Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 12
Tuesday February 12, 2013

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

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

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEB</td>
<td>Tamper Evident Eag (AMPAC, Item #GCS1013 small or #GCS1216 large or MMF Industries, Item #2362010N20 small or #2362011N20 large)</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>IW</td>
<td>Internal Witness</td>
</tr>
<tr>
<td>SSC</td>
<td>Safe Security Commander</td>
</tr>
<tr>
<td>KSR</td>
<td>Key Signing Request</td>
</tr>
<tr>
<td>FD</td>
<td>Flash Drive</td>
</tr>
<tr>
<td>CA</td>
<td>Ceremony Administrator</td>
</tr>
<tr>
<td>CO</td>
<td>Crypto Officer</td>
</tr>
<tr>
<td>SA</td>
<td>System Administrator</td>
</tr>
<tr>
<td>MC</td>
<td>Master of Ceremony</td>
</tr>
<tr>
<td>IKOS</td>
<td>ICANN KSK Operations Security</td>
</tr>
<tr>
<td>SKR</td>
<td>Signed Key Response</td>
</tr>
<tr>
<td>RZM</td>
<td>Root Zone Maintainer</td>
</tr>
</tbody>
</table>

**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/Citizenship</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Mehmet Akcin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW1</td>
<td>Francisco Arias</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA1</td>
<td>Alexander Kulik</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC1</td>
<td>Selina Harrington</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC2</td>
<td>Geoff Bickers, Leo Vayoda</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA2</td>
<td>Matt Childs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO1</td>
<td>Masato Mnda / JP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO2</td>
<td>Dmitry Burkov / RU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO3</td>
<td>Joao Darras / PT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO5</td>
<td>Edward Lewis / US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO7</td>
<td>Subramanian Moonesamy / MU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW1</td>
<td>Alejandro Bolivar / VeriSign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW2</td>
<td>Cheryan Huang / PricewaterhouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW3</td>
<td>Exavier Ciabata / PricewaterhouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW4</td>
<td>Chris Griffiths / Comcast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW5</td>
<td>Martin Levy / Hurricane Electric</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW6</td>
<td>Dalini Khemlani / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA2</td>
<td>Richard Lamb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW2/KOS</td>
<td>Tomofumi Okubo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA3</td>
<td>Brian Marin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locksmith</td>
<td>Mike Jacobs / Industrial Lock and Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW3</td>
<td>Kim Davies</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Not present FA*

12 February 2013 01:09
Note: Dual Occupancy enforced. CA leads ceremony. Only CAS, IWs, or SAs can enter ceremony room and/or escort other participants. Only CA+IW can enter safe room and/or escort other participants. CAS, SAs or IWs may let individuals out of the ceremony room but only when CA+IW remain in the ceremony room. No one may leave when CA+IW are in safe room. Participants must sign in and out of ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before completion of the ceremony. The SA starts filming before the participants enter the room.

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

<table>
<thead>
<tr>
<th>Letter</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alfa</td>
</tr>
<tr>
<td>B</td>
<td>Bravo</td>
</tr>
<tr>
<td>C</td>
<td>Charlie</td>
</tr>
<tr>
<td>D</td>
<td>Delta</td>
</tr>
<tr>
<td>E</td>
<td>Echo</td>
</tr>
<tr>
<td>F</td>
<td>Foxtrot</td>
</tr>
<tr>
<td>G</td>
<td>Golf</td>
</tr>
<tr>
<td>H</td>
<td>Hotel</td>
</tr>
<tr>
<td>I</td>
<td>India</td>
</tr>
<tr>
<td>J</td>
<td>Juliet</td>
</tr>
<tr>
<td>K</td>
<td>Kilo</td>
</tr>
<tr>
<td>L</td>
<td>Lima</td>
</tr>
<tr>
<td>M</td>
<td>Mike</td>
</tr>
<tr>
<td>N</td>
<td>November</td>
</tr>
<tr>
<td>O</td>
<td>Oscar</td>
</tr>
<tr>
<td>P</td>
<td>Papa</td>
</tr>
<tr>
<td>Q</td>
<td>Quebec</td>
</tr>
<tr>
<td>R</td>
<td>Romeo</td>
</tr>
<tr>
<td>S</td>
<td>Sierra</td>
</tr>
<tr>
<td>T</td>
<td>Tango</td>
</tr>
<tr>
<td>U</td>
<td>Uniform</td>
</tr>
<tr>
<td>V</td>
<td>Victor</td>
</tr>
<tr>
<td>W</td>
<td>Whiskey</td>
</tr>
<tr>
<td>X</td>
<td>Xray</td>
</tr>
<tr>
<td>Y</td>
<td>Yankee</td>
</tr>
<tr>
<td>Z</td>
<td>Zulu</td>
</tr>
<tr>
<td>0</td>
<td>Zero</td>
</tr>
<tr>
<td>1</td>
<td>One</td>
</tr>
<tr>
<td>2</td>
<td>Two</td>
</tr>
<tr>
<td>3</td>
<td>Three</td>
</tr>
<tr>
<td>4</td>
<td>Four</td>
</tr>
<tr>
<td>5</td>
<td>Five</td>
</tr>
<tr>
<td>6</td>
<td>Six</td>
</tr>
<tr>
<td>7</td>
<td>Seven</td>
</tr>
<tr>
<td>8</td>
<td>Eight</td>
</tr>
<tr>
<td>9</td>
<td>Nine</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL-FAH</td>
</tr>
<tr>
<td>BRAH-VOH</td>
</tr>
<tr>
<td>CHAR-LEE</td>
</tr>
<tr>
<td>DELL-TAH</td>
</tr>
<tr>
<td>ECK-OH</td>
</tr>
<tr>
<td>FOKS-TROT</td>
</tr>
<tr>
<td>GOLF</td>
</tr>
<tr>
<td>HOH-TEL</td>
</tr>
<tr>
<td>IN-DEE-AH</td>
</tr>
<tr>
<td>JEW-LEE-ETT</td>
</tr>
<tr>
<td>KEY-LOH</td>
</tr>
<tr>
<td>LEE-MAH</td>
</tr>
<tr>
<td>MIKE</td>
</tr>
<tr>
<td>NO-VEM-BER</td>
</tr>
<tr>
<td>OSS-CAH</td>
</tr>
<tr>
<td>PAH-PAH</td>
</tr>
<tr>
<td>KEH-BECK</td>
</tr>
<tr>
<td>ROW-ME-OH</td>
</tr>
<tr>
<td>SEE-AR-RAH</td>
</tr>
<tr>
<td>TANG-GO</td>
</tr>
<tr>
<td>YOU-NEE-FORM</td>
</tr>
<tr>
<td>VIK-TAH</td>
</tr>
<tr>
<td>WISS-KEY</td>
</tr>
<tr>
<td>ECKS-RAY</td>
</tr>
<tr>
<td>YANG-KEY</td>
</tr>
<tr>
<td>ZOO-LOO</td>
</tr>
<tr>
<td>WUN</td>
</tr>
<tr>
<td>TOO</td>
</tr>
<tr>
<td>TREE</td>
</tr>
<tr>
<td>FOW-ER</td>
</tr>
<tr>
<td>FIFE</td>
</tr>
<tr>
<td>SIX</td>
</tr>
<tr>
<td>SEV-EN</td>
</tr>
<tr>
<td>AIT</td>
</tr>
<tr>
<td>NIN-ER</td>
</tr>
<tr>
<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>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SA starts video recording and online streaming. SAs or IWs escort participants into the Ceremony Room and all participant sign into the Ceremony Room log.</td>
<td>FA</td>
<td>21:04</td>
</tr>
</tbody>
</table>

**Emergency Evacuation Procedures**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>CA or IW reviews emergency evacuation procedures with participants.</td>
<td>FA</td>
<td>21:04</td>
</tr>
</tbody>
</table>

**Verify Time and Date**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room: Date and time: <strong>12 February 2013 21:04</strong></td>
<td>FA</td>
<td>21:04</td>
</tr>
</tbody>
</table>

All entries into this script or any logs should follow this common source of time.

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>CA and IW1 escort SSC2, COs and locksmith into the safe room together. CA brings a flashlight when entering the safe room.</td>
<td>FA</td>
<td>21:05</td>
</tr>
<tr>
<td>5.</td>
<td>SSC2, while shielding combination from camera, opens Safe #2.</td>
<td>FA</td>
<td>21:04</td>
</tr>
<tr>
<td>6.</td>
<td>SSC2 takes out safe log and prints name, date, time, signature, and reason (i.e. &quot;open safe&quot;) in safe log. IW1 initials this entry.</td>
<td>FA</td>
<td>21:08</td>
</tr>
<tr>
<td></td>
<td>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**COs extract OP Cards from safe deposit boxes**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>One by one, the selected COs checks the SO cards and retrieves the OP cards following the steps shown below.</td>
</tr>
<tr>
<td></td>
<td>a) With the assistance of CA (and his/her common key), opens her/his safe deposit box.</td>
</tr>
<tr>
<td></td>
<td>b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below.</td>
</tr>
<tr>
<td></td>
<td>c) Returns SO cards, retains OP TEB and locks box.</td>
</tr>
<tr>
<td></td>
<td>d) Makes an entry in safe log indicating verification of integrity of contents and OP TEB removal with box #, printed name, date, time and signature.</td>
</tr>
</tbody>
</table>

**Note:** If log entry is pre-printed, verify the entry, record time of completion and sign.

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

**CO 1:** Masato Minda  
Box # 1788  
OP TEB # BB21369028  
SO TEB # A13004340

**CO 2:** Dmitry Burkov  
Box # 1793  
OP TEB # A'4365424  
SO TEB # A'3004336

**CO 3:** João Damás  
Box # 1071  
OP TEB # BB21369030  
SO TEB # A13004343

**CO 5:** Edward Lewis  
Box # 1790  
OP TEB # A14365388  
SO TEB # A13004326

**CO 7:** Subramanian-Mooresamy  
Box # 1792  
OP TEB # B324369033  
SO TEB # A16608558

FA 21:18
### Remove out-of-order Safe Deposit Box Locks

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>CA confirms that the boxes below are currently not in use then the locksmith removes the malfunctioning dual nose Mosler locks from the safe deposit box. The box that needs replacement is as below. Box 1070 Box 1789</td>
<td>FA</td>
<td>21:25</td>
</tr>
</tbody>
</table>

### Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Once all safe deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>21:27</td>
</tr>
<tr>
<td>10.</td>
<td>SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and card reader indicator is green.</td>
<td>FA</td>
<td>21:27</td>
</tr>
<tr>
<td>11.</td>
<td>IW1, CA, SSC2, and COs leave safe room, with OP cards in TEBs, closing the door behind them.</td>
<td>FA</td>
<td>21:28</td>
</tr>
<tr>
<td>12.</td>
<td>SA escorts the locksmith out of the key management facility</td>
<td>FA</td>
<td>21:30</td>
</tr>
</tbody>
</table>

### Open Equipment Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.</td>
<td>FA</td>
<td>21:31</td>
</tr>
<tr>
<td>14.</td>
<td>SSC1, while shielding combination from camera, opens Safe #1.</td>
<td>FA</td>
<td>21:32</td>
</tr>
<tr>
<td>15.</td>
<td>SSC1 takes cut safe log and prints name, date, time, signature and reason (i.e., &quot;opened safe&quot;) in safe log. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>21:33</td>
</tr>
</tbody>
</table>

### Remove Equipment from Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.</td>
<td>CA CAREFULLY removes HSM1 (in TEB) from the safe and completes the entry in the safe log indicating &quot;HSM1 Removal,&quot; TEB # and serial number, printed name date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry. HSM1: TEB# A2826760 / serial # K6002020 Verify the integrity of the other HSM that will not be in used this time. HSM2: TEB# BB24049957 / serial # K6002018 (last used)</td>
<td>F/T</td>
<td>21:35</td>
</tr>
</tbody>
</table>
### ICANN Root DNSSEC KSK Ceremony 12

#### Step 17

<table>
<thead>
<tr>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA takes out the items listed below from the safe and completes the entry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in the safe log indicating each item, TEB#, serial number if available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printed name, date, time and signature. CA places the item on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>equipment cart. IW1 initials this entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laptop1 (Dell ATG6400): TEB# BB24049956 / serial# 37240147333</td>
<td>FA</td>
<td>21:37</td>
</tr>
<tr>
<td>O/S DVD (Rev600) + HSMFD: TEB# BB21369041</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify the integrity of the other Laptop that will not be used this time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laptop2: TEB# A2734916 / serial # 7292928457</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td>SSC1 makes an entry including printed name, date, time and signature</td>
<td>FA</td>
<td>21:38</td>
</tr>
<tr>
<td></td>
<td>in the safe log indicating, “Close safe”. IW1 initials this entry.</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>19.</td>
<td>SSC1 puts log back in safe and locks Safe #1 (spin dial at least two</td>
<td>FA</td>
<td>21:38</td>
</tr>
<tr>
<td></td>
<td>full revolutions each way, counter clock wise then clock wise).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA and IW1 verify that the safe is locked and door indicator light is</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>green.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the</td>
<td>FA</td>
<td>21:39</td>
</tr>
<tr>
<td></td>
<td>door to the safe room securely behind them.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Act 2. Confirm and Sign the Key Signing Request

## Set Up Laptop

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. Laptop1 (Dell ATG6400); TEB# BB24049956 / serial# 37240147333</td>
<td>FA</td>
<td>21:43</td>
</tr>
<tr>
<td>2.</td>
<td>CA inspects the OS DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. OS DVD (Rev600) + HSMFD: TEB# BB21369041</td>
<td>FA</td>
<td>21:44</td>
</tr>
<tr>
<td>3.</td>
<td>CA takes the laptop out of TEB placing it on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from OS DVD.</td>
<td>FA</td>
<td>21:47</td>
</tr>
<tr>
<td>4.</td>
<td>CA presses &quot;CTRL+ALT+F2&quot; to get a console prompt and logs in as root.</td>
<td>FA</td>
<td>21:49</td>
</tr>
<tr>
<td>5.</td>
<td>CA enters the commands <code>system-config-display --noui</code> and <code>killall Xorg</code> CA ensures that external display works.</td>
<td>FA</td>
<td>21:52</td>
</tr>
<tr>
<td>6.</td>
<td>CA logs in as 'root'.</td>
<td>FA</td>
<td>21:52</td>
</tr>
<tr>
<td>7.</td>
<td>CA configures printer as default and prints test page by going to System &gt; Administration &gt; Printing.</td>
<td>FA</td>
<td>21:54</td>
</tr>
<tr>
<td>8.</td>
<td>CA opens a terminal window and maximizes its size for visibility by going to Applications &gt; Accessories &gt; Terminal.</td>
<td>FA</td>
<td>21:55</td>
</tr>
<tr>
<td>9.</td>
<td>CA checks and fixes date and time on laptop based on wall clock ensuring UTC time zone has been chosen by going to System &gt; Administration &gt; Date and Time.</td>
<td>FA</td>
<td>21:56</td>
</tr>
<tr>
<td>10.</td>
<td>CA inserts USB port expander into laptop.</td>
<td>FA</td>
<td>21:56</td>
</tr>
</tbody>
</table>
### Format and label blank FD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system window and formats the drive by executing `dmesg</td>
<td>grep -A 5 usb-storage<code>&lt;br&gt;to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc),&lt;br&gt;</code>umount /dev/sdal<code>&lt;br&gt;to unmounts the drive (change drive letter if necessary),&lt;br&gt;</code>mkfs.vfat -n HSMFD -I /dev/sda`&lt;br&gt;to execute a FAT32 format and label it as HSMFD.</td>
<td>FA</td>
</tr>
<tr>
<td>12.</td>
<td>CA repeats step 29 for the 2nd blank FD</td>
<td>FA</td>
<td>21:59</td>
</tr>
<tr>
<td>13.</td>
<td>CA repeats step 29 for the 3rd blank FD</td>
<td>FA</td>
<td>22:00</td>
</tr>
<tr>
<td>14.</td>
<td>CA repeats step 29 for the 4th blank FD</td>
<td>FA</td>
<td>22:00</td>
</tr>
<tr>
<td>15.</td>
<td>CA repeats step 29 for the 5th blank FD</td>
<td>FA</td>
<td>22:00</td>
</tr>
</tbody>
</table>

### Connect HSMFD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.</td>
<td>CA plugs HSMFD into free USB slot on the laptop -NOT EXPANDER- and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD than closes the file system window.</td>
<td>FA</td>
<td>22:01</td>
</tr>
</tbody>
</table>

### Start Logging Terminal Session

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code></td>
<td>FA</td>
<td>22:02</td>
</tr>
<tr>
<td>18.</td>
<td>CA executes <code>script script-20130212.log</code>&lt;br&gt;to start a capture of terminal output.</td>
<td>FA</td>
<td>22:03</td>
</tr>
</tbody>
</table>

### Start Logging HSM Output

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>CA connects a serial to USB null modem cable to laptop.</td>
<td>FA</td>
<td>22:01</td>
</tr>
<tr>
<td>20.</td>
<td>CA opens a second terminal screen and executes <code>cd /media/HSMFD</code>&lt;br&gt;and executes <code>ttyaudit /dev/ttyUSB0</code>&lt;br&gt;to start logging HSM serial port outputs. Note: DO NOT unplug USB serial port from laptop as this causes logging to stop.</td>
<td>FA</td>
<td>22:05</td>
</tr>
</tbody>
</table>
### Power Up HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. HSM1: TEB# A2828760 / serial # K6002020</td>
<td>FA</td>
<td>22:07</td>
</tr>
<tr>
<td>22.</td>
<td>CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.</td>
<td>FA</td>
<td>22:07</td>
</tr>
<tr>
<td>23.</td>
<td>CA switches to the tyaudit terminal window and connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSV serial number with above. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it since the scripts that does the logging to the laptop adds a timestamp.)</td>
<td>FA</td>
<td>22:09</td>
</tr>
</tbody>
</table>

### Enable/Activate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td>CA calls a CO, CO opens TEB with OP card and hands to CA who places card in cardholder visible to all.</td>
<td>FA</td>
<td>22:13</td>
</tr>
<tr>
<td>25.</td>
<td>Repeat the step above until all OP cards are placed on the cardholder.</td>
<td>FA</td>
<td>22:14</td>
</tr>
<tr>
<td>26.</td>
<td>CA inserts 3 cards into HSM to activate the unit (via “Set Online” menu item). Type in the default PIN “11223344” when prompted. IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card of 7 2nd OP card of 7 3rd OP card of 7</td>
<td>FA</td>
<td>22:17</td>
</tr>
</tbody>
</table>

### Check Network between Laptop and HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.</td>
<td>CA connects HSM to laptop using Ethernet cable.</td>
<td>FA</td>
<td>22:17</td>
</tr>
<tr>
<td>28.</td>
<td>CA tests network connectivity between laptop and HSM by entering <code>ping 192.160.0.2</code> on the laptop terminal window and looking for responses. Ctrl-C to exit program.</td>
<td>FA</td>
<td>22:18</td>
</tr>
</tbody>
</table>
February 1st, 2013

To Whom It May Concern:

This is a letter of Verification of Employment for Alejandro A. Bollivar. Verisign, Inc. has employed Alejandro A. Bollivar full-time since September 8th, 1997 as a Senior Engineer in our Info Services/Corporate Naming Resolution Operations department.

Verisign is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day our identity protection and registry services allow companies and consumers all over the world to engage in trusted communications and commerce.

For over 10 years, Verisign Internet infrastructure has been at the very heart of the Internet, enabling key transactions and protecting valuable data. Verisign facilitates as many as 31 billion authoritative Domain Name System (DNS) queries a day, and has been providing this service since 1998 with 100% availability. Over the years the Verisign Internet infrastructure has scaled quickly and dramatically, and has the capacity to scale just as dramatically in the coming years, as the world moves to Internet-based transactions. Verisign’s Network Intelligence and Availability team helps protect against distributed denial of service or DDoS attacks through an in-the-cloud monitoring and mitigation services. Verisign’s iDefense Security Intelligence Services help identify and track vulnerabilities, malicious code, threats, and helps provide comprehensive intelligence to enable customers to proactively manage risk.

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

Sincerely,

[Signature]

David Carney
HR Services Consultant | Verisign, Inc. | 703-948-4143 | dcarney@verisign.com
12 February 2013

The SHA256 hash of the 2013 Q2 KSR file is:

e20491dba323dacebd74479b8d91e793d9b18d9f5348e5b984a8b150821572856

The PGP wordlist for the hash above is:
tiger alkali pheasant suspicious reform cannonball
surmount revival stopwatch designing jawbone
provincial sugar Burlington jawbone crucifix puppy
borderline sugar visitor choking microwave erase
narrative dogsled Medusa backfield antenna blackjack
Eskimo breadline escapade

Attested on behalf of VeriSign by:

Alejandro Boliva:
Senior Engineer, Cryptographic Business Operations
VeriSign, Inc.
Insert Copy of KSR to be signed

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td>CA plugs FD labeled &quot;KSR&quot; with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA points out the KSR file to be signed then closes the file system window.</td>
<td>FA</td>
<td>22:23</td>
</tr>
</tbody>
</table>

Execute KSR signer

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.</td>
<td>CA identifies the KSR to be signed and runs, in the terminal window kersigner 1jgmt7v /media/KSR/kkr-root-2013-q2-0.xml</td>
<td>FA</td>
<td>22:24</td>
</tr>
</tbody>
</table>
| 31.  | The KSR signer will ask whether the HSM is activated or not as below: Activate HSM prior to accepting in the affirmative!! (y/n): CA confirms that the HSM is online and then enters "y" to proceed to verification.  
Note: DO NOT enter "y" for the "Is this correct y/n?" yet. | FA | 22:29 |

Final Verification of the Hash (validity) of the KSR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to identify him/herself, present identification document for IW1 to retain and read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN. IW1 enters RZM representative’s name here: ( \text{\LaTeX} ) ( A ) ( e ) ( \text{\LaTeX} ) ( \backslash \text{\LaTeX} ) ( B ) ( o ) ( \text{\LaTeX} ) ( i ) ( e ) ( \text{\LaTeX} ) ( v ) ( \text{\LaTeX} ) ( e ) ( \text{\LaTeX} )</td>
<td>FA</td>
<td>22:26</td>
</tr>
<tr>
<td>33.</td>
<td>Participants match the hash read out with that displayed on the terminal. CA asks, “are there any objections”?</td>
<td>FA</td>
<td>22:26</td>
</tr>
<tr>
<td>34.</td>
<td>CA then enters “y” in response to “Is this correct y/n?” to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in /media/KSR/skr-root-2013-q2-0.xml</td>
<td>FA</td>
<td>22:27</td>
</tr>
</tbody>
</table>
Starting: krsigner Kjqmt7V ksr-root-2010-q4-1.xml
Use RSM /opt/dnssec/asp-ehmconfig?
Activate RSM prior to accepting in the affirmative!! (y/N): y
RSM /opt/dnssec/asp-ehmconfig activated.

Loaded /opt/Keyper/PCS11Provider/pcs11.GCC4.0.2.so.4.07 Slot=0

Valdation last SKR with RSM...

Validate and Process SKR /media/KSR/ksr-root-2010-q4-1.xml...

SMB256 hash of SKR:

验证通过，无需进一步操作。
Starting: krsigner Ejgqmt7v /media/KSR/krs-root-2013-q2-0.xml (at Tue Feb 12 22:24:29 2013 UTC)
Use HSM /opt/dnssec/aep.hsmconfig
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
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/PECS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
  Label: ICANNKSK
  ManufacturerID: AEP Networks
  Model: Keyper Pro 0405
  Serial: K5002020

Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
  1 2013-01-01T00:00:00 2013-01-15T23:59:59 24220,40323 19036
  2 2013-01-11T00:00:00 2013-01-25T23:59:59 40323 19036
  3 2013-01-21T00:00:00 2013-02-04T23:59:59 40323 19036
  4 2013-01-31T00:00:00 2013-02-14T23:59:59 40323 19036
  5 2013-02-10T00:00:00 2013-02-24T23:59:59 40323 19036
  6 2013-02-20T00:00:00 2013-03-06T23:59:59 40323 19036
  7 2013-03-02T00:00:00 2013-03-16T23:59:59 40323 19036
  8 2013-03-12T00:00:00 2013-03-26T23:59:59 40323 19036
  9 2013-03-21T00:00:00 2013-04-05T23:59:59 20580,40323 19036

...VALIDATED.

Validate and Process KSR /media/KSR/krs-root-2013-q2-0.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
  1 2013-04-01T00:00:00 2013-04-15T23:59:59 20580,40323 19036
  2 2013-04-11T00:00:00 2013-04-25T23:59:59 20580 19036
  3 2013-04-21T00:00:00 2013-05-05T23:59:59 20580 19036
  4 2013-05-01T00:00:00 2013-05-15T23:59:59 20580 19036
  5 2013-05-11T00:00:00 2013-05-25T23:59:59 20580 19036
  6 2013-05-21T00:00:00 2013-06-04T23:59:59 20580 19036
  7 2013-06-10T00:00:00 2013-06-14T23:59:59 20580 19036
  8 2013-06-19T00:00:00 2013-06-24T23:59:59 20580 19036
  9 2013-06-30T00:00:00 2013-07-05T23:59:59 49656,20580 19036

...PASSED.

SHA256 hash of KSR:
E20491DBA323DA4CDBD74479BD9793D9B18D9F5348E5B984A8B150821572856

>> tiger alkali pheasant suspicious reform cannonball surmount revival stopwatch designing jawbone provincial sugar Burlington crucifix puppy borderline sugar visitor choking microwave erase narrative dogsaed Medusa backfield antenna blackjack Eskimo breadline escapee <<

Generated new SKR in /media/KSR/skr-root-2013-q2-0.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
  1 2013-04-01T00:00:00 2013-04-15T23:59:59 20580,40323 19036
SHA256 hash of SKR:
1B7A09BB40C409A0E409ECADB8B853E4597601693B441222B7A7354240FAECBC66
>> beeswax infancy Algol publisher crackdown reproduce Algol Orlando tonic applicant tumor perceptive obtuse enterprise tonic examine inverse adviser gazelle consulting crump led backwater blockade processor repay conformist crowfoot Dakota wallet unicorn showgirl gossamer <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
### Print Copies of the Operation for Participants

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>CA prints out sufficient number of copies for participants using <code>printlog ksrsigner-20130212-*.log N</code> where <code>ksrsigner-20130212-*.log</code> is replaced by log output file displayed by program. (this example generates N copies) and hands copies to participants.</td>
<td>FA</td>
<td>22:31</td>
</tr>
<tr>
<td>36</td>
<td>IW1 attaches a copy to his/her script.</td>
<td>FA</td>
<td>22:31</td>
</tr>
</tbody>
</table>

### Backup Newly Created SKR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>CA copies the contents of the KSR FD by running <code>cp -p /media/KSR/*</code> for posting back to RZM. Confirm overwrite by entering &quot;y&quot; when prompted.</td>
<td>FA</td>
<td>22:32</td>
</tr>
<tr>
<td>38</td>
<td>CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR</code> and then unmounts the KSR FD using <code>umount /media/KSR</code></td>
<td>FA</td>
<td>22:33</td>
</tr>
<tr>
<td>39</td>
<td>CA removes KSR FD containing SKR and gives it to the RZM representative.</td>
<td>FA</td>
<td>22:33</td>
</tr>
</tbody>
</table>

### Disable/Deactivate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>CA inserts 3 cards into HSM to deactivate the unit (via “Set Offline” menu item). Type in the default PIN “11223344” when prompted. IW1 records the used cards below. Each card is returned to cardholder after use. CA makes sure the card(s) NOT used to activate are used to deactivate the HSM. <code>1st OP card 1 of 7</code>  <code>2nd OP card 2 of 7</code>  <code>3rd OP card 5 of 7</code> Confirm the ready light turns off.</td>
<td>FA</td>
<td>22:35</td>
</tr>
</tbody>
</table>
Act. 3 Secure Hardware and Close the Ceremony

Return HSM to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.</td>
<td>FA</td>
<td>22:37</td>
</tr>
<tr>
<td>2.</td>
<td>CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below.</td>
<td>FA</td>
<td>22:38</td>
</tr>
<tr>
<td></td>
<td>HSM1: TEB#BB24706521 / serial # K6002020</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IW1 initials the TEB and keep the sealing strips for later inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA places item on equipment cart.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stop Recording Serial Port Activity and Logging Terminal Output

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Closing ttyaudit terminal window</td>
<td>FA</td>
<td>22:39</td>
</tr>
<tr>
<td></td>
<td>CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of ttyaudit terminal window by typing &quot;exit&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Terminating the logging script</td>
<td>FA</td>
<td>22:39</td>
</tr>
<tr>
<td></td>
<td>CA stops logging terminal output by entering &quot;exit&quot; in the other terminal window. This only stops the script logging and will NOT close window.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Backup HSMFD Contents

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Set dotglob by executing</td>
<td>FA</td>
<td>22:40</td>
</tr>
<tr>
<td></td>
<td>shopt -s dotglob</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This allows copying everything in the original HSMFD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Calculate the md5hash of the contents on the original HSMFD.</td>
<td>FA</td>
<td>22:40</td>
</tr>
<tr>
<td></td>
<td>find -P /media/HSMFD -type f -print0</td>
<td>sort -z</td>
<td>xargs -0 cat</td>
</tr>
<tr>
<td>7.</td>
<td>Copy and paste the md5hash and paste it on Text Editor by going to Applications &gt; Accessories &gt; Text Editor. Print two copies. One for the audit bundle and the other for the HSMFD package.</td>
<td>FA</td>
<td>22:46</td>
</tr>
<tr>
<td>8.</td>
<td>CA displays contents of HSMFD by executing</td>
<td>FA</td>
<td>22:46</td>
</tr>
<tr>
<td></td>
<td>ls -ltr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the OVS (as HSMFD_); and copies the contents of the HSMFD to the blank drive for backup by executing cp -Rp * /media/HSMFD_</td>
<td>FA</td>
<td>22:47</td>
</tr>
</tbody>
</table>

version 1.6
Script started on Tue 12 Feb 2013 00:33:12 PM UTC

--- 192.168.0.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8000ms
rtt min/avg/max/mdev = 0.236/0.303/0.699/0.140 ms

--- 192.168.0.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8000ms
rtt min/avg/max/mdev = 0.236/0.303/0.699/0.140 ms

Starting: ksigner Ksign7p7/media/KSR/kir-root-2013-q2-0 (at Tue Feb 12 22:42:29 2013 UTC)
Use HSM /opt/inssec/aep_xamconfig
Activate HSM prior to accepting in the affirmative! (y/N): y
HSM /opt/inssec/aep_xamconfig activated.
debbug setenv KEYPER_LIBRARY_PATH=/opt/inssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.0.4
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.0.4
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.0.4 Slot-0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper Pro 0405
Serial: K6002020

Validating last SKR with HSM...
# Inception | Expiration | ZSK Tags | RSK Tag(CKA_LABEL)
1 2013-01-01T00:00:00 2013-01-15T23:59:59 24220,40323 19036
2 2013-01-11T00:00:00 2013-01-25T23:59:59 40323 19036
3 2013-01-21T00:00:00 2013-02-04T23:59:59 40323 19036
4 2013-01-31T00:00:00 2013-02-14T23:59:59 40323 19036
5 2013-02-10T00:00:00 2013-03-04T23:59:59 40323 19036
6 2013-03-02T00:00:00 2013-03-16T23:59:59 40323 19036
7 2013-03-12T00:00:00 2013-03-26T23:59:59 40323 19036
9 2013-03-21T00:00:00 2013-03-05T23:59:59 40323,40532 19036
...VALIDATED.

Validating and Process RSK /media/KSR/kir-root-2013-q2-0.xml...
# Inception | Expiration | ZSK Tags | RSK Tag(CKA_LABEL)
1 2013-04-01T00:00:00 2013-04-15T23:59:59 24220,40323 19036
2 2013-04-11T00:00:00 2013-04-25T23:59:59 40323 19036
3 2013-04-21T00:00:00 2013-05-05T23:59:59 40323 19036
4 2013-05-01T00:00:00 2013-05-25T23:59:59 40323 19036
5 2013-05-11T00:00:00 2013-06-04T23:59:59 40323 19036
6 2013-05-31T00:00:00 2013-06-14T23:59:59 40323 19036
7 2013-06-10T00:00:00 2013-06-24T23:59:59 40323 19036
8 2013-06-20T00:00:00 2013-07-03T23:59:59 49656,20580
...PASSED.

SHA256 hash of RSK:
e20491DA33ACD3774479BA9B1879309B1EDF534865899A68B1058217289E
>> tiger alkali phreatomagmatic spruce cmnalewse surmount stopwatch desii
jumbo provincial sugar Burlington jumbo crucifix puppy borderline sugar vital
or choking microwave erase narrative dogged Medusa backfield antenna blackjack
biskri breath escapade <<
Is this correct (y/N): y

Generated new SKR in /media/KSR/kir-root-2013-q2-0.xml
# Inception | Expiration | ZSK Tags | RSK Tag(CKA_LABEL)
1 2013-04-01T00:00:00 2013-04-15T23:59:59 20580,40323 19036
2 2013-04-11T00:00:00 2013-04-25T23:59:59 20580,40323 19036

64 bytes from 192.168.0.2: icmp_seq=9 ttl=255 time=0.236 ms
SRA256 hash of SKR:
197A0984043C40904409EAC9438553E45976J9633441222B7A7354240FAD3C566
>> Deevaw infency Aygul publisher D6K6Dm reproduce Aygul. Orlando tonic applicant t
umor perceptive obtuse enterprise tonic examine inverse adviser gazelle consulting cru
mpled backwater blockade processor repay conformist crowfoot Dakota wallet unicorn sho
wirl goamer <<

******** Log output in ./krsigner-20130212-222429.log ************

\033[0;8mroot@localhost:/media/NSMFD/007[root@localhost NSMFD]# ls -l | grep /media/NSK
\033[m

[2 lines * 15 copy] sent to printer

3 lines were wrapped

\033[0;8mroot@localhost:/media/NSMFD/007[root@localhost NSMFD]# cp -p /media/NSR/

\033[0;8mroot@localhost:/media/NSMFD/007[root@localhost NSMFD]# ls -ltr /media/NSK

\033[m

Script done on Tue 12 Feb 2013 10:39:13 PM UTC
ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Battery OK!
ttyUSB0
ttyUSB0
ttyUSB0 No Tamper Counts in BBRAM!
ttyUSB0
ttyUSB0 Loading Application (APP)
ttyUSB0
ttyUSB0 Starting loaded code.
ttyUSB0
\000Application - Feb 25 2010 11:08:02
ttyUSB0
ttyUSB0 wdog started
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Running DES POST Test
ttyUSB0
ttyUSB0 DES POST Test Passed
ttyUSB0
ttyUSB0 Running Triple DES POST Test
ttyUSB0
ttyUSB0 Triple DES POST Test Passed
ttyUSB0
ttyUSB0 Running AES POST Test
ttyUSB0
ttyUSB0 AES POST Test Passed
ttyUSB0
ttyUSB0 Running SHA1 POST Test
ttyUSB0
ttyUSB0 SHA1 POST Test Passed
ttyUSB0
ttyUSB0 Running SHA2 POST Test
ttyUSB0
ttyUSB0 SHA2 POST Test Passed
ttyUSB0
ttyUSB0 Running RandomGen SHA1 POST Test
ttyUSB0
ttyUSB0 RandomGen SHA1 POST Test Passed
ttyUSB0
ttyUSB0 Running RSA POST Test
ttyUSB0
ttyUSB0 RSA POST Test Passed
ttyUSB0
ttyUSB0 Running DSA POST Test
ttyUSB0
ttyUSB0 DSA POST Test Passed
ttyUSB0
ttyUSB0 Running RandomGen POST Test
ttyUSB0
ttyUSB0 RandomGen POST Test Passed
ttyUSB0
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 12/2/2013 at 20:49:00
ttyUSB0 0x100008
ttyUSB0
ttyUSB0
ttyUSB0

ttyUSB0 App Details Response:
ttyUSB0

ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0 Additional RandomGen POST Test Passed
ttyUSB0
ttyUSB0

ttyUSB0 Part Number: Keyer Pro 0405
ttyUSB0 Serial Number: Serial K6002020
ttyUSB0 App Build Number: App 020
ttyUSB0 AML Build Number: Aml 029
ttyUSB0 AL Build Number: AL 02A
ttyUSB0
ttyUSB0
ttyUSB0 CS Build Number: CS 029
ttyUSB0
ttyaudit-ttyUSB0-20130212-220521.log

2013-02-12T22:08:51+0000  ttyUSB0 Total Private Memory 4173377
2013-02-12T22:08:51+0000  ttyUSB0 Free Private Memory 4173377
2013-02-12T22:08:51+0000  ttyUSB0 Total Dynamic Memory 14569472
2013-02-12T22:08:51+0000  ttyUSB0 Free Dynamic Memory 14569472
2013-02-12T22:08:51+0000  ttyUSB0 Date and Time: 20:49:00 on 12/02/2013
2013-02-12T22:08:51+0000  ttyUSB0 Created socket 1 on port 3000.
2013-02-12T22:08:51+0000  ttyUSB0 0x100003
2013-02-12T22:08:51+0000  ttyUSB0 12/2/2013 at 20:49:01
2013-02-12T22:08:51+0000  ttyUSB0 12/2/2013 at 20:56:04
2013-02-12T22:15:54+0000  ttyUSB0 0x200023 0A400000B706296E
2013-02-12T22:15:54+0000  ttyUSB0 0x200023 0A400000D6296E
2013-02-12T22:16:23+0000  ttyUSB0 12/2/2013 at 20:56:32
2013-02-12T22:16:23+0000  ttyUSB0 0x200023 0A400000D6296E
2013-02-12T22:17:00+0000  ttyUSB0 12/2/2013 at 20:57:10
2013-02-12T22:17:00+0000  ttyUSB0 0x200023 0A400000D6296E
2013-02-12T22:17:03+0000  ttyUSB0 Created socket 1 on port 5000.
2013-02-12T22:17:03+0000  ttyUSB0 12/2/2013 at 20:57:12
2013-02-12T22:17:03+0000  ttyUSB0 0x100002
2013-02-12T22:17:03+0000  ttyUSB0 Accepted connection on address 210.247.192.168.0.1.
2013-02-12T22:24:57+0000  ttyUSB0 Free memory down from 14569472 to 11843072 (last mechanism 0)!
ttyaudit-ttyUSB0-20130212-220521.log

2013-02-12T22:24:57+0000
ttyUSB0 21:05:06 on 12-01-2013
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------
ttyUSB0 Closing connection on address 210.247.192.168.0.1.
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 12/2/2013 at 21:14:49
ttyUSB0
ttyUSB0 0x200023 0A400000B706296E
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 12/2/2013 at 21:15:19
ttyUSB0
ttyUSB0 0x200023 0A4000009D06296E
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
 ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection; address unavailable (errno 5009).
0x100003
ttyUSB0

ttyUSB0 12/2/2013 at 21:15:51
ttyUSB0
ttyUSB0
### ICANN Root DNSSEC KSK Ceremony 12

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>CA displays contents of HSMFD by executing <code>ls -ltr /media/HSMFD</code></td>
<td>FA</td>
<td>22:17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Calculate the md5Hash of the contents on the copied HSMFD. `find -P /media/HSMFD -type f -print0</td>
<td>sort -z</td>
<td>xargs -0 cat</td>
</tr>
<tr>
<td></td>
<td>Confirm that it matches the md5Hash of the original HSMFD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>CA unmounts new FD using <code>umount /media/HSMFD</code></td>
<td>FA</td>
<td>22:49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>CA removes HSMFD and places on table.</td>
<td>FA</td>
<td>22:49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>CA repeats step 9 to 13 for the 2nd copy</td>
<td>FA</td>
<td>22:50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>CA repeats step 9 to 13 for the 3rd copy</td>
<td>FA</td>
<td>22:51</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>CA repeats step 9 to 13 for the 4th copy</td>
<td>FA</td>
<td>22:52</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>CA repeats step 9 to 13 for the 5th copy</td>
<td>FA</td>
<td>22:53</td>
</tr>
</tbody>
</table>

### Print Logging Information

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td>CA prints out hard copies of logging information by executing <code>en crypt -pOc */tmp/2 script-20130212.log</code> <code>en crypt -Ocr */tmp/2 --font=&quot;Courier&quot; tt yaudit-ttyUSB --20130212-*.log</code> for attachment to IW1 and CA scripts. <strong>Note:</strong> Ignore the error regarding non-printable characters if prompted.</td>
<td>FA</td>
<td>22:56</td>
</tr>
</tbody>
</table>

### Returning HSMFD and O/S DVD to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>CA unmounts HSMFD by executing <code>cd /tmp</code> <code>umount /media/HSMFD</code></td>
<td>FA</td>
<td>22:57</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA removes HSMFD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>After all print jobs are complete, CA</td>
<td>FA</td>
<td>22:58</td>
</tr>
<tr>
<td></td>
<td>(a) Turns off the laptop by pressing the power switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) Turns on the laptop by pressing the power switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c) Remove the O/G DVD from the drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(d) Turns off the laptop again by pressing the power switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td>CA places two HSMFDs and OS/DVD in TEB; writes date, time and &quot;HSMFD&quot; in amount field; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. O/S DVD (Rev600) + HSMFD: TEB# BB21820463</td>
<td>FA</td>
<td>23:01</td>
</tr>
<tr>
<td></td>
<td>IW1 initials the TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA places TEB on equipment cart.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Distribute HSMFDs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 1 for himself), IKOS(1) to post SKR to RZM, and to review, analyze and improve on procedures.</td>
<td>FA</td>
<td>23:02</td>
</tr>
</tbody>
</table>

### Returning Laptop to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.</td>
<td>CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. Laptop1 (Dell ATG6400): TEB# BB24706822 / serial# 37240147333 IW1 initials the TEB and keep the sealing strips for later inventory. CA places TEB on equipment cart.</td>
<td>FA</td>
<td>23:04</td>
</tr>
</tbody>
</table>

### Returning OP Smartcards to TEBs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
</table>
| 24.  | CA calls each CO to the front of the room one at a time and repeats the steps below.  
   a) CA takes a TEB prepared for the CO and reads out the number and description while showing the bag to IW1 and CO. Figure 2 below for an example. 
   b) CA places OP into TEB, seals in front of IW1 and CO then initials bag and strip. 
   c) IW1 inspects the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. 
   d) CA hands the TEB containing the OP card to the CO. CO inspects and verifies TEB #s and contents then initials his/her bag. 
   e) CO enters completion time and signs for each TEB in the table below in IW1’s script. IW1 initials table entry. 
   f) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB. | FA | 23:11 |
<table>
<thead>
<tr>
<th>CO#</th>
<th>Card Type</th>
<th>TEB #</th>
<th>Printed Name</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
<th>IW1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO 1</td>
<td>OP 1 of 7</td>
<td>BB21820464</td>
<td>Masato Minda</td>
<td>[Signature]</td>
<td>12 February 2013</td>
<td>23:07</td>
<td>FA</td>
</tr>
<tr>
<td>CO 2</td>
<td>OP 2 of 7</td>
<td>BB21820459</td>
<td>Dmitry Burkov</td>
<td>[Signature]</td>
<td>12 February 2013</td>
<td>23:02</td>
<td>FA</td>
</tr>
<tr>
<td>CO 3</td>
<td>OP 3 of 7</td>
<td>BB21820460</td>
<td>Joao Damas</td>
<td>[Signature]</td>
<td>12 February 2013</td>
<td></td>
<td>FA</td>
</tr>
<tr>
<td>CO 5</td>
<td>OP 5 of 7</td>
<td>BB21820461</td>
<td>Edward Lewis</td>
<td>[Signature]</td>
<td>12 February 2013</td>
<td>23:11</td>
<td>FA</td>
</tr>
<tr>
<td>CO 7</td>
<td>OP 7 of 7</td>
<td>BB21820462</td>
<td>Subramanian Moonesamy</td>
<td></td>
<td>12 February 2013</td>
<td></td>
<td>FA</td>
</tr>
</tbody>
</table>
SEALING INSTRUCTIONS:
1. Use tamper proof tape to complete all information BEFORE sealing bag.
2. Remove tear-off receipt and keep with copy of deposit documentation.
3. Remove tapped air-pel off release line over sealing strip.
4. Press down firmly from center to edges.

DATE: 26 July, 2012

SAID TO CONTAIN: $ 10.10 ct. 7

1. $ 4. $  
2. $ 5. $  
3. $ 6. $  

FROM: Root DNSSEC KSK Ceremony 10

TO: Masato . Minda

Figure 2
### Returning Equipment to Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td>CA, IW1, SSC1 open safe room and enter with equipment cart.</td>
<td>FA</td>
<td>23:13</td>
</tr>
<tr>
<td>26.</td>
<td>SSC1 opens Safe #1 shielding combination from camera.</td>
<td>FA</td>
<td>23:14</td>
</tr>
</tbody>
</table>
| 27.  | SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry.  
*Note: If log entry is pre-printed, verify the entry, record time of completion and sign.* | FA | 23:14 |
| 28.  | CA records return of HSM in next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA CAREFULLY places the HSM into Safe #1 and IW1 initials the entry.  
HSM1: TEB# BB24706821 / serial # K6002020 | FA | 23:15 |
| 29.  | CA records return of laptop in next entry field of safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry.  
Laptop1 (Dell ATG6400): TEB# BB24706822 / serial# 37240147333 | FA | 23:15 |
| 30.  | CA records return of OIS DVD + HSMFD in next entry field of safe log with TEB #, printed name, date, time, and signature; places the OIS DVD + HSMFD into Safe #1 and IW1 initials the entry.  
OIS DVD (Rev500) + HSMFD: TEB# BB21820463 | FA | 23:15 |

### Close Equipment Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
</table>
| 31.  | SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry.  
*Note: If log entry is pre-printed, verify the entry, record time of completion and sign.* | FA | 23:16 |
| 32.  | SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise).  
IW1 and CA verify safe is locked and door indicator light is green. | FA | 23:16 |
| 33.  | IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them. | FA | 03:17 |

### Open Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td>After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP card TEB with them.</td>
<td>FA</td>
<td>23:19</td>
</tr>
<tr>
<td>35.</td>
<td>SSC2 opens Safe #2 while shielding combination from camera.</td>
<td>FA</td>
<td>00:58</td>
</tr>
</tbody>
</table>
| 36.  | SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry.  
*Note: If log entry is pre-printed, verify the entry, record time of completion and sign.* | FA | 00:59 |
### CO returns OP cards to Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.</td>
<td>One by one, each CO along with the CA (using his/her common key):&lt;br&gt;a) Open his/her respective safe deposit box and read out box number inside Safe #2.&lt;br&gt;b) CO makes an entry into the safe log indicating the return of OP card including Box #, TEB #, card type, printed name, date, time, and signature. W1 initials the entry after verifying contents and integrity of the TEB and comparing TEB#’s and card type to his/her script.&lt;br&gt;Note: If log entry is pre-printed, verify the entry, record time of completion and sign.&lt;br&gt;c) CO shows the bag to the camera and then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA. Repeat the steps above until all cards are returned to the deposit box.</td>
<td>FA</td>
<td>01:03</td>
</tr>
</tbody>
</table>

**CO 1:** Masač Minda  
Box # 1788  
OP TEB # B21820464  

**CO 2:** Dmitry Burkov  
Box # 1793  
OP TEB # B21820459  

**CO 3:** João Gomes  
Box # 1871  
OP TEB # B21820460  

**CO 5:** Edward Lewis  
Box # 1790  
OP TEB # B621820461  

**CO 7:** Subramanian Moonesamy  
Box # 1792  
OP TEB # B621820462
Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>Once all safe deposit boxes are closed, SSC2 makes an entry including</td>
<td>FA</td>
<td>01:01</td>
</tr>
<tr>
<td></td>
<td>printed name, date, time, and signature and notes “Close safe” into the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>safe log. IW1 initials the entry.</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>39.</td>
<td>SSC2 puts log back in safe and locks Safe #2 (spin dial at least two</td>
<td>FA</td>
<td>01:04</td>
</tr>
<tr>
<td></td>
<td>full revolutions each way, counter clock wise then clock wise).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IW1 and CA verify safe is locked and door indicator light is green.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40.</td>
<td>CA, IW1, SSC2, and COs leave safe room closing the door behind them</td>
<td>FA</td>
<td>01:05</td>
</tr>
<tr>
<td></td>
<td>making sure it is locked.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Participant Signing of IW1’s Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.</td>
<td>All participants enter printed name, date, time, and signature on IW1’s</td>
<td>FA</td>
<td>01:09</td>
</tr>
<tr>
<td></td>
<td>script coversheet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42.</td>
<td>CA reviews IW1’s script and signs it.</td>
<td></td>
<td>01:05</td>
</tr>
</tbody>
</table>

Signing out of Ceremony Room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.</td>
<td>IW2 ensures that all participants sign out of Ceremony Room log and are</td>
<td>FA</td>
<td>01:16</td>
</tr>
<tr>
<td></td>
<td>escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Room.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Filming Stops

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td>SA stops filming and makes 2 copies of film, one for on-site and one for</td>
<td>FA</td>
<td>01:35</td>
</tr>
<tr>
<td></td>
<td>off-site storage along with IW1 script copies made below.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Copying and Storing the Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td>IW1 makes at least 4 copies of his/her script: one for off-site audit bundle, one for IW1, one for KOS and copies for other participants, as requested. Audit bundles each contain: 1) Output of signer system – HSMF-D 2) Copy of IW1’s key ceremony script 3) Audio-visual recording 4) Logs from the Physical Access Control and Intrusion Detection System (Range is 07/26/2012 – 02/12/2013) 5) The IW attestation (A.1 below) 6) SA attestation (A.2, A.3 below) All in a TEB labeled “Key Ceremony 12”, dated and signed by IW1 and CA. Off-site audit bundle is delivered to off-site storage. The CA holds the ultimate responsibility for finalizing the audit bundle.</td>
<td>FA</td>
<td>02:46</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 placed within a tamper-evident bag, labeled, dated and signed by the CA and the IW1.

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

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

4. **Logs from the Physical Access Control and Intrusion Detection System (SA)**
   One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC-IDS configuration review, the list of the enrolled users, the event log file and the configuration audit log file in each audit bundle, each placed in a tamper-evident bag, labeled, dated and signed by the SA and the IW.

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

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

6. **Configuration review of the Firewall System (SA)**
   SA’s attestation and hard copies of the firewall configuration from the review process. See Appendix A.3.

7. **Other items**
   If applicable.
A.1 Key Ceremony Script (by IW)

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

Francisco Arias

Date: 12 February 2013
A.2 Access Control System Configuration Review (by SA)

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

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

Enclosed is also an electronic copy of the event log from the access control system ranging from the last log extraction on [date, time UTC] February 13, 2013 02:24 to now.

Alexander Kulik

Date: 12 February 2013
A.3 Firewall Configuration Review (by SA)

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

Enclosed is the configuration extract from the firewall unit.

Alexander Kulik

Date: 12 February 2013
--- JUNOS 10.1R1.8 built 2010-02-12 18:31:54 UTC
akulik@srx> show configuration | no-more
## Last commit: 2012-02-03 09:41:48 UTC by root
version 10.1R1.8;
system {
    host-name srx;
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-cut-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "$1$XlzwmIYq$i50YWAFS7h4SW4U27m.qM."; ## SECRET-DATA
    }
    name-server {
        199.4.28.18;
        199.4.28.28;
    }
    login {
        user akulik {
            full-name "Alex Kulik";
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "$1$Z09TLzzv$V9GNTNKqLHj9snvqUHZD21"; ## SECRET-DATA
            }
        }
        user reed {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "$1$KqBOyZR6$6S3oix0hSkL/N/j1TUXK210"; ## SECRET-DATA
            }
        }
    }
}
services;
syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    host 199.4.28.21 {
        any any;
        match RT_FLOW_SESSION;
        log-prefix SRX-KSK-LAX;
    }
    file messages {
        any critical;
        authorization info;
    }
    file interactive-commands {
        interactive-commands error;
    }
    source-address 199.4.28.145;
}
max-configurations-on-flash 5;
max-configuration-rollback 20;
archival {
    configuration {
        transfer-on-commit;
        archive-sites {
            "scp://srxkskcjr@199.4.28.21:/home/srxkskcjr" password "$9$GHiHmpu1ylM36reW8Vbs24Ji.Qz6"; ## SECRET-DATA
        }
    }
}
license {
    autocapdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
ntp {
    server 199.4.28.17;
    server 199.4.28.27;
    source-address 10.4.28.1;
}
}
interfaces {
    interface-range interfaces-trust {
        member ge-0/0/1;
        member fe-0/0/2;
member fe-0/0/3;
member fe-0/0/4;
member fe-0/0/5;
member fe-0/0/6;
member fe-0/0/7;
unit 0 {
    family ethernet-switching {
        vlan {
            members vlan-trust;
        }
    }
}
ge-0/0/0 {
    unit 0 {
        family inet {
            address 199.4.28.145/26;
        }
    }
}
vlan {
    unit 0 {
        family inet {
            address 10.4.28.1/24;
        }
    }
}
smmp {
    community dnss3c {
        clients [
            10.4.28.253/32;
        ]
    }
    trap-options {
        source-address 199.4.28.145;
        agent-address outgoing-interface;
    }
    trap-group kskwest {
        categories {
            authentication;
            link;
            routing;
            startup;
            configuration;
            services;
        }
    }
}
targets {
    199.4.28.21;
}

routing-options {
    static {
        route 0.0.0.0/0 next-hop 199.4.28.129;
    }
}

security {
    ssh-known-hosts {
        host 199.4.28.21 {
            rsso-key
            AAAAB3NzaC1yc2EAAAABEwAAAQEAuMQ5nC2+tk7W4nBHLZLFk1FFFlStiYP2w/5XR/x2hxxPZsoZ4uFppRdaB+G9DIcKvmZ7ovvL/QsEtR2holMk2C+ilAwPaqgPfo9XFQby/cwS400sYQHZAXqAV2wM4eGF8l7eGI2BKJcjpWmD+YTZ+d9j0d7bVdG248x1PF4eQmsyXsxm72ecm2e2I9q99G5M5+aR15NTXLJ4fTYgLmODMZLIThER2zdnZYXuU7cDZBTiJ9RQwfk8oVjipGZc0q4eNNZyrUKAr8XrQcuNOjQAqVzktS+BByi4JBFq/nLXzKdvd8rXkPoavCe9lNP0zAEbAKhKgfPc6QlfTFycpI34Ew==;
        }
    }
    nat {
        source {
            rule-set trust-to-untrust {
                from zone trust;
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
    zones {
        security-zone trust {
            address-book {
                address localnet 10.4.28.0/24;
            }
            host-inbound-traffic {
                system-services {

all;
}
protocols {
  all;
}
}
interfaces {
  vlan.0;
}
}
security-zone untrust {
  address-book {
    address icanndns 199.4.28.0/22;
  }
  interfaces {
    ge-0/0/0.0 {
      host-inbound-traffic {
        system-services {
          ping;
        }
      }
    }
  }
}
}
policies {
  from-zone trust to-zone untrust {
    policy trust-to-untrust {
      match {
        source-address localnet;
        destination-address icanndns;
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
}
}
vlans {
  vlan-trust {
    vlan-id 3;
    l3-interface vlan.0;
akulik@srx>
ICANN 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, e.g., BT3. Note time.

### Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td>FA</td>
<td>21:4</td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-- Joan Damos will not be participating as CO only as EW

-- End of DNSSEC Script Exception --
ICANN 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, e.g., R1/1. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td>FA</td>
<td>21:7</td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- SM will not be participating as CO, only EW

- End of DNSSEC Script Exception -
ICANN 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, e.g., 873. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td>FA</td>
<td>2:26</td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At step 9, boxes 1070 and 1784 were not closed since their locks were removed

--- End of DNSSEC Script Exception ---
ICANN 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, e.g., FA. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td>FA</td>
<td>22:53</td>
</tr>
<tr>
<td>2</td>
<td>IW describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Before step 3 on Act 3 we stop the ceremony temporarily for a big break.
ICANN 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, e.g., 873. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td>FA</td>
<td>23:30</td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At step 35, of Act 3 the safe #2 couldn't be opened by the SSC2. Everyone left the safe room for a few minutes.

– End of DNSSEC Script Exception –
ICANN 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, e.g., 873. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

we retried opening the safe 2 but it didn't work again. we all left the safe room.

we reentered at 23:50, Tomorijn joined this time to help.

--- End of DNSSEC Script Exception ---
# ICANN 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, e.g., **FA**. Note time.

**Note Exception Time**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
<td>FA</td>
<td>00:06</td>
</tr>
<tr>
<td></td>
<td><strong>13 FEBRUARY 2019</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Everyone left the safe room after failing again to open the safe. We are waiting for the lock to power off. SSC2 left the KMF to talk with the other SSC2. We took a break and a few people left the room for a big break.

The three COS left their OP cards in the table in order to take a big break. At 00:46 everyone and Tomomi entered the safe room again.

---

*End of DNSSEC Script Exception*