



Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 18

Thursday August 14, 2014

ICANN KSK Facility@Equinix LA3
1920 East Maple Avenue, El Segundo, CA 90245

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

AbbreviationsDraft

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

Participants

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

Title	Printed Name/Citizenship	Signature	Date	Time
CA	Francisco Arias / ICANN		14 August 2014	
IW1	Kim Davies / ICANN			
SA1	Connor Barthold / ICANN			
SSC1	Selina Harrington / ICANN			
SSC2	Leo Vegoda / ICANN			
CO2	Dmitry Burkov / RU			
CO4	Carlos Martinez / UY			
CO5	Olafur Gudmundsson / IS			
CO7	Subramanian Moonesamy / MU			
RZM	Alejandro Bolivar / Verisign			
RZM	Sanju Varghese / Verisign			
AUD	Tyson Thomas / PricewaterhouseCoopers			
AUD	Mike Sobhanian / PricewaterhouseCoopers			
SA2	Brian Martin / ICANN			
IW2	Dalini Khemlani / ICANN			
EW1	Martin Levy / CloudFlare			
EW1 / CA2	Richard Lamb / ICANN			
EW2	Edward Lewis / ICANN			
EW3	Ashwin Rangan / ICANN			
EW4	Flauribert Takwa / ICANN			
EW5	Alberto Duero / ICANN			
EW6	Andres Pavez / ICANN			
IKOS / CA3	Tomofumi Okubo / ICANN			

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	Initial	Time
1.	SA confirms that the videos are recorded and online streaming is live. IW confirms that all participants are signed into the Ceremony Room.		

Emergency Evacuation Procedures

Step	Activity	Initial	Time
2.	CA or IW reviews emergency evacuation procedures with participants.		

Verify Time and Date

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

Open Credential Safe #2

Step	Activity	Initial	Time
4.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.		
5.	SSC2, while shielding combination from camera, opens Safe #2.		
6.	SSC2 takes out safe log and 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.		

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initial	Time
7.	<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 SO TEB is old and the credentials are not boxed) 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. Note: If log entry is pre-printed, verify the entry, record time of completion and sign. <p>Repeat these steps until all required cards are removed. IW1 initials this entry when all CO have finished.</p> <p>CO 2: Dmitry Burkov Box # 1793 OP TEB # BB21820438 (Retain) SO TEB # BB21907262 (Check and return)</p> <p>CO 4: Carlos Martinez Box # 1068 OP TEB # BB21820434 (Retain) SO TEB # BB21820435 (Check and return)</p> <p>CO 5: Olafur Gudmundsson Box # 1789 OP TEB # BB21820436 (Retain) SO TEB # BB21907264 (Retain)</p> <p>CO 7: Subramanian Moonesamy Box # 1792 OP TEB # BB21907267 (Retain) SO TEB # BB21907268 (Check and return)</p>		

Close Credential Safe #2

Step	Activity	Initial	Time
8.	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.		
9.	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.		
10.	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	Initial	Time
11.	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.		
12.	SSC1, while shielding combination from camera, opens Safe #1.		
13.	SSC1 takes out safe log and prints name, date, time, signature and reason (i.e., "opened 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	Initial	Time
14.	CA CAREFULLY removes HSM2 (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. Note: If log entry is pre-printed, verify the entry, record time of completion and sign. HSM2: TEB# BB24646585 / serial # K6002018 Verify the integrity of the other HSM that will not be used this time and return it to the safe. HSM1: TEB# BB24706810 / serial # K6002020 (last used)		
15.	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. Note: If log entry is pre-printed, verify the entry, record time of completion and sign. Laptop1 (Dell ATG6400): TEB# BB24706809 / serial# 37240147333 O/S DVD (Rev600) + HSMFD: TEB# BB21820437 Verify the integrity of the other Laptop that will not be used this time and return it to the safe. Laptop2: TEB# BB24646591 / serial # 7292928457		

Close Equipment Safe #1 and exit safe room

Step	Activity	Initial	Time
16.	SSC1 makes an entry including printed name, date, time and signature into the safe log indicating, "Close safe". IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		
17.	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). CA and IW1 verify that the safe is locked and door indicator light is green.		
18.	CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.		

Act 2. Confirm and Sign the Key Signing Request

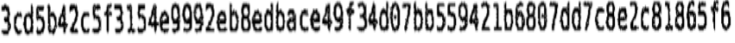
Set Up Laptop

Step	Activity	Initial	Time
1.	CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. Laptop1 (Dell ATG6400): TEB# BB24706809 / serial# 37240147333		
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# BB21820437		
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.		
6.	CA opens a terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal.		
7.	CA checks and fixes date and time on laptop based on wall clock ensuring UTC time zone has been chosen by going to System > Administration > Date and Time. CA executes date to confirm that it is properly configured.		
8.	CA inserts USB port expander into laptop.		

Format and label blank FD

Step	Activity	Initial	Time
9.	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 dmesg grep -A 5 usb-storage to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc), umount /dev/sda to unmounts the drive (change drive letter and partition if necessary), mkfs.vfat -n HSMFD -I /dev/sda to execute a FAT32 format and label it as HSMFD.		
10.	CA repeats step 9 for the 2 nd blank FD		
11.	CA repeats step 9 for the 3 rd blank FD		
12.	CA repeats step 9 for the 4 th blank FD		
13.	CA repeats step 9 for the 5 th blank FD		

Connect HSMFD

Step	Activity	Initial	Time
14.	CA plugs HSMFD into free USB slot on the laptop -NOT EXPANDER- and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.		
15.	Calculate the sha256 hash of the contents on the copied HSMFD. find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum IW confirms that the result matches the sha256 hash of the HSMFD that is on the annotated script from the Ceremony 16 . Previous hash should read as below (image from Ceremony 16 annotated script). 		

Start Logging Terminal Session

Step	Activity	Initial	Time
16.	CA changes the default directory to the HSMFD by executing cd /media/HSMFD		
17.	CA executes script script-20140814.log to start a capture of terminal output.		

Start Logging HSM Output

Step	Activity	Initial	Time
18.	CA connects a serial to USB null modem cable to laptop.		
19.	CA opens a second terminal screen and executes <code>cd /media/HSMFD</code> and executes <code>ttysd /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.		

Power Up HSM

Step	Activity	Initial	Time
20.	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# BB24646585 / serial # K6002018		
21.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		
22.	CA switches to the ttysd terminal window and connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with above. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it since the scripts that does the logging to the laptop adds a timestamp.)		

Enable/Activate HSM

Step	Activity	Initial	Time
23.	CA calls a CO, CO inspects the TEB for tamper evidence, opens the TEB and hands the OP card to the CA who places card in cardholder visible to all.		
24.	Repeat the step above until all OP cards are placed on the cardholder.		
25.	CA inserts 3 cards into HSM to activate the unit (via "Set Online" menu item). Type in the default PIN " 11223344 " when prompted. 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		

Check Network between Laptop and HSM

Step	Activity	Initial	Time
26.	CA connects HSM to laptop using Ethernet cable.		
27.	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	Initial	Time
28.	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	Initial	Time
29.	CA identifies the KSR to be signed and runs, in the terminal window ksrsigner Kjqmt7v /media/KSR/ksr-root-2014-q4-0.xml		
30.	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	Initial	Time
31.	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: <hr/>		
32.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?		
33.	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 /media/KSR/skr-root-2014-q4-0.xml		

```

$ ksrsigner Kjqmt7v ksr-root-2010-q4-1.xml

Starting: ksrsigner 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 ./ksrsigner-20100712-224426.log *****

```

Figure 1

Print Copies of the Operation for Participants

Step	Activity	Initial	Time
34.	CA prints out a sufficient number of copies for participants using printlog ksrsigner-20140814-*.log N where ksrsigner-20140814-*.log is replaced by log output file displayed by program. (this example generates N copies) and hands copies to participants.		
35.	IW1 attaches a copy to his/her script.		

Backup Newly Created SKR

Step	Activity	Initial	Time
36.	CA copies the contents of the KSR FD by running cp -p /media/KSR/* . for posting back to RZM. Confirm overwrite by entering “y” when prompted.		
37.	CA lists contents of KSR FD which should now have an SKR by running ls -ltr /media/KSR and then unmounts the KSR FD using umount /media/KSR		
38.	CA removes KSR FD containing SKR and gives it to the RZM representative.		

Disable/Deactivate HSM

Step	Activity	Initial	Time
39.	CA inserts 3 cards into HSM to deactivate the unit (via “Set Offline” menu item). Type in the default PIN “ 11223344 ” when prompted. IW1 records the used cards below. Each card is returned to cardholder after use. CA makes sure the card(s) NOT used to activate are used to deactivate the HSM. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7 Confirm the ready light turns off.		

Act. 3 Secure Hardware and Close the Ceremony

Return HSM to a TEB

Step	Activity	Initial	Time
1.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.		
2.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM2: TEB# BB24646600 / serial # K6002018 IW1 and CA initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.		

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initial	Time
3.	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".		
4.	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	Initial	Time
5.	Set dotglob by executing shopt -s dotglob This allows copying everything in the original HSMFD.		
6.	Calculate the sha256hash of the contents on the original HSMFD. find -P /media/HSMFD -type f -print0 sort -z xargs -0 cat sha256sum		
7.	Copy and paste the sha256hash and paste it on Text Editor by going to Applications > Accessories > Text Editor Print two copies. One for the audit bundle and the other for the HSMFD package.		
8.	CA displays contents of HSMFD by executing ls -ltr		
9.	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_		

Step	Activity	Initial	Time
10.	CA displays contents of HSMFD_ by executing <code>ls -ltr /media/HSMFD_</code>		
11.	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		
12.	CA unmounts new FD using <code>umount /media/HSMFD_</code>		
13.	CA removes HSMFD_ and places on table.		
14.	CA repeats step 9 to 13 for the 2 nd copy		
15.	CA repeats step 9 to 13 for the 3 rd copy		
16.	CA repeats step 9 to 13 for the 4 th copy		
17.	CA repeats step 9 to 13 for the 5 th copy		

Print Logging Information

Step	Activity	Initial	Time
18.	CA prints out hard copies of logging information by executing <code>enscript -2Gr -# 2 script-20140814.log</code> <code>enscript -Gr -# 2 --font="Courier8" ttyaudit-ttyUSB*-20140814-*.log</code> for attachment to IW1 and CA scripts. Note: Ignore the error regarding non-printable characters if prompted.		

Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initial	Time
19.	CA unmounts HSMFD by executing <code>cd /tmp</code> then <code>umount /media/HSMFD</code> CA removes HSMFD.		
20.	After all print jobs are complete, CA <ul style="list-style-type: none"> a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch c) Remove the O/S DVD from the drive d) Turns off the laptop again by pressing the power switch 		
21.	CA places TWO HSMFDs and OS/DVD, paper with printed hash in TEB; writes date, time and "HSMFD" in amount field; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. O/S DVD (Rev600) + HSMFD: TEB# BB21820426 IW1 initials the TEB. CA places TEB on equipment cart.		

Distribute HSMFDs

Step	Activity	Initial	Time
22.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 1 for himself), IKOS(1) to post SKR to RZM, and to review, analyze and improve on procedures.		

Returning Laptop to a TEB

Step	Activity	Initial	Time
23.	CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. Laptop1 (Dell ATG6400): TEB# BB24646599 / serial# 37240147333 IW1 initials the TEB and keep the sealing strips for later inventory. CA places TEB on equipment cart.		

Returning OP Smartcards to TEBs

Step	Activity	Initial	Time
24.	CA calls each CO to the front of the room one at a time and repeats the steps below. <ol style="list-style-type: none"> a) CA takes a 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 the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. e) CA hands the TEB containing the OP card to the CO. CO inspects and verifies TEB #s and contents then initials his/her TEB. f) CO enters completion time and signs for each 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. 		

Step	Activity	Initial	Time
25.	<p>Once the OP cards are packed, CA calls the CO 5 with an SO card to the front of the room and performs the steps below.</p> <ul style="list-style-type: none"> a) CO opens the SO card TEB and confirms the contents b) CO places the SO card into the labeled 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 the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. e) CA hands the TEB containing the SO card to the CO. CO inspects and verifies TEB #s and contents then initials his/her TEB. f) CO enters completion time and signs for each 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. 		