

Root DNSSEC KSK Ceremony 27

Thursday October 27, 2016

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

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

Abbreviations

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

Participants

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

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

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

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

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

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

Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.		1702
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.		1702

1704

Emergency Evacuation Procedures and Electronics Policy

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

Verify Time and Date

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

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.		1709
8.	SSC2, while shielding combination from camera, opens Safe #2.		1710
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 the 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>		1711

version 2.0

Close Credential Safe #2

Step	Activity	Initials	Time
11.	Once all relevant deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		1723
12.	SSC2 puts log in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		1724
13.	IW1, CA, SSC2, and Cos leave safe room, with OP cards and SO cards (if applicable) in TEBs, closing the door behind them.		1725

Open Equipment Safe #1

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

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	<p>CA CAREFULLY removes HSM1, HSM2, HSM3 and HSM4 (in TEB) from the safe and completes the entry on the safe log indicating HSMs Removal, TEB # and serial number, printed name, date, time, and signature. CA then places the items on the equipment cart. IW1 initials this entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>HSM1: TEB# BB24706804 / serial # K6002016</p> <p>HSM2: TEB# BB24646674 / serial # K6002013</p> <p>HSM3: TEB# BB24646616 / serial # H1403032</p> <p>HSM4: TEB# BB24646658 / serial # H1411011</p>		1730
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 then places the items on the equipment cart. IW1 initials each entry.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997</p> <p>O/S DVD (release 20160503) + HSMFD: TEB# BB46584299</p> <p>Verify the integrity of the other Laptop that will not be used this time and return it to the safe.</p> <p>Laptop1 (Dell ATG6400): TEB# BB24646657 / serial # 41593712005</p>		1732

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>		1733
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 verifies that the safe is locked and the "WAIT" light indicator is off.</p>		1734
21.	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.		1734

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

OS/DVD Acceptance Test

Step	Activity	Initials	Time
1.	CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997		1737
2.	CA inspects the O/S DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. O/S DVD (release 20160503) + HSMFD: TEB# BB46584299		1738
3.	CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on the key ceremony table; discards TEBs; connects laptop power, external display, general purpose external DVD drive and boots laptop from O/S DVD (release 20160503).		1744
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		1745
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		1746

Step	Activity	Initials	Time
6.	<p>CA inserts the new O/S DVD release 20161014 into the external DVD drive, waits for it to be recognized by the O/S and performs the following:</p> <ul style="list-style-type: none"> 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> <p>SHA256 hash for release 20161014:</p> <p>991f7be8cfbc3b4bdb6f5e5f84092486755a08a3c36712e37a26ccd808631692</p> <p>IW1 and participants confirm that the result matches the above, which also matches the one published on: https://data.iana.org/ksk-ceremony/27/KC-20161014.iso.sha256</p>		1750
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.		1751
8.	CA repeats step 6 and 7 for the 2 nd copy of the new O/S DVD release 20161014 .		1754
9.	<p>IW1 records the date, time then affixes his/her signature upon successful completion of the O/S DVD release 20161014 acceptance testing:</p> <p>O/S DVD Acceptance Test release 20161014</p> <p>Printed Name Patrick Jones</p> <p>Date 2016/10/27</p> <p>Time _____</p> <p>Signature _____</p>		1755
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) Turn off the laptop by pressing the power switch b) Turn on the laptop by pressing the power switch and immediately remove the old O/S DVD (release 20160503) from the laptop DVD drive c) Disconnect the laptop power to power off the laptop 		1757
11.	CA discards all the old O/S DVD (release 20160503) copies.		1759

Set Up Laptop

Step	Activity	Initials	Time
12.	CA connects the laptop power, printer and boots the laptop using the new O/S DVD release 20161014.		1803
13.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes <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		1804
14.	CA confirms that the printer is connected then configures printer as default and prints test page by going to System > Administration > Printing And follow the steps below: a) Click the New Printer icon (left side), leave everything default and then click the button Forward b) Under "Select Connection" choose the <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 " h) Close the printer setup windows		1806
15.	CA opens a terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal Follow the additional steps to maximize the terminal window: c) Click the View menu and select Zoom In d) Repeat the step above as necessary		1807
16.	CA updates the date and time on the laptop while referencing from the 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 "20161027 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.		1808

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.		1914
18.	CA repeats step 17 for the 2 nd blank FD		1914
19.	CA repeats step 17 for the 3 rd blank FD <i>bad / replaced no</i>		1915
20.	CA repeats step 17 for the 4 th blank FD		1916
21.	CA repeats step 17 for the 5 th blank FD		1916
22.	CA repeats step 17 for the 6 th blank FD		1917
23.	CA repeats step 17 for the 7 th blank FD		1917

Connect HSMFD

Step	Activity	Initials	Time
24.	CA plugs the previous HSMFD used in the ceremony 25 into the free USB slot on the laptop and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.		1821
25.	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 25. Previous hash should read as below (image from Ceremony 25 annotated script). 800faf1265dc41a79cfa35135118fd59edbd5c21b4b6ed887fb484166d3df629 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.		1922

Start Logging Terminal Session

Step	Activity	Initials	Time
26.	CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code>		1822
27.	CA executes <code>script script-20161027.log</code> to start a capture of terminal output.		1823

Start Logging HSM Output

Step	Activity	Initials	Time
28.	CA connects a serial to USB null modem cable to laptop.		1823
29.	CA opens a second terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal . Follow the additional steps to maximize the terminal window: a) Click the View menu and select Zoom In b) Repeat the step above as necessary and executes <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.		1824

Power Up HSM3

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

Enable/Activate HSM3

Step	Activity	Initials	Time
33.	<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 then places the cards in cardholder visible to all.</p> <p>CO 1: Frederico Neves OP TEB # BB46584314</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 7: Alain Aina OP TEB # BB46584319</p>		<p>1828</p> <p>1829</p> <p>1830</p> <p>1831</p> <p>1831</p>
34.	<p>CA will perform the following steps to activate the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "1.Set Online" hit ENT to confirm When "Set Online?" is displayed, hit ENT to confirm When "Insert Card OP #?" is displayed, insert the OP card from the cardholder When "PIN?" is displayed, enter "11223344" and hit ENT When "Remove Card?" is displayed, remove card 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>1</u> of 7 2nd OP card <u>4</u> of 7 3rd OP card <u>5</u> of 7</p>		<p>1834</p>

Check Network Connectivity Between Laptop and HSM3

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

Insert Copy of KSR to be signed

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

Execute KSR signer

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

Final Verification of the Hash (validity) of the KSR

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

Root DNSSEC SKS Ceremony 27

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

Starting: ksr signer 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 ccouncilman 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 ./ksr signer-20100712-224426.log *****
```

Figure 1

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
44.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog ksrsigner-20161027-*.log; done</code> where ksrsigner-20161027-*.log is replaced by log output file displayed by program. This generates X copies and hands copies to participants.		1845
45.	IW1 attaches a copy to his/her script.		1845

Backup Newly Created SKR

Step	Activity	Initials	Time
46.	CA copies the contents of the KSR FD by running <code>cp -p /media/KSR/* .</code> for posting back to RZM. Confirm overwrite by entering "y" when prompted.		1846
47.	CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR</code> flushes the system buffers: <code>sync</code> then unmounts the KSR FD using <code>umount /media/KSR</code>		1847
48.	CA removes the FD KSR containing SKR and gives it to the RZM representative.		1848

Act 3. New KSK Generation and Backup

Generate New Key

Step	Activity	Initials	Time
1.	<p>On the laptop terminal window, CA executes:</p> <p>kskgen</p> <p>to generate the new KSK inside the HSM and the Certificate Signing Request (CSR).</p> <p>When "Activate HSM prior to accepting in the affirmative! (y/n)" is displayed, confirm the hardware security module's "READY" LED is on and type "y" and press enter.</p> <p>If "slot" is asked type 0.</p> <p>Note: Displayed output should be similar to Figure 2.</p>		1850

```

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

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

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

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

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

Klaavzo.csr SHA256 thumbprint and hash:
61B8E6C3518A54FCEBC95623FD377A52C1AC476157F5B8753B2C700C51C0FE85
>> fallout provincial tracker replica drunken maverick eating Wilmington trouble retrospect egghead
cannonball willow consensus keyboard enrollment snapline penetrate dashboard frequency eightball
visitor select impartial clockwork Chicago guidance article drunken recipe woodlark leprosy <<

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

```

Figure 2

Print Copies of the Key Generation log

Step	Activity	Initials	Time
2.	CA prints out hard copies of the kskgen log output file by executing <code>printlog kskgen-20161027-*.log X</code> for attachment to IW1 script and copies for the participants. This generates X copies and hands copies to participants. CA explains the status of the new KSK.		1856

Record Keypair Label

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

Verify the New Key

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

Verify CSR

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

Certificate Request:

```

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

```

Figure 3

Disable/Deactivate HSM3

Step	Activity	Initials	Time
6.	<p>CA makes sure to utilize the cards that were NOT used to activate the HSM are used to deactivate the HSM.</p> <p>CA will perform the following steps to deactivate the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "2.Set Offline" hit ENT to confirm When "Set Offline?" is displayed, hit ENT to confirm When "Insert Card OP #?" is displayed, insert the OP card from the cardholder When "PIN?" is displayed, enter "11223344" hit ENT When "Remove Card?" is displayed, remove card Repeat steps d) to f) for the 2nd and 3rd OP cards <p>Confirm the "READY" led on the HSM is OFF.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <u>1</u> of 7 2nd OP card <u>3</u> of 7 3rd OP card <u>1</u> of 7</p>		1901

Ceremony Break

Step	Activity	Initials	Time
7.	CA initiates the ceremony break and requests the TCRs to leave the TEBs with SO cards on the ceremony table visible to the audit cameras.		1903
8.	<p>CA divides the participants that require ceremony break in groups and must ensure the following:</p> <ul style="list-style-type: none"> At least (1) CA and (1) IW should remain in front of the ceremony table when each group is escorted for ceremony break. At least (2) Crypto Officers and (1) Auditor should remain in the ceremony room when each group is escorted for ceremony break Audit Cameras are never obstructed <p>CA, IW or SA will escort each group of participants out of the ceremony room for ceremony break.</p>		
9.	Once all the groups have returned to the ceremony room, CA ensures that all participants are present, then distributes the TEBs with SO cards to the TCRs for the ceremony to resume.		1934

Create Temporary CO Cards

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

Create Temporary CO Cards

Step	Activity	Initials	Time
11.	<p>CA makes sure to utilize 3 SO cards from the same set to make Crypto Officer (CO) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "7.Role Mgmt" hit ENT to confirm c) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd and 3rd SO cards g) Select "1.Issue Cards" hit ENT to confirm h) Select "1.Issue CO Cards" hit ENT to confirm i) When "Issue CO Cards?" is displayed, hit ENT to confirm j) When "Num Cards?" is displayed, enter "2" and hit ENT to confirm k) When "Num Req Cards?" is displayed, enter "2" and hit ENT to confirm l) When "Insert Card #?" is displayed, insert the proper sequence of CO card from the cardholder m) When "PIN?" is displayed, enter "11223344" and hit ENT n) When "Remove Card?" is displayed, remove card o) Repeat steps l) to n) for the 2nd CO card p) When "CO Cards Issued" is displayed, hit ENT to confirm q) Hit CLR twice to return to the main menu "Secured" <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>1</u> of 7</p> <p>2nd SO card <u>3</u> of 7</p> <p>3rd SO card <u>4</u> of 7</p>		1944

Backup New KSK

Step	Activity	Initials	Time
12.	<p>CA will use the 2 CO cards to backup the New KSK into Application Key (APP. Key) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Insert Card CO #?" is displayed, insert the CO card from the cardholder d) When "PIN?" is displayed, enter "11223344" and hit ENT e) When "Remove Card?" is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select "3.App Keys" hit ENT to confirm h) Select "1.Backup" hit ENT to confirm i) When "Backup?" is displayed, hit ENT to confirm j) When "Which Media?" is displayed, select "2.Backup to Card" and hit ENT to confirm k) Using <> key, select "2.Specify key" hit ENT to confirm l) Using <> key until the new key generate above is display on the top of the list, then hit "A" to select the new key and hit ENT to confirm m) When "Insert B/U Card?" is displayed insert the proper APP. Key card from the cardholder n) When "Remove Card?" is displayed, remove card o) When "Backup Success" is displayed, hit ENT to confirm p) Repeat steps h) to o) for the 2nd, 3rd, and 4th backup copy q) Hit CLR twice to return to the main menu "Secured" <p>Note: As the backup cards are created, the CA writes the Keypair label on the card, then places it on the cardholder.</p>		1953

Return HSM3 to TEB

Step	Activity	Initials	Time
13.	CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.		1953
14.	CA places the HSM into a prepared TEB and seals it.		1955
15.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM3: TEB# BB24646656 / serial # H1403032 CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.		1956

Power Up HSM4

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

Import New KSK to HSM4

Step	Activity	Initials	Time
19.	<p>CA will use the 2 CO cards to import the new KSK using Application Key (APP. Key) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "5.Key Mgmt" hit ENT to confirm When "Insert Card CO #?" is displayed, insert the CO card from the cardholder When "PIN?" is displayed, enter "11223344" and hit ENT When "Remove Card?" is displayed, remove card Repeat steps c) to e) for the 2nd CO card Select "3.App Keys" hit ENT to confirm Select "2.Restore" hit ENT to confirm When "Restore?" is displayed, hit ENT to confirm When "Which Media?" is displayed, select "2. From Card" and hit ENT to confirm When "Insert Card #?" is displayed, insert any APP Key card from the cardholder When "Remove Card?" is displayed, remove card When "Restore Complete" is displayed, hit ENT to confirm Hit CLR twice to return to the main menu "Secured" <p>As the cards are used, the CA places it in the cardholder.</p>		2001

Enable/Activate HSM4

Step	Activity	Initials	Time
20.	<p>CA will perform the following steps to activate the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "1.Set Online" hit ENT to confirm When "Set Online?" is displayed, hit ENT to confirm When "Insert Card OP #?" is displayed, insert the OP card from the cardholder When "PIN?" is displayed, enter "11223344" and hit ENT When "Remove Card?" is displayed, remove card 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>1</u> of 7 2nd OP card <u>4</u> of 7 3rd OP card <u>5</u> of 7</p>		2004

Check Network Connectivity Between Laptop and HSM

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

Verify New Key

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

Generate and Verify CSR

Step	Activity	Initials	Time
24.	CA change directory by executing <code>cd /tmp</code> then <code>kskgen XXXX</code> where <code>XXXX</code> is replaced by the Keypair label generated in the step 3. When "Activate HSM prior to accepting in the affirmative! (y/n)" is displayed, confirm the hardware security module's "READY" LED is on and type "y" and press enter. If "slot" is asked type 0.		2007
25.	CA checks the integrity of the CSR by executing a) CA executes <code>displaycsr XXXX.csr</code> Where <code>XXXX</code> is replaced with the Keypair label indicated on Step 3. b) Verify the DS resource record matches with the printed copies from Step 2. c) Hit SPACE bar until the end of display, then hit "q" to end.		2008
26.	CA return to the working directory by executing <code>cd /media/HSMFD</code>		2008

Disable/Deactivate HSM4

Step	Activity	Initials	Time
27.	<p>CA will perform the following steps to deactivate the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "2.Set Offline" hit ENT to confirm When "Set Offline?" is displayed, hit ENT to confirm When "Insert Card OP #?" is displayed, insert the OP card from the cardholder When "PIN?" is displayed, enter "11223344" hit ENT When "Remove Card?" is displayed, remove card Repeat steps d) to f) for the 2nd and 3rd OP cards <p>Confirm the "READY" led on the HSM is OFF. IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>1st OP card <u>1</u> of 7 2nd OP card <u>5</u> of 7 3rd OP card <u>7</u> of 7</p> <p><i>5 of 7 contacts needed cleaning</i></p>		2012

Clear and Destroy CO Cards

Step	Activity	Initials	Time
28.	<p>CA makes sure to utilize 3 SO cards from the same set that were NOT used before to clear Crypto Officer (CO) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "7.Role Mgmt" hit ENT to confirm When "Insert Card SO #?" is displayed, insert the SO card from the cardholder When "PIN?" is displayed, enter "11223344" and hit ENT When "Remove Card?" is displayed, remove card Repeat steps c) to e) for the 2nd and 3rd SO card Select "4.Clear RoleCard" hit ENT to confirm When "Clear Card?" is displayed, hit ENT to confirm When "Num Cards?" is displayed, enter "2" and hit ENT to confirm When "Insert Card #?" is displayed, take the proper sequence of the CO card from the cardholder, show the CO card to the audit camera, then insert the CO into the HSM's card reader When "PIN?" is displayed, enter "11223344" and hit ENT When "Remove Card?" is displayed, remove card Repeat steps j) to l) for the 2nd CO cards Hit CLR to return to the main menu "Secured" <p>IW1 records the used cards below.</p> <p>Set # _____ 1st SO card <u>1</u> of 7 2nd SO card <u>3</u> of 7 3rd SO card <u>5</u> of 7</p> <p>CA uses the shredder to destroy the cleared CO cards.</p>		2018

Return HSM4 to TEB

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

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

Restart Serial Port Activity

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

Power Up HSM1

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

HSM1: List KSK

Step	Activity	Initials	Time
6.	<p>CA utilizes 3 SO cards from the same set to list the KSK stored in the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Key Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder e) When "PIN?" is displayed, enter "11223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select "4.Output Key Summary" hit ENT to confirm i) When "Key Summary?" is displayed, hit ENT to confirm j) Select "5.Output Key Details" hit ENT to confirm k) When "List Key?" is displayed, hit ENT to confirm l) Hit CLR to return to the previous menu <p>CA matches the displayed KSK label Kjgmt7v in the ttyaudit terminal window.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>7</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p>		2028

HSM1: Delete KSK

Step	Activity	Initials	Time
7.	<p>CA utilizes 3 SO cards from the same set to delete the KSK in the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Key Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder e) When "PIN?" is displayed, enter "11223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select "2.App Keys" hit ENT to confirm i) Select "7.Erase App Keys" hit ENT to confirm j) When "Erase App Keys?" is displayed, hit ENT to confirm k) When "Done" is displayed, hit ENT to confirm l) Select "4.Output Key Summary" hit ENT to confirm m) When "Key Summary?" is displayed, hit ENT to confirm n) Select "5.Output Key Details" hit ENT to confirm o) When "List Key?" is displayed, hit ENT to confirm p) Hit CLR to return to the previous menu <p>CA confirms there is not a key displayed in the ttyaudit terminal window.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>2</u></p> <p>1st SO card <u>3</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>1</u> of 7</p>		2031

HSM1: Zeroisation

Step	Activity	Initials	Time
8.	<p>CA utilizes 3 SO cards from the same set to place the HSM on "Initialized" state. This will zeroise the HSM and erase all keys (AAK, SMK, APP), settings and configuration:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "4.HSM Mgmt" hit ENT to confirm c) When "HSM Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder e) When "PIN?" is displayed, enter "11223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select "A.Go Initialised" hit ENT to confirm i) When "Go Initialised?" is displayed, hit ENT to confirm j) Wait until "Done" is displayed. <p>It may take a few minutes for HSM to restart after erasing all keys.</p> <p>When this operation is complete the HSM will reboot and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>2</u></p> <p>1st SO card <u>3</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>7</u> of 7</p>		2034

Return HSM1 to TEB

Step	Activity	Initials	Time
9.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected.		2035
10.	CA places the HSM into a prepared TEB and seals it.		2036
11.	<p>CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below.</p> <p>HSM1: TEB# BB24646647 / serial # K6002016</p> <p>CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory.</p> <p>CA then places the TEB on the equipment cart.</p>		2036

Power Up HSM2

Step	Activity	Initials	Time
12.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. HSM2: TEB# BB24646674 / serial # K6002013		2031
13.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		2038
14.	CA connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) HSM2: serial # K6002013 Note: The HSM date and time was set from the factory.		2039

HSM2: List the KSK

Step	Activity	Initials	Time
15.	<p>CA utilizes 3 SO cards from the same set to list the KSK in the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard and scroll through menu using <> key Select "5.Key Mgmt" hit ENT to confirm When "Key Mgmt?" is displayed, hit ENT to confirm When "Insert Card SO #?" is displayed, insert the SO card from the cardholder When "PIN?" is displayed, enter "11223344" and hit ENT When "Remove Card?" is displayed, remove card Repeat steps d) to f) for the 2nd and 3rd SO card Select "4.Output Key Summary" hit ENT to confirm When "Key Summary?" is displayed, hit ENT to confirm Select "5.Output Key Details" hit ENT to confirm When "List Key?" is displayed, hit ENT to confirm Hit CLR to return to the previous menu <p>CA matches displayed KSK keypair label <code>Kjgmt7v</code> in the ttyaudit terminal window.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>1</u> of 7</p> <p>2nd SO card <u>3</u> of 7</p> <p>3rd SO card <u>7</u> of 7</p>		2041

HSM2: Delete the KSK

Step	Activity	Initials	Time
16.	<p>CA utilizes 3 SO cards from the same set to delete the KSK in the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "5.Key Mgmt" hit ENT to confirm c) When "Key Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder e) When "PIN?" is displayed, enter "11223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select "2.App Keys" hit ENT to confirm i) Select "7.Erase App Keys" hit ENT to confirm j) When "Erase App Keys?" is displayed, hit ENT to confirm k) When "Done" is displayed, hit ENT to confirm l) Select "4.Output Key Summary" hit ENT to confirm m) When "Key Summary?" is displayed, hit ENT to confirm n) Select "5.Output Key Details" hit ENT to confirm o) When "List Key?" is displayed, hit ENT to confirm p) Hit CLR to return to the previous menu <p>CA confirms there is not a key displayed in the ttyaudit terminal window.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>2</u></p> <p>1st SO card <u>4</u> of 7</p> <p>2nd SO card <u>7</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p>		2044

HSM2: Zeroisation

Step	Activity	Initials	Time
17.	<p>CA utilizes 3 SO cards from the same set to place the HSM on "Initialized" state. This will zeroise the HSM and erase all keys (AAK, SMK, APP), settings and configuration:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select "4.HSM Mgmt" hit ENT to confirm c) When "HSM Mgmt?" is displayed, hit ENT to confirm d) When "Insert Card SO #?" is displayed, insert the SO card from the cardholder e) When "PIN?" is displayed, enter "11223344" and hit ENT f) When "Remove Card?" is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select "A.Go Initialised" hit ENT to confirm i) When "Go Initialised?" is displayed, hit ENT to confirm j) Wait until "Done" is displayed. <p>It may take a few minutes for HSM to restart after erasing all keys.</p> <p>When this operation is complete the HSM will reboot and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state.</p> <p>IW1 records the used cards below. Each card is returned to cardholder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>1</u> of 7</p> <p>2nd SO card <u>4</u> of 7</p> <p>3rd SO card <u>5</u> of 7</p>		2048

Act 5. Secure Hardware and Close the Ceremony

Return HSM2 to TEB

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

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".		2050
5.	Terminating the logging script CA stops logging terminal output by entering "exit" in the other terminal window. This only stops the script logging and will NOT close window.		2051

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA sets dotglob by executing <code>shopt -s dotglob</code> This allows copying everything in the original HSMFD.		2050
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>		2051
8.	CA copy and paste the sha256hash and paste it on Text Editor by going to Applications > Accessories > Text Editor		2052
9.	CA prints five copies of the hash, then writes "KSK 27" on all the pages One for the audit bundle and the other for the HSMFD packages.		2053
10.	CA displays contents of HSMFD by executing <code>ls -ltr</code>		2054
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>		2055
12.	CA displays contents of HSMFD_ by executing <code>ls -ltr /media/HSMFD_</code>		2055
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.		2056
14.	CA unmounts new FD using <code>umount /media/HSMFD_</code>		2056
15.	CA removes HSMFD_ and places it on the table.		2056
16.	CA repeats step 11 to 15 for the 2 nd copy.		2058
17.	CA repeats step 11 to 15 for the 3 rd copy.		2058
18.	CA repeats step 11 to 15 for the 4 th copy.		2059
19.	CA repeats step 11 to 15 for the 5 th copy.		2059
20.	CA repeats step 11 to 15 for the 6 th copy.		2100
21.	CA repeats step 11 to 15 for the 7 th copy.		2101

Print Logging Information

Step	Activity	Initials	Time
22.	CA prints out a hard copy of logging information by executing <code>enscript -2Gr -# 1 script-20161027.log</code> <code>enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20161027-*.log</code> for attachment to IW1 script. Note: Ignore the error regarding non-printable characters if prompted.		2105

Return HSMFD and O/S DVD to TEB

Step	Activity	Initials	Time
23.	CA unmounts HSMFD by executing <code>cd /tmp</code> then <code>umount /media/HSMFD</code> CA removes HSMFD.		2105
24.	CA performs the following to turn off the laptop. a) CA turns off the laptop by pressing the power switch b) CA turns on the laptop by pressing the power switch and immediately removes the O/S DVD from the laptop DVD drive c) CA turns off the laptop again by pressing the power switch		2106
25.	CA places TWO HSMFDs and two OS/DVD, paper with printed hash in prepared TEB; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. O/S DVD (release 20161014) + HSMFD: TEB# BB46584601		2107
26.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on the equipment cart.		2107

Pack APP. Key Backup Cards to TEB

Step	Activity	Initials	Time
27.	CA performs the following to secure the APP Key backups for this KSK facility. a) CA places TWO APP Key cards into the plastic case. b) CA places the plastic case, ONE HSMFD and ONE printed copy of the HSMFD HASH inside the TEB then seals it. c) CA and IW initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. d) CA reads out the TEB # and shows it to all participants to compare with the TEB # below. e) CA then places the TEB on the equipment cart. APP. Key: TEB # BB46584645		2110

Pack APP. Key Backups Cards to TEB

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

Distribute HSMFDs

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

Returning Laptop to TEB

Step	Activity	Initials	Time
30.	<p>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.</p> <p>Laptop2 (Dell ATG6400): TEB# BB24646655 / serial # 35063364997</p>		2116
31.	<p>CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory.</p> <p>CA then places the TEB on the equipment cart.</p>		2116

Return OP and SO Cards to TEB

Step	Activity	Initials	Time
32.	<p>CA calls each COs to the front of the room one at a time and repeats the steps below.</p> <p>a) CA takes the two TEBs prepared for the CO and reads out the TEB # and description while showing each bag.</p> <p>b) CO places his/her OP card into the plastic case.</p> <p>c) CO places his/her SO cards into the plastic case.</p> <p>d) CA places each plastic case into the proper TEBs, seals and initials TEB using a ballpoint pen.</p> <p>e) IW1 inspects each TEB, confirms description in the table on the next page and initials TEB using a ballpoint pen. IW1 keeps sealing strips for later inventory.</p> <p>f) CA hands each TEBs containing the OP and the SO cards to the CO. CO inspects and verifies TEB # and contents, then initials his/her TEB using a ballpoint pen.</p> <p>g) CO enters completion time and signs for each TEB in the table below in IW1's script. IW1 initials table entry.</p> <p>h) CO returns to his/her seat with the TEBs, being careful not to poke or puncture TEBs.</p> <p>CO 1: Frederico Neves OP TEB # BB46584591 SO TEB # BB46584592</p> <p>CO 3: Olaf Kolkman OP TEB # BB46584593 SO TEB # BB46584594</p> <p>CO 4: Robert Seastrom OP TEB # BB46584595 SO TEB # BB46584596</p> <p>CO 5: Christopher Griffiths OP TEB # BB46584597 SO TEB # BB46584598</p> <p>CO 7: Alain Aina OP TEB # BB46584599 SO TEB # BB46584600</p>		<p>2119 2120</p> <p>2123</p> <p>2125</p> <p>2128</p> <p>2131</p>

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584591	Frederico Neves				
CO 1	SO 1 of 7	BB46584592	Frederico Neves				
CO 3	OP 3 of 7	BB46584593	Olaf Kolkman				
CO 3	SO 3 of 7	BB46584594	Olaf Kolkman				
CO 4	OP 4 of 7	BB46584595	Robert Seastrom				
CO 4	SO 4 of 7	BB46584596	Robert Seastrom				
CO 5	OP 5 of 7	BB46584597	Christopher Griffiths				
CO 5	SO 5 of 7	BB46584598	Christopher Griffiths				
CO 7	OP 7 of 7	BB46584599	Alain Aina				
CO 7	SO 7 of 7	BB46584600	Alain Aina				

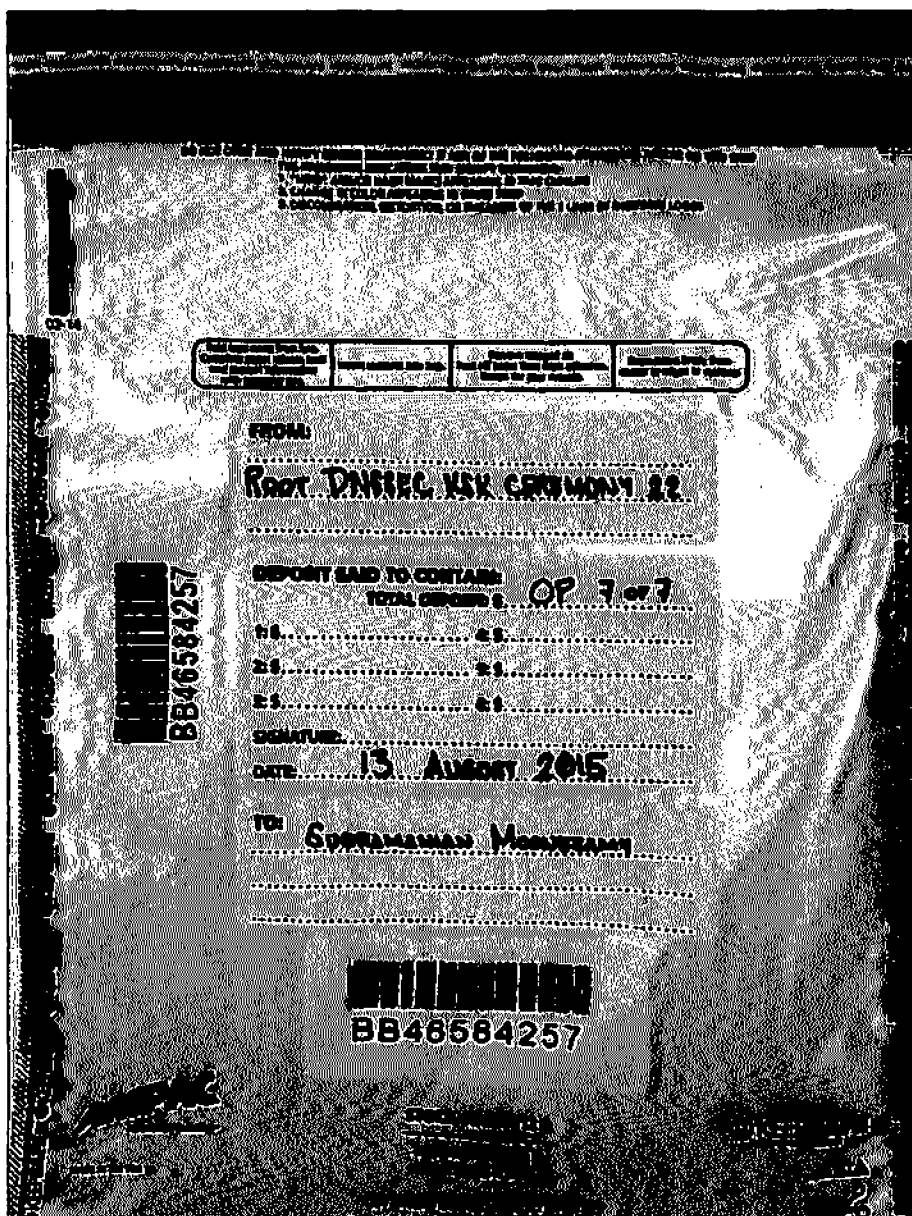


Figure 4

Returning Equipment to Safe #1

Step	Activity	Initials	Time
33.	CA, IW1, SSC1 open safe room and enter with the equipment cart.		2131
34.	SSC1 opens Safe #1 shielding combination from camera.		2132
35.	SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		2133
36.	CA records return of HSM1, HSM2, HSM3 and HSM4 in the next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA CAREFULLY places the HSMs into Safe #1 and IW1 initials the entry. HSM1: TEB# BB24646647 HSM2: TEB# BB24646652 HSM3: TEB# BB24646656 HSM4: TEB# BB24646654		2134
37.	CA records return of laptop in the next entry field of the safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry. Laptop2 (Dell ATG6400): TEB# BB24646655		2135
38.	CA records return of O/S DVD + HSMFD in the next entry field of the safe log with TEB #, printed name, date, time, and signature; places the O/S DVD + HSMFD into Safe #1 and IW1 initials the entry. O/S DVD (release 20161014) + HSMFD: TEB# BB46584601		2137
39.	CA records return of APP Key in the next entry field of the safe log with TEB #, printed name, date, time, and signature; then places the APP Key into Safe #1 and IW1 initials the entry. APP Key: TEB# BB46584645		2137

Close Equipment Safe #1

Step	Activity	Initials	Time
40.	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		2138
41.	SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise, then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		2139
42.	IW1, CA, and SSC1 return to ceremony room with the equipment cart closing the door behind them.		2138

Open Credential Safe #2

Step	Activity	Initials	Time
43.	CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP and SO cards (if applicable) in TEBs with them.		2139
44.	SSC2 opens Safe #2 while shielding combination from camera.		2140
45.	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		2141

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
46.	<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, 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 1: Frederico Neves Box # 1238 OP TEB # BB46584591 SO TEB # BB46584592</p> <p>CO 3: Olaf Kolkman Box # 1239 OP TEB # BB46584593 SO TEB # BB46584594</p> <p>CO 4: Robert Seastrom Box # 1260 OP TEB # BB46584595 SO TEB # BB46584596</p> <p>CO 5: Christopher Griffiths Box # 1240 OP TEB # BB46584597 SO TEB # BB46584598</p> <p>CO 7: Alain Aina Box # 1242 OP TEB # BB46584599 SO TEB # BB46584600</p>		<p>2144</p> <p>2146</p> <p>2148</p> <p>2150</p> <p>2151</p>

Close Credential Safe #2

Step	Activity	Initials	Time
47.	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "Close safe" into the safe log. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		2152
48.	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise, then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		2153
49.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.		2153

Participant Signing of IW1's Script

Step	Activity	Initials	Time
50.	One by one, all participants come to the front of the room, confirms the printed name and date, then, signs IW1's coversheet declaring that this script is a true and an accurate record of the ceremony. IW1 records the completion time once all participants have signed the coversheet. Note: If entry is pre-printed, verify the entry and sign.		2159
51.	CA reviews IW1's script and signs it.		2206

Stop Online Streaming

Step	Activity	Initials	Time
52.	CA acknowledges the participation of online participants and confirms with SA to stop online streaming.		2206

Sign Out of Ceremony Room

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

Stop Video Recording

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

Bundle Audit Materials

Step	Activity	Initials	Time
55.	<p>IW1 makes at least 1 copy of his/her script for off-site audit bundle.</p> <p>Audit bundles each contain:</p> <ul style="list-style-type: none"> a) Output of signer system – HSMFD b) Copy of IW1's key ceremony script c) Audio-visual recording d) Logs from the Physical Access Control and Intrusion Detection System (Range is 05/12/2016 – 10/27/2016) e) The IW1 attestation (A.1 below) f) SA attestation (A.2, A.3 below) <p>All in a TEB labeled "Root DNSSEC KSK Ceremony 27", dated and signed by IW1 and CA. Off-site audit bundle is delivered to off-site storage. The CA holds the ultimate responsibility for finalizing the audit bundle.</p>		

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

Audit Bundle Checklist:

1. Output of Signer System (CA)

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

2. Key Ceremony Scripts (IW1)

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

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

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

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

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

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

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

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

6. Configuration review of the Firewall System (SA1)

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

7. Other items

If applicable.

A.1 Key Ceremony Script (by IW1)

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

Patrick Jones

Date: 27 October 2016

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

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

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

Enclosed is also an electronic copy of the event log from the access control system ranging from the last log extraction on **12 May 2016 00:00 UTC** to now.

Connor Barthold

Date: 27 October 2016

A.3 Firewall Configuration Review (by SA1)

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

Enclosed is the configuration extract from the firewall unit.

Connor Barthold

Date: 27 October 2016