Root DNSSEC KSK Ceremony 39
Thursday November 14, 2019

Root Zone KSK Operator Key Management Facility
18155 Technology Drive, Culpeper, VA 22701

This ceremony is executed in accordance to the DNSSEC Practice Statement for the Root Zone KSK Operator Version 4th Edition (2016-10-01)
Abbreviations

AUD = Third Party Auditor  
EW = External Witness  
IW = Internal Witness  
OP = Operator  
RKOS = RZ KSK Operations Security  
SKR = Signed Key Response  
SSC = Safe Security Controller  
TEB = Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20)

CA = Ceremony Administrator  
FD = Flash Drive  
KMF = Key Management Facility  
PTI = Public Technical Identifiers  
RZM = Root Zone Maintainer  
SMK = Storage Master Key  
SW = Staff Witness  
CO = Crypto Officer  
HSM = Hardware Security Module  
KSR = Key Signing Request  
RKSH = Recovery Key Share Holder  
SA = System Administrator  
SO = Security Officer  
TCR = Trusted Community Representative

Participants

Key Ceremony roles are described on https://www.iana.org/help/key-ceremony-roles

Instructions: At the end of the ceremony, participants sign IW's script. IW records time of completion.

<table>
<thead>
<tr>
<th>Title / Roles</th>
<th>Printed Name</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Matthew Larson / ICANN</td>
<td>[Signature]</td>
<td>2019 Nov 14</td>
<td>20:38</td>
</tr>
<tr>
<td>IW</td>
<td>Shauna Royston / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC1</td>
<td>James Cole / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC2</td>
<td>Carlos Reyes / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO2</td>
<td>Anne-Marie Eklund Lowinder</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GO4</td>
<td>Robert Seastrom</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO5</td>
<td>Christopher Griffiths</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO6</td>
<td>Gaurab Upadhyaya</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RZM</td>
<td>Trevor Davis / Verisign</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Catherine Chih-Yun Wong / RSM</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Eylan Jordan Torres / RSM</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA</td>
<td>Reed Quinn / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA</td>
<td>Sean Freeark / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RKOS / CA Backup</td>
<td>Andres Pavez / PTI</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RKOS / IW Backup</td>
<td>Aaron Foley / PTI</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW</td>
<td>Matthew Beach</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUD</td>
<td>Karen Minh Phan</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: By signing this script, you are declaring that this document is a true and accurate record of the Root DNSSEC KSK ceremony to the best of your knowledge, and you agree that your personal data will be processed in accordance with the ICANN Privacy Policy available at https://www.icann.org/privacy/policy
Instructions for Root DNSSEC KSK Ceremony

The Root DNSSEC Key Signing Key (KSK) Ceremony is a scripted meeting where individuals with specific roles generate, or access the private key component of the root zone DNSSEC KSK. The process is audited by a third party firm for compliance with SOC 3 framework. The script and recordings are published online for the wider Internet community to review.

Ceremony Guidelines:

- The CA leads the ceremony
- Only CAs, IWs, or SAs can enter and escort other participants into Tier 4 (Key Ceremony Room)
- Dual Occupancy is enforced. IW with CA or SA must remain inside Tier 4 (Key Ceremony Room) if participants are present in the room
- CAs, IWs, or SAs may escort participants out of Tier 4 (Key Ceremony Room) at the CA’s discretion only if Tier 5 (Safe Room) is not occupied during the ceremony
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log
- The SA starts filming before the participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step
- CA reads each step aloud prior to its performance
- Upon completion of each step, IW announces the time of completion, records the completion time, and initials their copy of the script
- Ceremony participants who notice a problem or an error during the ceremony should interrupt the ceremony. Ceremony participants agree on a resolution before proceeding
- Questions and suggestions for improvement are welcome and can be discussed at any time or after the ceremony during the ceremony debrief

Unplanned events (exceptions) during the ceremony are evaluated, documented, and acted upon. It is the CA’s sole responsibility to decide on proper actions after consulting with the IW. In either case, an exception is regarded as an incident, and incident handling procedures are enacted.

Key Management Facility Tiers:

- Tiers 1-3: Consists of the facility areas between the outside environment and the Key Ceremony Room
- Tier 4: Consists of the Key Ceremony Room and is subject to Dual Occupancy
- Tier 5: Consists of the Safe Room (a cage only accessible from the Key Ceremony Room) and is subject to Dual Occupancy
- Tier 6: Consists of Safe #1 (Equipment Safe) and Safe #2 (Credentials Safe)
- Tier 7: Consists of the HSM stored in Safe #1 (Equipment Safe) and the safe deposit boxes installed in Safe #2 (Credentials Safe)
Preamble

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

<table>
<thead>
<tr>
<th>Character</th>
<th>Code Word</th>
<th>Pronunciation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alfa</td>
<td>AL-FAH</td>
</tr>
<tr>
<td>B</td>
<td>Bravo</td>
<td>BRAH-VOH</td>
</tr>
<tr>
<td>C</td>
<td>Charlie</td>
<td>CHAR-LEE</td>
</tr>
<tr>
<td>D</td>
<td>Delta</td>
<td>DEL-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-VEL-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>
## Root DNSSEC Script Exception

### Exception Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW writes the details of the ceremony exception:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Act: <em>1</em>  Step(s): <em>2</em>  Page(s): <em>5</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date and Time:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(COA) (AUD)</strong></td>
<td><strong>SVL</strong></td>
<td><strong>18:02</strong></td>
</tr>
<tr>
<td>2</td>
<td>IW describes the exception(s) and action(s) below.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Participants: ROBERT SEASTROM & CATHERINE CHIH YUN WONG. RSM NOT PRESENT.

AUDITOR HAS BEEN REPLACED WITH KAREN MINH PHAN.

ALL MENTIONS OF ROBERT SEASTROM WILL BE STRICKEN FROM SCRIPT.
Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

- Verify that the audit cameras are recording and the online video streaming is enabled
- Confirm that all of the ceremony attendees have signed in using the visitor log in Tier 3
- Review emergency evacuation procedures
- Explain the use of personal devices and the purpose of this ceremony
- Verify the time and date so that all entries into the script follow a common time source

At this point, the CA and IW will escort the SSCs and TCRs into Tier 5 (Safe Room) to retrieve the following materials:

- Safe #1: HSM, laptop, OS DVD, etc
- Safe #2: The TCRs' smartcards required to operate the HSM

Sign into Tier 4 (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>ZR</td>
<td>18:01</td>
</tr>
<tr>
<td>2</td>
<td>CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2.</td>
<td>ZR</td>
<td>18:02</td>
</tr>
<tr>
<td>3</td>
<td>CA asks that any first time ceremony participants introduce themselves.</td>
<td>ZR</td>
<td>18:03</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>4</td>
<td>CA reviews the emergency evacuation procedure with onsite participants.</td>
<td>ZR</td>
<td>18:04</td>
</tr>
<tr>
<td>5</td>
<td>CA explains the use of personal electronic devices during the ceremony.</td>
<td>ZR</td>
<td>18:04</td>
</tr>
<tr>
<td>6</td>
<td>CA briefly explains the purpose of the ceremony.</td>
<td>ZR</td>
<td>18:05</td>
</tr>
</tbody>
</table>

Verify the Time and Date

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: 2019/11/14 All entries into this script or any logs should follow this common source of time.</td>
<td>ZR</td>
<td>18:05</td>
</tr>
</tbody>
</table>
## Open Safe #2 (Tier 6, Credentials Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)</td>
<td>SK</td>
<td>18:00</td>
</tr>
<tr>
<td>9</td>
<td>SSC2 opens Safe #2 while shielding the combination from the camera.</td>
<td>JR</td>
<td>18:13</td>
</tr>
<tr>
<td></td>
<td>Perform the following steps to complete the safe log:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) IW provides the pre-printed safe log to SSC2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) SSC2 writes the date and time, then signs the safe log where &quot;Open Safe&quot; is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW verifies the entry then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>SL</td>
<td>18:14</td>
</tr>
</tbody>
</table>

## COs Extract the Credentials from Safe Deposit Boxes (Tier 7)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The selected CO then performs the following steps sequentially to retrieve the required TEBs:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) With the assistance of the CA (and the common key), the CO opens their safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Common Key is for the bottom lock, CO Key is for the top lock.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) CO reads aloud the safe deposit box number, verifies its integrity,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>then removes the OP TEB and SO TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) CO reads aloud the TEB numbers, then verifies their integrity while showing them to the audit camera above.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) CO retains the TEB(s) specified below, then locks the safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) CO writes the date and time, then signs the safe log where removal of a TEB is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) IW verifies the completed safe log entries, then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>CO2: Anne-Marie Eklund Lowinder</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1259</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584404 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SO TEB # BB46584403 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>CO4: Robert Seastrom</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1260</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584492 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SO TEB # BB46584491 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>CO5: Christopher Griffiths</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1240</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584400 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SO TEB # BB46584399 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>CO6: Gaurab Upadhaya</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1261</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB46584398 (Retain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SO TEB # BB46584397 (Retain)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Close Safe #2 (Tier 6, Credentials Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where “Close Safe” is indicated. IW verifies the entry then initials it.</td>
<td>S√L</td>
<td>18:20</td>
</tr>
<tr>
<td>13</td>
<td>SSC2 returns the safe log to Safe #2 and locks it by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the &quot;WAIT&quot; light indicator is off.</td>
<td>S√R</td>
<td>18:20</td>
</tr>
<tr>
<td>14</td>
<td>CA, IW, SSC2, and COs leave the safe room with TEBs, closing the door behind them.</td>
<td>S√L</td>
<td>10:21</td>
</tr>
</tbody>
</table>

Open Safe #1 (Tier 6, Equipment Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)</td>
<td>S√L</td>
<td>10:23</td>
</tr>
<tr>
<td>16</td>
<td>SSC1 opens Safe #1 while shielding the combination from the camera.</td>
<td>S√R</td>
<td>10:23</td>
</tr>
<tr>
<td>17</td>
<td>Perform the following steps to complete the safe log:</td>
<td>S√R</td>
<td>10:24</td>
</tr>
<tr>
<td></td>
<td>a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) IW provides the pre-printed safe log to SSC1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) SSC1 writes the date and time, then signs the safe log where &quot;Open Safe&quot; is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW verifies the entry then initials it.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>CA performs the following steps to extract each piece of equipment from the safe:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) CAREFULLY remove each equipment TEB from the safe.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Read aloud each TEB number, then verify its integrity while</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>showing it to the audit camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Place each equipment TEB on the cart as specified on the list below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Write the date, time, and signature on the safe log where “Remove”</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) IW verifies the safe log entry, then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM3: TEB # BB51184525 (Place on Cart)</td>
<td>N</td>
<td>8:31</td>
</tr>
<tr>
<td></td>
<td>HSM4: TEB # BB51184506 (Place on Cart)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM5E: TEB # BB51184524 (Check and Return)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laptop3: TEB # BB81420094 (Place on Cart)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laptop4: TEB # BB81420106 (Check and Return)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584394 (Place on Cart)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>KSK-2017: TEB # BB46584393 (Check and Return)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM3 Physical Keyboard Key: TEB # BB21907247 (Place on Cart)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# Close Safe #1 (Tier 6, Equipment Safe) Exit Tier 5 (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 and time, then signs the safe log where Close Safe is indicated. IW verifies the safe log entry then initials it.</td>
<td>E</td>
<td>18:31</td>
</tr>
<tr>
<td>20</td>
<td>SSC1 returns the safe log back to Safe #1 and locks it by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the &quot;WAIT&quot; light indicator is off.</td>
<td>E</td>
<td>18:32</td>
</tr>
<tr>
<td>21</td>
<td>CA, IW, and SSC1 leave the safe room with the cart, closing the door behind them.</td>
<td>N</td>
<td>18:33</td>
</tr>
</tbody>
</table>
# Act 2: Equipment Setup

The CA will set up the equipment by performing the following steps:

- Boot the laptop using the OS DVD (the laptop has no permanent storage device)
- Set up the printer
- Verify the laptop date and time
- Connect the HSMFD
- Start the log sessions
- Power ON the HSVI (Tier 7)

## Laptop Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 1    | CA performs the following steps to prepare the listed equipment:  
  a) Remove all equipment TEBs from the cart and place them on the ceremony table.  
  b) Inspect each equipment TEB for tamper evidence.  
  c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used.  
  d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.  
  
  HSM4: TEB # BB51184506 / Serial # H1411011  
  Last Verified: KSK37 2019-05-16  
  Laptop3: TEB # BB81420094 / Service Tag # J8SVSG2  
  Last Verified: KSK35 2019-11-15  
  OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584394  
  Last Verified: KSK37 2019-05-16 | 🎯 | 10:25 |
| 2    | CA performs the following steps to confirm that no hard drive and battery are in the laptop:  
  a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty.  
  b) Open the latch on the left side of the laptop to confirm that the battery slot is empty. | 🎯 | 10:37 |
| 3    | CA performs the following steps to boot the laptop:  
  a) Connect the USB printer cable into the rear USB port of the laptop.  
  b) Connect the null modem cable into the serial port of the laptop.  
  c) Connect the external HDMI display cable.  
  d) Connect the power supply.  
  e) Immediately insert the OS DVD release coen-0.4.0[1] after the laptop power is switched ON. | 🎯 | 10:39 |
| 4    | CA verifies whether the external display works, then performs adjustments if necessary:  
  To change the font size of the terminal:  
  Click the View menu and select Zoom In or Zoom Out  
  To change the resolution of each screen:  
  Go to Applications > Settings > Display | 🎯 | 10:43 |
### OS DVD Checksum Verification

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
</table>
| 5    | CA uses the terminal window to execute the following steps:  
|      | a) Calculate the SHA-256 hash by executing:  
|      | `sha2wordlist[^2] < /dev/sr0`  
|      |  
|      | IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.  
|      | Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.  
| 5    | SHA-256 hash:  
|      | 8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f  
|      | PGP Words:  
|      | minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document  
|      | Note: The SHA-256 hash of the OS DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/39 |

### Printer Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
</table>
| 6    | CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page:  
|      | `configure-printer[^3]`  

### Date Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
</table>
| 7    | CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock.  
|      | If the date/time do not match, perform the following steps:  
|      | a) Execute `date -s "20191114 HH:MM:00"` to set the time.  
|      | where `HH` is two-digit hour, `MM` is two-digit minutes and `00` is zero seconds.  
|      | b) Execute `date` to confirm the date/time matches the clock.  

**Connect the HSMFD**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 8    | CA plugs the **Ceremony 37 HSMFD** into the USB slot, then performs the steps below:  
  a) Wait for the OS to recognize it.  
  b) Display the HSMFD contents to all participants.  
  c) Close the file system window. | SML | 18:48 |
| 9    | CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD:  
  ```bash
  hsmfd-hash[4] -c
  ```  
  IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 37 annotated script.  
  Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script. | SML | 18:49 |

**Distribute Previous HSMFD**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>CA gives the unused <strong>HSMFD 37</strong> and the sheet of paper with the printed HSMFD hash to RKOS.</td>
<td>SRL</td>
<td>18:49</td>
</tr>
</tbody>
</table>

**Start the Terminal Session Logging**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 11   | CA executes the command below using the terminal window to change the working directory to HSMFD:  
  ```bash
  cd /media/HSMFD
  ``` | SRL | 18:49 |
| 12   | CA executes the command below to log activities of the **Commands** terminal window:  
  ```bash
  script script-20191114.log
  ``` | SRL | 18:50 |
**Start the HSM Activity Logging**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 13   | CA performs the following steps using the HSM Output terminal window to capture the activity logs of the HSM:  
  a) Change the working directory to HSMFD by executing:  
    `cd /media/HSMFD`  
  b) Set the serial port baud rate by executing:  
    `stty -F /dev/ttyS0 115200`  
  c) Start logging the serial output by executing:  
    `ttyaudit` /dev/ttyS0  
  Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port. | SML | 18:51 |

**Power ON the HSM (Tier 7)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 14   | CA performs the following steps to prepare the HSM:  
  a) Plug the null modem cable into the serial port of the HSM.  
  b) Connect the power to the HSM, then switch it ON.  
  Note: Status information should appear on the HSM activity logging screen.  
  c) Scroll the logging screen up and locate the HSM serial number.  
  d) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom.  
  HSM4: Serial # H1411011  
  Note: The date and time on the HSM is not used as a reference for logging and timestamp. | SML | 18:50 |
Act 3: Activate HSM (Tier 7) and Generate Signatures

Using the korsigner application the CA takes the Key Signing Requests (KSRs) and generates the Signed Key Responses (SKRs) by performing the steps below.

- The CA activates the HSM using the TCRs' smartcards
- After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop
- The korsigner application uses the private key stored in the HSM to generate the SKR
- Note: The SKR contains the digital signatures of the ZSK slated to be used in the next quarter
- The CA then prints the signer log, backs up the newly created SKR, and deactivates the HSM

TCR Credentials Check

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 1    | The CA calls each of the COs listed below sequentially to perform the following steps:  
  a) CO reads aloud the TEB number, then CA inspects it for tamper evidence.  
  b) CO and CA open the TEB, then the CA removes the plastic case containing the card(s).  
  c) CA opens the plastic case, then places the card(s) within on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table.  
  CO2: Anne-Marie Eklund Lowinder  
  OP TEB # BB46584404 ✔  
  SO TEB # BB46584403 ✔  
  CO4: Robert Stensstrom  
  OP TEB # BB46584402  
  SO TEB # BB46584401  
  CO5: Christopher Griffiths  
  OP TEB # BB46584400 ✔  
  SO TEB # BB46584399 ✔  
  CO6: Gaurab Upadhaya  
  OP TEB # BB46584398 ✔  
  SO TEB # BB46584397 ✔  

BLC 18:56
Enable/Activate the HSM (Tier 7)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 2    | CA performs the following steps to activate the HSM:  
      a) Utilize the HSM's keyboard to scroll through the menu using <>  
      b) Select "1.Set Online", press ENT to confirm.  
      c) When "Set Online?" is displayed, press ENT to confirm.  
      d) When "Insert Card OP #X?" is displayed, insert the OP card.  
      e) When "PIN?" is displayed, enter "11223344", then press ENT.  
      f) When "Remove Card?" is displayed, remove the OP card.  
      g) Repeat steps d) to f) for the 2nd and 3rd OP cards.  
      Confirm the "READY" LED on the HSM is ON.  
      IW records the cards that were used below. Each card is returned to its designated card holder after use.  
      1st OP card \( \frac{2}{7} \) of 7  
      2nd OP card \( \frac{5}{7} \) of 7  
      3rd OP card \( \frac{6}{7} \) of 7  
      Note: If the card is unreadable, gently wipe its metal contacts and try again. | SVN | 18:58 |

Check the Network Connectivity Between Laptop and HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>CA connects the HSM to the laptop using an ethernet cable in the LAN ports.</td>
<td>SK</td>
<td>18:59</td>
</tr>
</tbody>
</table>
| 4    | CA performs the following steps to test the network connectivity between laptop and HSM:  
      a) Use the Commands terminal window  
      b) Test connectivity by executing:  
         ping hsm\(^{[6]}\)  
         Ctrl + C  
      c) Wait for responses, then exit by pressing: | SR | 19:00 |

Insert the KSR FD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 5    | CA plugs the FD labeled "KSR" 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.  
      Note: The KSR FD was transferred to the facility by the RKOS. It contains 1 KSR. | SR | 19:01 |
November 13, 2019

To Whom It May Concern:

This is a letter of Verification of Employment for Trevor Lewis Davis. VeriSign, Inc. ("VeriSign") has employed Trevor Lewis Davis full-time since September 29th, 2014, currently as a Manager - CBO in our Production Operations organization.

VeriSign, a global provider of domain name registry services and internet infrastructure, enables internet navigation for many of the world’s most recognized domain names. VeriSign enables the security, stability, and resiliency of key internet infrastructure and services, including providing root zone maintainer services, operating two of the 13 global internet root servers, and providing registration services and authoritative resolution for the .com and .net top-level domains, which support the majority of global e-commerce. To learn more about what it means to be Powered by VeriSign, please visit Verisign.com.

For more than 21 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 153 million .com and .net domain names and processing more than 167 billion transactions daily-keeping the world connected online, seamlessly and securely. VeriSign is experienced in and provides support for both IPv6 and DNSSEC.

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
14 November 2019

The SHA256 hash of the 2020 Q1 KSR file is:

ksr-root-2020-q1-0.xml:

adc32b0107b522346e1076ee7b0c5da6d67cfc59f4eed4506d7a64450baf203f

The PGP wordlist for the hash above is:

**PGP Words:** ringbolt replica briefcase adviser ahead positive blockade confidence goldfish autopsy inverse universe kickoff article exceed paragon stockman informant wayside examine upshot universe steamship embezzle goggles infancy flytrap detector alone pharmacy bison customer

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.
ksrsigner-20191114-190143.log

Starting: ksrsigner /media/KSR/KSR39/ksr-root-2020-q1-0.xml (at Thu Nov 14 19:01:43 2019 UTC)
Use HSM /opt/dhsecxsec/asy.hmmconfig
New /opt/dhsecxsec/hmmconfig activated.
setenv KEYPER_LIBRARY_PATH="/opt/dhsec
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot-0
HSM Information:
  Label: ICANNKSK
  ManufacturerID: Ultra Electronics ASP Networks
  Model: Keyper 9860-2
  Serial: M411031

Validating last SKR with HSM...
1 2019-10-01T00:00:00 2019-10-22T00:00:00 59944,22545 20326(Klajeysy)/S
2 2019-10-11T00:00:00 2019-11-01T00:00:00 22545 20326(Klajeysy)/S
3 2019-10-21T00:00:00 2019-11-11T00:00:00 22545 20326(Klajeysy)/S
4 2019-10-31T00:00:00 2019-12-01T00:00:00 22545 20326(Klajeysy)/S
5 2019-11-10T00:00:00 2019-12-01T00:00:00 22545 20326(Klajeysy)/S
6 2019-11-20T00:00:00 2019-12-11T00:00:00 22545 20326(Klajeysy)/S
7 2019-12-10T00:00:00 2019-12-21T00:00:00 22545 20326(Klajeysy)/S
8 2019-12-20T00:00:00 2020-01-11T00:00:00 33853,22545 20326(Klajeysy)/S
9 2019-12-20T00:00:00 2020-01-11T00:00:00 33853,22545 20326(Klajeysy)/S

...VALIDATED.

Validate and Process SKR /media/LSR/KSR39/ksr-root-2020-q1-0.xml...
1 2020-01-01T00:00:00 2020-01-22T00:00:00 33853,22545
2 2020-01-11T00:00:00 2020-02-01T00:00:00 33853
3 2020-01-21T00:00:00 2020-02-11T00:00:00 33853
4 2020-01-31T00:00:00 2020-02-21T00:00:00 33853
5 2020-02-01T00:00:00 2020-03-01T00:00:00 33853
6 2020-02-20T00:00:00 2020-03-11T00:00:00 33853
7 2020-03-01T00:00:00 2020-03-21T00:00:00 33853
8 2020-03-11T00:00:00 2020-04-01T00:00:00 33853
9 2020-03-21T00:00:00 2020-04-11T00:00:00 46903,33853

...PASSED.

SHA256 hash of SKR:
563076377778d33a97ff77f5456e7c1731bf0aad02b7a01567d1c0ce2a5cd7726749d
>> rigbott replica briefcase adviser ahead positive blockade confidence goldfish autopsy inverse universe kickoff artic
>> exceed paragon stockman informant wayside examine upshot universe steamship embezzle goggles infancy flytrap detector a
> lone pharmacy bison customer <<

Reading SKR schedule "normal [2017]" from "kskschedule.json"
1 20326(Klajeysy)/S
2 20326(Klajeysy)/S
3 20326(Klajeysy)/S
4 20326(Klajeysy)/S
5 20326(Klajeysy)/S
6 20326(Klajeysy)/S
7 20326(Klajeysy)/S
8 20326(Klajeysy)/S
9 20326(Klajeysy)/S

Generated new SKR in /media/KSR/KSR39/ksr-root-2020-q1-0.xml
1 2020-01-01T00:00:00 2020-01-22T00:00:00 33853,22545 20326(Klajeysy)/S
2 2020-01-11T00:00:00 2020-02-01T00:00:00 33853
3 2020-01-21T00:00:00 2020-02-11T00:00:00 33853
4 2020-01-31T00:00:00 2020-02-21T00:00:00 33853
5 2020-02-01T00:00:00 2020-03-01T00:00:00 33853
6 2020-02-20T00:00:00 2020-03-11T00:00:00 33853
7 2020-03-01T00:00:00 2020-03-21T00:00:00 33853
8 2020-03-11T00:00:00 2020-04-01T00:00:00 33853
9 2020-03-21T00:00:00 2020-04-11T00:00:00 33853,49903

SHA256 hash of SKR:
563076377778d33a97ff77f5456e7c1731bf0aad02b7a01567d1c0ce2a5cd7726749d
>> mghead comando inverse consensus virus surrender cleanup supportive virus integrate eating escape guide becksel
> ler chatter lettheshead dogeled eximtice briefcase infancy absurd gravity involve scavenger spigot Atlantic brickyard san
dawood involve caretaker indoors congregate <<

Uploaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot-0
### Execute the KSR Signer for KSR 2020 Q1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 6    | CA executes the command below on the terminal window to sign the KSR file:  
ksrsigner[7] /media/KSR/KSK39/ksr-root-2020-q1-0.xml | SNL | 19:01 |
| 7    | When the KSR signer displays the prompt:  
**Activate ESM prior to accepting in the affirmative!! (y/N):**  
CA confirms that the HSM is online, then enters "y" to proceed. | SNL | 19:03 |

### Verify the KSR Hash for KSR 2020 Q1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 8    | When the hash of the KSR is displayed on the terminal window, perform the following:  
a) CA asks the Root Zone Maintainer (RZM) representative to identify themself in front of the room and provide documents for IW to review off camera for the purpose of authentication.  
b) IW retains the hash and PGP word list for KSR 2020 Q1, and employment verification letter provided by the RZM representative and writes their name on the following line:  

```
TREvor DAVIs
```

c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used. | SNR | 19:03 |
| 9    | Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks "are there any objections?" | SNR | 19:08 |
| 10   | CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in:  
/media/KSR/KSK39/ksr-root-2020-q1-0.xml | SNL | 19:08 |

### Print Copies of the KSR Signer log

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 11   | CA executes the commands below using the terminal window to print the KSR Signer log:  
a) `lpadmin -p HP -o copies-default=X`  
*Note: Replace "X" with the amount of copies needed for the participants.*  
b) `printlog[8] ksrsigner-201911*.log` | SNL | 19:05 |
| 12   | IW attaches a copy of the required ksrsigner log to their script. | SNL | 19:06 |
### Back up the Newly Created SKR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 13   | CA executes the following commands using the terminal window:  
   a) List the contents of the KSR FD by executing:
   ```bash
   ls -ltrR /media/KSR
   ```
   b) Copy the contents of the KSR FD to the HSMFD by executing:
   ```bash
   cp -pR /media/KSR/* .
   ```
   Note: Confirm overwrite by entering "y" if prompted.
   c) List the contents of the HSMFD to verify it has been copied successfully by executing:
   ```bash
   ls -ltrR
   ```
   d) Unmount the KSR FD by executing:
   ```bash
   umount /media/KSR
   ``` | SNL | 19:07 |
| 14   | CA removes the KSR FD containing the SKR files, then gives it to the RZM representative. | SNL | 19:07 |

### Disable/Deactivate the HSM (Tier 7)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 15   | CA utilizes the unused OP cards to deactivate the HSM:  
   a) CA displays the HSM activity logging terminal window  
   b) Utilize the HSM's keyboard to scroll through the menu using < >  
   c) Select "2.Set Offline", press ENT to confirm.  
   d) When "Set Offline?" is displayed, press ENT to confirm.  
   e) When "Insert Card OP #X?" is displayed, insert the OP card from the card holder.  
   f) When "PIN?" is displayed, enter "11223344", then press ENT.  
   g) When "Remove Card?" is displayed, remove the OP card.  
   h) Repeat steps e) to g) for the 2nd and 3rd OP cards.  
   Confirm the "READY" LED on the HSM is OFF.  
   IW records the cards that were used below. Each card is returned to its designated card holder after use.  
   1st OP card _6_ of 7  
   2nd OP card _5_ of 7  
   3rd OP card _2_ of 7  
   Note: If the card is unreadable, gently wipe its metal contacts and try again. | SNL | 19:09 |
## Place the HSM (Tier 7) into a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. <strong>Note:</strong> DO NOT unplug the cable connections on the laptop.</td>
<td>JL</td>
<td>19:10</td>
</tr>
<tr>
<td>17</td>
<td>CA places the HSM into a prepared TEB, then seals it.</td>
<td>JL</td>
<td>19:11</td>
</tr>
</tbody>
</table>
| 18   | CA performs the following steps:  
   a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.  
   b) Confirm with IW that the TEB number and HSM serial number match below.  
   c) Initial the TEB along with IW using a ballpoint pen.  
   d) Give IW the sealing strips for post-ceremony inventory.  
   e) Place the HSM TEB on the cart.  | SM | 19:12 |

**HSM4: TEB # BB51184226 / Serial # H1411011**
Act 4: Zeroize and Dismantle Hardware Security Module

To conclude its period of service, the HSM will be zeroized and have its critical components removed and securely destroyed.

- CA will generate temporary CO cards
- CA will remove all keys from the HSM
- CA will destroy temporary CO cards
- CA will zeroize the HSM
- CA will intentionally tamper the HSM
- CA will dismantle the HSM and extract its critical components
- CA will place the components into a TEB in preparation for offsite secure destruction

Remove the HSM from TEB and Power On

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CA selects the HSM Output terminal window.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2    | CA performs the following steps to prepare the HSM:  
   a) Remove the TEB from the cart and place it on the ceremony table.  
   b) Inspect the TEB for tamper evidence.  
   c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used.  
   d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.  
   e) Plug the null modem cable into the serial port of the HSM.  
   f) Connect the power to the HSM, then switch it ON.  
   Note: Status information should appear on the HSM activity logging screen.  
   g) Scroll the logging screen up and locate the HSM serial number.  
   h) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. |          |       |

HSM3: TEB # BB51184525 / Serial # H1403032
Last Verified: KSK37 2019-05-16
Note: The date and time on the HSM is not used as a reference for logging and timestamp.
### Issue Temporary Crypto Officer (CO) Cards

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>CA performs the following steps, ensuring that three cards from only one of the two SO card sets are used to issue Crypto Officer (CO) cards</td>
<td></td>
<td>19:19</td>
</tr>
<tr>
<td></td>
<td>a) Utilize the HSM's keyboard to scroll through the menu using &lt;&gt;</td>
<td>SR</td>
<td>19:19</td>
</tr>
<tr>
<td></td>
<td>b) Select &quot;7. Role Mgmt&quot;, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) When &quot;Insert Card SO #X?&quot; is displayed, insert the SO card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) When &quot;PIN?&quot; is displayed, enter &quot;11223344&quot;, then press ENT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) When &quot;Remove Card?&quot; is displayed, remove the SO card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) Repeat steps c) to e) for the 2nd and 3rd SO card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) Select &quot;1. Issue Cards&quot;, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) Select &quot;1. Issue CO Cards&quot;, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) When &quot;Issue CO Cards?&quot; is displayed, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>j) When &quot;Num Cards?&quot; is displayed, enter &quot;2&quot;, then press ENT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>k) When &quot;Num Req Cards?&quot; is displayed, enter &quot;2&quot;, then press ENT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>l) When &quot;Insert Card #X?&quot; is displayed, insert the required CO card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>m) When &quot;PIN?&quot; is displayed, enter &quot;11223344&quot;, then press ENT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n) When &quot;Remove Card?&quot; is displayed, remove the CO card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>o) Repeat steps l) to n) for the 2nd CO card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>p) When &quot;CO Cards Issued&quot; is displayed, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>q) Press CLR twice to return to the &quot;Secured&quot; menu.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IW records the cards used below. Each card is placed on the card holder that is visible to everyone.

<table>
<thead>
<tr>
<th>Set #</th>
<th>1st SO card</th>
<th>2nd SO card</th>
<th>3rd SO card</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2 of 7</td>
<td>5 of 7</td>
<td>6 of 7</td>
</tr>
</tbody>
</table>

Note: If the card is unreadable, gently wipe its metal contacts and try again.
List and Delete the KSK(s) present in the HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 4    | CA performs the following steps to list the KSK(s) present in the HSM:  
   a) Utilize the HSM’s keyboard to scroll through the menu using < >  
   b) Select "5.Key Mgmt", press ENT to confirm.  
   c) When "Insert CO Card #X?" is displayed, insert the CO card.  
   d) When "PIN?" is displayed, enter "11223344", then press ENT.  
   e) When "Remove Card?" is displayed, remove the CO card.  
   f) Repeat steps a) to e) for the 2nd CO card.  
   g) Select "2.Key Details", press ENT to confirm.  
   h) When "List Keys?" is displayed, press ENT.  
   i) Select "1.Key Summary", press ENT to confirm.  
   j) When "Key Summary?" is displayed, press ENT. | SR | 19:31 |

Each card is returned to its designated card holder after use.  
**Note:** If the card is unreadable, gently wipe its metal contacts and try again.

| 5    | CA matches the displayed KSK label(s) in the HSM Output terminal window.  
   **KSK-2017: Klajeyz** | SR | 19:31 |

| 6    | CA performs the following steps to delete the KSK(s) from the HSM:  
   a) Utilize the HSM's keyboard to scroll through the menu using < >  
   b) Select "3.App Keys" from the same menu "Key Mgmt", press ENT to confirm.  
   c) Select "7.Erase App Key", press ENT to confirm.  
   d) When "Erase App Keys?" is displayed, press ENT to confirm.  
   e) Select "1.All Keys", press ENT to confirm.  
   f) The Klajeyz key(s) will be selected in the HSM's display with a visible (*) asterisk. Press ENT to confirm. **There is no system confirmation prompt.**  
   g) When Done is displayed, press ENT to return to the App Key Menu.  
   h) Press CLR to return to the Key Mgmt menu. | SR | 19:31 |

| 7    | CA performs the following steps to list the KSK(s) from the HSM:  
   a) Utilize the HSM's keyboard to scroll through the menu using < >  
   b) Select "2.Key Details", press ENT to confirm.  
   c) When "List Keys?" is displayed, press ENT.  
   d) Select "1.Key Summary", press ENT to confirm.  
   e) When "Key Summary?" is displayed, press ENT.  
   f) Press CLR to return to the menu "Secured". | SR | 19:31 |

CA confirms that KSK-2017: Klajeyz has been deleted.
## Root DNSSEC Script Exception

### Exception Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW writes the details of the ceremony exception:</td>
<td>SK</td>
<td>19:28</td>
</tr>
<tr>
<td></td>
<td>Act: 4  Step(s): 8(K) Page(s): 31</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date and Time: 2019/11/14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IW describes the exception(s) and action(s) below.</td>
<td>GM</td>
<td>19:28</td>
</tr>
</tbody>
</table>

8K WAS NOT NEEDED
### Clear and Destroy CO Cards

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 8    | CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to clear Crypto Officer (CO) cards:  
   a) Utilize the HSM’s keyboard to scroll through the menu using <->  
   b) Select "7. Role Mgmt", press ENT to confirm.  
   c) When "Insert Card SO #X?" is displayed, insert the SO card.  
   d) When "PIN?" is displayed, enter "11223344", then press ENT.  
   e) When "Remove Card?" is displayed, remove the SO card.  
   f) Repeat steps c) to e) for the 2nd and 3rd SO card.  
   g) Select "4. Clear RoleCard", press ENT to confirm.  
   h) When "Clear Card?" is displayed, press ENT to confirm.  
   i) When "Num Cards?" is displayed, enter "2", then press ENT.  
   j) When "Insert Card #X?" is displayed, take the required CO #X card from the cardholder, show the CO #X card to the audit camera and then insert the CO #X card into the HSM’s card reader.  
   k) When "Are you sure?" is displayed, press ENT to confirm.  
   l) When "PIN?" is displayed, enter "11223344", then press ENT.  
   m) When "Remove Card?" is displayed, remove the CO card.  
   n) Repeat steps j) to m) for the 2nd CO card.  
   o) Press CLR to return to the main menu "Secured".  
   
IW records the cards that were used below. Each card is returned to its designated card holder after use.  
Set #1  
1st SO card 2 of 7  
2nd SO card 5 of 7  
3rd SO card 6 of 7  

Note: If the card is unreadable, gently wipe its metal contacts and try again. |
| 9    | CA uses the shredder to destroy the cleared CO cards. Use scissors to slice through the center of the chip before inserting cards into the shredder. |  |  |
## Unsecure and Tamper the HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 10   | CA performs the following steps to return the HSM to its **Unsecure** factory default state. This will erase all keys, settings, and configuration.  
   a) Utilize the HSM's keyboard to scroll through the menu using <->  
   b) Select "6.HSM Mgmt", press ENT to confirm.  
   c) When "Insert Card SO #X?" is displayed, insert the SO card.  
   d) When "PIN?" is displayed, enter "11223344", then press ENT.  
   e) When "Remove Card?" is displayed, remove the SO card.  
   f) Repeat steps c) to e) for the 2nd and 3rd SO card.  
   g) Select '5.Unsecure", press ENT to confirm.  
   h) When "Unsecure?" is displayed, then press ENT.  
|      | It may take a few minutes for the HSM to restart after the zeroization is complete. The HSM will reboot into the "Unsecured State" and after the completion of the HSM self test the display should show "Important Read Manual" indicating the HSM is in the initialized state.  
|      | IW records the cards used below. Each card is placed on the card holder that is visible to everyone.  
|      | Set # _2_  
|      | 1st SO card _2_ of 7  
|      | 2nd SO card _5_ of 7  
|      | 3rd SO card _6_ of 7  
|      | Note: If the card is unreadable, gently wipe its metal contacts and try again.  
| 11   | CA performs the following steps to tamper the HSM equipment listed below:  
|      | a) Using Tool B, press and hold the recessed button on the rear panel of the HSM located between the LAN and serial ports, then release it after 10 seconds to activate the tampering mechanism. **IMK missing recovery mode** will be displayed on the HSM.  
|      | b) Turn OFF the HSM using the rocker switch on the rear panel. Turn ON the HSM with the same switch and wait until the ALERT LED light is ON and **IMK missing recovery mode** is displayed to verify the tampered state.  
|      | c) Disconnect the power from the HSM.  

Open the HSM Case and Remove the Logic Board from HSM3

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>IW reads steps 13 to 16 while the CA dismantles HSM3: Serial # H1403032.</td>
<td>3R</td>
<td>19:20</td>
</tr>
<tr>
<td></td>
<td>CA performs the following steps to access the HSM's critical components:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Using Tool A+Bit 2, remove the two screws which secure the serial port to the rear panel.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Using Tool A+Bit 1, remove the four screws from the rear panel of the case which secure the shell.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Using Tool A+Bit 1, remove the four screws from the bottom of the case which secure the shell.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Using Tool C, slice the tamper stickers on the bottom of the case along the seam with the shell.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Slide the shell toward the back of the case to remove it and place it in the HSM Parts bin on the ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) Using Tool A+Bit 3, remove the two logic board screws nearest to the front panel which secure the plastic logic board cover.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) Remove the plastic logic board cover and place it in the HSM Parts bin on the ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) Using Tool A+Bit 3, remove the two remaining screws which secure the logic board near the rear panel.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Detach the four cables from the front of the logic board. Open the latches outward to release each of the ribbon cables.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>j) Using Tool A+Bit 4, remove the nut from the cryptographic module securing the ring terminal of the green/yellow wire and slide the ring terminal off of the threaded stud.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>k) Detach the cable from each side of the cryptographic module connecting it to the logic board.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>2R</td>
<td>19:41</td>
</tr>
<tr>
<td>14</td>
<td>CA performs the following steps to remove the logic board and batteries:</td>
<td>2R</td>
<td>19:43</td>
</tr>
<tr>
<td></td>
<td>a) Separate the logic board from the HSM case by pulling the logic board up then toward the front of the case.</td>
<td>2R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Using Tool D, cut the battery terminals that connect the batteries to the logic board.</td>
<td>2R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Pry the batteries from the logic board by placing the logic board flat on the table and pulling up on each battery with sufficient force to break the adhesive bond.</td>
<td>2R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Place the batteries in the HSM Parts bin on the ceremony table.</td>
<td>2R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Place the logic board in the Critical Parts bin on the ceremony table.</td>
<td>2R</td>
<td></td>
</tr>
</tbody>
</table>
## Remove Cryptographic Module and Card Reader from HSM3

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 15   | CA performs the following steps to remove the cryptographic module:  
✓ a) Using Tool A+Bit 4, remove the 4 nuts which secure the cryptographic module to the case. 
✓ b) Lift the cryptographic module up to separate it from the case. 
✓ c) Using Tool C, remove both connectors from the cryptographic module as flush with the case as possible. 
✓ d) Place the cryptographic module in the Critical Parts bin, and the connectors in the HSM Parts bin on the ceremony table. | SM       | 17:45  |
| 16   | CA performs the following steps to remove the front panel and card reader:  
✓ a) Using Tool A+Bit 4, remove the 4 nuts which secure the front panel to the bottom of the case. 
✓ b) Place the front panel in the HSM Parts bin on the ceremony table. 
✓ c) Using Tool A+Bit 4, remove the nut which secures the card reader. 
✓ d) Using Tool A+Bit 3, remove the 3 screws which secure the card reader. 
✓ e) Lift the card reader up to separate it from the case and place it with the ribbon cable in the Critical Parts bin on the ceremony table. 
✓ f) Place the HSM case in the HSM Parts bin on the ceremony table. | SR       | 19:47  |

## Place the Critical HSM3 parts into a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 17   | CA places the container with the following critical parts into a prepared TEB, then seals it.  
   a) Cryptographic Module  
   b) Logic Board  
   c) Card Reader | LK       | 19:49  |

**Note:** The HSM case will not be destroyed.

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 18   | CA performs the following steps:  
   a) Read aloud the TEB number, then show it to the audit camera above for participants to see.  
   b) Confirm with IW that the TEB number matches below.  
   c) Initial the TEB along with IW using a ballpoint pen.  
   d) Give IW the sealing strips for post-ceremony inventory.  
   e) Give RKOS the TEB for destruction. | LK       | 19:50  |

**HSM3: TEB # BB81420110**
## Retire HSM Physical Keyboard Key

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 19   | CA performs the following steps to retire the listed HSM Physical Keyboard Key:  
      a) Remove the TEB from the cart.  
      b) Inspect TEB for tamper evidence.  
      c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used.  
      d) Remove and discard the TEB.  
      e) RKOS will take possession of the HSM Physical Keyboard Key and place in its designated area. | 8P | 19:53 |

**HSM3 Physical Keyboard Key: TEB # BB21907247**  
**Last Verified: AT21 2015-03-19**
Act 5: Secure Hardware

The CA will secure the ceremony hardware by performing the steps below:

- Back up the HSMFD contents
- Print log information
- Place the equipment and TCR credentials inside of TEBs
- Along with IW, escort SSC1 and equipment cart into Tier 5 (Safe Room) to return equipment to Safe #1
- Along with IW, escort SSC2 and TCRs into Tier 5 (Safe Room) to return TCRs' smartcards to Safe #2.

Stop logging the Serial Output and the Terminal Session

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 1    | CA performs the following steps to stop logging:  
   a) Disconnect the null modem and ethernet cables from the laptop.  
   b) Perform the following steps using the HSM Output terminal window to stop logging the serial output (ttyaudit):  
      i) Press Ctrl + C  
      ii) Execute exit  
   c) Execute the command below using the Commands terminal window to stop logging the terminal session:  
      exit  
   Note: The Commands terminal session window will remain open. |  |  | 19:54 |
# find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist

SHA-256: 51368713ada52cdeaf1f0c9ab34d1b30c9422bc6f8e46d6467e85db2128deeb6b
PGP Words: drunken congregate Neptune barbecue ringbolt pandemic Burbank unify Trojan businessman ammo newsletter scallion disruptive beeswax commando spaniel December showgirl hemisphere orca detergent stockman detergent locale leprosy suspense Camelot breadline telephone trouble Hamilton
## Prepare blank FDs and back up the HSMFD Contents

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>CA executes the command below using the terminal window to enable copying of all content from the HSMFD: <code>shopt -s dotglob</code></td>
<td>5L</td>
<td>19:55</td>
</tr>
</tbody>
</table>
| 3    | CA executes the following command twice using the terminal window to print 2 copies of the hash for the HSMFD content: `hsmfd-hash[^1] -p`  
Note: One copy for audit bundle and one copy for HSMFD package. | 5L      | 19:56|
| 4    | CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrxR` | 5L      | 19:56|
| 5    | CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs: `mkdir /media/HSMFD1` | 5L      | 19:56|
| 6    | CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it. | 5L      | 19:57|
| 7    | CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: `df` | 5L      | 19:57|
| 8    | CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD:  
   a) `umount /dev/sdcl`  
   b) `mkfs.vfat -n HSMFD /dev/sdcl`  
   c) `mount /dev/sdcl /media/HSMFD1`  
   d) `cp -pR * /media/HSMFD1` | 5L      | 19:58|
| 9    | CA executes the commands below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy, then unmounts the flash drive before removal:  
   a) `hsmfd-hash[^1] -m`  
   b) `umount /media/HSMFD1` | 5L      | 19:59|
| 10   | CA removes the HSMFD copy, then places it on the holder.  
   Wait for the activity light on the backup HSMFD to stop flashing before removal. | 5L      | 19:59|
| 11   | CA repeats step 6 to 10 for the 2nd copy.  
   Wait for the activity light on the backup HSMFD to stop flashing before executing each step. | 5L      | 20:00|
| 12   | CA repeats step 6 to 10 for the 3rd copy.  
   Wait for the activity light on the backup HSMFD to stop flashing before executing each step. | 5L      | 20:01|
| 13   | CA repeats step 6 to 10 for the 4th copy.  
   Wait for the activity light on the backup HSMFD to stop flashing before executing each step. | 5L      | 20:02|
| 14   | CA repeats step 6 to 10 for the 5th copy.  
   Wait for the activity light on the backup HSMFD to stop flashing before executing each step. | 5L      | 20:03|
Script started on Thu Nov 14 18:50:02 2019
root@conen:media/HSMPD# ping hsmp
PING hsmp (192.168.0.2) 56 bytes of data.
64 bytes from hsmp (192.168.0.2): icmp_seq=1 ttl=255 time=0.433 ms
64 bytes from hsmp (192.168.0.2): icmp_seq=2 ttl=255 time=0.579 ms
64 bytes from hsmp (192.168.0.2): icmp_seq=3 ttl=255 time=0.721 ms
--- hsmp ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 0.433/0.567/0.721/0.150 ms

root@conen:media/HSMPD# ksergner /media/KSER/KSK39/kser-root-2020-ql-0.xml
Starting ksergner /media/KSER/KSK39/kser-root-2020-ql-0.xml 14 Oct 2019
10:01:43 UTC
Use DSM /opt/dnssec/aep-hsmconfig.py
Activate DSM prior to accepting in the affirmative!!
[y/N]: y

DSM /opt/dnssec/aep-hsmconfig activated.
debag setenv KEYSER/LibraryPath /opt/dnssec
debag setenv PCIeSSLPath /opt/KerberosPcEsslPath
[pcsk11+lib/gnu/g4_1_2_glib/c_2_x86_64.so]c 0.5.0

Found 1 slots on DSM /opt/KerberosPcEsslPath/pcsk11+lib/gnu/g4_1_2_glib/c_2_x86_64.so.c 0.5.0

DSM slot 0 included
Load /opt/KerberosPcEsslPath/pcsk11+lib/gnu/g4_1_2_glib/c_2_x86_64.so.c 0.5.0 Slot 0

DSM Information:
Label: ICANW4RK
ManufacturerID: Ultra Electronics AFM Networks
Model: Kerberos K860-2
Serial: HU113101

Validating last SKR with DSM...

# Inception Expiration ZSK Tags KSK Tag (CRA_LABEL)
1 2019-10-01T00:00:00 2020-10-22T00:00:00 SHA256 (Keja) /S
2 2019-10-11T00:00:00 2020-11-03T00:00:00 SHA256 (Keja) /S
3 2019-10-21T00:00:00 2020-11-03T00:00:00 SHA256 (Keja) /S
4 2019-10-31T00:00:00 2020-12-03T00:00:00 SHA256 (Keja) /S
5 2019-11-10T00:00:00 2020-12-03T00:00:00 SHA256 (Keja) /S
6 2019-11-20T00:00:00 2020-12-31T00:00:00 SHA256 (Keja) /S
7 2019-11-30T00:00:00 2020-12-31T00:00:00 SHA256 (Keja) /S
8 2019-12-10T00:00:00 2020-12-31T00:00:00 SHA256 (Keja) /S
9 2019-12-20T00:00:00 2020-01-03T00:00:00 SHA256 (Keja) /S
10 2019-12-30T00:00:00 2020-01-03T00:00:00 SHA256 (Keja) /S

Validate Process DSM /media/KSER/KSK39/kser-root-2020-ql-0.xml...

# Inception Expiration ZSK Tags KSK Tag (CRA_LABEL)
1 2019-10-01T00:00:00 2020-10-22T00:00:00 SHA256 (Keja) /S
2 2019-10-11T00:00:00 2020-11-03T00:00:00 SHA256 (Keja) /S
3 2019-10-21T00:00:00 2020-11-03T00:00:00 SHA256 (Keja) /S
4 2019-10-31T00:00:00 2020-12-03T00:00:00 SHA256 (Keja) /S
5 2019-11-10T00:00:00 2020-12-03T00:00:00 SHA256 (Keja) /S
6 2019-11-20T00:00:00 2020-12-31T00:00:00 SHA256 (Keja) /S
7 2019-11-30T00:00:00 2020-12-31T00:00:00 SHA256 (Keja) /S
8 2019-12-10T00:00:00 2020-12-31T00:00:00 SHA256 (Keja) /S
9 2019-12-20T00:00:00 2020-01-03T00:00:00 SHA256 (Keja) /S
10 2019-12-30T00:00:00 2020-01-03T00:00:00 SHA256 (Keja) /S

...VALIDATED.

Successfully processed SKR...
script-20191114.log

-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Apr 11 2018 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 19 2017 sksxml 201711141932400
-rw-r--r-- 1 root root 24928 Oct 19 2017 sksxml 201710161931150

./KSS31-3-c_to_c:

total 112
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 19556 Oct 13 2017 kar-root-2018-q-3-e_to_c.xml
-rw-r--r-- 1 root root 1344 Apr 11 2018 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 19 2017 sksxml 201711141932400
-rw-r--r-- 1 root root 24928 Oct 19 2017 sksxml 201710161931150

./KSS31-3-b_to_c:

total 104
-rw-r--r-- 1 root root 24928 Apr 20 2017 skr.xml 20170427183953
-rw-r--r-- 1 root root 19556 Apr 20 2017 kar-root-2017-q-3-o_to_d.xml
-rw-r--r-- 1 root root 1344 Apr 20 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Apr 27 2017 skr.xml 20170427183953
-rw-r--r-- 1 root root 1344 Apr 27 2017 skrschedule.json

./KSS29-0-c_to_d:

total 104
-rw-r--r-- 1 root root 24928 Apr 20 2017 skr.xml 20170427183953
-rw-r--r-- 1 root root 19556 Apr 20 2017 kar-root-2017-q-2-e_to_c.xml
-rw-r--r-- 1 root root 1344 Apr 20 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Apr 27 2017 skr.xml 20170427183953
-rw-r--r-- 1 root root 24928 Apr 27 2017 skr.xml 20170427183953

./KSS29-2_c_to_c:

total 104
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150

./KSS31-1-c_to_d:

total 128
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 19556 Oct 13 2017 kar-root-2018-q-3-e_to_c.xml
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150

./KSS31-2-c_to_d:

total 128
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150

./KSS31-1-c_to_c:

total 128
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150

./KSS31-2_c_to_c:

total 128
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150

./KSS31-0-c_to_d:

total 128
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150

./KSS31-1-c_to_d:

total 128
-rw-r--r-- 1 root root 24928 Oct 13 2017 skr.xml 201710161931150
-rw-r--r-- 1 root root 1344 Oct 13 2017 skrschedule.json
-rw-r--r-- 1 root root 24928 Oct 18 2017 skr.xml 201710161931150
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 TcplListener: Created IPv6 socket 16 on port 5000.</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 Audit on 14/11/2019 17:32:58 00100002</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 TcplListener: Accepted connection on socket 14 from address 192.168.0.1.</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 TcplListener: Accepted connection on socket 17 from address 192.168.0.1.</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 TcplListener: Closed IPv6 socket 15 on port 5000.</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 TcplListener: Closed IPv6 socket 16 on port 5000.</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 Audit on 14/11/2019 17:44:10 00100003</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 H19403032 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 BBL CRC32: 0x7575754CA</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 Running applicationBootLoader at 0xEFDC0000</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 H19403032 011403 ABL 011 : Tamper Challenge Response Key</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 ABL CRC32: 0x27E0FAA</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0</td>
</tr>
<tr>
<td>2019-11-14T18:58:31+0000</td>
<td>ttyS0 <em>encoded text</em></td>
</tr>
</tbody>
</table>
Current Tamper Counts (decimal 0-255):

- vinoosTamperCount: 0
- vinoosTamperCount: 49
- vbboosTamperCount: 0
- mnsrtempTamperCount: 0
- mnsrtempTamperCount: 0
- meshTamperCount: 0
- extampSMKTamperCount: 0
- extampIMKTamperCount: 0
- tempdiffTamperCount: 0
- pFTamperCount: 49
- restartTamperCount: 157

Current tamper bitmaps:

- currentTamper bitmap: 0x0000 0b .... .... ....
- lastTamper bitmap: 0x0000 0b .... 1.... | EXT_POWER_DOWN

Bitmapped Change Record (most recent first):

- Running cryptoApplication at 0xEBF00000
- Jumping to startup & 0x001037B4
- board is F2020D8
- board_smp_init: 2 cpu
ttyS0: Running RandomGen POST Test
2019-11-14T19:14:20+0000
ttyS0: RandomGen POST Test Passed
2019-11-14T19:14:20+0000
ttyS0: Running RSA POST Test
2019-11-14T19:14:20+0000
ttyS0: RSA POST Test Passed
2019-11-14T19:14:20+0000
ttyS0: Running ECC POST Test
2019-11-14T19:14:20+0000
ttyS0: ECC POST Test Passed
2019-11-14T19:14:20+0000
ttyS0: Audit on 14/11/2019 17:42:59 00100008
2019-11-14T19:14:20+0000
ttyS0: Keyper 9860-2 Serial Number H1403032
2019-11-14T19:14:20+0000
ttyS0: Memory Usage:
2019-11-14T19:14:20+0000
ttyS0: RAM (free/total) 197Mb/256Mb
2019-11-14T19:14:20+0000
ttyS0: Flash (free/total) 127Mb/128Mb
2019-11-14T19:14:20+0000
ttyS0: black store 400b
2019-11-14T19:14:20+0000
ttyS0: statistics 112b
2019-11-14T19:14:20+0000
ttyS0: other 116b
2019-11-14T19:14:20+0000
ttyS0: fwdStore (free/total) 109Kb/128Kb
2019-11-14T19:14:20+0000
ttyS0: Network Configuration:
2019-11-14T19:14:20+0000
ttyS0: IPv4: enabled
2019-11-14T19:14:20+0000
ttyS0: IPv6: enabled
2019-11-14T19:14:20+0000
ttyS0: MAC/IP address(es): 00:EO:06:CO:B2:3D / 192.168.0.24 , 2001::2e0:6ff:feee:0000b3d/64
2019-11-14T19:14:20+0000
ttyS0: DSM Port: 05000
2019-11-14T19:14:20+0000
ttyS0: DSM Gateway(s): 0.0.0.0 ::
2019-11-14T19:14:20+0000
ttyS0: Software Versions:
Klajeyz, RSA, FIPS, 2045, wt, atednu

Dumping HSM Key Summary

RSA, 2046, Private, 1

Audit on 14/11/2019 17:50:40 00200068

No keys present!

Audit on 14/11/2019 17:52:18 00400023 00600000C8A2156D
Audit on 14/11/2019 17:52:43 00200023 00600002788F156D
Audit on 14/11/2019 17:53:03 00200023 00600002998F156D
Audit on 14/11/2019 17:54:58 00200070 38800000D5B3276
Audit on 14/11/2019 17:56:11 00200070 3880000058E32976
Audit on 14/11/2019 17:59:37 00200023 00600002ACF156D
Audit on 14/11/2019 17:59:56 00200023 006000028CF156D
Audit on 14/11/2019 13:00:15 00200023 00600002A50F156D
Audit on 14/11/2019 18:00:44 0000001f

Shutting down daemons...

AuditBuffer rw'd [-l] (3)

shutting down audit service.

Terminated

netListener::accept() : No such process

Shutting down filesystems...

NetEnv013032 011397 BSL 010 : Factory Software Verification Key : CPLD version 1.9

BSL CRC32: 0x757574CA

Running application BootLoader at 0x5FDC0000

NetEnv013032 011403 BSL 011 : Tamper Challenge Response Key

BSL CRC32: 0x750FA6A

# # ABL tamper records # #

Current Tamper Counts (decimal 0-255):

+---------------------------------------+
| Name                        | Value |
+---------------------------------------+
| ext.oosTamperCount           | 0     |
| vint.oosTamperCount           | 0     |
| vbiosTamperCount              | 0     |
| mixstrtempTamperCount         | 0     |
| minstrtempTamperCount         | 0     |
| mshTamperCount                | 0     |
| e2temp2KTempTamperCount       | 0     |
| extamp2KTempTamperCount       | 0     |
| extamp2KTempTamperCount       | 0     |
+---------------------------------------+
ttyaudit ttyS0 20191114-185111.log

2019-11-14 T19:32:44+0000
ttyS0 tempdiffTamperCount:  0
2019-11-14 T19:32:44+0000
ttyS0 pTamperCount:  49
2019-11-14 T19:32:44+0000
ttyS0 restartTamperCount:  157
2019-11-14 T19:32:44+0000
ttyS0 Current tamper bitmaps:
2019-11-14 T19:32:44+0000
ttyS0
2019-11-14 T19:32:44+0000
ttyS0 currentTamper bitmap: 0x0000 0b .... .... .... ....
2019-11-14 T19:32:44+0000
ttyS0 lastTamper bitmap: 0x0800 0b .... 1... .... |EXT_POWER_DOWN

2019-11-14 T19:32:44+0000
ttyS0 Bitmapped Change Record (most recent first):
2019-11-14 T19:32:44+0000
ttyS0
2019-11-14 T19:32:44+0000
ttyS0 Running cryptoApplication at 0x3BF00000
2019-11-14 T19:32:45+0000
ttyS0 Jumping to startup 0x00013784
2019-11-14 T19:32:45+0000
ttyS0 Board is P2020BN
2019-11-14 T19:32:45+0000
ttyS0 board_smp_init: 2 cpu
2019-11-14 T19:32:45+0000
ttyS0
2019-11-14 T19:32:45+0000
ttyS0 Cpu_clk=10000000000, Sys_clk=100000000, CCS=5000000000
2019-11-14 T19:32:46+0000
ttyS0
2019-11-14 T19:32:46+0000
ttyS0 System page at phys:0000b000 user:0000b000 kern:0000b000
2019-11-14 T19:32:46+0000
ttyS0 Starting next program at v001513c
2019-11-14 T19:32:46+0000
ttyS0 Starting R-Series Kernel
2019-11-14 T19:32:46+0000
ttyS0 Copyright AFG Networks Ltd. All Rights Reserved.
2019-11-14 T19:32:46+0000
ttyS0
2019-11-14 T19:32:46+0000
ttyS0 Thu Nov 14 18:01:26 2019
2019-11-14 T19:32:46+0000
ttyS0 Starting auditd v2.0 ... started.
2019-11-14 T19:32:46+0000
ttyS0 Interface 0 configured for IPv6.
2019-11-14 T19:32:46+0000
ttyS0 Interface 0 configured for IPv4.
2019-11-14 T19:32:47+0000
ttyS0 route: writing to routing socket: Network is unreachable
2019-11-14 T19:32:48+0000
ttyS0 add net default: gateway :: Network is unreachable
ttyS0: writing to routing socket: Network is unreachable

ttyS0: and net default: gateway 0.0.0.0: Network is unreachable

Starting USB driver...

9160 v2.3 Keyper Application - Nov 8 2013 13:17:33

Running DES POST Test
DES POST Test Passed

Running Triple DES POST Test
Triple DES POST Test Passed

Running AES POST Test
AES POST Test Passed

Running SHA1 POST Test
SHA1 POST Test Passed

Running SHA2 POST Test
SHA2 POST Test Passed

Running RandomGen POST Test
RandomGen POST Test Passed

Running RSA POST Test
RSA POST Test Passed

Running DSA POST Test
DSA POST Test Passed

Running ECC POST Test
ECC POST Test Passed

Keyper 9160-2 Serial Number H1403032
ttyaud-ttyS0-20191114-185111.log

Memory Usage:

ttyS0  Memory Usage:

ttyS0  RAM (free/total)  197Mb/256Mb

ttyS0  Flash (free/total)  127Mb/128Mb

ttyS0  black store  44b

ttyS0  statistics  112b

ttyS0  other  116b

ttyS0  Redisstore (free/total)  109Kb/128Kb

ttyS0  Network Configuration:

ttyS0  IPv4: enabled

ttyS0  IPv6: enabled

ttyS0  MAC/IP address (en): 00:20:06:C0:B2:3D / 192.168.0.2/24 , 2001::2c0:6ff:fe00:b3d/64

ttyS0  DNS Port: 05000

ttyS0  DNS Gateway: 0.0.0.0

ttyS0  Network Configuration:

ttyS0  Software Versions:

ttyS0  BML 010 ARL 011 App 023

ttyS0  CPLD Version:

ttyS0  1.9

ttyS0  SCR Firmware Version:

ttyS0  CROS-B2.29-R1.20

ttyS0  Audit on 14/11/2019 16:01:31 00100001

ttyS0  E1403032 011397 BML 010 : Factory Software Verification Key : CPLD version 1.9

ttyS0  BRL CRC32: 0x747574CA

ttyS0  Running application Bootloader at 0x0FDC0000
ttyS0

2019-11-14T19:35:06+0000
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
ttyS0
Current Tamper Counts (decimal 0-255):
ttyS0

vexcoosTamperCount: 0
ttyS0
vinoosTamperCount: 49
ttyS0
vhoosTamperCount: 0
ttyS0
maxstrtempTamperCount: 0
ttyS0
minstrtempTamperCount: 0
ttyS0
meshTamperCount: 0
ttyS0
extampSKT TamperCount: 0
ttyS0
extampIMKTamperCount: 1
ttyS0
tempdiffTamperCount: 0
ttyS0
gfTamperCount: 49
ttyS0
restartTamperCount: 157
ttyS0

Current tamper bitmaps:
ttyS0

---

ttyS0
current Tamper bitmap: 0x0040 0b ... ... ... ... ... ... ... ... [EXTAMP_IMK]
ttyS0
last Tamper bitmap: 0x0040 0b ... ... ... ... ... ... ... ... [EXTAMP_IMK]
ttyS0

Bitmapped Change Record (most recent first):
ttyS0

---
0x0049 0b .... ..... 1.... 1.... |EXTAMP.IMX

*****Ramelog: dumlog()******

eeprom.read()...complete in 63 ms.

WARNING: eeprom buffer CRC failure

eeprom.write()...complete in 85 ms.

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:

EXTAMP.IMX

Cks::lock() obtained.

currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000
tty00  EITAMP_1MK
2019-11-14T19:35:21+0000
tty00  Cks::lock() obtained.
2019-11-14T19:35:21+0000
tty00  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
2019-11-14T19:35:21+0000  ttyS0  EXITAMP IMK
2019-11-14T19:35:21+0000  ttyS0  Csks::lock() obtained.
2019-11-14T19:35:21+0000  ttyS0  currentTamper status bits:
Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:

Cks::lock() obtained.
currentTamper status bits:
Print Logging Information

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 15   | CA executes the following commands using the terminal window to print a copy of the logging information:  
   a) `ladmin -p HP -o copies-default=1 -o fit-to-page-default=true`  
   b) `enscript -2Gr script-201911*.log`  
   c) `enscript -Gr --font="Courier8" ttyaudit-tty*-201911*.log` | SR | 20:55 |
|      | Attach the printed copies to IW script. Note: Ignore the error regarding non-printable characters if prompted. | | |

Place HSMFDs and OS DVDs into a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 16   | CA executes the following commands using the terminal window to unmount the HSMFD:  
   a) `cd /tmp`  
   b) `umount /media/HSMFD` | SR | 20:45 |
|      | CA removes the HSMFD, then places it on the holder. | | |
| 17   | CA performs the following steps to switch OFF the laptop and remove the OS DVD:  
   a) Remove the OS DVD from the laptop.  
   b) Turn OFF the laptop by pressing the power button.  
   c) Disconnect all connections from the laptop including power, printer, and display. | SR | 20:40 |
| 18   | CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it. | SR | 20:23 |
| 19   | CA performs the following steps to verify the TEB:  
   a) Read aloud the TEB number, then show it to the audit camera above for participants to see.  
   b) Confirm with IW that the TEB number matches the information below.  
   c) Initial the TEB along with IW using a ballpoint pen.  
   d) Give IW the sealing strips for post-ceremony inventory.  
   e) Place the OS DVD TEB on the cart. | SR | 20:08 |
|      | `OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46S84443` | | |

Distribute the HSMFDs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 20   | CA distributes the remaining HSMFDs:  
   2 for IW (for audit bundles).  
   2 for RKOS (for SKR exchange with RZM and process review). | Q | 20:05 |
## Place the laptop into a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>CA places the laptop into a prepared TEB, then seals it.</td>
<td>8L</td>
<td>20:09</td>
</tr>
</tbody>
</table>
| 22   | CA performs the following steps:  
  a) Read aloud the TEB number and Laptop serial number, then show it to the audit camera above for participants to see.  
  b) Confirm with IW that the TEB number and Laptop serial number matches with the information below.  
  c) Initial the TEB along with IW using a ballpoint pen.  
  d) Give IW the sealing strips for post-ceremony inventory.  
  e) Place the Laptop TEB on the cart. | 8L | 20:10 |

**Laptop3: TEB # BB81420111 / Service Tag # J8SVSG2**
# Place HSM Cards into TEBs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) CA takes the OP TEB and plastic case prepared for the CO.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) CO takes their OP card from the card holder 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 aloud the TEB number and description, then seals it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) CA gives the TEB containing the card to the CO.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Repeat steps for the 2 SO cards respectively, ensuring they're facing outward in the plastic case and placed into the prepared SO TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>j) CO writes the date and time, then signs the table of IW's script, then IW initials the entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>k) CO returns to their seat with their credentials, being especially careful not to compromise any TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>l) Repeat steps for all the remaining COs on the list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CO2: Anne-Marie Eklund Lowinder**  
OP TEB # BB46584435  
SO TEB # BB46584436

**CO4: Robert Seastrom**  
OP TEB # BB46584437  
SO TEB # BB46584438

**CO5: Christopher Griffiths**  
OP TEB # BB46584439  
SO TEB # BB46584440

**CO6: Gaurab Upadhyaya**  
OP TEB # BB46584441  
SO TEB # BB46584442
<table>
<thead>
<tr>
<th>TCR</th>
<th>Card Type</th>
<th>TEB #</th>
<th>Printed Name</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
<th>IV/ Initials</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO2</td>
<td>OP 2 of 7</td>
<td>OP TEB # BB46584435</td>
<td>Anne-Marie Eklund Lowinder</td>
<td></td>
<td>2019 Nov 14</td>
<td>20:13</td>
<td>912</td>
</tr>
<tr>
<td></td>
<td>SO 2 of 7</td>
<td>SO TEB # BB46584436</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO4</td>
<td>OP 4 of 7</td>
<td>OP TEB # BB46584437</td>
<td>-Robert Seastrom</td>
<td></td>
<td>2019 Nov</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SO 4 of 7</td>
<td>SO TEB # BB46584438</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO5</td>
<td>OP 5 of 7</td>
<td>OP TEB # BB46584439</td>
<td>Christopher Griffiths</td>
<td></td>
<td>2019 Nov 14</td>
<td>20:15</td>
<td>912</td>
</tr>
<tr>
<td></td>
<td>SO 5 of 7</td>
<td>SO TEB # BB46584440</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO6</td>
<td>OP 6 of 7</td>
<td>OP TEB # BB46584441</td>
<td>Gaurab Upadhaya</td>
<td></td>
<td>2019 Nov 14</td>
<td>20:16</td>
<td>912</td>
</tr>
<tr>
<td></td>
<td>SO 6 of 7</td>
<td>SO TEB # BB46584442</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Return the Equipment to Safe #1 (Tier 6, Equipment Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>SSC1 opens Safe #1 while shielding the combination from the camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>SSC1 removes the safe log, then writes the date and time, then signs the safe log where Open Safe is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 27   | CA performs the following steps to return each piece of equipment to the safe:  
  a) CAREFULLY remove the equipment TEB from the cart.  
  b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1  
  c) Write the date, time, and signature on the safe log where "Return" is indicated.  
  d) IW verifies the safe log entry, then initials it. |          |      |

HSM4: TEB # BB51184226  
Laptop3: TEB # BB81420111  
OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584443

## Close Safe #1 (Tier 6, Equipment Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>SSC1 writes the date and time, then signs the safe log where Close Safe is indicated. IW verifies the entry, then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>SSC1 returns the safe log back to Safe #1 and locks it by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the &quot;WAIT&quot; light indicator is off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and closing the door behind them.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Open Safe #2 (Tier 6, Credentials Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>SSC2 opens Safe #2 while shielding the combination from the camera.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>SSC2 removes the safe log, then writes the date and time, then signs the safe log where Open Safe is indicated. IW verifies this entry, then initials it. 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 Return the Credentials to Safe Deposit Boxes (Tier 7)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>The COs return all credential TEBs to their respective safe deposit boxes by performing the steps below sequentially:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) CO reads aloud the TEB number(s), then verifies the integrity while showing the TEB(s) to the audit camera above</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) With the assistance of the CA (and the common key), the CO opens their safe deposit box. Note: Common Key is for the bottom lock. CO Key is for the top lock.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) CO reads aloud the safe deposit box number, places their TEB(s) inside, then locks the safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) CO writes the date and time, then signs the safe log where &quot;Return&quot; is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) IW verifies the completed safe log entry, then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CO2: Anne-Marie Eklund Lowinder</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1259</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OP TEB # BB46584435</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SO TEB # BB46584436</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CO4: Robert Seastrom</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1260</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OP TEB # BB46584437</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SO TEB # BB46584438</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CO5: Christopher Griffiths</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1240</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OP TEB # BB46584439</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SO TEB # BB46584440</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CO6: Gaurab Upadhyaya</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1261</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OP TEB # BB46584441</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SO TEB # BB46584442</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Close Safe #2 (Tier 6, Credentials Safe)

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>Once all relevant safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where Close Safe is indicated. IW verifies the safe log entry, then initials it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>SSC2 returns the safe log back to Safe #2 and locks it by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the &quot;WAIT&quot; light indicator is off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>CA, IW, SSC2, and COs leave safe room closing the door behind them.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Act 6: Close the Key Signing Ceremony

The CA will finish the ceremony by:

- Reading any exceptions that occurred during the ceremony
- Calling the ceremony participants to sign the IW's script
- Stopping the online streaming and video recording
- Ensuring that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room)
- Preparing the audit bundle materials

### Participants Signing of IW's Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CA reads all exceptions that occurred during the ceremony.</td>
<td>SYL</td>
<td>20:30</td>
</tr>
<tr>
<td>2</td>
<td>CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. All signatures declare that this script is a true and accurate record of the ceremony.</td>
<td>SYL</td>
<td>20:30</td>
</tr>
<tr>
<td>3</td>
<td>CA reviews IW's script, then signs the participants list.</td>
<td>SYL</td>
<td>20:30</td>
</tr>
<tr>
<td>4</td>
<td>IW signs the list and records the completion time once all participants have competed.</td>
<td>SYL</td>
<td>20:30</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>5</td>
<td>CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.</td>
<td>SYL</td>
<td>20:39</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>6</td>
<td>CA informs onsite participants of post ceremony activities.</td>
<td>SYL</td>
<td>20:40</td>
</tr>
<tr>
<td>7</td>
<td>Ceremony participants take a group photo.</td>
<td>SYL</td>
<td>20:45</td>
</tr>
</tbody>
</table>

### Sign Out of Tier 4 (Key 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>8</td>
<td>RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.)</td>
<td>SYL</td>
<td>20:49</td>
</tr>
<tr>
<td></td>
<td>SA, IW, and CA must remain in Tier 4 (Key Ceremony Room.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CA requests that an SA stop the audit camera video recording.</td>
<td>SYL</td>
<td>20:50</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>10</td>
<td>IW makes a copy of their script for off-site audit bundle. Each Audit bundle contains:</td>
<td></td>
<td>21:40</td>
</tr>
<tr>
<td></td>
<td>a) Output of signer system – HSMFD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Copy of IW’s key ceremony script.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Audio-visual recording from the audit cameras.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Logs from the Physical Access Control System and Intrusion Detection System:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range: 20190516 00:00:00 to 20191115 00:00:00 UTC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) IW’s attestation (Appendix C).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) SA’s attestation (Appendix D and E).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All TEBs are labeled <strong>Root DNSSEC KSK Ceremony 39</strong>, dated and initialized by IW and CA. An off-site audit bundle is delivered to an off-site storage.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix A: References

The numeric items listed below has been referenced in the script.

1. **coen**: The Ceremony Operating ENvironment (COEN) is a Reproducible ISO image consisting of a live operating system. More information and the OS image source code can be found at https://github.com/iana-org/coen

2. **sha2wordlist**: Is an application written in C by Kirei AB, which digests STDIN and output a SHA-256 checksum displayed as PGP words. The source code is available at https://github.com/kirei/sha2wordlist

3. **configure-printer**: Is a bash script used to install the HP LaserJet printer from the command line instead using system-config-printer. The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb

4. **hsmfd-hash**: Is a bash script used to calculate, print and compare SHA-256 checksums for the HSMFD flash drives. It has the following options:
   a) `-c` Calculate the HSMFD SHA-256 hash and PGP Word List
   b) `-p` Print the calculated HSMFD SHA-256 hash and PGP Word List using the default printer
   c) `-m` Compare the calculated SHA-256 hashes between HSMFDs

The following is the main command invoked by this script:

```
find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist[2]
```

Note: The sort command has a different behavior depending on the locale settings specified in environment variables. Current OS locale setting is `LC_COLLATE=POSIX`

The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb

5. **ttyaudit**: Is a perl script use to capture and logging the HSM output. The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb

6. **ping hsm**: The HSM static IP address 192.168.0.2 has been included in the `/etc/hosts` file.

7. **ksrsigner**: Is an application written in C by Dr. Richard Lamb, which uses the KSK private key stored in the HSM to generate digital signatures for the ZSK. The source code is available at https://github.com/iana-org/dnssec-keytools

8. **printlog**: Is a bash script use to print the Key Signing Log output from ksrsigner application. The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb

* A debian package is an ar archive. To extract data from a deb package, use the command `ar -x ksk-tools-0.1.0coen_amd64.deb`
Then extract the files with `tar -zxvf data.tar.xz`
The file will be located in the directory: `/opt/icann/bin/`
Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)
Each audit bundle will contain one HSMFD. All bundles will be placed inside TEBs that are prelabeled Audit Original and Audit Copy.

2. Key Ceremony Script (by IW)
Hard copies of the IW's key ceremony script, notes during the ceremony and attestation. See Appendix C.

3. Audio-Visual Recordings from the KSK Ceremony (by SA)
Two sets of the audit camera footages - One for the original audit bundle and the other for the duplicate audit bundle.

4. Logs from the Physical Access Control System and Intrusion Detection System (by SA)
Two electronic copies of the following:
   1. Firewall configuration
   2. Configuration reports
   3. Personnel/cardholder reports
   4. Activity and audit log reports

These files will be placed inside two separate Flash Drives that are labeled "Audit".
The contents of the Flash Drive will be confirmed by the IW before placing each of them inside the original and the duplicate audit bundles.

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

6. Configuration review of the Firewall System (by SA)
SA's attestation and hard copies of the firewall configuration from the review process. See Appendix E. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Other items
If applicable.
Appendix C: Key Ceremony Script (by IW)

I hereby attest that the Key Ceremony was conducted in accordance to this script. Any exceptions that occurred were accurately and properly documented.

IW: Shauna Roysten

Signature: [Signature]

Date: 2019 Nov 14
Appendix D: Access Control System Configuration Review (by SA)

In my review of the KMP's Access Control System, I attest that the following are true and correct to the best of my knowledge:

   a) There were NO discrepancies found on the system configurations, assigned authorizations and audit logs.
   b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

Below are the reports that were generated from the access control system:

2. Configuration of Areas and Access Groups.
3. Logs for Access Event activities and Configuration activities.

Range: 20190516 00:00:00 to 20191115 00:00:00 UTC.

SA: Reed Quinn

Signature: Reed Quinn

Date: 2019 Nov 14
Appendix E: Firewall Configuration Review (by SA)

I have reviewed and confirmed that the firewall configuration satisfies the requirements of the DNSSEC Practice Statement with version 4th Edition (2016-10-01). There are no part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA: Reed Quinn

Signature: Reed Quinn

Date: 2019 Nov 4