



Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 23

Thursday November 12, 2015

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	Richard Lamb / ICANN		12 November 2015	
IW1	Owen Smigelski / ICANN			
SSC1	Julie Hedlund / ICANN			
SSC2	Grace Abuhamad / ICANN			
CO1	Frederico Neves / BR			
CO2	Anne-Marie Eklund Lowinder / SE			
CO3	Olaf Kolkman / NL			
CO4	Robert Seastrom / US			
CO5	Christopher Griffiths / US			
CO7	Alain Aina / TG			
RZM	Alejandro Bolivar / Verisign			
RZM	Jose Barreros / Verisign			
RZM	James Simometti / Verisign			
AUD	Kenneth Harrer / PricewaterhouseCoopers			
AUD	Timothy Chang / PricewaterhouseCoopers			
SA1	Connor Barthold / ICANN			
SA2	Reed Quinn / ICANN			
CA2 / IKOS	Alberto Duero / ICANN			
IW2 / IKOS	Andres Pavez / ICANN			
CA 3	Edward Lewis / ICANN			
Staff Witness	Alain Durand / ICANN			
EW1	Simon Klose			
EW2	Svante Lodén			

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

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.		
2.	CA confirms that all participants are signed into the Ceremony Room.		

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.		
4.	CA explains the use of personal electronics devices during ceremony.		

Verify Time and Date

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

Open Credential Safe #2

Step	Activity	Initials	Time
6.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.		
7.	SSC2, while shielding combination from camera, opens Safe #2.		
8.	<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>		

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
9.	<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 1: Frederico Neves Box # 1238 OP TEB # BB21907186 (Retain) SO TEB # BB21820443 (Check and return)</p> <p>CO 2: Anne-Marie Eklund Lowinder Box # 1259 OP TEB # BB21907214 (Retain) SO TEB # BB21907211 (Check and return)</p> <p>CO 3: Olaf Kolkman Box # 1239 OP TEB # BB21907258 (Retain) SO TEB # BB21907253 (Check and return)</p> <p>CO 4: Robert Seastrom Box # 1260 OP TEB # BB21907204 (Retain) SO TEB # BB21907203 (Check and return)</p> <p>CO 5: Christopher Griffiths Box # 1240 OP TEB # BB21907208 (Retain) SO TEB # BB21907206 (Check and return)</p> <p>CO 7: Alain Aina Box # 1242 OP TEB # BB21907209 (Retain) SO TEB # BB21907212 (Check and return)</p>		

Close Credential Safe #2

Step	Activity	Initials	Time
10.	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.		
11.	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 verify that the safe is locked and card reader indicator is green.		
12.	IW1, CA, SSC2, and COs leave safe room, with OP cards and SO cards (if applicable) in TEBs, closing the door behind them.		

Open Equipment Safe #1

Step	Activity	Initials	Time
13.	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.		
14.	SSC1, while shielding combination from camera, opens Safe #1.		
15.	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.		

Remove Equipment from Safe #1

Step	Activity	Initials	Time
16.	<p>CA CAREFULLY removes HSM3 (in TEB) from the safe and completes the entry in 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>HSM3: TEB# BB24646676 / serial # H1403032</p> <p>Verify the integrity of the other HSM that will not be used this time and return it to the safe.</p> <p>HSM1: TEB# BB24706804 / serial # K6002016</p> <p>HSM2: TEB# BB24646674 / serial # K6002013</p> <p>HSM4: TEB# BB24646675 / serial # H1411011</p>		
17.	<p>CA takes out the items listed below from the safe and completes the entry in 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>Laptop2 (Dell ATG6400): TEB# BB24646602 / serial # 35063364997</p> <p>O/S DVD (Rev600) + HSMFD: TEB# BB21907244</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# BB24646672 / serial # 41593712005</p>		

Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
18.	<p>SSC1 makes an entry including printed name, date, time and signature into 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>		
19.	<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>		
20.	<p>CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.</p>		

Act 2. Confirm and Sign the Key Signing Request

Set Up Laptop

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# BB24646602 / serial # 35063364997		
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# BB21907244		
3.	CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from O/S DVD.		
4.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes system-config-display --noui c) CA executes killall Xorg d) CA confirms that external display works. e) CA logs in as root		
5.	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) To finish click the button Apply f) Under "Local Printers" from the left menu, select " printer " g) Click the button " Make Default Printer " and " Print Test Page "		
6.	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		

Step	Activity	Initials	Time
7.	<p>CA checks and fixes the date and time on the laptop while referencing the laptop wall clock. On the laptop terminal windows, CA executes:</p> <pre>cp /usr/share/zoneinfo/UTC /etc/localtime</pre> <p>When “cp: overwrite `/etc/localtime' ?” is displayed, type “y” and press enter.</p> <p>then</p> <pre>date -s "20151112 HH:MM:00"</pre> <p>where HH is two digits Hour, MM is two digit Minutes and 00 is Zero Seconds.</p> <p>CA executes date using the Terminal window to confirm the date is properly configured.</p>		

Format and label blank FD

Step	Activity	Initials	Time
8.	<p>CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system popup window and formats the drive by executing df</p> <p>to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc),</p> <pre>umount /dev/sda1</pre> <p>to unmounts the drive (change drive letter and partition if necessary),</p> <pre>mkfs.vfat -n HSMFD -I /dev/sda1</pre> <p>to execute a FAT32 format and label it as HSMFD.</p> <p>CA unplugs the FD.</p>		
9.	CA repeats step 8 for the 2 nd blank FD		
10.	CA repeats step 8 for the 3 rd blank FD		
11.	CA repeats step 8 for the 4 th blank FD		
12.	CA repeats step 8 for the 5 th blank FD		

Connect HSMFD

Step	Activity	Initials	Time
13.	<p>CA plugs the previous HSMFD used in the ceremony 21 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.</p>		

Step	Activity	Initials	Time
14.	<p>Calculate the sha256 hash of the contents on the copied HSMFD.</p> <pre>find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum</pre> <p>IW confirms that the result matches the sha256 hash of the HSMFD that is on the annotated script from the Ceremony 21.</p> <p>Previous hash should read as below (image from Ceremony 21 annotated script).</p> <pre>4ca2ccbe6d4be643d8c13742e9a3d450754328dae04cddce494eaa33223bdaed</pre> <p>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.</p>		

Start Logging Terminal Session

Step	Activity	Initials	Time
15.	CA changes the default directory to the HSMFD by executing <pre>cd /media/HSMFD</pre>		
16.	CA executes <pre>script script-20151112.log</pre> to start a capture of terminal output.		

Start Logging HSM Output

Step	Activity	Initials	Time
17.	CA connects a serial to USB null modem cable to laptop.		
18.	<p>CA opens a second terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal.</p> <p>Follow the additional steps to maximize the terminal window:</p> <ul style="list-style-type: none"> a) Click the View menu and select Zoom In b) Repeat the step above as necessary <p>and executes <pre>cd /media/HSMFD</pre></p> <p>and executes <pre>stty -F /dev/ttyUSB0 115200</pre></p> <p><pre>ttyaudit /dev/ttyUSB0</pre></p> <p>to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.</p>		

Power Up HSM

Step	Activity	Initials	Time
19.	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# BB24646676 / serial # H1403032		
20.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		
21.	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.		

Enable/Activate HSM

Step	Activity	Initials	Time
22.	One by one, CA calls each COs listed below to inspect the TEB for tamper evidence, opens the TEB and hands the OP to the CA who places the cards in cardholder visible to all. CO 1: Frederico Neves OP TEB # BB21907186 CO 2: Anne-Marie Eklund Lowinder OP TEB # BB21907214 CO 3: Olaf Kolkman OP TEB # BB21907258 CO 4: Robert Seastrom OP TEB # BB21907204 CO 5: Christopher Griffiths OP TEB # BB21907208 CO 7: Alain Aina OP TEB # BB21907209		

Step	Activity	Initials	Time
23.	<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 ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7</p>		

Check Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
24.	CA connects HSM3 to laptop using Ethernet cable in LAN port.		
25.	CA tests network connectivity between laptop and HSM by entering ping 192.168.0.2 on the laptop terminal window and looking for responses. Ctrl-C to exit program.		

Insert Copy of KSR to be signed

Step	Activity	Initials	Time
26.	The KSR is downloaded to the KSRFD and transferred to the facility by the IKOS. CA plugs FD labeled "KSR" with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA points out the KSR file to be signed then closes the file system window.		

Execute KSR signer

Step	Activity	Initials	Time
27.	CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR/ksr-root-2016-q1-0.xml</code>		
28.	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.		

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
29.	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: _____		
30.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?		
31.	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-2016-q1-0.xml</code>		



ICANN Root DNSSEC KSK Ceremony 23

```
$ 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 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 ./ksr signer-20100712-224426.log *****
```

Figure 1

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
32.	CA prints out a sufficient number of copies for participants using <code>for i in \$(seq X); do printlog ksrsigner-20151112-*.log; done</code> where ksrsigner-20151112-*.log is replaced by log output file displayed by program. This example generates X copies and hands copies to participants.		
33.	IW1 attaches a copy to his/her script.		

Backup Newly Created SKR

Step	Activity	Initials	Time
34.	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.		
35.	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> and then unmounts the KSR FD using <code>umount /media/KSR</code>		
36.	CA removes KSR FD containing SKR and gives it to the RZM representative.		

Disable/Deactivate HSM

Step	Activity	Initials	Time
37.	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 ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7		

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.		
2.	CA places the HSM into a prepared TEB and seals it.		
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM3: TEB# BB24646616 / serial # H1403032 IW1 and CA initials the TEB and keeps the sealing strip for later inventory. CA places item on equipment cart.		

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".		
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.		

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	Set dotglob by executing shopt -s dotglob This allows copying everything in the original HSMFD.		
7.	Calculate the sha256hash of the contents on the original HSMFD. find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum		
8.	Copy and paste the sha256hash and paste it on Text Editor by going to Applications > Accessories > Text Editor		
9.	Print two copies. One for the audit bundle and the other for the HSMFD package.		
10.	CA displays contents of HSMFD by executing ls -ltr		
11.	CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the O/S (as HSMFD_); and copies the contents of the HSMFD to the blank drive for backup by executing cp -Rp * /media/HSMFD_		
12.	CA displays contents of HSMFD_ by executing ls -ltr /media/HSMFD_		
13.	Calculate the sha256hash of the contents on the copied HSMFD. find -P /media/HSMFD_ -type f -print0 sort -z xargs -0 cat sha256sum Confirm that it matches the sha256hash of the original HSMFD		
14.	CA unmounts new FD using umount /media/HSMFD_		
15.	CA removes HSMFD_ and places it on the table.		
16.	CA repeats step 8 to 12 for the 2 nd copy		
17.	CA repeats step 8 to 12 for the 3 rd copy		
18.	CA repeats step 8 to 12 for the 4 th copy		
19.	CA repeats step 8 to 12 for the 5 th copy		

Print Logging Information

Step	Activity	Initials	Time
20.	CA prints out a hard copy of logging information by executing enscript -2Gr -# 1 script-20151112.log enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20151112-*.log for attachment to IW1 script. Note: Ignore the error regarding non-printable characters if prompted.		

Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initials	Time
21.	CA unmounts HSMFD by executing <code>cd /tmp</code> then <code>umount /media/HSMFD</code> CA removes HSMFD.		
22.	After all print jobs are complete, CA a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch c) Remove the O/S DVD from the drive d) Turns off the laptop again by pressing the power switch		
23.	CA places TWO HSMFDs and 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 (Rev600) + HSMFD: TEB# BB46584320		
24.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.		

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.		

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. Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997		
27.	CA and IW1 initials the TEB and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.		

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 cards 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 1: Frederico Neves OP TEB # BB46584314</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 7: Alain Aina OP TEB # BB46584319</p>		

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584314	Frederico Neves		12 November 2015		
CO 2	OP 2 of 7	BB46584315	Anne-Marie Eklund Lowinder		12 November 2015		
CO 3	OP 3 of 7	BB46584316	Olaf Kolkman		12 November 2015		
CO 4	OP 4 of 7	BB46584267	Robert Seastrom		12 November 2015		
CO 5	OP 5 of 7	BB46584317	Christopher Griffiths		12 November 2015		
CO 7	OP 7 of 7	BB46584319	Alain Aina		12 November 2015		

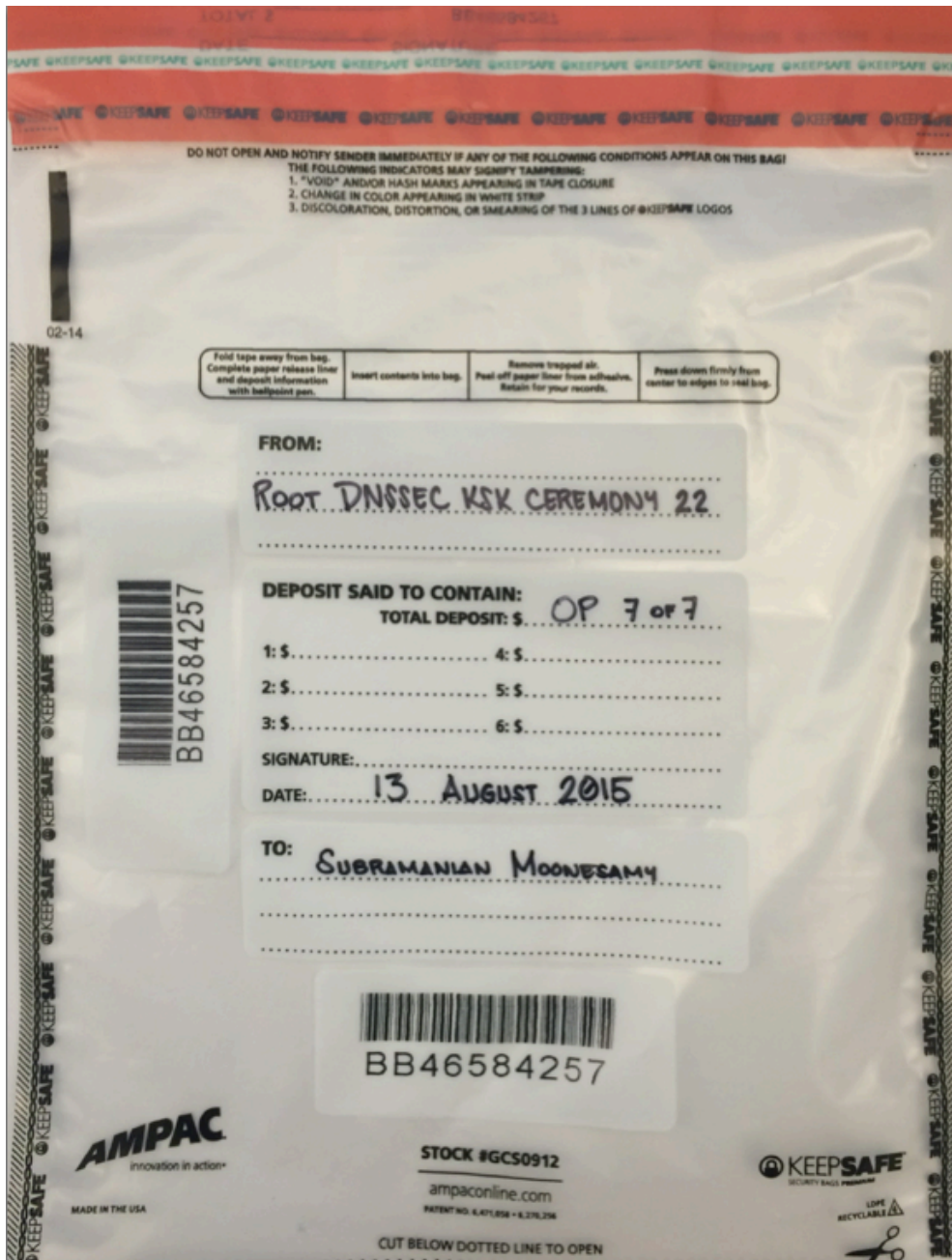


Figure 2

Returning Equipment to Safe #1

Step	Activity	Initials	Time
29.	CA, IW1, SSC1 open safe room and enter with equipment cart.		
30.	SSC1 opens Safe #1 shielding combination from camera.		
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.		
32.	CA records return of HSM3 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. HSM3: TEB# BB24646616		
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. Laptop2 (Dell ATG6400): TEB# BB24646617 / serial # 35063364997		
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 (Rev600) + HSMFD: TEB# BB46584320		

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.		
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.		
37.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.		

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.		
39.	SSC2 opens Safe #2 while shielding combination from camera.		
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.		

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> <ul style="list-style-type: none"> a) Open his/her respective safe deposit box and read out box number inside Safe #2. # Common Key is bottom lock and CO Key is top lock b) CO makes an entry into the safe log indicating the return of OP card and SO cards (if applicable) including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB# s and card type to his/her script. Note: If log entry is pre-printed, verify the entry, record time of completion and sign. c) CO shows each TEB to the camera and then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA. <p>Repeat the steps above until all cards are returned to the deposit box.</p> <p>CO 1: Frederico Neves Box # 1238 OP TEB # BB46584314</p> <p>CO 2: Anne-Marie Eklund Lowinder Box # 1259 OP TEB # BB46584315</p> <p>CO 3: Olaf Kolkman Box # 1239 OP TEB # BB46584316</p> <p>CO 4: Robert Seastrom Box # 1260 OP TEB # BB46584267</p> <p>CO 5: Christopher Griffiths Box # 1240 OP TEB # BB46584317</p> <p>CO 7: Alain Aina Box # 1242 OP TEB # BB46584319</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. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		
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.		
44.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.		

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. IW records the completion time once all participants have signed the coversheet. Note: If entry is pre-printed, verify the entry and sign.		
46.	CA reviews IW1's script and signs it.		

Online Streaming Stops

Step	Activity	Initials	Time
47.	CA confirms with SA to stop online streaming		

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.		

Filming Stops

Step	Activity	Initials	Time
49.	CA confirms with SA to stop filming.		

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 04/09/2015 – 11/12/2015) e) The IW attestation (A.1 below) f) SA attestation (A.2, A.3 below) All in a TEB labeled “ Root DNSSEC KSK Ceremony 23 ”, 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.		

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 IW’s notes and the IW’s attestation. See Appendix A.1.

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

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

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

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 SA and the IW.

IW 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 (SA)

SA’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 (SA)

SA’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 IW)

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.

Owen Smigelski

Date: 12 November 2015

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

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 **09 April 2015 00:00 UTC** to now.

Connor Barthold

Date: 12 November 2015

A.3 Firewall Configuration Review (by SA)

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 November 2015