Root DNSSEC KSK Ceremony 30
Thursday August 17, 2017

Root Zone KSK Operator Key Management Facility
1920 East Maple Avenue, El Segundo, CA 90245

This ceremony is executed under the DNSSEC Practice Statement for the Root Zone
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUD</td>
<td>Third Party Auditor</td>
</tr>
<tr>
<td>EW</td>
<td>External Witness</td>
</tr>
<tr>
<td>IW</td>
<td>Internal Witness</td>
</tr>
<tr>
<td>OP</td>
<td>Operator</td>
</tr>
<tr>
<td>RZM</td>
<td>Root Zone Maintainer</td>
</tr>
<tr>
<td>SO</td>
<td>Security Officer</td>
</tr>
<tr>
<td>CA</td>
<td>Ceremony Administrator</td>
</tr>
<tr>
<td>FD</td>
<td>Flash Drive</td>
</tr>
<tr>
<td>KMF</td>
<td>Key Management Facility</td>
</tr>
<tr>
<td>PTI</td>
<td>Public Technical Identifiers</td>
</tr>
<tr>
<td>SA</td>
<td>System Administrator</td>
</tr>
<tr>
<td>SSC</td>
<td>Safe Security Controller</td>
</tr>
<tr>
<td>CO</td>
<td>Crypto Officer</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>KSR</td>
<td>Key Signing Request</td>
</tr>
<tr>
<td>RKOS</td>
<td>RZ KSK Operations Security</td>
</tr>
<tr>
<td>SKR</td>
<td>Signed Key Response</td>
</tr>
<tr>
<td>SW</td>
<td>Staff Witness</td>
</tr>
</tbody>
</table>

**TEB** = Tamper Evident Bag (APAC, item #0331010, item #03300112 small or #03301012 large or MMF Devices, item #0332010120 small or #0332011120)

### 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 / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW1</td>
<td>Jonathan Denton / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC1</td>
<td>Anand Mishra / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC2</td>
<td>Jessica Castillo / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO1</td>
<td>Argoget Fabian / TZ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO2</td>
<td>Dmitriy Burkov / RU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO5</td>
<td>Olafur Gudmundsson / IS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO6</td>
<td>Nicolas Antonio / UY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO7</td>
<td>Subramanian Moonsamy / 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>John Palmmukal / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RZM</td>
<td>Duane Wesseels / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Rafael Mencahca / PricewaterhouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Evan Higashiyama / 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 / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW2</td>
<td>Andres Pavez / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SW</td>
<td>Victoria Yang / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SW</td>
<td>Shaurlo Anderson / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SW</td>
<td>Matt Larson / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SW</td>
<td>LV McCoy / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW</td>
<td>Gaurab Upadchaya</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW</td>
<td>Rafael Lito Ibarra</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW</td>
<td>Luciano Minuchin</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.

version 2.0
Note: The CA leads the ceremony. Dual Occupancy is enforced. Only CAs, IWs, or SAs can enter and escort other participants to the Ceremony room. Only CA+IW can enter the safe room and escort other participants. CAs, IWs, or SAs may escort participants out of the ceremony room at the CA's discretion and only when an IW + CA or SA remain inside the ceremony. No one may leave the Ceremony room if the safe room is occupied. All participants are required to sign in and out of the ceremony room using the visitor log. The SA starts filming before the participants enter the ceremony room.

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

<table>
<thead>
<tr>
<th>A</th>
<th>Alfa</th>
<th>AL-FAH</th>
</tr>
</thead>
<tbody>
<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-ETT</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 video streaming is enabled.</td>
<td>jg</td>
<td>20:00:55</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 participants list on Page 2.</td>
<td>jg</td>
<td>20:02:14</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>jg</td>
<td>20:02:29</td>
</tr>
<tr>
<td>4.</td>
<td>CA explains the use of personal electronic devices during ceremony.</td>
<td>jg</td>
<td>20:03:16</td>
</tr>
<tr>
<td>5.</td>
<td>CA briefly explains the purpose of the ceremony.</td>
<td>jg</td>
<td>20:04:24</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>
</table>
| 6.   | IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room:  
Date and time: **2017/08/17 20:04:52**  
All entries into this script or any logs should follow this common source of time. | jg       | 20:04:52 |

**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 brings a flashlight then escorts SSC2, COs into the safe room.</td>
<td>jg</td>
<td>20:07:10</td>
</tr>
<tr>
<td>8.</td>
<td>SSC2, while shielding combination from camera, opens Safe #2</td>
<td>jg</td>
<td>20:08:31</td>
</tr>
</tbody>
</table>
| 9.   | SSC2 removes the existing safe log and shows the most recent page to the audit camera. IW1 provides a pre-printed safe log to the SSC2.  
SSC2 writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry then initials it. | jg       | 20:09:53 |
**COs Extract Credentials From the Safe Deposit Boxes**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 10.  | One by one, the selected CO retrieves the required OP TEB and SO TEB (as specified on the list below) by following the steps.  
  a) With the assistance of the CA (and his/her common key), the CO opens her/his safe deposit box.  
  Note: Common Key is for the bottom lock. CO Key is for the top lock  
  b) CO verifies the integrity of the safe deposit box, reads out its number, then removes his/her OP TEB and SO TEB  
  c) CO reads out the TEB #s, then verifies its integrity.  
  d) CO retains OP TEB and SO TEB (as specified below) then locks the box.  
  e) CO writes date/time and signature on the safe log where the removal of their TEBs are indicated.  
  f) IW1 verifies the completed safe log entries then initial it.  
 Repeat these steps until all required cards listed below are removed. |          |      |
|      | CO 1: Arbogast Fabian  
  Box # 1791  
  OP TEB # BB46584450 (Retain) ✓  
  SO TEB # BB46584451 (Check and Return) ✓ | j0   | 20:20:57 |
|      | CO 2: Dmitry Burkov  
  Box # 1793  
  OP TEB # BB46584452 (Retain) ✓  
  SO TEB # BB46584453 (Check and Return) ✓ |          |      |
|      | CO 5: Olafur Gudmundsson  
  Box # 1789  
  OP TEB # BB46584660 (Retain) ✓  
  SO TEB # BB46584666 (Check and Return) ✓ |          |      |
|      | CO 6: Nicolas Antoniello  
  Box # 1073  
  OP TEB # BB46584458 (Retain) ✓  
  SO TEB # BB46584459 (Check and Return) ✓ |          |      |
|      | CO 7: Subramanian Moonesamy  
  Box # 1792  
  OP TEB # BB46584460 (Retain) ✓  
  SO TEB # BB46584461 (Check and Return) ✓ |          |      |
## Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>Once all relevant deposit boxes are closed and locked, SSC2 writes the</td>
<td></td>
<td>20:21:41</td>
</tr>
<tr>
<td></td>
<td>date/time and signature on the safe log where &quot;Close Safe&quot; is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IW1 verifies the safe log entry then initials it.</td>
<td>J0</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>SSC2 returns the safe log back in the Safe #2 and locks it (spin dial at</td>
<td></td>
<td>20:22:11</td>
</tr>
<tr>
<td></td>
<td>least two full revolutions each way, counter clock wise then clock wise).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA and IW1 verifies that the safe is locked and the &quot;WAIT&quot; light indicator is off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>IW1, CA, SSC2, and COs leave safe room, with OP TEB and SO TEB (if</td>
<td></td>
<td>20:23:09</td>
</tr>
<tr>
<td></td>
<td>applicable), closing the door behind them.</td>
<td>J0</td>
<td></td>
</tr>
</tbody>
</table>

## 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>CA, IW1 and SSC1 enter the safe room with an empty equipment cart.</td>
<td>J0</td>
<td>20:23:17</td>
</tr>
<tr>
<td>15.</td>
<td>SSC1, while shielding combination from camera, opens Safe #1.</td>
<td>GJ</td>
<td>20:25:17</td>
</tr>
<tr>
<td>16.</td>
<td>SSC1 takes out the existing safe log and shows the most recent page to the audit camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry then initials it.</td>
<td>J0</td>
<td>20:26:10</td>
</tr>
</tbody>
</table>
Remove Equipment from Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>CA CAREFULLY removes HSM3 (in TEB) from the safe; Reads out the TEB # and HSM serial # then places it on the equipment cart. CA then writes the date/time and signature on the safe log where HSM removal is indicated. IW1 verifies the safe log entry then initials it. HSM3: TEB# BB51184611 / serial # H1403033 CA verifies the integrity of the other HSM that will not be used, then returns it in the safe. HSM4: TEB# BB51184612 / serial # H1411006</td>
<td>go</td>
<td>20:18:50</td>
</tr>
<tr>
<td>18.</td>
<td>CA removes each of the following equipment TEBs from the safe, reads out the TEB # and serial # then places it on the equipment cart. CA then writes the date/time and signature on the safe log where the removed item(s) are indicated. IW1 verifies the safe log entry then initials it. Laptop1 (Dell ATG6400): TEB# BB51184609 / serial # 37240147333 OS DVD (release 20161014) + HSMFD: TEB# BB46584447 CA verifies 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</td>
<td>go</td>
<td>20:20:39</td>
</tr>
</tbody>
</table>

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>
<tbody>
<tr>
<td>19.</td>
<td>SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry then initials it.</td>
<td>go</td>
<td>20:31:12</td>
</tr>
<tr>
<td>20.</td>
<td>SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the &quot;WAIT&quot; light indicator is off.</td>
<td>go</td>
<td>20:31:54</td>
</tr>
<tr>
<td>21.</td>
<td>CA, SSC1 and IW1 leaves the safe room with the equipment cart, closing the door behind them.</td>
<td>go</td>
<td>20:32:33</td>
</tr>
</tbody>
</table>
## Act 2. OS DVD Acceptance Test, Confirm and Sign the Key Signing Requests

### OS DVD Acceptance Test

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CA inspects the laptop TEB for tamper evidence; reads out the TEB # and</td>
<td>JD</td>
<td>20:35:15</td>
</tr>
<tr>
<td></td>
<td>serial # while IW1 observes and matches it with the prior ceremony script</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>in this facility. CA then places the laptop on the key ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Laptop1 (Dell ATG6400): TEB# BB51184609 / serial # 37240147333</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CA inspects the OS DVD + HSMFD TEB for tamper evidence; reads out</td>
<td>J0</td>
<td>20:35:50</td>
</tr>
<tr>
<td></td>
<td>TEB # while IW1 observes and matches it with the prior ceremony script</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>in this facility. CA then places the items on the key ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OS DVD (release 20161014) + HSMFD: TEB# BB45584447</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CA removes and discards the TEB from the laptop, OS DVD + HSMFD, then</td>
<td>J0</td>
<td>20:42:51</td>
</tr>
<tr>
<td></td>
<td>connects the laptop power, external display, general purpose external</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DVD drive. CA then boots the laptop from OS DVD (release 20161014).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CA sets up the laptop by following the steps below.</td>
<td>J0</td>
<td>20:44:09</td>
</tr>
<tr>
<td></td>
<td>a) Press &quot;CTRL+ALT+F2&quot; to get a console prompt and log in as root.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Execute <code>system-config-display --noui</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Execute <code>killall Xorg</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Confirm that the external display works.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Log in as root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>CA opens a terminal window and maximizes its size for visibility by</td>
<td>J0</td>
<td>20:44:35</td>
</tr>
<tr>
<td></td>
<td>going to <code>Applications &gt; Accessories &gt; Terminal</code>. Follow the additional</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>steps to maximize the terminal window:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Click the View menu and select Zoom In</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Repeat the step above as necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Activity</td>
<td>Initials</td>
<td>Time</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>------</td>
</tr>
</tbody>
</table>
| 6.   | CA inserts the new OS DVD release 20170403 into the external DVD drive, waits for it to be recognized by the OS and performs the following:  
   - a) Close the file system popup window  
   - b) Confirm the assigned drive letter by executing `df`  
   - c) Unmount the DVD drive by executing `umount /dev/scd1`  
   - d) Calculate the SHA-256 hash by executing `sha256sum < /dev/scd1` | J0 | 20:49:59 |
|      | IW1 and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.  
  Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash written on the ceremony script.  
  SHA-256:  
  4d127c7d6e564399c8f4e8b346e7611e23b256d6df3a428a1e531285841  
  PGP Words: dreadful backwater kodi insincere sailboat paperweight flytrap corporate python atmosphere drifter adroitness scallion disruptive Geiger inputps Athens tomorrow cobra suspicious prefer sandalwood flytrap vertigo regain cellulose ratchet Galveston bedlamp cellulose dinosauria decadence  
  Note: The SHA-256 hash of the OS DVD is also published on the IANA website https://data.iana.org/ksk-ceremony/29/12/20170403/iso.sha256 | J0 | |
| 7.   | CA removes the OS DVD by pressing the eject button on the external DVD drive, then places it on the ceremony table, having it visible to the audit camera and the participants. | J0 | 20:50:32 |
| 8.   | CA repeats step 6 and 7 for the 2nd copy of the new OS DVD release 20170403. | J0 | 20:54:39 |
| 9.   | IW1 records the date, time then affixes his/her signature upon successful completion of the OS DVD release 20170403 acceptance testing:  
   - OS DVD Acceptance Test release 20170403  
   - Printed Name: Jonathan Denison  
   - Date: 2017/08/17  
   - Time: 20:54:52  
   - Signature | J0 | 20:54:59 |
| 10.  | CA disconnects the general purpose external DVD drive from the laptop, then removes the OS DVD by performing:  
   - a) Turn off the laptop by pressing the power switch  
   - b) Turn on the laptop by pressing the power switch and immediately remove the old OS DVD (release 20161014) from the laptop DVD drive  
   - c) Disconnect the laptop to power off | J0 | 20:54:28 |
| 11.  | CA discards all the old OS DVD (release 20161014) copies. | J0 | 20:57:01 |
## Set Up Laptop

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>CA boots the laptop by following the steps below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Connect the power supply and USB printer cable.</td>
<td>j0</td>
<td>21:02:10</td>
</tr>
<tr>
<td></td>
<td>b) Switch ON the laptop and immediately insert the new OS DVD release 20170403</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>CA sets up the laptop by following the steps below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Press &quot;CTRL+ALT+F2&quot; to get a console prompt and log in as root.</td>
<td>j0</td>
<td>21:03:58</td>
</tr>
<tr>
<td></td>
<td>b) Execute <code>system-config-display --noui</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Execute <code>killall Xorg</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Confirm that external display works.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Log in as root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>CA confirms that the printer is connected then configures printer as default and prints test page by going to System &gt; Administration &gt; Printing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>And follow the steps below:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Click the New Printer icon (left side), leave everything default and then click the button Forward</td>
<td>j0</td>
<td>21:07:31</td>
</tr>
<tr>
<td></td>
<td>b) Under &quot;Select Connection&quot; choose the first device &quot;HP Laserjet xxxx&quot; and then click the button Forward.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The xxxx is the Printer Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Select HP and click the button Forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Under &quot;Models&quot; scroll up and select &quot;Laserjet&quot;, and then click the button Forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Click the button Apply to finish</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) Under &quot;Local Printers&quot; from the left menu, select &quot;printer&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) Click the button &quot;Make Default Printer&quot; and &quot;Print Test Page&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) Close the printer setup windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>CA opens a terminal window and maximizes its size for visibility by going to Applications &gt; Accessories &gt; Terminal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Follow the additional steps to maximize the terminal window:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Click the View menu and select Zoom In</td>
<td>j0</td>
<td>21:08:07</td>
</tr>
<tr>
<td></td>
<td>d) Repeat the step above as necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal window, CA executes: <code>date -s &quot;20170817 HH:MM:00&quot;</code></td>
<td>j0</td>
<td>21:08:55</td>
</tr>
<tr>
<td></td>
<td>where HH is two-digit Hour, MM is two digit Minutes and 00 is Zero Seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA executes <code>date</code> 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>17.</td>
<td>CA plugs a new FD into the laptop, then waits for it to be recognized by the OS, 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 unmount 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>90</td>
<td>21:10:27</td>
</tr>
<tr>
<td>18.</td>
<td>CA repeats step 17 for the 2nd blank FD</td>
<td>90</td>
<td>21:11:17</td>
</tr>
<tr>
<td>19.</td>
<td>CA repeats step 17 for the 3rd blank FD</td>
<td>90</td>
<td>21:12:00</td>
</tr>
<tr>
<td>20.</td>
<td>CA repeats step 17 for the 4th blank FD</td>
<td>90</td>
<td>21:12:48</td>
</tr>
<tr>
<td>21.</td>
<td>CA repeats step 17 for the 5th blank FD</td>
<td>90</td>
<td>21:13:26</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>22.</td>
<td>CA plugs the previous HSMFD used in the ceremony 28 into the free USB slot on the laptop and waits for OS to recognize it. CA displays the HSMFD contents to all participants then closes the file system window.</td>
<td>90</td>
<td>21:14:50</td>
</tr>
<tr>
<td>23.</td>
<td>CA calculates the SHA-256 hash of the contents on the copied HSMFD by executing <code>hsmfd-hash -c</code></td>
<td>90</td>
<td>21:17:23</td>
</tr>
<tr>
<td></td>
<td>IW1 confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 28 annotated script (image from Ceremony 28 annotated script).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SHA-256 hash: <code>cf2cecc7219eb7bfa1f176dfffcd63c3869ee86e510c50cf8eacc376a584b1f6c</code></td>
<td>90</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PGP Wordlist of the SHA-256 hash:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PGP Words: stagehand Chicago tumor retraction blackjack onlooker seabird rebellion ratchet vacancy inverse therapist willow sandalwood flatfoot replica optic universe necklace travesty assume resistor ammo warrant Trojan revolver clamshell hamburger endorsedisable billiard unicorn</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash written on the ceremony script.</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>24.</td>
<td>CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code></td>
<td>j0</td>
<td>21:17:43</td>
</tr>
<tr>
<td>25.</td>
<td>CA executes <code>script script-20170817.log</code> to start a capture of terminal output.</td>
<td>j0</td>
<td>21:18:04</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>26.</td>
<td>CA connects a serial to USB null modem cable to laptop.</td>
<td>j0</td>
<td>21:18:43</td>
</tr>
</tbody>
</table>
| 27.  | CA opens a second terminal window and maximizes its size for visibility by going to `Applications > Accessories > Terminal`.  
     | Follow the additional steps to maximize the terminal window:             |          |       |
     | a) Click the `View` menu and select `Zoom In`                            |          |       |
     | b) Repeat the step above as necessary                                  |          |       |
     | and executes `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>28.</td>
<td>CA inspects the HSM TEB for tamper evidence; reads out the TEB # and HSM serial # while IW1 observes and matches it with the prior ceremony script in this facility. HSM3: TEB# BB51184611 / serial # H1403033</td>
<td>j0</td>
<td>21:23:37</td>
</tr>
<tr>
<td>29.</td>
<td>CA removes and discards the TEB of the HSM, then plugs ttyUSB0 null modem serial cable to the back of the HSM.</td>
<td>j0</td>
<td>21:23:23</td>
</tr>
</tbody>
</table>
| 30.  | CA switches to the ttyaudit terminal window and connects power to HSM and switches the power ON. Status information should appear on the serial logging screen. IW1 matches the displayed HSM serial number with below. HSM3: serial # H1403033  
     | Note: The date/time on the HSM is not used as a reference for logging and timestamp. | j0       | 21:23:39 |
Enable/Activate HSM3

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.</td>
<td>One by one, CA calls each COs listed below to inspect the TEB for tamper evidence. With the help of the CA, the CO opens the TEB and hands the OP cards to the CA, then places it on the cardholder visible to everyone.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 1: Arborgast Fabian</td>
<td>OP TEB # BB46584450</td>
<td>107</td>
<td></td>
</tr>
<tr>
<td>CO 2: Dmitry Burkov</td>
<td>OP TEB # BB46584452</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 5: Olafur Gudmundsson</td>
<td>OP TEB # BB46584660</td>
<td>56-7</td>
<td></td>
</tr>
<tr>
<td>CO 6: Nicolas Antoniello</td>
<td>OP TEB # BB46584458</td>
<td>62-7</td>
<td></td>
</tr>
<tr>
<td>CO 7: Subramanian Moonesamy</td>
<td>OP TEB # BB46584460</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>

| 32.  | CA activates the HSM by following the steps below:  
a) Utilize the HSM's keyboard to scroll through the menu using < >  
b) Select "1.Set Online", then hit ENT to confirm  
c) When "Set Online?" is displayed, then 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", then hit ENT  
f) When "Remove Card?" is displayed, then remove the card  
g) Repeat steps d) to f) for the 2nd and 3rd OP cards |  |  |

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 _1_ of 7  
2nd OP card _2_ of 7  
3rd OP card _3_ of 7 |  |  |
Check Network Connectivity Between Laptop and HSM3

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>CA connects the HSM to the laptop using Ethernet cable in LAN port.</td>
<td>J0</td>
<td>21:18:59</td>
</tr>
<tr>
<td>34.</td>
<td>CA switches to the terminal window and tests network connectivity between laptop and HSM by executing: ping 192.168.0.2 and looking for responses. Ctrl-C to exit program.</td>
<td>J0</td>
<td>21:19:28</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>35.</td>
<td>The KSR FD was transferred to the facility by the RKOS. It contains four KSRs. One is for the normal operation and three are for fallback scenarios. CA plugs the FD labeled &quot;KSR&quot; then waits for it to be recognized by the OS. CA points out the KSR file that will be signed on each folder, then closes the file system window.</td>
<td>J0</td>
<td>21:36:48</td>
</tr>
</tbody>
</table>

Execute KSR Signer for Phase D to E

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.</td>
<td>CA uses the terminal window to sign the KSR file by executing the following: ksr signer /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml</td>
<td>J0</td>
<td>21:40:55</td>
</tr>
<tr>
<td>37.</td>
<td>The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/n): CA confirms that the HSM is online, then enters &quot;y&quot; to proceed.</td>
<td>J0</td>
<td>21:41:15</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>38.</td>
<td>When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room. The RZM provides identification document for the IW1 to review and retain. RZM, then reads out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. IW1 enters the RZM representative’s name here: __________________________</td>
<td>J0</td>
<td>21:42:59</td>
</tr>
<tr>
<td>39.</td>
<td>Participants match the hash read out displayed on the terminal window. CA asks, &quot;are there any objections?&quot;</td>
<td>J0</td>
<td>21:43:31</td>
</tr>
<tr>
<td>40.</td>
<td>CA then enters &quot;y&quot; in response to &quot;Is this correct y/n?&quot; to complete the KSR signing operation. The SKR is located on /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml</td>
<td>J0</td>
<td>21:43:51</td>
</tr>
</tbody>
</table>
# Root DNSSEC Script Exception

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

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

### Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>IW1 notes date and time of key ceremony exception and signs here:</td>
<td>JH</td>
<td>21:33:12</td>
</tr>
<tr>
<td>2.</td>
<td>IW1 Describes exception and action below.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When inserting the KSR FD, it's possible the HSMFD may have disturbed and disrupted the script. As a matter of precaution, CA cancelled TTY audit window started second window for TTY audit script window restarted script command.

*Additional notes were written prior to step 16 April.*

---

*End of Root DNSSEC Script Exception*
August 12th, 2017

To Whom It May Concern:

This is a letter of Verification of Employment for Alejandro A. Bolivar. Verisign, Inc. has employed Alejandro A. Bolivar full-time since September 8th, 1997, currently as a Sr. Engineer – CBO in our Product Operations organization.

Verisign is the trusted provider of Internet infrastructure services and operates the authoritative directory of all .com, .net, .cc, .tv, and .name domain names and the back-end systems for all .gov, .jobs and .edu domain names. Verisign manages and protects the global domain name system (DNS) infrastructure for more than 113 million domain names and processes approximately 60 billion queries daily, while maintaining 100 percent operational accuracy and stability for more than a decade. Our services also help ensure that online businesses are as available as the Web itself.

As the global leader in domain names, Verisign powers the invisible navigation that takes people to where they want to go on the Internet. For more than 19 years, Verisign has operated the infrastructure for a portfolio of top-level domains that today includes .com, .net, .tv .edu, .gov, .jobs, .name, and .cc, as well as two of the world’s 13 Internet root servers. Verisign’s product suite also includes Distributed Denial of Service (DDoS) Protection Services and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit Verisign.com.

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

Sincerely,

[Signature]

David Carney
HR Specialist | Verisign, Inc. | 703-948-4143 | dcarney@verisign.com
17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

80cccf481a6f5b5eff1841889b0c31cfc6ec7d4ff22def5e74a1be83b46b8252

The PGP wordlist for the hash above is:

merit revolver stagehand dictator beehive hemisphere erase finicky Zulu borderline cranky maritime puppy article chatter Saturday southward unicorn klaxon document uproot clergyman uncut finicky indoors outfielder skydive Jamaica scenic Hamilton miser enrollment

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.
ksrigner-20170817-214009.log

Starting: ksrigner /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml (at Thu Aug 17 21:40:05 2017 UTC)
Use HSM /opt/dnsssec/keep_bcmconfig
setenv KEYRING_LIBRARY_PATH=/opt/dnsssec
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: AE8 Networks
Model: Keyper 9658-2
Serial: H103633

Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-07-01T00:00:00 2017-07-32T00:00:00 14796,15768 19036(Kjgmt7v)/S
2 2017-07-11T00:00:00 2017-08-01T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
4 2017-07-31T00:00:00 2017-08-21T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
5 2017-08-11T00:00:00 2017-09-11T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
6 2017-08-21T00:00:00 2017-09-21T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
7 2017-09-11T00:00:00 2017-09-21T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
8 2017-09-30T00:00:00 2017-09-30T00:00:00 15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
9 2017-09-15T00:00:00 2017-10-10T00:00:00 46809,15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 15768,46809 19036(Kjgmt7v)/S
2 2017-10-21T00:00:00 2017-11-01T00:00:00 46809 20326(Klajeysy)/P
3 2017-10-31T00:00:00 2017-11-31T00:00:00 46809 20326(Klajeysy)/P
4 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(Klajeysy)/P
5 2017-11-30T00:00:00 2017-12-31T00:00:00 46809 20326(Klajeysy)/P
6 2017-12-01T00:00:00 2017-12-10T00:00:00 46809 20326(Klajeysy)/P
7 2017-12-10T00:00:00 2017-12-20T00:00:00 46809 20326(Klajeysy)/P
8 2017-12-20T00:00:00 2018-01-01T00:00:00 46809,46809 20326(Klajeysy)/P,19036(Kjgmt7v)/S

...PASSED.

SHA256 hash of KSR:
9BCC5C4F41A4EF5F2F1B418990B3C31FC68C27D4FF72DEF5E74A1BE83B46689252
>> merit revolver stagehand dictator beehive hemisphere erase finicky Zulu borderline cranky maritime puppy article chatter Saturday southward unicorn lexicon document uproot oligarchy uncut finicky indoors outfielder skydive Jamaica scenario Hamilton enlistment <<

Reading KSR schedule "rollover(2010,2017)" from "kskschedule.json"
# KSK Tag(CKA_LABEL)
1 19036(Kjgmt7v)/S,20326(Klajeysy)/P
2 19036(Kjgmt7v)/P,20326(Klajeysy)/S
3 19036(Kjgmt7v)/P,20326(Klajeysy)/S
4 19036(Kjgmt7v)/P,20326(Klajeysy)/S
5 19036(Kjgmt7v)/P,20326(Klajeysy)/S
6 19036(Kjgmt7v)/P,20326(Klajeysy)/S
7 19036(Kjgmt7v)/P,20326(Klajeysy)/S
8 19036(Kjgmt7v)/P,20326(Klajeysy)/S
9 19036(Kjgmt7v)/P,20326(Klajeysy)/S

Generated new SKR in /media/KSR/KSK30-0-D_to_E/ksr-root-2017-q4-0-d_to_e.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-22T00:00:00 46809,15768 20326(Klajeysy)/P,19036(Kjgmt7v)/S
2 2017-10-21T00:00:00 2017-11-01T00:00:00 46809 20326(Klajeysy)/P,19036(Kjgmt7v)/P
3 2017-10-31T00:00:00 2017-11-31T00:00:00 46809 20326(Klajeysy)/P,19036(Kjgmt7v)/P
4 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(Klajeysy)/P,19036(Kjgmt7v)/P
5 2017-11-30T00:00:00 2017-12-31T00:00:00 46809 20326(Klajeysy)/P,19036(Kjgmt7v)/P
6 2017-12-01T00:00:00 2017-12-10T00:00:00 46809 20326(Klajeysy)/P,19036(Kjgmt7v)/P
7 2017-12-10T00:00:00 2017-12-20T00:00:00 46809 20326(Klajeysy)/P,19036(Kjgmt7v)/P
8 2017-12-20T00:00:00 2018-01-01T00:00:00 46809,41024 20326(Klajeysy)/P,19036(Kjgmt7v)/P
9 2017-12-20T00:00:00 2018-01-01T00:00:00 46809,41024 20326(Klajeysy)/P,19036(Kjgmt7v)/P

SHA256 hash of SKR:
C90365F5139CC9ACE3D43F2F12706321F3D33A0933CE277B920
>> slowdown narrative trauma equipment bedlamp article reform telephone vapor Hamilton befriend pedigree some handiwork crackdown distortion cement adviser bronchial amulet cement pharmacy stapler replica repay amnistice classroom retraction uproot inception trauma tobacco <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
### Execute KSR Signer for Phase E to D

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.</td>
<td>CA uses the terminal window to sign the KSR file by executing the following: krsigner /media/KSR/KSK30-1-E_to_D/ksr-root-2017-q4-1-e_to_d.xml</td>
<td>00</td>
<td>21:41:44</td>
</tr>
<tr>
<td>42.</td>
<td>The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/n): CA confirms that the HSM is online, then enters ‘y’ to proceed.</td>
<td>00</td>
<td>21:44:55</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>43.</td>
<td>When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.</td>
<td>00</td>
<td>21:45:36</td>
</tr>
<tr>
<td>44.</td>
<td>Participants match the hash read out displayed on the terminal window. CA asks, “are there any objections?”</td>
<td>00</td>
<td>21:45:49</td>
</tr>
<tr>
<td>45.</td>
<td>CA then enters “y” in response to “Is this correct y/n?” to complete the KSR signing operation. The SKR is located on  /media/KSR/KSK30-1-E_to_D/skr-root-2017-q4-1-e_to_d.xml</td>
<td>00</td>
<td>21:46:12</td>
</tr>
</tbody>
</table>

### Execute KSR Signer for Phase D to D

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td>CA uses the terminal window to sign the KSR file by executing the following: krsigner /media/KSR/KSK30-2-D_to_D/ksr-root-2017-q4-2-d_to_d.xml</td>
<td>00</td>
<td>21:46:40</td>
</tr>
<tr>
<td>47.</td>
<td>The KSR signer will provide the following prompt: Activate HSM prior to accepting in the affirmative!! (y/n): CA confirms that the HSM is online, then enters ‘y’ to proceed.</td>
<td>00</td>
<td>21:46:51</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>48.</td>
<td>When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.</td>
<td>00</td>
<td>21:47:34</td>
</tr>
<tr>
<td>49.</td>
<td>Participants match the hash read out displayed on the terminal window. CA asks, “are there any objections?”</td>
<td>00</td>
<td>21:47:43</td>
</tr>
<tr>
<td>50.</td>
<td>CA enters “y” in response to “Is this correct y/n?” to complete the KSR signing operation. The SKR is located on /media/KSR/KSK30-2-D_to_D/skr-root-2017-q4-2-d_to_d.xml</td>
<td>00</td>
<td>21:48:03</td>
</tr>
</tbody>
</table>
17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

\texttt{aa23456d408436f33678fae23d81ac861782f1866f9374600f4b681de5d9fec}

The PGP wordlist for the hash above is:

\texttt{reward cannonball crusade hazardous crackdown Jupiter Christmas vertigo Christmas indigo wallet tomorrow commence inventive ribcage letterhead banjo Istanbul unwind letterhead gremlin molasses indoors fortitude artist disable frighten breakaway orca filament quota unicorn}

Attested on behalf of VeriSign by:

\textbf{Alejandro Bolívar}
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.
17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

57f78fa5800b04e90ef37d0fbabcca5875701122851206ae1b91c7404cb07c55

The PGP wordlist for the hash above is:

eightball voyager payday paperweight merit armistice
adrift ultimate apple vertigo klaxon atmosphere shadow
pyramid spellbind everyday indulge hesitate Athens
candidate music backwater afflict performance beeswax
miracle soybean Dakota drainage phonetic kiwi equipment

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.
Starting: kersigner /media/KSR/KSR30-2-D_to_D/krs-root-2017-q4-2-d_to_d.xml (at Thu Aug 17 21:16:02 2017 UTC)
Use HSM /opt/dnssec/asp.hsmconfign
HSM /opt/dnssec/asp.hsmconfign activated.
setenv KEYER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keypair/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keypair/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot-0
HSM slot 0 included
Loaded /opt/Keypair/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot-0
HSM Information:
Label: TCANNXSK
ManufacturerID: AED Networks
Model: Keyper 9600-2
Serial: h100333

Valuating last KSR with HSM...

# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-07-01T00:00:00 2017-07-21T00:00:00 14736,15768 19036(Kjgmt7v)/S
2 2017-07-01T00:00:00 2017-08-01T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
4 2017-07-31T00:00:00 2017-08-21T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
5 2017-08-10T00:00:00 2017-08-31T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
6 2017-08-20T00:00:00 2017-09-10T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
7 2017-08-30T00:00:00 2017-09-20T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
8 2017-09-09T00:00:00 2017-09-30T00:00:00 15768 20326(Klajey)/P,19036(Kjgmt7v)/S
9 2017-09-19T00:00:00 2017-10-10T00:00:00 46809,15768 20326(Klajey)/P,19036(Kjgmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSR30-2-D_to_D/krs-root-2017-q4-2-d_to_d.xml...

# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-21T00:00:00 15768,46809 19036(Kjgmt7v)/S
2 2017-10-11T00:00:00 2017-10-31T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
3 2017-10-21T00:00:00 2017-11-10T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
9 2017-12-20T00:00:00 2018-01-01T00:00:00 41824,46809 20326(Klajey)/P,19036(Kjgmt7v)/S

...PASSED.

SHA256 hash of KSR:
7e5d8e2e19a43c422026c03f863a41630c356a1cd150d96c3
>> eightball voyager payday paperweight merit armistice adrift ultimate apple vertigo klaxon atmosphere shadow pyramid id spellbind everyday indulge hesitantate Athens candidate music backwater afflict performance beeswax miracle soybean Dakota drainage phonetic klw1 equipment <<

Reading KSR schedule *publish+(2010,2017)* from *kkschedule.jaon*

# KSK Tag(CKA_LABEL)
1 19036(Kjgmt7v)/S,20326(Klajey)/P
2 19036(Kjgmt7v)/S,20326(Klajey)/P
3 19036(Kjgmt7v)/S,20326(Klajey)/P
4 19036(Kjgmt7v)/S,20326(Klajey)/P
5 19036(Kjgmt7v)/S,20326(Klajey)/P
6 19036(Kjgmt7v)/S,20326(Klajey)/P
7 19036(Kjgmt7v)/S,20326(Klajey)/P
8 19036(Kjgmt7v)/S,20326(Klajey)/P
9 19036(Kjgmt7v)/S,20326(Klajey)/P

Generated new KSR in /media/KSR/KSR30-2-D_to_D/krs-root-2017-q4-2-d_to_d.xml

# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2017-10-01T00:00:00 2017-10-21T00:00:00 46809,15768 20326(Klajey)/P,19036(Kjgmt7v)/S
2 2017-10-11T00:00:00 2017-10-31T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
3 2017-10-21T00:00:00 2017-11-10T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
4 2017-10-31T00:00:00 2017-11-21T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
5 2017-11-10T00:00:00 2017-12-01T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
6 2017-11-20T00:00:00 2017-12-11T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
7 2017-11-30T00:00:00 2017-12-21T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
8 2017-12-10T00:00:00 2017-12-31T00:00:00 46809 20326(Klajey)/P,19036(Kjgmt7v)/S
9 2017-12-20T00:00:00 2018-01-01T00:00:00 41824,46809 20326(Klajey)/P,19036(Kjgmt7v)/S

SHA256 hash of KSR:
7e5d8e2e19a43c422026c03f863a41630c356a1cd150d96c3
>> eightball voyager payday paperweight merit armistice adrift ultimate apple vertigo klaxon atmosphere shadow pyramid id spellbind everyday indulge hesitantate Athens candidate music backwater afflict performance beeswax miracle soybean Dakota drainage phonetic klw1 equipment <<

Unloaded /opt/Keypair/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot-0
### Execute KSR Signer for Phase C to C

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>51.</td>
<td>CA uses the terminal window to sign the KSR file by executing the following: \texttt{krsigner /media/KSR/KSK30-3-C_to_C/krs-root-2017-q4-3-c_to_c.xml}</td>
<td>J0</td>
<td>21:48:34</td>
</tr>
<tr>
<td>52.</td>
<td>The KSR signer will provide the following prompt: \texttt{Activate HSM prior to accepting in the affirmative!! (y/N)}: CA confirms that the HSM is online, then enters \texttt{y} to proceed.</td>
<td>J0</td>
<td>21:49:16</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>53.</td>
<td>When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.</td>
<td>J0</td>
<td>21:49:26</td>
</tr>
<tr>
<td>54.</td>
<td>Participants match the hash read out displayed on the terminal window. CA asks, &quot;are there any objections&quot;?</td>
<td>J0</td>
<td>21:49:36</td>
</tr>
<tr>
<td>55.</td>
<td>CA enters \texttt{y} in response to \texttt{&quot;Is this correct y/n?&quot;} to complete the KSR signing operation. The SKR is located on \texttt{/media/KSR/KSK30-3-C_to_C/skr-root-2017-q4-3-c_to_c.xml}</td>
<td>J0</td>
<td>21:49:49</td>
</tr>
</tbody>
</table>

### 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>56.</td>
<td>CA prints out sufficient number of copies for participants by executing the following command on the terminal window for i in $(ls -l krsigner-20170817-*.log); do printlog $i X; done \textbf{Note:} Replace X with the number of copies for the participants.</td>
<td>J0</td>
<td>21:51:04</td>
</tr>
<tr>
<td>57.</td>
<td>MW1 attaches a copy of each krsigner log to his/her script.</td>
<td>J0</td>
<td>21:54:30</td>
</tr>
</tbody>
</table>
17 August, 2017

The SHA256 hash of the 2017 Q4 KSR file is:

57c004641175eb804236a9ea091665c2c182720b506d4a03f527fa2b337e523a

The PGP wordlist for the hash above is:

eightball recipe adrift getaway Athens impartial trouble intention crowfoot congregate revenge undaunted Algol bodyguard fracture repellent snapline Istanbul highchair armistice drumbeat hazardous dogsled aggregate vapor celebrate wallet Cherokee chisel insurgent Dupont corrosion

Attested on behalf of VeriSign by:

Alejandro Bolívar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.
Starting: krsigner /media/KSR/KSK30-3-C_to_C/kar-root-2017-q4-3-c_to_c.xml (at Thu Aug 17 21:47:56 2017 UTC)
Use IEM /opt/dnsssec/aep.homeconfig
HSM /opt/dnsssec/aep.homeconfig activated.
setenv KEYER_LIBRARY_PATH=/opt/dnsssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyer/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyer/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included.
Loaded /opt/Keyer/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyer 9866-2
Serial: H1406553

Validating last SKR with HSM...

# Inception  Expiration  ZSK Tags  KSK Tag
1  2017-07-11T00:00:00  2017-07-22T00:00:00  14795,15768  19036(Kjgmt7v)/S
2  2017-07-21T00:00:00  2017-08-01T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
3  2017-07-21T00:00:00  2017-08-11T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
4  2017-07-31T00:00:00  2017-08-31T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
5  2017-08-10T00:00:00  2017-09-10T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
6  2017-08-20T00:00:00  2017-09-20T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
7  2017-09-09T00:00:00  2017-09-30T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
8  2017-09-09T00:00:00  2017-09-30T00:00:00  15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S
9  2017-09-19T00:00:00  2017-10-10T00:00:00  46609,15768  20326(Klaajezys/P)/19036(Kjgmt7v)/S

...VALIDATED.

Validate and Process KSR /media/KSR/KSK30-3-C_to_C/kar-root-2017-q4-3-c_to_c.xml...

# Inception  Expiration  ZSK Tags  KSK Tag
1  2017-10-01T00:00:00  2017-10-22T00:00:00  15768,46609  19036(Kjgmt7v)/S
2  2017-10-11T00:00:00  2017-11-01T00:00:00  46609  19036(Kjgmt7v)/S
3  2017-10-12T00:00:00  2017-11-12T00:00:00  46609  19036(Kjgmt7v)/S
4  2017-10-31T00:00:00  2017-11-21T00:00:00  46609  19036(Kjgmt7v)/S
5  2017-11-10T00:00:00  2017-12-01T00:00:00  46609  19036(Kjgmt7v)/S
6  2017-11-20T00:00:00  2017-12-11T00:00:00  46609  19036(Kjgmt7v)/S
7  2017-11-30T00:00:00  2017-12-21T00:00:00  46609  19036(Kjgmt7v)/S
8  2017-12-10T00:00:00  2018-01-10T00:00:00  41824,46609  19036(Kjgmt7v)/S

...PASSED.

SHA256 hash of KSR: 57506461E77EB60423639AD091666C2C8B272DB50DA01F527F2A337E552A
>> eighth ball recipe adrift getaway Athens impartial trouble intention crowfoot congregate revenue unadulterated Algol bo dyguard fracture repellent snapline Istanbul highbabe armistice drumbeat hazardous dogged aggregate vapor celebrat e wallet Cherokee chisel insurgent Dupont corrosion <<

Reading KSR schedule "normal(2010)" from "kskschedule.json"
# KSK Tag(CKA_LABEL)
1 19036(Kjgmt7v)/S
2 19036(Kjgmt7v)/S
3 19036(Kjgmt7v)/S
4 19036(Kjgmt7v)/S
5 19036(Kjgmt7v)/S
6 19036(Kjgmt7v)/S
7 19036(Kjgmt7v)/S
8 19036(Kjgmt7v)/S
9 19036(Kjgmt7v)/S

Generated new SKR in /media/KSR/KSK30-3-C_to_C/kar-root-2017-q4-3-c_to_c.xml
# Inception  Expiration  ZSK Tags  KSK Tag
1  2017-10-01T00:00:00  2017-10-22T00:00:00  46609,15768  19036(Kjgmt7v)/S
2  2017-10-11T00:00:00  2017-11-01T00:00:00  46609  19036(Kjgmt7v)/S
3  2017-10-12T00:00:00  2017-11-12T00:00:00  46609  19036(Kjgmt7v)/S
4  2017-10-31T00:00:00  2017-11-21T00:00:00  46609  19036(Kjgmt7v)/S
5  2017-11-10T00:00:00  2017-12-01T00:00:00  46609  19036(Kjgmt7v)/S
6  2017-11-20T00:00:00  2017-12-11T00:00:00  46609  19036(Kjgmt7v)/S
7  2017-11-30T00:00:00  2017-12-21T00:00:00  46609  19036(Kjgmt7v)/S
8  2017-12-10T00:00:00  2018-01-10T00:00:00  41824,46609  19036(Kjgmt7v)/S

SHA256 hash of SKR: 43A7091235D4AA3572B602D3555B05C65702CBAE190D464AC2D9585D9D1855E1
>> drifter paragraph augur Caselet classroom alkali regrettime customer gazelle hazardous regrettime resistor stairway fas cinate spindle intention eyeless graduate bison revenue tempest millionaire upshot getaway ribcage clergyman preclu de leprosy shadow photograph minnow tolerance <<
Uploaded /opt/Keyer/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
Backup Newly Created SKR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 58.  | CA copies the contents of the KSR FD by executing the following command on the terminal window
      | `cp -pR /media/KSR/* .` Confirm overwrite by entering “y” when prompted. | J0 | 21:55:16 |
| 59.  | CA uses the terminal window to perform the following commands:
      | a) list the contents of the KSR FD by executing `ls -ltr /media/KSR`
      | b) flush the system buffers by executing `sync`
      | c) unmount the KSR FD by executing `umount /media/KSR` | J0 | 21:56:22 |
| 80.  | CA removes the KSR FD containing the SKR files, then gives it to the RZM representative. | J0 | 21:56:55 |

Disable/Deactivate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 61.  | CA ensures to utilize the cards that were NOT used on the prior steps.
      | CA will perform the following steps to deactivate the HSM:
      | a) Utilize the HSM’s keyboard to scroll through the menu using < >
      | b) Select “2. Set Offline”, then hit ENT to confirm
      | c) When “Set Offline?” is displayed, then 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”, then hit ENT
      | f) When “Remove Card?” is displayed, then remove the card
      | g) Repeat steps d) to f) for the 2nd and 3rd OP cards
      | Confirm the “READY” LED on the HSM is OFF.
      | IVW1 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 | J0 | 21:56:07 |
Act 3. Secure Hardware and Close the Ceremony

Return HSM to 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 HSM to power OFF, then disconnects the power and laptop</td>
<td></td>
<td>21:00:19</td>
</tr>
<tr>
<td></td>
<td>(serial and Ethernet) connections.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: DO NOT unplug the connections on the laptop end.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>CA places the HSM into a prepared TEB, then seals it.</td>
<td>J0</td>
<td>22:01:43</td>
</tr>
<tr>
<td>3.</td>
<td>CA reads out the TEB # and the HSM serial #, then shows it to the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>participants. IW1 confirms the TEB # and HSM serial # below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM3: TEB# BB51184623 / serial # H1403033</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sealing strips for later inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA places the HSM TEB on the 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</td>
<td>J0</td>
<td>22:03:24</td>
</tr>
<tr>
<td></td>
<td>CA terminates the HSM serial output capture by disconnecting the USB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>serial adaptor from the laptop. CA then exits out of Serial Port Activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ttyaudit) terminal window by typing &quot;exit&quot;, then press enter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Terminating the logging script</td>
<td>J0</td>
<td>22:03:58</td>
</tr>
<tr>
<td></td>
<td>CA stops the logging terminal output by typing &quot;exit&quot;, then press enter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: This only stops the script logging and will NOT close the terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>window.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

version 2.0
### 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 sets dotglob by executing the following command on the terminal window&lt;br&gt;<code>shopt -s dotglob</code>&lt;br&gt;Note: This enables copying of all files from the original HSMFD.</td>
<td>j0</td>
<td>22:01:03</td>
</tr>
<tr>
<td>7.</td>
<td>CA prints two copies of the hash by executing the following command on the terminal window&lt;br&gt;<code>for i in $({seq 2}); do hsmfd-hash -p; done</code>&lt;br&gt;Note: One copy for audit bundle and one copy for HSMFD package.</td>
<td>j0</td>
<td>22:04:32</td>
</tr>
<tr>
<td>8.</td>
<td>CA displays contents of HSMFD by executing the following command on the terminal window&lt;br&gt;<code>ls -ltR</code></td>
<td>j0</td>
<td>22:05:30</td>
</tr>
<tr>
<td>9.</td>
<td>CA plugs a blank FC labeled HSMFD into a free USB slot on the laptop, then waits for the OS to recognize it as HSMFD_.&lt;br&gt;CA closes the file system window and creates a backup of the HSMFD by executing following command on the terminal window&lt;br&gt;<code>cp -pr * /media/HSMFD_</code></td>
<td>j0</td>
<td>22:06:21</td>
</tr>
<tr>
<td>10.</td>
<td>CA displays the contents of HSMFD_ by executing the following command on the terminal window&lt;br&gt;<code>ls -ltR /media/HSMFD_</code></td>
<td>j0</td>
<td>22:06:39</td>
</tr>
<tr>
<td>11.</td>
<td>CA matches the SHA-256 hash between the original HSMFD and the copy HSMFD by executing the following command on the terminal window&lt;br&gt;<code>hsmfd-hash -m</code></td>
<td>j0</td>
<td>22:07:12</td>
</tr>
<tr>
<td>12.</td>
<td>CA unmounts the HSMFD copy by executing the following command on the terminal window&lt;br&gt;<code>umount /media/HSMFD_</code></td>
<td>j0</td>
<td>22:07:21</td>
</tr>
<tr>
<td>13.</td>
<td>CA removes the HSMFD_ and places it on the holder.</td>
<td>j0</td>
<td>22:07:57</td>
</tr>
<tr>
<td>14.</td>
<td>CA repeats step 9 to 13 for the 2\textsuperscript{nd} copy.</td>
<td>j0</td>
<td>22:08:11</td>
</tr>
<tr>
<td>15.</td>
<td>CA repeats step 9 to 13 for the 3\textsuperscript{rd} copy.</td>
<td>j0</td>
<td>22:08:45</td>
</tr>
<tr>
<td>16.</td>
<td>CA repeats step 9 to 13 for the 4\textsuperscript{th} copy.</td>
<td>j0</td>
<td>22:09:28</td>
</tr>
<tr>
<td>17.</td>
<td>CA repeats step 9 to 13 for the 5\textsuperscript{th} copy.</td>
<td>j0</td>
<td>22:09:51</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>18.</td>
<td>CA prints out a hard copy of the logging information by executing the following command on the terminal window&lt;br&gt;<code>enscript -ZGr -# 1 script-20170817.log</code>&lt;br&gt;<code>enscript -GGr -# 1 --font=&quot;Courier8&quot; ttyaudit-ttyUSB*20170817-* .log</code>&lt;br&gt;Note: Ignore the error regarding non-printable characters if prompted.</td>
<td>j0</td>
<td>22:15:07</td>
</tr>
</tbody>
</table>
# find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha2wordlist

SHA-256: 5f378217c62d0556dae2122c8dd32b89cf8d51e7e4f9d3b512b79ab9bf2336c0

PGP Words: eyetooth consensus miser bookseller southward clergyman adult escapade surmount tomorrow atlas Chicago optic sociable briefcase matchmaker stagehand microscope drunken graduate tonic Waterloo stapler positive atlas processor pupil proximate slingshot cannonball Christmas recipe
Reading KSR schedule "rollover(2010.10)" from kekschedule.json

# KEK Tag (KRA_LABEL)
1 19356(Kjgmt7v)/P,20326(Klaeyes)/S
2 19356(Kjgmt7v)/F,20326(Klaeyes)/P
3 19356(Kjgmt7v)/F,20326(Klaeyes)/S
4 19356(Kjgmt7v)/F,20326(Klaeyes)/S
5 19503(Kjgmt7v)/F,20326(Klaeyes)/S
6 19356(Kjgmt7v)/F,20326(Klaeyes)/S
7 19356(Kjgmt7v)/F,20326(Klaeyes)/S
8 19356(Kjgmt7v)/F,20326(Klaeyes)/S
9 19356(Kjgmt7v)/F,20326(Klaeyes)/S
Validating and Process KSR /media/KSR/KSK30-1-E_to_D/ker-root-2017-q4-1-a_to_d.xml...
  # Inception    Expiration    ZEK Tags    ZEK Tag(CKA_LABEL)
  1 2017-10-01T00:00:00 2017-09-30T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  2 2017-09-01T00:00:00 2017-09-30T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  3 2017-09-01T00:00:00 2017-10-01T00:00:00 46609,15768 20326(Klajeys)/P.19036(Kjgmt)
...VALIDATED.

Validating and Process KSR /media/KSR/KSK30-1-E_to_D/ker-root-2017-q4-1-a_to_d.xml...
  # Inception    Expiration    ZEK Tags    ZEK Tag(CKA_LABEL)
  1 2017-10-01T00:00:00 2017-10-27T00:00:00 15768,46609
  2 2017-10-11T00:00:00 2017-11-01T00:00:00 46609
  3 2017-10-21T00:00:00 2017-11-01T00:00:00 46609
  4 2017-11-01T00:00:00 2017-11-21T00:00:00 46609
  5 2017-11-11T00:00:00 2017-11-21T00:00:00 46609
  6 2017-11-21T00:00:00 2017-11-30T00:00:00 46609
  7 2017-12-01T00:00:00 2017-12-31T00:00:00 46609
  8 2017-12-10T00:00:00 2018-01-10T00:00:00 41824,46609
...PASSED.

SHA256 hash of KSR:
64D35D9F6C4760022D5A0B5217FEAEC6CE76C7807CD13F10D4D7C9BA4
> draconet Apollo clockwork warranty village meagren dashboard fortiude accrus caren
n spellbind disable ames Istanbul lookup unify zilage hardwork transit meagren jawbo
ne intention kim scavenger cowbell Vegan assume Jupiter steampship informer quiver
Pandora <=
Unloaded:/opt/Keyper/PKCS11Provider/pkcs11.GC4.0.2.so.0.47 bcle=0

********** Log output in /kşrsigner-20170817-214402.log **********
[033]0;root@localhost:/media/HSM/HD0/D07/rootLocalhost HSMID=1 kşrsigner /media/KSR
16633/KRSAK30-1-D_to_D/ker-root-2017-q4-2_d_d.xml (at Thu Aug 17 21:44:02 2017 UTC)
Use KSR /opt/dnssec/asp-hmsconfig? Activate KSM prior to accepting in the affirmative!! (Y/N): y
BESM /opt/dnssec/asp-hmsconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GC4.0.2.so.0.47
Found 1 slots on BSM /opt/Keyper/PKCS11Provider/pkcs11.GC4.0.2.so.0.47
BESM slot 0 included
Loaded:/opt/Keyper/PKCS11Provider/pkcs11.GC4.0.2.so.0.47 Bcle=0

BESM Information:
  label: 1000000
  ManufacturerID: keystore Networks
  Model: 9850-2
  Serial: H140033

Validating last KSR with BESM...
  # Inception    Expiration    ZEK Tags    ZEK Tag(CKA_LABEL)
  1 2017-07-01T00:00:00 2017-07-31T00:00:00 14796,15768 19036(Kjgmt)
  2 2017-07-01T00:00:00 2017-08-01T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  3 2017-07-21T00:00:00 2017-08-11T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  4 2017-08-01T00:00:00 2017-08-31T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  5 2017-08-01T00:00:00 2017-08-31T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  6 2017-08-01T00:00:00 2017-09-01T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  7 2017-08-01T00:00:00 2017-09-01T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  8 2017-08-01T00:00:00 2017-09-01T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
  9 2017-08-01T00:00:00 2017-09-01T00:00:00 15768 20326(Klajeys)/P.19036(Kjgmt)
...PASSED.

Validating and Process KSR /media/KSR/KSK30-2-D_to_D/ker-root-2017-q4-2_d_d.xml...
  # Inception    Expiration    ZEK Tags    ZEK Tag(CKA_LABEL)
  1 2017-10-01T00:00:00 2017-10-27T00:00:00 15768,46609
  2 2017-10-11T00:00:00 2017-11-01T00:00:00 46609
  3 2017-10-21T00:00:00 2017-11-01T00:00:00 46609
  4 2017-11-01T00:00:00 2017-11-21T00:00:00 46609
  5 2017-11-11T00:00:00 2017-11-21T00:00:00 46609
  6 2017-11-21T00:00:00 2017-11-30T00:00:00 46609
  7 2017-12-01T00:00:00 2017-12-31T00:00:00 46609
  8 2017-12-10T00:00:00 2018-01-10T00:00:00 41824,46609
...PASSED.
SRA256 hash of KSR:
7F78F5A8310343C19D7ABC57501126513126E1B91C76504CB7C55
>> eightball voyager payday paperweight merit armistice adrift ultimate apple vertigo k laxon atmosphere shadow pyramid spellbound everyday indulge hesitate Athens candidate music backwater afflict performance beeswax miracle soybean Dakota drainage phonetic k

Reading KSR schedule "publish" (2016, 2017) from "kkschedule.json" # KSR Tag (CRN_LABEL):
1 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
2 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
3 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
4 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
5 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
6 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
7 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
8 19036(Kjgmt7v)/S, 20326(Kejej7y)/P
Generated new KSR in /media/KSR/KSRK30-2-D_to_D/skr-root-2017-q4-2-d_to_d.xml
# Inception Expiration KSR Tags KSR Tag (CRN_LABEL):
1 2017-01-01T00:00:00 2017-12-31T00:00:00 46809, 15768 20326(Kejej7y)/P, 19036(Kjgmt7v)
2 2017-02-01T00:00:00 2017-12-31T00:00:00 46809 20326(Kejej7y)/P, 19036(Kjgmt7v)
3 2017-03-01T00:00:00 2017-12-31T00:00:00 46809 20326(Kejej7y)/P, 19036(Kjgmt7v)
4 2017-04-01T00:00:00 2017-12-31T00:00:00 46809 20326(Kejej7y)/P, 19036(Kjgmt7v)
5 2017-05-01T00:00:00 2017-12-31T00:00:00 46809 20326(Kejej7y)/P, 19036(Kjgmt7v)
6 2017-06-01T00:00:00 2017-12-31T00:00:00 46809 20326(Kejej7y)/P, 19036(Kjgmt7v)
7 2017-07-01T00:00:00 2017-12-31T00:00:00 46809 20326(Kejej7y)/P, 19036(Kjgmt7v)
8 2017-08-01T00:00:00 2017-12-31T00:00:00 46809, 15768 20326(Kejej7y)/P, 19036(Kjgmt7v)

SRA256 hash of KSR:
7F78BFB594DAAF042C2201FC22A5F13F965A9A26E633536A41C2D1F50996CB
>> lookup axodus allingshot enlooker cranky newsletter regain Wilmington crowfoot butter rustcandied wilfington blokehead exulence eyecloth barbecue woodlark monument reform tradition rehbar waters headwater clothe conformist shadow decadence spigot scavenger vapo r a steezo prefer revival <<
Unloaded /opt/Kejey/KICX11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in /karassigner/20170817-214602.log ***********
10:33] /root@localhost:/media/KSMNT/007[root@localhost:KSMNT]# karsnl07gnr /media/KSR/KXRK09d8w3C_to_C/kxr-root-2017-q4-3-c_to_c.xml [at Thu Aug 17 21:47:56 2017 UTC]
Use KSM /opt/dnsecseap.ahimconfig?
Activate KSM prior to accepting in the affirmative!! (Y/N): y

KSM /opt/dnsecseap.ahimconfig activated.
[debug] setenv KEYER_LIBRARIES_PATH=/opt/dnsecseap

Found 1 slots on KSM /opt/Kejey/KICX11Provider/pkcs11.GCC4.0.2.so.4.07
Loadd /opt/Kejey/KICX11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

SRA256 hash of KSR:
7F78C4D4617588D43EAD091666EC2C18272D350604A0FS27E932378523A
>> eightball recipe adrift getaway Athens imperial trouble intention cowfoot congrue are zevenge undaunted Algol bodyguard fracture repellent snalepin Istanbul highchair a moonlight drubbeat hazardous dogged aggregate vapor celebrate wallet Cherokee chisel i
nuagent Dupont corrosion <<

Is this correct (Y/N)? y

Reading KSR schedule "normal(2010)" from "kkschedule.json" # KSR Tag (CRN_LABEL):
1 19036(Kjgmt7v)/S
2 19036(Kjgmt7v)/S
3 19036(Kjgmt7v)/S
4 19036(Kjgmt7v)/S
5 19036(Kjgmt7v)/S
6 19036(Kjgmt7v)/S
7 19036(Kjgmt7v)/S
8 19036(Kjgmt7v)/S
Generated new KSR in /media/KSR/KXRK09d8w3C_to_C/kxr-root-2017-q4-3-c_to_c.xml
# Inception Expiration KSR Tags KSR Tag (CRN_LABEL):
1 2017-01-01T00:00:00 2017-12-31T00:00:00 46809, 15768 19036(Kjgmt7v)/S
The output is from the `./ksrsigner` command. The logs include various error messages related to file permissions, access denied, and issues with execution permissions. The access denied errors occur multiple times throughout the log.

Here are some key points from the log:

- A user is trying to execute a script using a command-line interface.
- The script seems to be failing due to permission issues.
- The user is running the script with elevated privileges.
- The errors are related to files in the directory `/var/log`.

The log output is focused on various error messages and system calls, but it's clear that the main issue is related to permission issues that prevent the script from running successfully.
08/17/17 22:02:55

script-20170817-2.log
ttyUSB0 pp
ttyUSB0
ttyUSB0 1403033 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
ttyUSB0 1403033 011397 BBL CRC32: 0x757574CA
ttyUSB0
ttyUSB0
ttyUSB0 Running application: Bootloader at 0x8EDC0000
ttyUSB0
ttyUSB0
ttyUSB0 1403033 011403 ABL 011 : Tamper Challenge Response Key
ttyUSB0
ttyUSB0 ABL CRC32: 0x57E0FA6A
ttyUSB0
ttyUSB0
ttyUSB0 ####################################################################
ttyUSB0
ttyUSB0 ### ABL tamper records ###
ttyUSB0
ttyUSB0 ####################################################################
ttyUSB0
ttyUSB0 Current Tamper Counts (decimal 0-255):
ttyUSB0
ttyUSB0
ttyUSB0 vextosTamperCount: 0
ttyUSB0
ttyUSB0 vintrtoTamperCount: 44
ttyUSB0
ttyUSB0 wbboosTamperCount: 0
ttyUSB0
ttyUSB0 mexsttempTamperCount: 0
ttyUSB0
ttyUSB0 minsttempTamperCount: 0
ttyUSB0
ttyUSB0 meshTamperCount: 0
ttyUSB0
ttyUSB0 extampSMTTamperCount: 0
ttyUSB0
ttyUSB0 extampMKTamperCount: 0
ttyUSB0
ttyUSB0 tempdifTamperCount: 0
ttyUSB0
ttyUSB0 pfTamperCount: 44
ttyUSB0
ttyUSB0 restartTamperCount: 146
ttyUSB0
ttyUSB0
ttyUSB0 Current tamper bitsmaps:
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 currentTamper bitmap: 0x0000 0b .... .... .... ....
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  lastTamper bitmap:  0x0008 Ob .... .... 1 .... ... | EXT_POWER_DOWN
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  Bitmapped Change Record (most recent first):
2017-08-17T21:21:20+0000  ttyUSB0  --------------------------------------------------------------
2017-08-17T21:21:20+0000  ttyUSB0  Running cryptoApplication at 0xEBF00000
2017-08-17T21:21:20+0000  ttyUSB0  Jumping to startup 0 0x01037B4
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  Board is P2020RD0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  board_smp_init: 2 cpu
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  Cpu_clk=1000000000, Sys_clk=1000000000, CCE=500000000
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  System page at phys:00000000 user:00000000 kern:00000000
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  Thu Aug 17 20:39:17 2017
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0  Starting auditd v1.0 ... started.
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
2017-08-17T21:21:20+0000  ttyUSB0
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Running DES POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 DES POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Running Triple DES POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Triple DES POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Running AES POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 AES POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Running SHA1 POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 SHA1 POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Running SHA2 POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:26+0000</td>
<td>ttyUSB0 Running RandomGen POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 RandomGen POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 Running RSA POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 RSA POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 Running DSA POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 DSA POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 Running ECC POST Test</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 ECC POST Test Passed</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 Audit on 17/8/2017 20:39:28 00100000</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:27+0000</td>
<td>ttyUSB0 Keyper 9860-2 Serial Number H1403033</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0 Memory Usage:</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0 RAM (free/total) 197Mb/256Mb</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0 Flash (free/total) 127Mb/128Mb</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0</td>
</tr>
<tr>
<td>2017-08-17T21:28+0000</td>
<td>ttyUSB0 black store 472b</td>
</tr>
</tbody>
</table>
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2017-08-17 14:42+0000  ttyUSB0
2017-08-17 14:42+0000  ttyUSB0  TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
## Place HSMFD and OS DVD into the TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 19.  | CA unmounts the HSMFD by executing the following commands on the terminal window  
      cd /tmp  
      umount /media/HSMFD  
      CA removes the HSMFD, then places it on the holder. | J0       | 22:19:41 |
| 20.  | CA performs the following steps to turn off the laptop.  
      a) Turn off the laptop by pressing the power switch.  
      b) Turn on the laptop by pressing the power switch and immediately removes the OS DVD from the laptop DVD drive.  
      c) Disconnect power from the laptop. | J0       | 22:19:32 |
| 21.  | CA places (2) HSMFDs, (2) OS DVD and (1) paper with printed HSMFD hash into a prepared TEB, then seals it.  
      CA reads out the TEB #, then shows it to IW1 and participants to confirms.  
      OS DVD (release 20170403) + HSMFD: TEB# BB46584431 | J0       | 22:16:52 |
| 22.  | CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory.  
      CA places the OS DVD and HSMFD TEB on the equipment cart. | J0       | 22:16:55 |

## Distribute HSMFDs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 23.  | CA distributes the remaining HSMFDs:  
      Two for IW1 (for audit bundles)  
      Two for both RKOS (for SKR exchange with RZM and for process review) | J0       | 22:17:26 |

## Returning Laptop to TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 24.  | CA disconnects all connections to the laptop including printer, display and network, then places it into a prepared TEB, then seals it.  
      CA reads out the TEB #, then shows it to IW1 and participants to confirm.  
      Laptop1 (Dell ATG6400): TEB# BB51164625 / serial # 3724014733 | J0       | 22:18:58 |
| 25.  | CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory.  
      CA places the laptop TEB on the equipment cart. | J0       | 22:19:17 |
Return OP Card to TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>One by one, CA calls each COs listed below to the ceremony table to perform the following steps.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) CA takes OP TEB and plastic case prepared for the CO.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) CO takes his/her OP card from the cardholder and places it inside the plastic case.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) CO gives the plastic case containing the OP card to the CA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) CA places the plastic case into the prepared TEB, reads out the TEB # and description and then seals it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) CA initials the TEB with a ballpoint pen, then IW1 keeps the sealing strips for later inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) IW1 inspects the TEB, confirms the TEB # with the list below and then initials it with a ballpoint pen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) CA gives the TEB containing the OP card to the CO.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) CO inspects the TEB, verifies its content, then initials it with a ballpoint pen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) CO writes the date/time and signature on the table of IW1's script, then IW1 initials the entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>j) CO returns to his/her seat with the TEB and careful not to poke or puncture the TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>k) Repeat steps for all the remaining COs on the list.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- CO 1: Arbogast Fabian ✓  
  OP TEB # BB46584476

- CO 2: Dmitry Burkov ✓  
  OP TEB # BB46584477

- CO 5: Olafur Gudmundsson ✓  
  OP TEB # BB46584478

- CO 6: Nicolas Antoniello ✓  
  OP TEB # BB46584479

- CO 7: Subramanian Moonesamy ✓  
  OP TEB # BB46584480
<table>
<thead>
<tr>
<th>CO #</th>
<th>Card Type</th>
<th>TES #</th>
<th>Printed Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>OP 1 of 7</td>
<td>BB46584476</td>
<td>Arbogast Fabian</td>
<td></td>
</tr>
<tr>
<td>CO2</td>
<td>OP 2 of 7</td>
<td>BB46584477</td>
<td>Dmitry Burkov</td>
<td></td>
</tr>
<tr>
<td>CO3</td>
<td>OP 5 of 7</td>
<td>BB46584478</td>
<td>Öfvar Gudnundsson</td>
<td></td>
</tr>
<tr>
<td>CO4</td>
<td>OP 5 of 7</td>
<td>BB46584479</td>
<td>Nicolas Antonio</td>
<td></td>
</tr>
<tr>
<td>CO5</td>
<td>OP 6 of 7</td>
<td>BB46584480</td>
<td>Subramanian Moonesamy</td>
<td></td>
</tr>
</tbody>
</table>
## 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>27.</td>
<td>CA, IW1, SSC1 enters the safe room with the equipment cart.</td>
<td></td>
<td>22:21:58</td>
</tr>
<tr>
<td>28.</td>
<td>SSC1, while shielding the combination from the camera, opens Safe #1.</td>
<td></td>
<td>22:21:00</td>
</tr>
<tr>
<td>29.</td>
<td>SSC1 removes the safe log and writes the date/time and signature on the</td>
<td></td>
<td>22:22:00</td>
</tr>
<tr>
<td></td>
<td>safe log where the Open Safe is indicated. IW1 verifies the safe log</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>entry and then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If log entry is pre-printed, verify the entry, record time of</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>completion and sign.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30.</td>
<td>CA CAREFULLY removes the HSM TEB from the cart, reads out the TEB #</td>
<td></td>
<td>22:32:58</td>
</tr>
<tr>
<td></td>
<td>and the HSM serial #, then CAREFULLY places it inside Safe #1. CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>writes the date/time and signature on the safe log where &quot;HSM return&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is indicated. IW1 verifies the safe log entry and initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM3: TEB# BB5184623 / serial # H1403033</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31.</td>
<td>CA removes each of the following TEBs from the equipment cart; reads</td>
<td></td>
<td>22:34:16</td>
</tr>
<tr>
<td></td>
<td>out the TEB # and serial # (if applicable), then places it inside the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safe #1. CA writes the date/time and signature on the safe log where</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the returned item is indicated. IW1 verifies the safe log entry and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>initials it. Laptop1 (Dell ATG8400): TEB# BB5184625 / serial # 37240147333</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OS DVD (release 20170403) + HSMFD: TEB# BB46554481</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>32.</td>
<td>SSC1 writes the date/time and signature on the safe log where Close</td>
<td></td>
<td>22:34:41</td>
</tr>
<tr>
<td></td>
<td>Safe is indicated. IW1 verifies the safe log entry and then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33.</td>
<td>SSC1 returns the safe log back to Safe #1 and locks it (spin dial at</td>
<td></td>
<td>22:35:19</td>
</tr>
<tr>
<td></td>
<td>least two full revolutions each way, counter clock wise then clock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>wise). CA and IW1 verifies that the safe is locked and the &quot;WAIT&quot; light</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicator is off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34.</td>
<td>CA, SSC1 and IW1 leaves the safe room with the equipment cart closing</td>
<td></td>
<td>22:35:46</td>
</tr>
<tr>
<td></td>
<td>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>35.</td>
<td>CA and IW1 brings a flashlight, then escorts SSC2, COs with their OP</td>
<td></td>
<td>22:36:13</td>
</tr>
<tr>
<td></td>
<td>Card and SO Cards (if available) in TEBs into the safe room.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36.</td>
<td>SSC2, while shielding combination from the camera, opens Safe #2.</td>
<td></td>
<td>22:37:24</td>
</tr>
<tr>
<td>37.</td>
<td>SSC2 removes the safe log and writes the date/time and signature on the</td>
<td></td>
<td>22:38:01</td>
</tr>
<tr>
<td></td>
<td>safe log where Open Safe is indicated. IW1 verifies the safe log entry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If log entry is pre-printed, verify the entry, record time of</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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>
| 38.  | One by one, the selected CO returns the TEBs of OP and SO cards (as specified on the list below) by following the steps below.  
   a) CO reads out their OP card TEB # and SO card TEB # (as specified on the list) and verifies its integrity  
   b) With the assistance of the CA (and his/her common key), the CO opens his/her safe deposit box.  
   Note: Common Key is for the bottom lock. CO Key is for the top lock  
   c) CO reads out the safe deposit box number, verifies its integrity, places his/her TEBs inside it and then locks it.  
   d) CO writes the date/time and signature on the safe log that indicates return of the cards.  
   e) WV1 verifies the completed safe log entries and then initials it.  
|      | Repeat these steps until all the required cards listed below are returned. |  |  |

CO 1: Arbegast Fabian ✓  
Box # 1791  
OP TEB # BB46584476

CO 2: Dmitry Burkov ✓  
Box # 1793  
OP TEB # BB46584477

CO 5: Olafur Gudmundsson ✓  
Box # 1789  
OP TEB # BB46584478

CO 6: Nicolas Antonello ✓  
Box # 1073  
OP TEB # BB46584479

CO 7: Subramanian Moonesamy ✓  
Box # 1792  
OP TEB # BB46584480
## Close 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>Once all relevant deposit boxes are closed and locked, SSC2 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry and then initials it.</td>
<td>J0</td>
<td>22:45:37</td>
</tr>
<tr>
<td>40.</td>
<td>SSC2 returns the safe log back to Safe #2 and then locks it (spin dial must go at least two full revolutions each way, counter clock-wise then clock-wise). CA and IW1 verifies that the safe is locked and the “WAIT” light indicator is off.</td>
<td>J0</td>
<td>22:56:20</td>
</tr>
<tr>
<td>41.</td>
<td>CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.</td>
<td>J0</td>
<td>22:44:20</td>
</tr>
</tbody>
</table>

## Participant Signing of IW1’s Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.</td>
<td>CA reads the exceptions that may have occurred during the ceremony.</td>
<td>J0</td>
<td>22:44:20</td>
</tr>
<tr>
<td>43.</td>
<td>CA calls each attendee on the participants list to proceed to the ceremony table to confirm their printed name and date. Each attendee will sign IW1's participants list declaring that this script is a true and accurate record of the ceremony. IW1 records the completion time once all participants have signed the participants list.</td>
<td>J0</td>
<td>22:51:09</td>
</tr>
<tr>
<td>44.</td>
<td>CA reviews IW1’s script and signs the participants list.</td>
<td>J0</td>
<td>22:52:20</td>
</tr>
</tbody>
</table>

## Stop Online Streaming

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td>CA acknowledges the participation of the online participants and then notifies the SA to stop the online streaming.</td>
<td>J0</td>
<td>22:53:50</td>
</tr>
</tbody>
</table>

## Post Ceremony Information

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td>CA informs onsite participants about post ceremony activities.</td>
<td>J0</td>
<td>23:58:00</td>
</tr>
</tbody>
</table>

## Sign Out of Ceremony Room and Stop Video Recording

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.</td>
<td>RKOS ensures that all participants sign out of the Ceremony Room log and are then escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.</td>
<td>J0</td>
<td>23:09:30</td>
</tr>
<tr>
<td>48.</td>
<td>CA notifies the SA to stop video recording.</td>
<td>J0</td>
<td>23:05:01</td>
</tr>
</tbody>
</table>
## Bundle Audit Materials

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.</td>
<td>IW1 makes (1) copy of his/her script for off-site audit bundle. Each Audit bundle contains: 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 System and Intrusion Detection System (Range is 02/02/2017 – 08/17/2017) e) IW1 attestation (Section A.1) f) SA attestation (Sections A.2 and A.3) All TEBs are labeled “Root DNSSEC KSK Ceremony 30”, dated and signed by IW1 and CA. An off-site audit bundle is delivered to an off-site storage. The CA holds the ultimate responsibility to finalize the audit bundle collection.</td>
<td></td>
<td>2017/03/19 60:17:00</td>
</tr>
</tbody>
</table>

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 bundle is placed inside a tamper-evident bag that is labeled, dated and signed by the CA and the IW1.

2. **Key Ceremony Scripts (IW1)**
   Hard copies of the IW1’s key ceremony scripts, including the IW1’s notes and the IW1’s attestation. See Appendix A.1.

3. **Audio-visual recordings from the key ceremony (SA1)**
   One set is for the original audit bundle and the other as a duplicate.

4. **Logs from the Physical Access Control System (PACS) and Intrusion Detection System (IDS) (SA1)**
   One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PACS and IDS configuration review, the list of enrolled users, the event log and configuration audit log files are contained in each audit bundle. Each audit bundle is placed in a tamper-evident bag that is labeled, dated and signed by the SA1 and the IW1.

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

5. **Configuration review of the Physical Access Control System and Intrusion Detection System (SA1)**
   SA1’s attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix A.2.

6. **Configuration review of the Firewall System (SA1)**
   SA1’s attestation and hard copies of the firewall configuration from the review process. See Appendix A.3. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. **Other Items**
   If applicable.
A.1 Key Ceremony Script (by IW1)

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

Jonathan Denison

Date: 18 August 2017
A.2 Access Control System Configuration Review (by SA1)

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

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

Enclosed is also an electronic copy of the event log from the access control system ranging from the last log extraction on 2 February 2017 00:00 UTC to now.

Connor Barthold

Date: 19 August 2017
A.3 Firewall Configuration Review (by SA1)

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

Enclosed is the configuration extract from the firewall unit.

Connor Barthold

Date: 17 August 2017
cbarnhold@srp> show configuration | no-more
Last commit: 2017-01-12 22:30:47 UTC by jenkins
version 12.3.0.6-055.3;

system {
  host-name srp;
  domain-name kst.lax.dent.icsan.org;
  location {
    country-code US;
    postal-code 90245;
    building Equalink (A3);
    floor 1;
    rack 1;
  }
  ports {
    console {
      log-out-on-disconnect;
      type vt100;
    }
  }
  root-authentication {
    encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; # SECRET-DATA
  }
  name-server {
    8.8.8.8;
    8.8.4.4;
  }
  login {
    user lbarnold {
      full-name "Brian Barnold";
      uid 2006;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; # SECRET-DATA
      }
    }
    user dbarnhold {
      full-name "Don Barnold";
      uid 2004;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; # SECRET-DATA
      }
    }
    user jenkins {
      full-name "Josh Jenkins";
      uid 2007;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; # SECRET-DATA
      }
    }
    user rqullen {
      full-name "Bob Qullen";
      uid 2009;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; # SECRET-DATA
      }
    }
  }
  services {
    ssh {
      root-login deny;
    }
    netconf {
      ssh;
    }
  }
  syslog {
    archive size 100k files 3;
    user *
      any emergency;
    file messages
      any critical;
      authorization info;
    file interactive-commands
      interactive-commands error;
  }
  max-configurations-on-flash 5;
  max-configuration-rollback 20;
  license {
    autoupdate {
      url https://an1.jupiter.net/junos/key_retrieve;
    }
  }
}
chassis {
  config-button no-rescue no-clear;
}

interfaces {
  interface-range access {
    member-range ge-0/0/0 to ge-0/0/8;
    unit 0 {
      family ethernet-switching {
        vlan {
          members vlan-access;
        }
      }
    }
  }
  interface-range video {
    member-range ge-0/0/9 to ge-0/0/12;
    unit 0 {
      family ethernet-switching {
        vlan {
          members vlan-video;
        }
      }
    }
  }
  interface-range wifi {
    member ge-0/0/13;
    unit 0 {
      family inet {
        address 10.100.1.1/24;
      }
    }
  }
  interface-range guest {
    member ge-0/0/14;
    member ge-0/0/15;
    unit 0 {
      family ethernet-switching {
        vlan {
          members vlan-guest;
        }
      }
    }
  }
}

ge-0/0/0 {
  description "Access Control Server";
}

ge-0/0/1 {
  description "Access Control Client Custom Solution";
}

ge-0/0/2 {
  description "Intrusion Detection Panel";
}

ge-0/0/3 {
  description "Environment Monitoring";
}

ge-0/0/4 {
  description "Monitoring Server";
}

ge-0/0/5 {
  description "IRIS Enrollment";
}

ge-0/0/6 {
  description "Iris Scanner T2";
  /* Not available at KMF-West */
  disable;
}

ge-0/0/7 {
  description "Iris Scanner T3";
}

ge-0/0/8 {
  description "Iris Scanner T4";
}

ge-0/0/9 {
  description "Video Surveillance Server";
}

ge-0/0/10 {
  description "Camera 1";
}

ge-0/0/11 {
  description "Camera 2";
}

ge-0/0/12 {
  description "Camera 3";
ge-0/0/13 {
    description "WiFi Connection";
}
ge-0/0/14 {
    description "Streaming Laptop";
}
ge-0/0/15 {
    description "Audio Camera Client";
}
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.35.201/26;
        }
    }
    led {
        unit 0 {
            family inet {
                filter {
                    input route-engine-filter;
                }
            }
        }
    }
}
eth {
    unit 1 {
        description "IPSec KMF-West";
    }
}
vlan {
    unit 0 {
        family inet {
            address 10.4.28.193/26;
        }
    }
    unit 1 {
        family inet {
            address 10.4.28.129/26;
        }
    }
    unit 2 {
        family inet {
            address 10.4.28.1/25;
        }
    }
}
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.0.35.201;
        route 10.4.28.0/24 next-hop 10.4.28.1;
        route 192.168.1.148/32 next-hop 192.0.35.201;
    }
}
policy-options {
    prefix-list resolver-servers {
        8.8.8.4/32;
        8.8.4.8/32;
    }
    prefix-list local-prefixes {
        10.4.28.0/24;
    }
    prefix-list ntp-servers {
        129.6.15.28/32;
        129.6.15.29/32;
    }
}
security {
    ike {
        policy ike-policyKMF {
            pre-shared-key ascii-text "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
        }
    }
    gateway gateway-to-KMF-East {
        like-policy ike-policyKMF;
        address 152.194.1.148;
        external-interface ge-1/0/0;
    }
}
ipseckm {
    proposal IPSecProposal {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
policy defaultPolicy {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSecProposal;
}

vpn vpn-to-KMF-East {
    blind-interface std.1;
    key {
        gateway Gateway-to-KMF-East;
        peer policy defaultPolicy;
    }
    establish tunnels immediately;
}

screen {
    id-option external-screen {
        icmp {
            ping-death;
        }
        wr {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
    }
    nat {
        rule-set internal-to-external {
            from zone [ access guest wif ];
            to zone untrust;
            rule source-nat-rule {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat { interface; }
                }
            }
        }
    }
}
policies {
    from-zone access to-zone untrust {
        policy allow-mail {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address /can;
                application junos smtp;
            }
            then {
                permit;
                log [ session-close; ]
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address [ lcam-dns google-dns ];
                application [ junos-dns-udp junos-dns-tcp ];
            }
            then {
                permit;
                log [ session-close; ]
            }
        }
        policy allow-simplex {
            match {
                source-address iDP;
                destination-address simplex;
                application any;
            }
        }
    }
}
then
    permit;
log { session-close; }
}
}
)
from-zone access to-zone video {
policy access-to-video {
    match {
        source-address NMS;
destination-address kmf_west_video;
        application junos-icmp-all;
    }
    then {
        permit;
    }
}
)
from-zone access to-zone ipsec {
policy allow-access-to-ipsec {
    match {
        source-address ACS ACC;
destination-address [ kmf_west_acs kmf_east_acs ];
        application any;
    }
    then {
        permit;
        log {
            session-close;
        }
    }
}
)
policy allow-icmp {
    match {
        source-address any;
destination-address any;
        application junos-icmp-ping;
    }
    then {
        permit;
    }
}
)
policy allow-access-access {
    match {
        source-address kmf_west_access;
destination-address kmf_east_access;
        application any;
    }
    then {
        permit;
    }
}
)
from-zone ipsec to-zone access {
policy allow-ipsec-to-access {
    match {
        source-address [ kmf_east_acs kmf_east_acs ];
destination-address [ ACS ACC ];
        application any;
    }
    then {
        permit;
        log {
            session-close;
        }
    }
}
)
policy allow-icmp {
    match {
        source-address any;
destination-address any;
        application junos-icmp-ping;
    }
    then {
        permit;
    }
}
)
policy allow-access-access {
    match {
        source-address kmf_east_access;
destination-address kmf_west_access;
        application any;
    }
    then {
        permit;
    }
}
)
from zone video to zone ipsec {
    policy allow video to ipsec {
        match {
            source-address vss;
            destination-address knf east vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
}

deploy policy allow access video {
    policy allow access video {
        match {
            source-address knf west vss;
            destination-address knf east vss;
            application any;
        }
        then {
            permit;
        }
    }
}

from zone guest to zone untrust {
    policy allow guest to untrust {
        match {
            source-address knf west guest;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

from zone wifi to zone untrust {
    policy allow wifi to untrust {
        match {
            source-address knf west wifi;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

from zone ipsec to zone video {
    policy allow ipsec to video {
        match {
            source-address knf east vss;
            destination-address vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
}

policy allow tcp {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

policy allow access video {
    match {
        source-address knf east vss;
        destination-address knf west vss;
        application any;
    }
    then {
        permit;
    }
}

from zone guest to zone access {
    policy allow access {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
then {
  permit;
}

from-zone video to-zone video {
  policy allow-ntp {
    match {
      source-address any;
      destination-address video-ntp-server;
      application [nport-ntp];
    }
    then {
      permit;
    }
  }
}

default policy {
  deny-all;
}

zones {
  security-zone access {
    address-book {
      address ACS 10.4.28.203/32;
      address ACC 10.4.28.202/32;
      address IP 10.4.28.201/32;
      address EVM 10.4.28.200/32;
      address IVS 10.4.28.204/32;
      address E1 10.4.28.210/32;
      address E3 10.4.28.212/32;
      address E4 10.4.28.213/32;
      address kmf_west_access 10.4.28.192/26;
      address localnet 10.4.28.0/24;
      address-set lhrscanners {
        address E1;
        address E3;
        address E4;
      }
    }
    interfaces {
      wlan.0 {
        host-inbound-traffic {
          system-services {
            ping;
            ntp;
          }
        }
      }
    }
  }
  security-zone untrust {
    address-book {
      address Icann 192.0.32.0/20;
      address icann-dns 192.0.32.53/32;
      address google-dns1 8.8.8.8/32;
      address google-dns2 8.8.4.4/32;
      address simplex1 216.224.218.31/32;
      address simplex2 216.224.218.32/32;
      address simplex3 216.224.218.33/32;
      address simplex4 216.224.218.34/32;
      address-set google-dns {
        address google-dns1;
        address google-dns2;
      }
      address-set simplex {
        address simplex1;
        address simplex2;
        address simplex3;
        address simplex4;
      }
    }
    screen external-screen;
    interfaces {
      ge-1/0/0.0 {
        host-inbound-traffic {
          system-services {
            ping;
            ssh;
          }
        }
      }
    }
  }
  security-zone video {
    address-book {
      address kmf_west_video 10.4.28.128/26;
      address VSS 10.4.28.150/32;
      address C1 10.4.28.151/32;
    }
address C2 10.4.28.152/32;
adress C3 10.4.28.153/32;
address video-nip-server 10.28.4.129/32;
address-set cameras {
  address C1;
  address C2;
  address C3;
}
}
interfaces {
  vlan.1 {
    host-inbound-traffic {
      system-services {
        ping;
      }
    }
  }
}
security-zone guest {
  address-book {
    address STR 10.4.28.26/32;
    address VCC 10.4.28.32/32;
    address kmf_west_guest 10.4.28.0/25;
  }
  interfaces {
    vlan.2 {
      host-inbound-traffic {
        system-services {
        }
      }
    }
  }
}
security-zone ipsec {
  address-book {
    address kmf_east_access 10.4.28.192/26;
    address kmf_east_video 10.4.29.128/26;
    address kmf_east_ces 10.4.29.204/32;
    address kmf_east_acc 10.4.29.202/32;
    address kmf_east_xip 10.4.29.201/32;
    address kmf_east_cvx 10.4.29.200/32;
    address kmf_east_div 10.4.29.203/32;
    address kmf_east_c2 10.4.29.210/32;
    address kmf_east_c2 10.4.29.211/32;
    address kmf_east_c3 10.4.29.212/32;
    address kmf_east_f4 10.4.29.213/32;
    address kmf_east_yss 10.4.29.150/32;
    address kmf_east_c1 10.4.29.151/32;
    address kmf_east_C2 10.4.29.152/32;
    address kmf_east_C3 10.4.29.153/32;
  }
  interfaces {
    st0.1 {
      host-inbound-traffic {
        system-services {
          ping;
          live;
          ssh;
        }
      }
    }
  }
}
security-zone wifi {
  address-book {
    address kmf_west_wifi 10.100.1.0/24;
  }
  interfaces {
    go-O/3/13.0 {
      host-inbound-traffic {
        system-services {
        }
      }
    }
  }
}
firewall {
  family inet {
    filter route-engine-filter {
      term deny-icmp-redirects {
        from {
          protocol icmp;
          icmp-type redirect;
        }
        then {
        }
      }
    }
  }
}
discard;

} } term allow-icmp {
from {
protocol icmp;
icmp-type [ echo-request echo-reply unreachable time-exceede
d ];
} then {
policer small-bw-limit;
accept;
}
} term allow-traceroute {
from {
protocol udp;
port 33434-33534;
} then {
policer small-bw-limit;
accept;
}
} term allow-dns {
from {
source-prefix-list {
resover-servers;
} protocol udp;
source-port domain;
} then {
policer small-bw-limit;
accept;
}
} term allow-ntp {
from {
source-prefix-list {
local-prefixes;
nip-servers;
} protocol udp;
port ntp;
} then {
policer small-bw-limit;
accept;
}
} term allow-establish {
from {
protocol tcp;
tcp-established;
} then accept;
} term allow-ipssec-esp {
from {
protocol esp;
} then accept;
} term allow-ipssec-udp {
from {
protocol udp;
port 500;
} then accept;
} term allow-ssh {
from {
source-address {
192.168.1.0/24;
10.4.20.0/24;
10.4.28.0/24;
} protocol tcp;
destination-port ssh;
} then accept;
} term LAST {
then {
discard;
}
}
policer small-bw-limit {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
poe {
    Interface all;
}
vlans {
    vlan-access {
        vlan-id 3;
        13-interface vlan.0;
    }
    vlan-guest {
        vlan-id 5;
        13-interface vlan.2;
    }
    vlan-video {
        vlan-id 4;
        13-interface vlan.1;
    }
}