2A / 192.168.0.2/24 , 2001::2e0:6ff:Fec0:b32a/64
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 HSM Port: 05000
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 HSM Gateway(s): 0.0.0.0 :
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 Software Versions:
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 BBL 010 ABL 011 App 023
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 CPLD Version:
2016-05-12T18:51:39+0000 ttyUSB0 1.9
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 SCR Firmware Version:
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 Audit on 12/5/2016 18:27:59 00100003
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 Audit on 12/5/2016 18:36:00 00200069 0680004A7A73296D
2016-05-12T18:51:39+0000 ttyUSB0
2016-05-12T18:51:39+0000 ttyUSB0 Audit on 12/5/2016 18:36:49 00200069 0680004A7B33296D
2016-05-12T18:51:39+0000 ttyUSB0
```

05/12/16
19:41:24

ttyaudit-ttyUSB0-20160512-184752.log

```
2016-05-12T19:00:59+0000 ttyUSB0 Audit on 12/5/2016 18:37:19 00200069 0880004A7AB3296D
2016-05-12T19:00:59+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0 TcpListener: Created IPv4 socket 15 on port 5000.
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:02+0000 ttyUSB0 TcpListener: Created IPv6 socket 16 on port 5000.
2016-05-12T19:01:02+0000 ttyUSB0
2016-05-12T19:01:03+0000 ttyUSB0 Audit on 12/5/2016 18:37:23 00100002
2016-05-12T19:01:03+0000 ttyUSB0
2016-05-12T19:06:59+0000 ttyUSB0
2016-05-12T19:06:59+0000 ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-05-12T19:12:46+0000 ttyUSB0
2016-05-12T19:12:46+0000 ttyUSB0
2016-05-12T19:12:46+0000 ttyUSB0
2016-05-12T19:12:46+0000 ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-05-12T19:12:46+0000 ttyUSB0
2016-05-12T19:23:54+0000 ttyUSB0
2016-05-12T19:23:54+0000 ttyUSB0
2016-05-12T19:23:54+0000 ttyUSB0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2016-05-12T19:26:19+0000 ttyUSB0
2016-05-12T19:26:19+0000 ttyUSB0
2016-05-12T19:26:19+0000 ttyUSB0
2016-05-12T19:34:36+0000 ttyUSB0
2016-05-12T19:34:36+0000 ttyUSB0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2016-05-12T19:35:51+0000 ttyUSB0
2016-05-12T19:35:51+0000 ttyUSB0 Audit on 12/5/2016 19:10:56 00200069 0880004A83E3296D
2016-05-12T19:36:23+0000 ttyUSB0
2016-05-12T19:36:23+0000 ttyUSB0 Audit on 12/5/2016 19:12:11 00200069 0880004A7B73296D
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0 TcpListener: Closed IPv4 socket 15 on port 5000.
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0 TcpListener: Closed IPv6 socket 16 on port 5000.
2016-05-12T19:36:29+0000 ttyUSB0
2016-05-12T19:36:29+0000 ttyUSB0 Audit on 12/5/2016 19:12:50 00100003
2016-05-12T19:36:29+0000 ttyUSB0
```

05/12/16
19:42:02

script-20160512.log

```
Script started on Thu 12 May 2016 06:45:56 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.1033[1033[K
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=.43 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.372 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.649 ms

--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.372/0.819/1.438/0.452 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsl\007gner Kjgmt7v /m
edia/KSR2048/ksr-root-2016-q3-0.xml
Starting: ksrsgner Kjgmt7v /media/KSR2048/ksr-root-2016-q3-0.xml (at Thu May 12 19:06
:19 2016 UTC)
Use HSM /opt/dnssec/aep.hsmcconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y
```

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

```
Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2016-04-01T00:00:00 2016-04-15T23:59:59 54549,60615 19036
2 2016-04-11T00:00:00 2016-04-25T23:59:59 60615 19036
3 2016-04-21T00:00:00 2016-05-05T23:59:59 60615 19036
4 2016-05-01T00:00:00 2016-05-15T23:59:59 60615 19036
5 2016-05-11T00:00:00 2016-05-25T23:59:59 60615 19036
6 2016-05-21T00:00:00 2016-06-04T23:59:59 60615 19036
7 2016-05-31T00:00:00 2016-06-14T23:59:59 60615 19036
8 2016-06-10T00:00:00 2016-06-24T23:59:59 60615 19036
9 2016-06-20T00:00:00 2016-07-05T23:59:59 46551,60615 19036
...VALIDATED.
```

```
Validate and Process KSR /media/KSR2048/ksr-root-2016-q3-0.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2016-07-01T00:00:00 2016-07-15T23:59:59 60615,46551
2 2016-07-11T00:00:00 2016-07-25T23:59:59 46551
3 2016-07-21T00:00:00 2016-08-04T23:59:59 46551
4 2016-07-31T00:00:00 2016-08-14T23:59:59 46551
5 2016-08-10T00:00:00 2016-08-24T23:59:59 46551
6 2016-08-20T00:00:00 2016-09-03T23:59:59 46551
7 2016-08-30T00:00:00 2016-09-13T23:59:59 46551
8 2016-09-09T00:00:00 2016-09-24T23:59:59 46551
9 2016-09-20T00:00:00 2016-10-05T23:59:59 39291,46551
...PASSED.
```

```
SHA256 hash of KSR:
89A14A441E218C00CDB001182FA490716795C6A4FECB6549CA2856A4A982AD
>> nightbird outfielder crumpled Pandora cranky unify blackjack megaton aardvark sanda
lwood ruffled adviser beaming combustion regain millionaire hamlet graduate preclude r
esponsive regain yesterday spheroid glossary deckhand revenue headline escapade rega
in passenger miser perceptive <<
```

```
Is this correct (Y/N)? y
Generated new SKR in /media/KSR2048/ksr-root-2016-q3-0.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2016-07-01T00:00:00 2016-07-15T23:59:59 46551,60615 19036
2 2016-07-11T00:00:00 2016-07-25T23:59:59 46551 19036
3 2016-07-21T00:00:00 2016-08-04T23:59:59 46551 19036
4 2016-07-31T00:00:00 2016-08-14T23:59:59 46551 19036
5 2016-08-10T00:00:00 2016-08-24T23:59:59 46551 19036
6 2016-08-20T00:00:00 2016-09-03T23:59:59 46551 19036
7 2016-08-30T00:00:00 2016-09-13T23:59:59 46551 19036
8 2016-09-09T00:00:00 2016-09-24T23:59:59 46551 19036
9 2016-09-20T00:00:00 2016-10-05T23:59:59 46551,39291 19036
```

```
SHA256 hash of SKR:
FE137AB391405D79F9C7B3018A7B995E5341385A41E11AE86FB3E0843F3D561
>> woodlark barbecue keyboard pocketful pleasant Dakota sterling stethoscope quota Oc
ober kickoff commando beaming paragraph sentence Montana topmost confidence Aztec lef
osy regain Burlington Athens performance tracker Wichita tissue antenna crucial verti
o sterling frequency <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
***** log output in ./ksrsgner-20160512-190619.log *****
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# for i in $(seq 15); do
rln\007;log ksr\007
ksr-root-2010-q3-2.xml ksrsgner-20110511-181632.log
ksr-root-2011-q1-0.xml ksrsgner-20110930-181607.log
ksr-root-2011-q3-0.xml ksrsgner-20120522-151741.log
ksr-root-2012-q1-0.xml ksrsgner-20121112-151522.log
ksr-root-2012-q3-0.xml ksrsgner-20130502-190252.log
ksr-root-2013-q1-0.xml ksrsgner-20130502-190633.log
ksr-root-2013-q3-0.xml ksrsgner-20131024-184618.log
ksr-root-2014-q1-0.xml ksrsgner-20140417-183604.log
ksr-root-2014-q3-0.xml ksrsgner-20141120-201132.log
ksr-root-2015-q1-0.xml ksrsgner-20150409-183038.log
ksr-root-2015-q3-0.xml ksrsgner-20150409-193635.log
ksr-root-2016-q1-0.xml ksrsgner-20150409-205227.log
ksrsgner-20100616-214329.log ksrsgner-20151112-193232.log
ksrsgner-20101101-181303.log ksrsgner-20151112-193232.log
ksrsgner-20110511-181351.log
[root@localhost HSMFD]# for i in $(seq 15); do printlog ksr
ksr-root-2010-q3-2.xml ksrsgner-20110511-181632.log
ksr-root-2011-q1-0.xml ksrsgner-20110930-181607.log
ksr-root-2011-q3-0.xml ksrsgner-20120522-151741.log
ksr-root-2012-q1-0.xml ksrsgner-20121112-151522.log
ksr-root-2012-q3-0.xml ksrsgner-20130502-190252.log
ksr-root-2013-q1-0.xml ksrsgner-20130502-190633.log
ksr-root-2013-q3-0.xml ksrsgner-20131024-184618.log
ksr-root-2014-q1-0.xml ksrsgner-20140417-183604.log
ksr-root-2014-q3-0.xml ksrsgner-20141120-201132.log
ksr-root-2015-q1-0.xml ksrsgner-20150409-183038.log
ksr-root-2015-q3-0.xml ksrsgner-20150409-193635.log
ksrsgner-20100616-214329.log ksrsgner-20151112-193232.log
ksrsgner-20101101-181303.log ksrsgner-20151112-193232.log
ksrsgner-20110511-181351.log
[root@localhost HSMFD]# for i in $(seq 15); do printlog ksrsg
done
{ 2 pages * i copy } sent to printer
3 lines were wrapped
i 2 pages * i copy } sent to printer
3 lines were wrapped
```


Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initials	Time
21.	CA unmounts HSMFD by executing cd /tmp then umount /media/HSMFD CA removes HSMFD.	jo	20:00
22.	After all print jobs are complete, CA d) Turns off the laptop by pressing the power switch e) Turns on the laptop by pressing the power switch f) Remove the O/S DVD from the drive g) Turns off the laptop again by pressing the power switch	jo	20:01
23.	CA places TWO HSMFDs and two OS/DVD, paper with printed hash in prepared TEB; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. O/S DVD (release 20160503) + HSMFD: TEB# BB46584299	jo	20:04
24.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.	jo	20:04

Distribute HSMFDs

Step	Activity	Initials	Time
25.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 2 for IKOS) to post SKR to RZM, and to review, analyze and improve on procedures.	jo	20:05

Returning Laptop to a TEB

Step	Activity	Initials	Time
26.	CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. Laptop1 (Dell ATG6400): TEB# BB24646657 / serial # 41593712005	jo	20:07
27.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.	jo	20:08



Returning OP Cards to TEBs

Step	Activity	Initials	Time
28.	<p>CA calls each COs to the front of the room one at a time and repeats the steps below.</p> <ul style="list-style-type: none"> a) CA takes the TEB prepared for the CO and reads out the number and description while showing the bag to IW1 and CO. Figure 2 below for an example. b) CO places the OP card into the plastic case. c) CA places the plastic case into the TEB, seals in front of IW1 and CO then the CA initials TEB and strip. d) IW1 inspects each TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. e) CA hands TEB containing the OP card to the CO. CO inspects and verifies TEB # and contents then initials his/her TEB. f) CO enters completion time and signs for TEB in the table below in IW1's script. IW1 initials table entry. g) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB. <p>CO 2: Anne-Marie Eklund Lowinder OP TEB # BB46584651</p> <p>CO 3: Olaf Kolkman OP TEB # BB46584302</p> <p>CO 4: Robert Seastrom OP TEB # BB46584303</p> <p>CO 5: Christopher Griffiths OP TEB # BB46584541</p> <p>CO 6: Gaurab Upadhaya OP TEB # BB46584298</p> <p><i>NOTE: CO 3 ALSO SIGNATURE SEALING STRIP Due To Lowinder</i></p>	<p>DD</p>	<p>20:30</p>



CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 2	OP 2 of 7	BB46584651	Anne-Marie Eklund Lowinder		12 May 2016	20:12	
CO 3	OP 3 of 7	BB46584302	Olaf Kolkman		12 May 2016	20:20	
CO 4	OP 4 of 7	BB46584303	Robert Seastrom		12 May 2016	20:24	
CO 5	OP 5 of 7	BB46584541	Christopher Griffiths		12 May 2016	20:27	
CO 6	OP 6 of 7	BB46584298	Gaurab Upadhaya		12 May 2016	20:30	

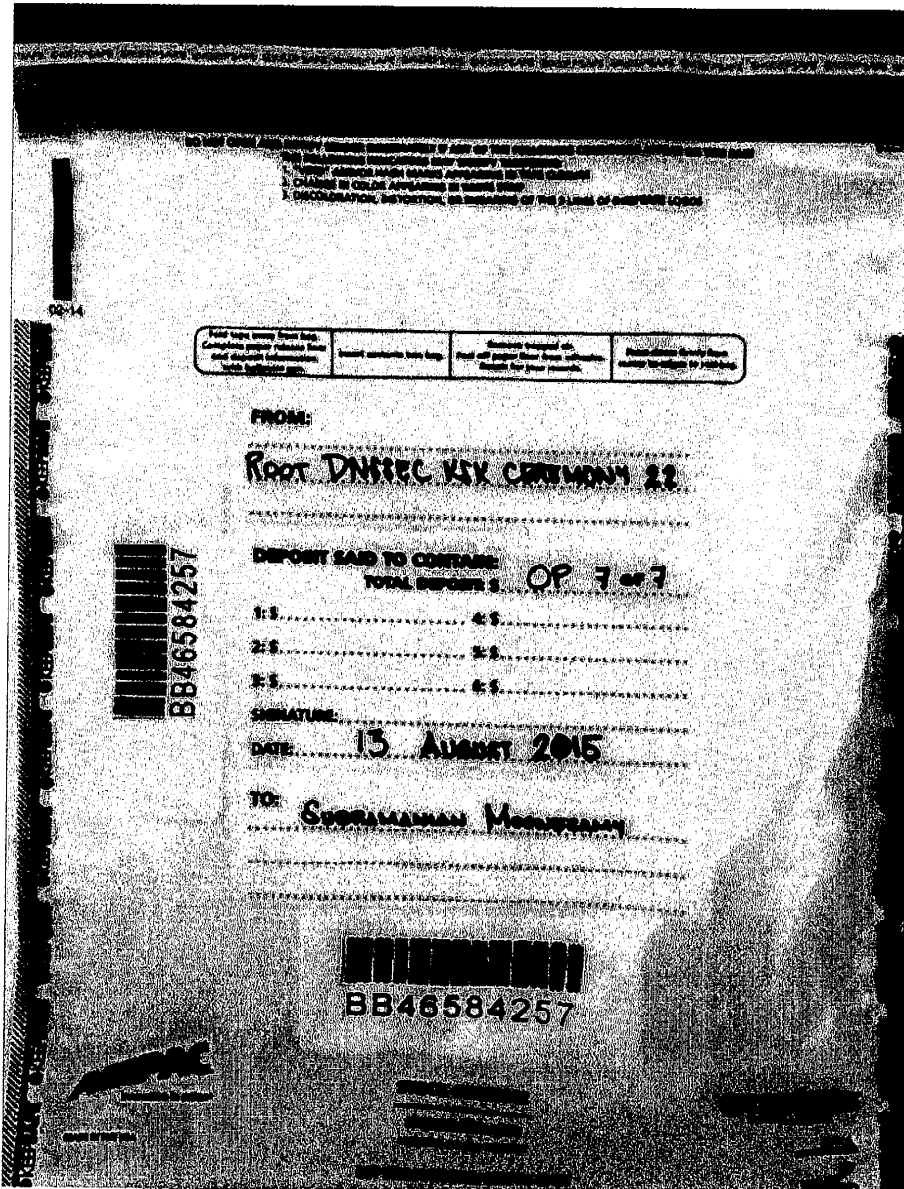


Figure 2



Returning Equipment to Safe #1

Step	Activity	Initials	Time
29.	CA, IW1, SSC1 open safe room and enter with equipment cart.	jo	20:33
30.	SSC1 opens Safe #1 shielding combination from camera.	jo	20:39
31.	SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	jo	20:42
32.	CA records return of HSM4 in next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA CAREFULLY places the HSMs into Safe #1 and IW1 initials the entry. HSM4: TEB# BB24646658	jo	20:44
33.	CA records return of laptop in next entry field of safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry. Laptop1 (Dell ATG6400): TEB# BB24646657	jo	20:46
34.	CA records return of O/S DVD + HSMFD in next entry field of safe log with TEB #, printed name, date, time, and signature; places the O/S DVD + HSMFD into Safe #1 and IW1 initials the entry. O/S DVD (release 20160503) + HSMFD: TEB# BB46584299	jo	20:47

Close Equipment Safe #1

Step	Activity	Initials	Time
35.	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	jo	20:47
36.	SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise). IW1 and CA verify safe is locked and door indicator light is green.	jo	20:44
37.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.	jo	20:50

Open Credential Safe #2

Step	Activity	Initials	Time
38.	After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP and SO cards (if applicable) in TEBs with them.	jo	20:52
39.	SSC2 opens Safe #2 while shielding combination from camera.	jo	20:53
40.	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	jo	20:55



CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
41.	<p>One by one, each COs along with the CA (using his/her common key):</p> <p>a) Open his/her respective safe deposit box and read out box number inside Safe #2. # Common Key is bottom lock and CO Key is top lock</p> <p>b) CO makes an entry into the safe log indicating the return of OP card and SO cards (if applicable) including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB #s and card type to his/her script.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>c) CO shows each TEB to the camera and then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA.</p> <p>Repeat the steps above until all cards are returned to the deposit box.</p> <p>CO 2: Anne-Marie Eklund Lowinder Box # 1259 OP TEB # BB46584651</p> <p>CO 3: Olaf Kolkman Box # 1239 OP TEB # BB46584302</p> <p>CO 4: Robert Seastrom Box # 1260 OP TEB # BB46584303</p> <p>CO 5: Christopher Griffiths Box # 1240 OP TEB # BB46584541</p> <p>CO 6: Gaurab Upadhaya Box # 1261 OP TEB # BB46584298</p>	<p style="text-align: center;">JN</p>	<p style="text-align: center;">21:03</p>



Close Credential Safe #2

Step	Activity	Initials	Time
42.	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "Close safe" into the safe log. IW1 initials the entry. <i>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</i>	JD	21:04
43.	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). IW1 and CA verify safe is locked and door indicator light is green.	JD	21:05
44.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	JD	21:05

Participant Signing of IW1's Script

Step	Activity	Initials	Time
45.	One by one, all participants come to the front of the room, confirms printed name and date. Then, the participant declares that this script is a true and accurate record of the ceremony by signing on IW1's script coversheet. IW1 records the completion time once all participants have signed the coversheet. <i>Note: If entry is pre-printed, verify the entry and sign.</i>	JD	21:07
46.	CA reviews IW1's script and signs it.	JD	21:07

Online Streaming Stops

Step	Activity	Initials	Time
47.	CA acknowledges the participation of online participants and confirms with SA to stop online streaming.	JD	21:18


Signing Out of Ceremony Room

Step	Activity	Initials	Time
48.	IKOS ensures that all participants sign out of Ceremony Room log and are escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.	JD	21:29

Filming Stops

Step	Activity	Initials	Time
49.	CA confirms with SA to stop filming.	JD	21:30

Copying and Storing the Script

Step	Activity	Initials	Time
50.	IW1 makes at least 1 copy of his/her script for off-site audit bundle. Audit bundles each contain: a) Output of signer system – HSMFD b) Copy of IW1's key ceremony script c) Audio-visual recording d) Logs from the Physical Access Control and Intrusion Detection System (Range is 11/12/2015 – 05/12/2016) e) The IW1 attestation (A.1 below) f) SA attestation (A.2, A.3 below) All in a TEB labeled " Root DNSSEC KSK Ceremony 25 ", dated and signed by IW1 and CA . Off-site audit bundle is delivered to off-site storage. The CA holds the ultimate responsibility for finalizing the audit bundle.		22:42

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

Audit Bundle Checklist:

1. Output of Signer System (CA)

One electronic copy (physical flash drive) of the HSMFD in each audit bundle, each placed within a tamper-evident bag, labeled, dated and signed by the CA and the IW1

2. Key Ceremony Scripts (IW1)

Hard copies of the IW1's key ceremony scripts, including the IW1's notes and the IW1's attestation. See Appendix A.1.

3. Audio-visual recordings from the key ceremony (SA1)

One set for the original audit bundle and the other for duplicate.

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

One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC-IDS configuration review, the list of the enrolled users, the event log file and the configuration audit log file in each audit bundle, each placed in a tamper-evident bag, labeled, dated and signed by the SA1 and the IW1.

IW1 confirms the contents of the logs before placing the logs in the audit bundle.

5. Configuration review of the Physical Access Control and Intrusion Detection System (SA1)

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

6. Configuration review of the Firewall System (SA1)

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

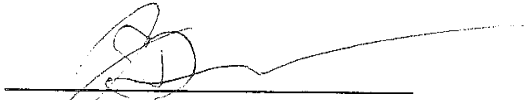
7. Other items

If applicable.

A.1 Key Ceremony Script (by IW1)

I hereby attest that the Key Ceremony was conducted in accordance with this script and any exceptions that may have occurred were accurately and properly documented.

Jonathan Denison



Date: 12 May 2016

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

I have reviewed the access control system configuration, the configuration audit log and the assigned authorizations from the other KMF and not found any discrepancies or anything else out of the ordinary.

Enclosed are the configuration audit log, the list of assigned authorizations and the screenshots of the roles configurations.

Enclosed is also an electronic copy of the event log from the access control system ranging from the last log extraction on **12 November 2015 00:00 UTC** to now.

Connor Barthold



Date: 12 May 2016

A.3 Firewall Configuration Review (by SA1)

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

Enclosed is the configuration extract from the firewall unit.

Connor Barthold



Date: 12 May 2016


```
root@srx# run show configuration | no-more
## Last commit: 2015-03-20 05:33:11 UTC by reed
version 12.1X44-D35.5;
system {
    host-name srx;
    domain-name ksk.cjr.dns.icann.org;
    location {
        country-code US;
        postal-code 22701;
        building TerreMark-Admin;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "xxxxxxxxxxxx"; ## SECRET-DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user reed {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
    }
}
services {
    ssh {
        root-login allow;
    }
}
syslog {
```

```

archive size 100k files 3;
user * {
    any emergency;
}
file messages {
    any critical;
    authorization info;
}
file interactive-commands {
    interactive-commands error;
}
}
max-configurations-on-flash 5;
max-configuration-rollback 20;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
processes {
    idp-policy disable;
}
ntp {
    server 129.6.15.28;
    server 129.6.15.29;
    source-address 10.4.29.1;
}
}
interfaces {
    interface-range interfaces-trust {
        member ge-0/0/1;
        member fe-0/0/2;
        member fe-0/0/3;
        member fe-0/0/4;
        member fe-0/0/5;
        member fe-0/0/6;
        member ge-0/0/0;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
}
fe-0/0/7 {
    unit 0 {
        family inet {
            address 10.100.1.1/24;
        }
    }
}

```

```

    }
  }
  ge-1/0/0 {
    unit 0 {
      family inet {
        address 152.194.1.148/28;
      }
    }
  }
  vlan {
    unit 0 {
      family inet {
        address 10.4.29.1/24;
      }
    }
  }
}
routing-options {
  static {
    route 0.0.0.0/0 next-hop 152.194.1.145;
  }
}
security {
  nat {
    source {
      rule-set trust-to-untrust {
        from zone trust;
        to zone untrust;
        rule source-nat-rule {
          match {
            source-address 0.0.0.0/0;
          }
          then {
            source-nat {
              interface;
            }
          }
        }
      }
    }
    rule-set media-to-untrust {
      from zone media;
      to zone untrust;
      rule source-nat-rule-1 {
        match {
          source-address 0.0.0.0/0;
        }
        then {
          source-nat {
            interface;
          }
        }
      }
    }
  }
}

```

```

    }
  }
}
policies {
  from-zone trust to-zone untrust {
    policy trust-to-untrust {
      match {
        source-address localnet;
        destination-address [ icann dns simplexgrinnell
simplexgrinnell2 simplex simplex2 icann google ];
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
  from-zone media to-zone untrust {
    policy media-to-untrust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
}
zones {
  security-zone trust {
    address-book {
      address localnet 10.4.29.0/24;
    }
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
  }
}

```

```

    }
    interfaces {
        vlan.0;
    }
}
security-zone untrust {
    address-book {
        address icann dns 199.4.28.0/22;
        address simplexgrinnell 12.30.47.110/32;
        address simplexgrinnell2 205.145.182.128/32;
        address simplex 216.224.218.31/32;
        address simplex2 216.224.219.32/32;
        address icann 192.0.32.0/20;
        address google 8.8.8.8/32;
    }
    interfaces {
        ge-1/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone media {
    interfaces {
        fe-0/0/7.0;
    }
}
}
}
applications {
    application sg {
        protocol udp;
        source-port 3060;
        destination-port 3061;
    }
    application sg2 {
        protocol udp;
        source-port 3065;
        destination-port 3061;
    }
    application simplexout {
        protocol udp;
        source-port 3060;
        destination-port 18031;
    }
    application simplexout2 {
        protocol udp;
    }
}

```

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

```
[edit]
root@srx#
```