Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 24
Thursday February 11, 2016

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
Abbreviations

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

OP = Operator

SW = Staff Witness

MC = Master of Ceremony

AUD = Third Party Auditor

FD = Flash Drive

Abbreviations:

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

CA = Kim Davies / ICANN

IW1 = Yuko Green / ICANN

SSC1 = Marilia Hirano / ICANN

SSC2 = Flauribert Takwa / ICANN

CO1 = Arbogast Fabian / TZ

CO2 = Dmitry Burkov / RU

CO3 = Joao Damas / PT

CO4 = Carlos Martinez / UY

CO6 = Nicolas Antoniello / UY

CO7 = Subramanian Moonesamy / MU

RZM = Alejandro Bolivar / Verisign

RZM = Duane Wessels / Verisign

RZM = Sanju Varghesel / Verisign

AUD = Jackie Kwong / PricewaterhouseCoopers

AUD = Abbey Beam / PricewaterhouseCoopers

SA1 = Connor Barthold / ICANN

SA2 = Josh Jenkins / ICANN

CA2 / IKOS = Alberto Duero / ICANN

IW2 / IKOS = Andres Pavez / ICANN

EW = Reg Levy

EW = James Gannon

Participants

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

<table>
<thead>
<tr>
<th>Title</th>
<th>Printed Name</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Kim Davies / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW1</td>
<td>Yuko Green / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC1</td>
<td>Marilia Hirano / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC2</td>
<td>Flauribert Takwa / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO1</td>
<td>Arbogast Fabian / TZ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO2</td>
<td>Dmitry Burkov / RU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO3</td>
<td>Joao Damas / PT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO4</td>
<td>Carlos Martinez / UY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO6</td>
<td>Nicolas Antoniello / UY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO7</td>
<td>Subramanian Moonesamy / MU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RZM</td>
<td>Alejandro Bolivar / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RZM</td>
<td>Duane Wessels / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RZM</td>
<td>Sanju Varghesel / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Jackie Kwong / PricewaterhouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Abbey Beam / PricewaterhouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA1</td>
<td>Connor Barthold / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA2</td>
<td>Josh Jenkins / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA2</td>
<td>Alberto Duero / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW2</td>
<td>Andres Pavez / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW</td>
<td>Reg Levy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW</td>
<td>James Gannon</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

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

Participants Arrive and Sign into Key Ceremony Room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CA confirms with SA that all audit cameras are recording and online streaming is live.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Emergency Evacuation Procedures and Electronics Policy

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>CA reviews emergency evacuation procedures with participants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>CA explains the use of personal electronics devices during ceremony.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>CA briefly explains the purpose of the ceremony.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verify Time and Date

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date and time: ________________________________________</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All entries into this script or any logs should follow this common source of time.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Open Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>SSC2, while shielding combination from camera, opens Safe #2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>SSC2 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 SSC2. 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. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### COs Extract Credentials From the Safe Deposit Boxes

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>One by one, the selected COs retrieves required OP cards and SO cards (if applicable) following the steps shown below.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below.</td>
</tr>
<tr>
<td></td>
<td>c) Retains OP TEB and SO TEB (if applicable) and locks box.</td>
</tr>
<tr>
<td></td>
<td>d) Makes an entry in safe log indicating OP TEB and SO TEB removal (if applicable) with box #, printed name, date, time and signature.</td>
</tr>
<tr>
<td></td>
<td>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
</tr>
</tbody>
</table>

Repeat these steps until all required cards are removed. IW1 initials this entry when all COs have finished.

CO 1: Arbogast Fabian  
Box #: 1791  
OP TEB # BB46584261 (Retain)  
SO TEB # BB46584262 (Check and return)

CO 2: Dmitry Burkov  
Box #: 1793  
OP TEB # BB46584255 (Retain)  
SO TEB # BB46584256 (Check and return)

CO 3: Joao Damas  
Box #: 1071  
OP TEB # BB21907274 (Retain)  
SO TEB # BB21820433 (Check and return)

CO 4: Carlos Martinez  
Box #: 1068  
OP TEB # BB46584253 (Retain)  
SO TEB # BB46584254 (Check and return)

CO 6: Nicolas Antoniello  
Box #: 1073  
OP TEB # BB21368989 (Retain)  
SO TEB # BB21907266 (Retain)

CO 7: Subramanian Moonesamy  
Box #: 1792  
OP TEB # BB46584257 (Retain)  
SO TEB # BB46584258 (Check and return)
### Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 11.  | Once all safe deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry.  
  Note: If log entry is pre-printed, verify the entry, record time of completion and sign.                                                                                               |          |      |
| 12.  | 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.         |          |      |
| 13.  | 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>SSC1, while shielding combination from camera, opens Safe #1.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 16.  | SSC1 takes out the existing safe log and shows the most current page to the camera.  
  IW1 provides a blank pre-printed safe log to the SSC1.  
  SSC1 appends the new safe log then prints name, date, time, signature, and reason (i.e. “open safe”) in safe log. IW1 initials this entry.  
  Note: If log entry is pre-printed, verify the entry, record time of completion and sign.                                          |          |      |
### Remove Equipment from Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 17. | CA CAREFULLY removes HSM3 (in TEB) from the safe and completes the entry on the safe log indicating HSM Removal, TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry.  
Note: If log entry is pre-printed, verify the entry, record time of completion and sign.  
HSM3: TEB# BB24646665 / serial # H1403033  
Verify the integrity of the other HSMs that will not be used and return them to the safe.  
HSM1: TEB# BB24646605 / serial # K6002020  
HSM2: TEB# BB24646669 / serial # K6002018  
HSM4: TEB# BB24646664 / serial # H1411006 | | |
| 18. | CA takes out the items listed below from the safe and completes the entry on the safe log indicating each item, TEB#, serial number if available. Printed name, date, time and signature. CA places the item on the equipment cart. IW1 initials this entry.  
Note: If log entry is pre-printed, verify the entry, record time of completion and sign.  
Laptop1 (Dell ATG6400): TEB# BB24646663  
O/S DVD (Rev600) + HSMFD: TEB# BB46584331  
Verify the integrity of the other Laptop that will not be used this time and return it to the safe.  
Laptop2 (Dell ATG6400): TEB# BB24646591 / serial# 7292928457 | | |

### Close Equipment Safe #1 and exit safe room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 19. | SSC1 makes an entry including printed name, date, time and signature on 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. | | |
| 20. | 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. | | |
| 21. | 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 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# BB24646663 / 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# BB46584331** |          |      |
| 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 first device **"HP Laserjet xxxx"** and then click the button **Forward**  
   c) (Note: The xxxx is the Printer Model)  
   d) Select **HP** and click the button **Forward**  
   e) Under "Models" scroll up and select **"Laserjet"**, and then click the button **Forward**  
   f) To finish click the button **Apply**  
   g) Under "Local Printers" from the left menu, select **"printer"**  
   h) 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 |          |      |
7. CA checks and fixes the date and time on the laptop while referencing the laptop wall clock. On the laptop terminal windows, CA executes:

```
    cp /usr/share/zoneinfo/UTC /etc/localtime
```

When “cp: overwrite `/etc/localtime’?” is displayed, type “y” and press enter.

Then

```
    date -s “20160211 HH:MM:00”
```

where HH is two digit Hour, MM is two digit Minutes and 00 is Zero Seconds

CA executes `date` using the Terminal window to confirm the date is properly configured.

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>CA checks and fixes the date and time on the laptop while referencing the laptop wall clock. On the laptop terminal windows, CA executes: <code>cp /usr/share/zoneinfo/UTC /etc/localtime</code> When “cp: overwrite <code>/etc/localtime’?” is displayed, type “y” and press enter. Then </code>date -s “20160211 HH:MM:00”<code>where HH is two digit Hour, MM is two digit Minutes and 00 is Zero Seconds CA executes</code>date` using the Terminal window to confirm the date is properly configured.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Format and label blank FD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>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/sdal</code> to unmounts the drive (change drive letter and partition if necessary), <code>mkfs.vfat -n HSMFD -I /dev/sdal</code> to execute a FAT32 format and label it as HSMFD. CA unplugs the FD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>CA repeats step 8 for the 2nd blank FD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>CA repeats step 8 for the 3rd blank FD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>CA repeats step 8 for the 4th blank FD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>CA repeats step 8 for the 5th blank FD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Connect HSMFD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>CA plugs the previous HSMFD used in the ceremony 22 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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Start Logging Terminal Session

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>CA executes <code>script script-20160211.log</code> to start a capture of terminal output.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Start Logging HSM Output

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>CA connects a serial to USB null modem cable to laptop.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 18.  | CA opens a second terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal. Follow the additional steps to maximize the terminal window:  
   a) Click the View menu and select Zoom In  
   b) Repeat the step above as necessary  
and executes `cd /media/HSMFD` and executes `stty -F /dev/ttyUSB0 115200` `ttyaudit /dev/ttyUSB0` to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop. | | |
Power Up HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM3: TEB# BB24646665 / serial # H1403033</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td>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.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM3: serial # H1403033</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The HSM date and time was set from the factory.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enable/Activate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>One by one, CA calls each COs listed below to inspect the TEB for tamper evidence, opens the TEB and hands the OP cards to the CA who places the cards in cardholder visible to all.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO 1: Arbogast Fabian</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584261</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO 2: Dmitry Burkov</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584255</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO 3: Joao Damas</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB21907274</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO 4: Carlos Martinez</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584253</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO 6: Nicolas Antoniello</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB21368989</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO 7: Subramanian Moonesamy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584257</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CA will perform the following steps to activate the HSM:

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

Confirm the “READY” led on the HSM is ON.
IW1 records the used cards below. Each card is returned to cardholder after use.
1st OP card ____ of 7
2nd OP card ____ of 7
3rd OP card ____ of 7

### Check Network Connectivity Between Laptop and HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td>CA connects HSM to laptop using Ethernet cable in LAN port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25.</td>
<td>CA tests network connectivity between laptop and HSM by entering <code>ping 192.168.0.2</code> on the laptop terminal window and looking for responses. Ctrl-C to exit program.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Insert Copy of KSR to be signed

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Execute KSR signer

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.</td>
<td>CA identifies the KSR to be signed and runs, in the terminal window <code>ksrsigner Kjqmt7v /media/KSR/ksr-root-2016-q2-0.xml</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28.</td>
<td>The KSR signer will ask whether the HSM is activated or not as below. <strong>Activate HSM prior to accepting in the affirmative!!</strong> (y/N) : CA confirms that the HSM is online and then enters “y” to proceed to verification. <strong>Note: DO NOT</strong> enter “y” for the “Is this correct y/n?” yet.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Final Verification of the Hash (validity) of the KSR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td>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:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30.</td>
<td>Participants match the hash read out with that displayed on the terminal. CA asks, “are there any objections”?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31.</td>
<td>CA then enters “y” in response to “<strong>Is this correct y/n?</strong>” 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-q2-0.xml</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
$ 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 Slot=0
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  2010-08-04T23:59:59  41248        19036
3  2010-07-31T00:00:00  2010-08-14T23:59:59  41248        19036
4  2010-08-10T00:00:00  2010-08-24T23:59:59  41248        19036
5  2010-08-20T00:00:00  2010-09-03T23:59:59  41248        19036
6  2010-08-30T00:00:00  2010-09-13T23:59:59  41248        19036
7  2010-09-10T00:00:00  2010-09-24T00:00:00  41248        19036
8  2010-09-20T00:00:00  2010-10-05T23:59:59  40288,41248   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   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  21639,40288  19036

...PASSED.

SHA256 hash of KSR:
A17E539793B2611112C4F591A06AF4FBC2221DDDD71794BC72D5ABE910C72543

>> 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/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   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:
00CC341B78B3BAAE2626B1AAC6A58DE07F02EK4G53E6A6ABE07CEFF2741257

>> aardvark revolver choking bravado kickoff councilman robust tomorrow tracker Cherokee beehive paragon reindeer microscope uncut amusement unearth coherence deckhand embizzle 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 **********
### Print Copies of the Operation for Participants

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>CA prints out a sufficient number of copies for participants using &lt;br&gt; <code>for i in $(seq X); do printlog ksrsigner-20160211-*.log; done</code>&lt;br&gt; where ksrsigner-20160211-*.log is replaced by log output file displayed by program. This example generates X copies and hands copies to participants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33.</td>
<td>IW1 attaches a copy to his/her script.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Backup Newly Created SKR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td>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 &quot;y&quot; when prompted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35.</td>
<td>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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36.</td>
<td>CA removes KSR FD containing SKR and gives it to the RZM representative.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Disable/Deactivate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.</td>
<td>CA makes sure to utilize the cards that were NOT used to activate the HSM are used to deactivate the HSM.&lt;br&gt;CA will perform the following steps to deactivate the HSM:&lt;br&gt; a) Utilize the HSM’s keyboard and scroll through menu using &lt;&gt; key&lt;br&gt; b) Select “2.Set Offline” hit ENT to confirm&lt;br&gt; c) When “Set Offline?” is displayed, hit ENT to confirm&lt;br&gt; d) When “Insert Card OP #?” is displayed, insert the OP card from the cardholder&lt;br&gt; e) When “PIN?” is displayed, enter “11223344” hit ENT&lt;br&gt; f) When “Remove Card?” is displayed, remove card&lt;br&gt; g) Repeat steps d) to f) for the 2nd and 3rd OP cards&lt;br&gt; Confirm the “READY” led on the HSM is OFF.&lt;br&gt; IW1 records the used cards below. Each card is returned to cardholder after use.&lt;br&gt; 1st OP card ____ of 7&lt;br&gt; 2nd OP card ____ of 7&lt;br&gt; 3rd OP card ____ of 7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Act 3. Secure Hardware and Close the Ceremony

Return HSM to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>CA places the HSM into a prepared TEB and seals it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. \nHSM3: TEB# BB24646618 / serial # H1403033 \nIW1 and CA initials the TEB and keeps the sealing strip for later inventory. CA places item on equipment cart.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stop Recording Serial Port Activity and Logging Terminal Output

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Closing ttyaudit terminal window \nCA 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”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Terminating the logging script \nCA stops logging terminal output by entering “exit” in the other terminal window. This only stops the script logging and will NOT close window.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Backup HSMFD Contents

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>CA set dotglob by executing <code>shopt -s dotglob</code>&lt;br&gt;This allows copying everything in the original HSMFD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>CA calculates the sha256hash of the contents on the original HSMFD.&lt;br&gt;`find -P /media/HSMFD -type f -print0</td>
<td>sort -z</td>
<td>xargs -0 cat</td>
</tr>
<tr>
<td>8.</td>
<td>CA copy and paste the sha256hash and paste it on Text Editor by going to Applications &gt; Accessories &gt; Text Editor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>CA prints two copies of the hash. One for the audit bundle and the other for the HSMFD package then writes “KSK 24” on the printed copies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>CA displays contents of HSMFD by executing <code>ls -ltr</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>CA displays contents of HSMFD_ by executing <code>ls -ltr /media/HSMFD_</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Calculate the sha256hash of the contents on the copied HSMFD.&lt;br&gt;`find -P /media/HSMFD_ -type f -print0</td>
<td>sort -z</td>
<td>xargs -0 cat</td>
</tr>
<tr>
<td>14.</td>
<td>CA unmounts new FD using <code>umount /media/HSMFD_</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>CA removes HSMFD_ and places it on the table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>CA repeats step 11 to 15 for the 2\textsuperscript{nd} copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>CA repeats step 11 to 15 for the 3\textsuperscript{rd} copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>CA repeats step 11 to 15 for the 4\textsuperscript{th} copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>CA repeats step 11 to 15 for the 5\textsuperscript{th} copy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Print Logging Information

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.</td>
<td>CA prints out a hard copy of logging information by executing&lt;br&gt;<code>enscript -2Gr -# 1 script-20160211.log</code>&lt;br&gt;<code>enscript -Gr -# 1 --font=&quot;Courier8&quot; ttyaudit-ttyUSB*-20160211-*.log</code>&lt;br&gt;for attachment to IW1 script.&lt;br&gt;Note: Ignore the error regarding non-printable characters if prompted.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*version 2.0*
Returning HSMFD and O/S DVD to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>CA unmounts HSMFD by executing <code>cd /tmp</code> then <code>umount /media/HSMFD</code> CA removes HSMFD.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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# BB46584278 |  | |
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returning Laptop to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 26.  | CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below.  
   **Laptop1 (Dell ATG6400): TEB# BB24646619 / serial # 37240147333** |  | |
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.</td>
<td>CA calls each COs to the front of the room one at a time and repeats the steps below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) CO places the OP card into the plastic case.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) CA places the plastic case into the TEB, seals in front of IW1 and CO then the CA initials TEB and strip.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW1 inspects each TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) CA hands TEB containing the OP card to the CO. CO inspects and verifies TEB # and contents then initials his/her TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) CO enters completion time and signs for TEB in the table below in IW1’s script. IW1 initials table entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CO 1: Arbogast Fabian  
OP TEB # BB46584279  

CO 2: Dmitry Burkov  
OP TEB # BB46584280  

CO 3: Joao Damas  
OP TEB # BB46584281  

CO 4: Carlos Martinez  
OP TEB # BB46584282  

CO 6: Nicolas Antoniello  
OP TEB # BB46584283  

CO 7: Subramanian Moonesamy  
OP TEB # BB46584285
Change SO 6 card TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td>CA calls the CO 6 with a SO card TEB to the front of the room and performs the steps below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) CO opens the SO card TEB and confirms the contents</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) CO places the SO card into the plastic case (if applicable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) CA places the plastic case into the TEB, seals in front of IW1 and CO then the CA initials TEB and strip.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW1 inspects the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) CA hands TEB containing the SO cards to the CO, CO inspects and verifies TEB # and contents then initials his/her TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) CO enters completion time and signs for TEB in the table below in IW1’s script. IW1 initials table entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CO 6: Nicolas Antoniello  
SO TEB # BB46584284
<table>
<thead>
<tr>
<th>CO #</th>
<th>Card Type</th>
<th>TEB #</th>
<th>Printed Name</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
<th>IW1 Initials</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO 1</td>
<td>OP 1 of 7</td>
<td>BB46584279</td>
<td>Arbogast Fabian</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 2</td>
<td>OP 2 of 7</td>
<td>BB46584280</td>
<td>Dmitry Burkov</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 3</td>
<td>OP 3 of 7</td>
<td>BB46584281</td>
<td>Joao Damas</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 4</td>
<td>OP 4 of 7</td>
<td>BB46584282</td>
<td>Carlos Martinez</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 6</td>
<td>OP 6 of 7</td>
<td>BB46584283</td>
<td>Nicolas Antoniello</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 6</td>
<td>SO 6 of 7</td>
<td>BB46584284</td>
<td>Nicolas Antoniello</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 7</td>
<td>OP 7 of 7</td>
<td>BB46584285</td>
<td>Subramanian Moonesamy</td>
<td></td>
<td>11 February 2016</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 2
### Returning Equipment to Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.</td>
<td>CA, IW1, SSC1 open safe room and enter with equipment cart.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31.</td>
<td>SSC1 opens Safe #1 shielding combination from camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33.</td>
<td>CA records return of <strong>HSM3</strong> 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. <strong>HSM3: TEB# BB24646618</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34.</td>
<td>CA records return of <strong>laptop</strong> 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. <strong>Laptop1 (Dell ATG6400): TEB# BB24646619</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35.</td>
<td>CA records return of <strong>O/S DVD + HSMFD</strong> in next entry field of safe log with TEB #, printed name, date, time, and signature; places the <strong>O/S DVD + HSMFD</strong> into Safe #1 and IW1 initials the entry. <strong>O/S DVD (Rev600) + HSMFD: TEB# BB46584278</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Close Equipment Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>38.</td>
<td>IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Open Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40.</td>
<td>SSC2 opens Safe #2 while shielding combination from camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41.</td>
<td>SSC2 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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## CO Returns Credentials to Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 42.  | One by one, each COs along with the CA (using his/her common key):  
   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. Repeat the steps above until all cards are returned to the deposit box. |          |      |

**CO 1: Arbogast Fabian**  
Box #: 1791  
OP TEB # BB46584279  

**CO 2: Dmitry Burkov**  
Box #: 1793  
OP TEB # BB46584280  

**CO 3: Joao Damas**  
Box #: 1071  
OP TEB # BB46584281  

**CO 4: Carlos Martinez**  
Box #: 1068  
OP TEB # BB46584282  

**CO 6: Nicolas Antoniello**  
Box #: 1073  
OP TEB # BB46584283  
SO TEB # BB46584284  

**CO 7: Subramanian Moonesamy**  
Box #: 1792  
OP TEB # BB46584285
Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 43.  | 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. |          |      |
| 44.  | 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. |          |      |
| 45.  | CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked. |          |      |

Participant Signing of IW1’s Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 46.  | 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. |          |      |
| 47.  | CA reviews IW1’s script and signs it. |          |      |

Online Streaming Stops

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>48.</td>
<td>CA acknowledges the participation of online participants and confirms with SA to stop online streaming.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signing Out of Ceremony Room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Filming Stops

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>50.</td>
<td>CA confirms with SA to stop filming.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Copying and Storing the Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 51.  | 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 08/13/2015 – 02/11/2016)  
      e) The IW attestation (A.1 below)  
      f) SA attestation (A.2, A.3 below)  
      All in a TEB labeled “Root DNSSEC KSK Ceremony 24”, 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.

Yuko Green

Date: 11 February 2016
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 13 August 2015 00:00 UTC to now.

Connor Barthold

____________________________________

Date: 11 February 2016
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: 11 February 2016