Root DNSSEC KSK Ceremony 41
Thursday April 23, 2020

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

This ceremony is executed in accordance to the DNSSEC Practice Statement for the Root Zone KSK Operator 5th Edition (2020-04-07)
Abbreviations

AUD = Third Party Auditor  CA = Ceremony Administrator  CO = Crypto Officer
EW = External Witness  FD = Flash Drive  HSM = Hardware Security Module
IW = Internal Witness  KMF = Key Management Facility  KSR = Key Signing Request
OP = Operator  PTI = Public Technical Identifiers  RKSH = Recovery Key Share Holder
RKOS = RZKSK Operations Security  RZM = Root Zone Maintainer  SA = System Administrator
SKR = Signed Key Response  SMK = Storage Master Key  SO = Security Officer
SSC = Safe Security Controller  SW = Staff Witness  TCR = Trusted Community Representative
TEB = Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20)

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>Francisco Arias / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW</td>
<td>Jonathan Denison / ICANN</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC1</td>
<td>Sabrina Tanamal / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC2</td>
<td>Anand Mishra / ICANN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA</td>
<td>Patrick Tudor / ICANN</td>
<td></td>
<td></td>
<td>2020</td>
</tr>
<tr>
<td>RKOS / CA Backup</td>
<td>Andres Pavez / PTI</td>
<td></td>
<td>Apr 23</td>
<td>20.10</td>
</tr>
<tr>
<td>RKOS / IW Backup</td>
<td>Aaron Foley / PTI</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Root DNSSEC KSK Ceremony 41
Instructions for a 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 a CA, IW, or SA 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
- During a ceremony a CA, IW, or SA may escort participants out of Tier 4 (Key Ceremony Room) at the CA’s discretion if Tier 5 (Safe Room) is not occupied
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log located in Tier 3
- The SA starts filming before the majority of participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step in order to attest to the ceremony’s proper performance
- The CA reads each step aloud prior to its performance
- Upon the successful completion of a step, the IW will announce and record its time of completion, and initials that step in their script
- A ceremony participant who has cause for concern or detects an issue is encouraged to interrupt the ceremony for discussion. The issue is brought to resolution before the ceremony resumes
- 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: Consist 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)
Some steps during the ceremony may require the participants to recite and/or confirm identifiers comprised of numbers and letters. When spelling identifiers, the phonetic alphabet shown below should 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>DELL-TAH</td>
</tr>
<tr>
<td>E</td>
<td>Echo</td>
<td>ECK-OH</td>
</tr>
<tr>
<td>F</td>
<td>Foxtrot</td>
<td>FOKS-TROT</td>
</tr>
<tr>
<td>G</td>
<td>Golf</td>
<td>GOLF</td>
</tr>
<tr>
<td>H</td>
<td>Hotel</td>
<td>HOH-TEL</td>
</tr>
<tr>
<td>I</td>
<td>India</td>
<td>IN-DEE-AH</td>
</tr>
<tr>
<td>J</td>
<td>Juliet</td>
<td>JEW-LEE-ETT</td>
</tr>
<tr>
<td>K</td>
<td>Kilo</td>
<td>KEY-LOH</td>
</tr>
<tr>
<td>L</td>
<td>Lima</td>
<td>LEE-MAH</td>
</tr>
<tr>
<td>M</td>
<td>Mike</td>
<td>MIKE</td>
</tr>
<tr>
<td>N</td>
<td>November</td>
<td>NO-VEE-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-AY-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>0</td>
<td>Zero</td>
<td>ZEE-RO</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>EET</td>
</tr>
<tr>
<td>9</td>
<td>Nine</td>
<td>NIN-ER</td>
</tr>
</tbody>
</table>
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's 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

The CA and IW will then escort the SSCs into Tier 5 (Safe Room) to retrieve the following materials:

- Safe #1: HSM, laptop, OS DVD, etc
- Safe #2: The COs' 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>JD</td>
<td>17:06</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>JD</td>
<td>17:06</td>
</tr>
<tr>
<td>3</td>
<td>CA asks that any first time ceremony participants in the room introduce themselves.</td>
<td>JD</td>
<td>17:06</td>
</tr>
</tbody>
</table>
| 4    | CA confirms that additional required personnel including COs, R2M, and Auditors are connected to the remote call. Scheduled remote participants are:  
  CO4: Carlos Martinez (Key scripted for use) 17:07  
  CO5: Olafur Gudmundsson (Key scripted for use) 17:07  
  CO6: Nicolas Antoniello (Key scripted for use) 17:07  
  CO3: Joao Damas (Key designated as backup) 17:07  
  R2M: Duane Wessel / Verisign 17:07  
  R2M: Trevor Davis / Verisign 17:07  
  AUD: James Kim / RSM 17:07 | JD       | 17:08 |

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>5</td>
<td>CA reviews emergency evacuation procedures with onsite participants.</td>
<td>JD</td>
<td>17:06</td>
</tr>
<tr>
<td>6</td>
<td>CA explains the use of personal electronic devices during the ceremony.</td>
<td>JD</td>
<td>17:08</td>
</tr>
<tr>
<td>7</td>
<td>CA summarizes the purpose of the ceremony.</td>
<td>JD</td>
<td>17:10</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>
</table>
| 8    | IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room):  
  Date and time: 2020-04-23 17:41 | JD       | 17:41 |

Note: All entries into this script or any logs should follow this common source of time.
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Carlos Martinez, am hereby entrusting my safe deposit box key enclosed in TEB #1BB91951Z84 for safe deposit box #1068 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name  

Carlos Martinez

Signature  

Carlos Martinez

Date  

April 13, 2020

* TEB #: BB 919 51 284
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Olafur Gudmundsson, am hereby entrusting my safe deposit box key enclosed in TEB #66 9195127 for safe deposit box #1789 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name  OLAFUR GUDMUNDSSON

Signature  Olafur  \\

Date  2020/4/11
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Nicolas Antoniello, em hereby entrusting my safe deposit box key enclosed in TEB #6B91951289 for safe deposit box #1073 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name: Nicolas Antoniello

Signature:

Date: 4/4/2020
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Joao Luis Silva Damas, am hereby entrusting my safe deposit box key enclosed in TEB # R91451281 for safe deposit box #1069 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name ____________

Joao Luis Silva Damas

Signature ____________

JLP12

Date ____________

15/4/2020
## Crypto Officer Key Verification

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 9    | The CA performs the following steps to verify the listed CO keys:  
  a) Remove the TEB from the shipping envelope and discard the shipping envelope.  
  b) Inspect the TEB for tamper evidence.  
  c) Read aloud the TEB number and place it on the ceremony table visible to the audit camera.  
  d) Open the TEB and place its contents on the ceremony table.  
  e) Give the CO key declaration to IW to verify the TEB number, and then insert in the audit bundle.  
  f) Discard the TEB.  
  g) Attach the CO tenant key to its corresponding pre-labeled key ring.  
  h) Give the CO tenant key to the IW. | JD       | 17:23 |

**CO4: Carlos Martinez**  
Key TEB # BB91951284 (See Appendix F on page 35)

**CO5: Olafur Gudmundsson**  
Key TEB # BB91951277 (See Appendix G on page 36)

**CO6: Nicolas Antoniello**  
Key TEB # BB91951289 (See Appendix H on page 37)

**Note 1:** The CO3 Joan Damaro Safe Deposit Box Key TEB # BB91951281 has been designated as a backup. See Appendix I on page 38.

**Note 2:** The COs' tenant keys were individually transmitted to separate trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.

## 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>10</td>
<td>CA and IW transport a flashlight, and escort SSC2 into Tier 5 (Safe Room.)</td>
<td>JD</td>
<td>17:24</td>
</tr>
</tbody>
</table>
| 11   | SSC2 opens Safe #2 while shielding the combination from the camera.  
  Note: SSC2 begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination. | JD       | 17:26 |
| 12   | Perform the following steps to complete the safe log:  
  a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera.  
  b) IW provides the pre-printed safe log to SSC2.  
  c) SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated.  
  d) IW verifies the entry then initials it. | JD       | 17:28 |
### Extract CO 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>13</td>
<td>IW performs the following steps sequentially to retrieve the required TEBs:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) IW announces the name of the CO whose credentials will be extracted and CO confirms their authorization to open their safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) When the CO provides confirmation, the CA operates the guard key in the bottom lock, then the IW uses the CO's tenant key to operate the top lock and open their safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) IW reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) IW retains the TEB(s) specified below, returns any TEBs not required, then closes and locks the safe deposit box with assistance from the CA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) IW writes the date and time, then signs the safe log where &quot;Remove&quot; is indicated.</td>
<td>JD</td>
<td>17:46</td>
</tr>
<tr>
<td></td>
<td>g) CA verifies the completed safe log entries, then initials it.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CO4: Carlos Martinez**  
Box # 1068  
OP TEB # BB46592092 (Retain)  
SO TEB # BB46584665 (Check and Return)

**CO5: Olafur Gudmundsson**  
Box # 1789  
OP TEB # BB46584380 (Retain)  
SO TEB # BB46584381 (Check and Return)

**CO6: Nicolas Antoniello**  
Box # 1073  
OP TEB # BB46584382 (Retain)  
SO TEB # BB46584383 (Check and Return)

### 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>14</td>
<td>Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where &quot;Close Safe&quot; is indicated. IW verifies the entry then Initials it.</td>
<td>JD</td>
<td>17:46</td>
</tr>
<tr>
<td>15</td>
<td>SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked 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>JD</td>
<td>17:47</td>
</tr>
<tr>
<td>16</td>
<td>CA, IW, and SSC2 leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).</td>
<td>JD</td>
<td>17:48</td>
</tr>
<tr>
<td>17</td>
<td>IW places the TEBs on the ceremony table.</td>
<td>JD</td>
<td>17:48</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>18</td>
<td>CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)</td>
<td>Jd</td>
<td>17:49</td>
</tr>
<tr>
<td>19</td>
<td>SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.</td>
<td>Jd</td>
<td>17:51</td>
</tr>
</tbody>
</table>
| 20   | Perform the following steps to complete the safe log:  
    a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera.  
    b) IW provides the pre-printed safe log to SSC1.  
    c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated.  
    d) IW verifies the entry then initials it. | Jd | 17:52  |

### 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>
</table>
| 21   | CA performs the following steps to extract each piece of equipment from the safe:  
    a) CAREFULLY remove each equipment TEB from the safe.  
    b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera.  
    c) Place each equipment TEB on the cart as specified in the list below.  
    d) Write the date, time, and signature on the safe log where "Remove" is indicated.  
    e) IW verifies the safe log entry, then initials it. | Jd | 18:01  |
|      | HSM3: TEB # BB51184234 (Check and Return)  
      Last Verified: KSK40-AC 2020-02-16  
      HSM4: TEB # BB51184238 (Check and Return)  
      Last Verified: KSK40 2020-02-16  
      HSM5W: TEB # BB51184237 (Place on Cart)  
      Last Verified: KSK40-AC 2020-02-16  
      Laptop3: TEB # BB81420125 (Place on Cart)  
      Last Verified: KSK38 2019-08-14  
      Laptop4: TEB # BB81420119 (Check and Return)  
      Last Verified: KSK40 2020-02-16  
      OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951350 (Place on Cart)  
      Last Verified: KSK40 2020-02-16  
      KSK-2017: TEB # BB46584387 (Check and Return)  
      Last Verified: KSK38 2019-08-14 | Jd | 18:01  |

Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.
**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>22</td>
<td>SSC1 writes the date and time, then signs the safe log where &quot;Close Safe&quot; is indicated. IW verifies the safe log entry then initials it.</td>
<td>JD</td>
<td>18:02</td>
</tr>
<tr>
<td>23</td>
<td>SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked 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>JD</td>
<td>18:02</td>
</tr>
<tr>
<td>24</td>
<td>CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).</td>
<td>JD</td>
<td>18:03</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 HSM (Tier 7)

Laptop Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CA performs the following steps to prepare the listed equipment:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Remove all equipment TEBs from the cart and place them on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Inspect each equipment TEB for tamper evidence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Read aloud the TEB number and the serial number (if applicable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>while IW verifies the information using the previous ceremony</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>script where it was last used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Remove and discard the TEB, then place the equipment on its</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>designated area of the ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSM5W: TEB # BB51184237 / Serial # H1903017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Verified: KSK40-AC 2020-02-16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laptop3: TEB # BB81420126 / Service Tag # C8SVSG2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Verified: KSK38 2019-08-14</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951350</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Verified: KSK40 2020-02-16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: &quot;Last verified&quot; indicates the last time a piece of equipment was</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>placed in a new TEB during a ceremony. It is listed here for audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>tracking purposes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CA performs the following steps to confirm that no hard drive and battery</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are in the laptop:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Open the latch on the right side of the laptop to confirm that the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hard drive slot is empty.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Open the latch on the left side of the laptop to confirm that the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>battery slot is empty.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CA performs the following steps to boot the laptop:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) Connect the USB printer cable into the rear USB port of the laptop.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Connect the null modem cable into the serial port of the laptop.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Connect the external HDMI display cable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Connect the power supply.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Immediately insert the OS DVD release coen-0.4.0 after the laptop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>power is switched ON.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CA verifies functionality of the external display and performs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>adjustments if necessary:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To change the font size of the terminal:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click the View menu and select Zoom In or Zoom Out</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To change the resolution of each screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Go to Applications &gt; Settings &gt; Display</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Root DNSSEC KSK Ceremony 41  Page 10 of 38
### OS DVD Checksum Verification

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 5    | CA uses the terminal window to execute the following steps:  
a) Calculate the SHA-256 hash by executing:  
`sha2wordlist < /dev/ sr0`  
b) JW 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.  
SHA-256 hash:  
8105b885b176741d25ef9d391c6a302aecd3f6c916093a6218b65cb90d560774f  
PGP Words:  
minnow almighty select leprosy sailboat impetus indoors breakaway bombard  
unravel quadrant corporate befriended 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 coin-0.4.0 is also published on the IANA website  
https://www.iana.org/dnssec/ceremonies/41 | J D | 18:32 |

### Printer Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</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` | J D | 18:49 |

### Date Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</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 -u "20200423 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. | J P | 18:20 |
### 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 40 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. | JD | 18:21 |
| 9    | CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD:  
  `hsmfd-hash -c`  
  CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script. | JD | 18:24 |

```bash
find /media/HSMFD/ -type f -print0 | sort -t \n -o /media/txtlist.shab

SHA-256:  
09710df7963133332339964b9495a002c612f25263a00  

```

IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 40 annotated script.

---

### 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 HSMFD 40 and the sheet of paper with the printed HSMFD hash to RKOS.</td>
<td>JD</td>
<td>18:25</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:  
  `cd /media/HSMFD` | JD | 18:25 |
| 12   | CA executes the command below to log activities of the Commands terminal window:  
  `script script-20200423.log` | JD | 18:25 |

---

### 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:  
  `atxy -F /dev/tty80 115200`  
  c) Start logging the serial output by executing:  
  `ttyaudit /dev/tty80`  
  Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port. | JD | 18:27 |
## 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) Verify the label on the HSM reads **HSM5W**  
   b) Ensure an RJ45 blockout is present in the "MGMT" port of the HSM. Install one if not present.  
   c) Plug the null modem cable into the serial port of the HSM.  
   d) Connect the power to the HSM, then switch it ON.  
   e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H1903017**, then scroll back to the bottom. | JD | 18:30 |

**HSM5W: Serial # H1903017**

*Note: The date and time on the HSM is not used as a reference for logging and timestamp.*
Act 3: Activate HSM (Tier 7) and Generate Signatures

Using the krsigner 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 COs’ smart cards
- After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop
- The krsigner application uses the private key stored in the HSM to generate the SKR containing 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

Crypto Officer Credentials Verification

<table>
<thead>
<tr>
<th>Step</th>
<th>CA performs the following steps to verify the COs credentials:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a) Read aloud the TEB number, then inspect it for tamper evidence.</td>
</tr>
<tr>
<td></td>
<td>b) Open the TEB, then remove the plastic case containing the card(s).</td>
</tr>
<tr>
<td></td>
<td>c) Open the plastic case, then place the enclosed card(s) on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>JD</td>
<td>18:54</td>
</tr>
</tbody>
</table>

CO4: Carlos Martinez  
OP TEB # BB46592092

CO5: Olafur Gudmundsson  
OP TEB # BB46584380

CO6: Nicolas Antoniello  
OP TEB # BB46584382

Enable/Activate the HSM (Tier 7)

<table>
<thead>
<tr>
<th>Step</th>
<th>CA performs the following steps to activate the HSM:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a) Utilize the HSM’s keyboard to scroll through the menu using &lt; &gt;</td>
</tr>
<tr>
<td></td>
<td>b) Select &quot;1.Set Online&quot;, press ENT to confirm.</td>
</tr>
<tr>
<td></td>
<td>c) When &quot;Set Online?&quot; is displayed, press ENT to confirm.</td>
</tr>
<tr>
<td></td>
<td>d) When &quot;Insert Card OP #X?&quot; is displayed, insert the OP card.</td>
</tr>
<tr>
<td></td>
<td>e) When &quot;PIN?&quot; is displayed, enter &quot;11223344&quot;, then press ENT.</td>
</tr>
<tr>
<td></td>
<td>f) When &quot;Remove Card?&quot; is displayed, remove the OP card.</td>
</tr>
<tr>
<td></td>
<td>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>JD</td>
<td>18:56</td>
</tr>
</tbody>
</table>

Confirm the "READY" LED on the HSM is ON.  
I&W records which cards were used below. Each card is returned to its designated card holder after use.

1st OP card 4 of 7
2nd OP card 5 of 7
3rd OP card 6 of 7

Note: If the card is unreadable, gently wipe its metal contacts and try again.
### 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>JD</td>
<td>18:39</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  
   c) Wait for responses, then exit by pressing:  
         Ctrl + C | JD | 18:39 |

### Insert the KSRFD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>CA plugs the FD labeled &quot;KSR&quot; into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window.</td>
<td>JD</td>
<td>18:41</td>
</tr>
</tbody>
</table>

*Note: The KSRFD was transferred to the facility by the RKOS. It contains 3 KSRs. One for the next calendar quarter and the remaining for subsequent quarter(s).*

### Execute the KSR Signer for KSR 2020 Q3

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 6    | CA executes the command below in the terminal window to sign the KSR file:  
   kersigner /media/KSR/KSK41-2020-Q3/ksr-zoot-2020-q3-0.xml | JD | 18:42 |
| 7    | When the KSR signer displays the prompt:  
   *Activate HSM prior to accepting in the affirmative!! (y/N):*  
   CA confirms that the HSM is online, then enters "y" to proceed. | JD | 18:42 |
April 22\textsuperscript{nd}, 2020

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 29\textsuperscript{th}, 2014, currently as 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 22 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 158.8 million .com and .net domain names and processing more than 210 billion query 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
23 April 2020

The SHA256 hash of the 2020 Q3 KSR file is:

ksr-root-2020-q3-0.xml:

7b5188b568b4e932d9ac26df804d28adbc09d70f186bafcc2ff067718bf9b973

The PGP wordlist for the hash above is:

PGP Words: kickoff enchanting newborn positive frighten politeness treadmill component sugar penetrate bookshelf therapist merit disruptive breadline perceptive showgirl applicant stopwatch atmosphere beaming Hamilton rocker revolver cement upcoming freedom hideaway obtuse Waterloo sentence hurricane

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.
23 April 2020

The SHA256 hash of the 2020 Q4 KSR file is:

ksr-root-2020-q4-0.xml:

e3068f0cfc5a69ce2c62e12295597607b099d3f1e6c99eb37b6fdbc77fc2f8a1

The PGP wordlist for the hash above is:

PGP Words: tissue amulet payday article wayside existence gazelle sardonic Burbank gadgetry tempest candidate preclude examine inverse amusement ruffled nebula stapler vacancy tracker retrospect quiver pocketful kickoff hemisphere suspense voyager lookup repellent Vulcan outfielder

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.
23 April 2020

The SHA256 hash of the 2021 Q1 KSR file is:

```
ksr-root-2021-q1-0.xml:
2dd682ff1b0dbdc746c1324b663793eb813c1aedd593f96ff8f3cc819dfe30643
```

The PGP wordlist for the hash above is:

**PGP Words:** button speculate miser Yucatan beeswax suspicious sweatband hydraulic glucose barbecue bluebird potato flatfoot inertia concert provincial Aztec recover robust tambourine endow customer prefer Yucatan payday crossover spaniel bottomless talon torpedo afflict decimal

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.
## Verify the KSR Hash for KSR 2020 Q3

<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 in the terminal window, perform the following:  
a) CA asks the Root Zone Maintainer (RZM) representative to identify  
   themselves. The IW verifies employment documents and  
identification off camera for the purpose of authentication while  
maintaining privacy.  
Note: If the RZM representative is not physically present in the room, write the  
representative’s name and "Remote Participant" next to the name on the signature  
line.  
b) IW retains the hash and PGP word list for the KSR(s), and  
employment verification letter provided by the RZM representative  
and writes their name on the following line:  
Note: If the RZM representative is not physically present in the room, the documents will  
be provided to RKOS in advance to be included in the final annotated script and audit  
bundle.  
   
[TREVOR LEWIS DAVIS (REMOTE PARTICIPANT)]  
c) RZM representative reads aloud the PGP word list SHA-256 hash  
of the KSR file being used. | JD | 18:45 |
| 9    | Participants confirm that the hash displayed on the terminal window  
matches with the RZM discourse, then CA asks "are there any objections?" | JD | 18:47 |
| 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/KSK41-2020-Q3/skr-root-2020-q3-0.xml | JD | 18:47 |

## Execute the KSR Signer for KSR 2020 Q4

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 11   | CA executes the command below in the terminal window to copy the  
previous quarter generated SKR, in order to construct a chain of trust to  
the next KSR:  
cp /media/KSR/KSK41-2020-Q3/skr-root-2020-q3-0.xml  
/media/KSR/KSK41-2020-Q4/skr.xml | JD | 18:49 |
| 12   | CA executes the command below in the terminal window to sign the  
KSR file:  
ksrsigner /media/KSR/KSK41-2020-Q4/skr-  
root-2020-q4-0.xml  
Note: It is expected that the KSR Signer Software will issue a warning since the requests  
signature will exceed the limit of 180 days of expiration in the future. This additional SKR  
will remain in the possession of the RZ KSK Operator until the time in which all RRSIG  
records in the set would not expire more than 180 days in the future. | JD | 19:50 |
| 13   | When the KSR signer displays the prompt:  
Activate HSM prior to accepting in the affirmative!! (y/N):  
CA confirms that the HSM is online, then enters "y" to proceed. | JD | 18:51 |
### Verify the KSR Hash for KSR 2020 Q4

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.</td>
<td>JD</td>
<td>18:52</td>
</tr>
<tr>
<td>15</td>
<td>Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks &quot;are there any objections?&quot;</td>
<td>JD</td>
<td>18:52</td>
</tr>
<tr>
<td>16</td>
<td>CA enters &quot;y&quot; in response to &quot;Is this correct (y/N)?&quot; to complete the KSR signing operation. The SKR is located in: /media/KSR/KSK41-2020-Q4/skr-root-2020-q4-0.xml</td>
<td>JD</td>
<td>18:52</td>
</tr>
</tbody>
</table>

### Execute the KSR Signer for KSR 2021 Q1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 17   | CA executes the command below in the terminal window to copy the previous quarter generated SKR, in order to construct a chain of trust to the next KSR:  
|      | cp /media/KSR/KSK41-2020-Q4/skr-root-2020-q4-0.xml /media/KSR/KSK41-2021-Q1/skr.xml | JD       | 18:54 |
| 18   | CA executes the command below in the terminal window to sign the KSH file:  
|      | karsigner /media/KSR/KSK41-2021-Q1/skr-root-2021-q1-0.xml | JD       | 18:54 |
|      | **Note:** It is expected that the KSR Signer Software will issue a warning since the requests signature will exceed the limit of 180 days of expiration in the future. This additional SKR will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set would not expire more than 180 days in the future. |        |      |
| 19   | When the KSR signer displays the prompt:  
|      | Activate HSM prior to accepting in the affirmative!! (y/N):  
|      | CA confirms that the HSM is online, then enters "y" to proceed. | JD       | 18:54 |

### Verify the KSR Hash for KSR 2021 Q1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.</td>
<td>JP</td>
<td>18:55</td>
</tr>
<tr>
<td>21</td>
<td>Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks &quot;are there any objections?&quot;</td>
<td>JD</td>
<td>18:56</td>
</tr>
<tr>
<td>22</td>
<td>CA enters &quot;y&quot; in response to &quot;Is this correct (y/N)?&quot; to complete the KSR signing operation. The SKR is located in: /media/KSR/KSK41-2021-Q1/skr-root-2C21-q1-0.xml</td>
<td>JD</td>
<td>18:56</td>
</tr>
</tbody>
</table>

### 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>
| 23   | CA executes the commands below using the terminal window to print the KSR Signer log:  
|      | a) 1padmin -p HP -o copies-default=+X  
|      | Note: Replace "X" with the amount of copies needed for the participants.  
|      | b) for i in `$(1s -i karsigner-202004.log); do  
|      | printlog $i; done | JD       | 18:58 |
| 24   | IW attaches a copy of the required karsigner log to their script. | JD       | 18:59 |
Starting: ksrserver /media/KSR/KSR41-2020-Q3/ksr-root-2020-q3-0.xml (at Thu Apr 23 18:42:06 2020 UTC)
Use HSM /opt/dnsec/sem.haconf activated.
setenv KESR_LIBPATH /opt/dnsec
setenv PKCS11_LIBRARY_PATH /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_3_2_glibc_2_5_x86_64.so.5.0.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_3_2_glibc_2_5_x86_64.so.5.0.2
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_3_2_glibc_2_5_x86_64.so.5.0.2 Slot-0
HSM Information:
Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H903617
Validating last KSK with HSM...
# Inception Expiration ZSK Tags KSK Tag (CKA_LABEL)
1 2020-04-01T00:00:00 2020-04-22T00:00:00 33853,48903 20326[Klaayez]/S
2 2020-04-11T00:00:00 2020-05-22T00:00:00 48903 20326[Klaayez]/S
3 2020-04-21T00:00:00 2020-05-12T00:00:00 48903 20326[Klaayez]/S
4 2020-05-01T00:00:00 2020-05-22T00:00:00 48903 20326[Klaayez]/S
5 2020-05-11T00:00:00 2020-06-01T00:00:00 48903 20326[Klaayez]/S
6 2020-05-21T00:00:00 2020-06-11T00:00:00 48903 20326[Klaayez]/S
7 2020-06-01T00:00:00 2020-06-21T00:00:00 48903 20326[Klaayez]/S
8 2020-06-10T00:00:00 2020-07-01T00:00:00 48903 20326[Klaayez]/S
9 2020-06-20T00:00:00 2020-07-11T00:00:00 45994,48903 20326[Klaayez]/S
...VALIDATED.
Validate and Process KSK /media/KSR/KSR41-2020-Q3/ksr-root-2020-q3-0.xml...
# Inception Expiration ZSK Tags KSK Tag (CKA_LABEL)
1 2020-07-01T00:00:00 2020-07-22T00:00:00 46594,48903 20326[Klaayez]/S
2 2020-07-11T00:00:00 2020-08-01T00:00:00 46594 20326[Klaayez]/S
3 2020-08-02T00:00:00 2020-08-12T00:00:00 46594 20326[Klaayez]/S
4 2020-08-10T00:00:00 2020-09-01T00:00:00 46594 20326[Klaayez]/S
6 2020-09-09T00:00:00 2020-10-01T00:00:00 46594 20326[Klaayez]/S
7 2020-09-09T00:00:00 2020-09-30T00:00:00 46594 20326[Klaayez]/S
9 2020-09-19T00:00:00 2020-10-10T00:00:00 26116,46594
...PASSED.
SHA256 hash of KSK:
7581B5B6A9B52D5A6263DF084D2D8BBCD09D75F16B6AFC2C2FF997156BF8973
>> kickoff enchanting newborn positive frighten politeness treadmill component sugar penetrate bookshelf therapist merit disruptive brendine persceptive showgirl applicant stopwatch atmosphere beaming Hamilton rocker revolver cement upcoming freedom hideaway obtuse Waterloo sentence hurricane <<
Reading KSK schedule "normal(2017)" from "kskschedule.json"
# KSK Tag (CKA_LABEL)
1 20326[Klaayez]/S
2 20326[Klaayez]/S
3 20326[Klaayez]/S
4 20326[Klaayez]/S
5 20326[Klaayez]/S
6 20326[Klaayez]/S
7 20326[Klaayez]/S
8 20326[Klaayez]/S
9 20326[Klaayez]/S
Generated new KSK in /media/KSR/KSR41-2020-Q3/ksr-root-2020-q3-0.xml
# Inception Expiration ZSK Tags KSK Tag (CKA_LABEL)
1 2020-07-01T00:00:00 2020-07-22T00:00:00 46594,48903 20326[Klaayez]/S
2 2020-07-11T00:00:00 2020-08-01T00:00:00 46594 20326[Klaayez]/S
3 2020-08-02T00:00:00 2020-08-12T00:00:00 46594 20326[Klaayez]/S
4 2020-08-10T00:00:00 2020-09-01T00:00:00 46594 20326[Klaayez]/S
5 2020-09-09T00:00:00 2020-10-01T00:00:00 26116,46594 20326[Klaayez]/S
SHA256 hash of KSK:
F42A22CCF173B8B3D3B18740526CD58799867B0C5C90573D1B30D8A9X04
>> tonic chambermaid breakup revolver unwind inferno tracker underfoot clockwork tambourine beeswax determine allow caravan glucose specialist frighten hesitate printer graduate showgirl handiwork ruffled vocalist treadmill aftermath berserk corporate staiway stupendous pupil akkia <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_3_2_glibc_2_5_x86_64.so.5.0.2 Slot-0
Validating last KSR with HSM...

$ Inception   Expiration   SKR Tags   KSK Tag  [GKA_LABEL]
1 2020-07-22T00:00:00  2020-08-17T00:00:00  46594,48963  20326[Xiajiey]/S
2 2020-08-17T00:00:00  2020-08-01T00:00:00  46594  20326[Xiajiey]/S
3 2020-08-21T00:00:00  2020-08-11T00:00:00  46594  26326[Xiajiey]/S
4 2020-08-31T00:00:00  2020-08-21T00:00:00  46594  20326[Xiajiey]/S
5 2020-08-10T00:00:00  2020-08-31T00:00:00  46594  20326[Xiajiey]/S
6 2020-08-02T00:00:00  2020-09-02T00:00:00  46594  20326[Xiajiey]/S
7 2020-08-30T00:00:00  2020-09-20T00:00:00  46594  20326[Xiajiey]/S
8 2020-09-09T00:00:00  2020-09-30T00:00:00  46594  20326[Xiajiey]/S
9 2020-09-19T00:00:00  2020-10-10T00:00:00  26116,46594  20326[Xiajiey]/S

...VALIDATED.

Validate and Process KSR /media/ksr/KSR41-2020-Q4/ksr-root-2020-q4-0.xml...

$ Inception   Expiration   SKR Tags   KSK Tag  [GKA_LABEL]
1 2020-10-01T00:00:00  2020-10-22T00:00:00  26116,46594
2 2020-10-11T00:00:00  2020-11-01T00:00:00  26116
3 2020-10-21T00:00:00  2020-11-11T00:00:00  26116
4 2020-10-31T00:00:00  2020-11-21T00:00:00  26116
5 2020-11-10T00:00:00  2020-12-01T00:00:00  26116
6 2020-11-20T00:00:00  2020-12-11T00:00:00  26116
7 2020-11-30T00:00:00  2020-12-21T00:00:00  26116
8 2020-12-10T00:00:00  2020-12-31T00:00:00  26116
9 2020-12-20T00:00:00  2021-01-10T00:00:00  42351,26116

*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***

...PASSED.

SHA256 hash of KSR:
E3O6F8DPCFCS8S69G9C6E26E12256555557657081963D3F186C69M73878877FCC2F8A1
>> tissue amulet payday article wayside existence gazelle sarcastic Burbank gadgetry tempest candidate proclade examine in verse amusement ruffled nebula stapler vacancy tracker retroscript quiver pocketful kickoff hemispheres suspense voyager lo skup repellent Vulcan outfitter <<

Reading KSR schedule "normal(2017)" from "kkskschedule.json"

$ KSK Tag  [GKA_LABEL]
1 20326[Xiajiey]/S
2 20326[Xiajiey]/S
3 20326[Xiajiey]/S
4 202326[Xiajiey]/S
5 20326[Xiajiey]/S
6 20326[Xiajiey]/S
7 20326[Xiajiey]/S
8 202326[Xiajiey]/S
9 20326[Xiajiey]/S

Generated new SKR in /media/ksr/KSR41-2020-Q4/skr-root-2020-q4-0.xml

$ Inception   Expiration   SKR Tags   KSK Tag  [GKA_LABEL]
1 2020-10-01T00:00:00  2020-10-22T00:00:00  26116,46594  20326[Xiajiey]/S
2 2020-10-11T00:00:00  2020-11-01T00:00:00  26116  20326[Xiajiey]/S
3 2020-10-21T00:00:00  2020-11-11T00:00:00  26116  20326[Xiajiey]/S
4 2020-10-31T00:00:00  2020-11-21T00:00:00  26116  20326[Xiajiey]/S
5 2020-11-10T00:00:00  2020-12-01T00:00:00  26116  20326[Xiajiey]/S
6 2020-11-20T00:00:00  2020-12-11T00:00:00  26116  20326[Xiajiey]/S
7 2020-11-30T00:00:00  2020-12-21T00:00:00  26116  20326[Xiajiey]/S
8 2020-12-10T00:00:00  2020-12-31T00:00:00  26116  20326[Xiajiey]/S
9 2020-12-20T00:00:00  2021-01-10T00:00:00  42351,26116  20326[Xiajiey]/S

SHA256 hash of KSR:
CDA23C5462D28B8F1F3D3D494C7D96833F5B56F89F4785406978BCC29DF63
>> spindly Pacific cobra equation flagship sensation armpit unsewed beewax cannonball steamship molecule rocker hurricane m skeleton Jamaica classroom Wohita backward forever music Yucatan virus leprosy drainage amulet preharrow microscope sp igot corporate stockman Jamaica <<

Unloaded /opt/Keyer/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
Validating last SKR with HSM...

1 2020-10-07T00:00:00Z 2020-10-22T00:00:00Z 26116,46594 26116,42351 20326(Kla_jeyes)/S
2 2020-10-11T00:00:00Z 2020-11-01T00:00:00Z 26116 20326(Kla_jeyes)/S
3 2020-10-21T00:00:00Z 2020-11-17T00:00:00Z 26116 20326(Kla_jeyes)/S
4 2020-10-31T00:00:00Z 2020-11-27T00:00:00Z 26116 20326(Kla_jeyes)/S
5 2020-11-10T00:00:00Z 2020-12-01T00:00:00Z 26116 20326(Kla_jeyes)/S
6 2020-11-20T00:00:00Z 2020-12-17T00:00:00Z 26116 20326(Kla_jeyes)/S
7 2020-11-30T00:00:00Z 2020-12-21T00:00:00Z 26116 20326(Kla_jeyes)/S
8 2020-12-10T00:00:00Z 2020-12-31T00:00:00Z 26116 20326(Kla_jeyes)/S
9 2020-12-20T00:00:00Z 2021-01-02T00:00Z 26116,46594 26116,42351 20326(Kla_jeyes)/S

...VALIDATED.

Validate and Process SKR in /media/KSR/KSK41-2021-Q1/kser-root-2021-q1-6.xml...

1 2021-01-01T00:00:00Z 2021-01-22T00:00:00Z 42351,26116
2 2021-01-11T00:00:00Z 2021-02-01T00:00:00Z 42351
3 2021-01-21T00:00:00Z 2021-02-11T00:00:00Z 42351
4 2021-01-31T00:00:00Z 2021-02-21T00:00:00Z 42351
5 2021-02-10T00:00:00Z 2021-03-01T00:00:00Z 42351
6 2021-02-20T00:00:00Z 2021-03-13T00:00:00Z 42351
7 2021-03-02T00:00:00Z 2021-03-23T00:00Z 42351
8 2021-03-12T00:00:00Z 2021-04-02T00:00Z 42351
9 2021-03-22T00:00:00Z 2021-04-12T00:00Z 14631,42351

*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***

...PASSED.

SHA256 hash of SKR:
D0D682FF1BDDCC746C1324B663793E3B63C1AEDD992F96FSFCSGB195FE30643

>> button speculate minim Yucatan beeves suspect swaddled hydraulics glue barbecue bluebird potato flatfoot insert a concert provincial Arsen recovery robust tambourine endow customer prefer Yucatan payday crossover spaniel bottomless ta lion torpedo affix decimal <<

Reading KSK schedule "normal(2017)" from "kskschedule.json":

1 20326(Kla_jeyes)/S
2 20326(Kla_jeyes)/S
3 20326(Kla_jeyes)/S
4 20326(Kla_jeyes)/S
5 20326(Kla_jeyes)/S
6 20326(Kla_jeyes)/S
7 20326(Kla_jeyes)/S
8 20326(Kla_jeyes)/S
9 20326(Kla_jeyes)/S

Generated new SKR in /media/KSR/KSK41-2021-Q1/kser-root-2021-q1-6.xml:

1 2021-01-01T00:00:00Z 2021-01-22T00:00:00Z 26116,42351 20326(Kla_jeyes)/S
2 2021-01-11T00:00:00Z 2021-02-01T00:00:00Z 42351 20326(Kla_jeyes)/S
3 2021-01-21T00:00:00Z 2021-02-11T00:00:00Z 42351 20326(Kla_jeyes)/S
4 2021-01-31T00:00:00Z 2021-02-21T00:00:00Z 42351 20326(Kla_jeyes)/S
5 2021-02-10T00:00:00Z 2021-03-01T00:00:00Z 42351 20326(Kla_jeyes)/S
6 2021-02-20T00:00:00Z 2021-03-13T00:00:00Z 42351 20326(Kla_jeyes)/S
7 2021-03-02T00:00Z 2021-03-23T00:00Z 42351 20326(Kla_jeyes)/S
8 2021-03-12T00:00Z 2021-04-02T00:00Z 42351 20326(Kla_jeyes)/S
9 2021-03-22T00:00Z 2021-04-12T00:00Z 14621,42351 20326(Kla_jeyes)/S

SHA256 hash of SKR:
CONJUGAID09C5F2FB9230A66F57F15B9A819211A5F9DC1D1C7415513001

>> slowdown penetrate stapler retraction ratchet savagery offload October drifter inferno physique pocketful artist parag on dwelling Wichita hamlet examine dogged outfielder physique autobiography ratchet forever Belfast recover drainage hydraulic backfield Babylon chairlift adviser" <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_3_glibc_2_5_x86_64.so.5.02 Slot-0
### Back up the Newly Created SKR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>CA executes the following commands using the terminal window:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) List the contents of the KSRFD by executing:</td>
<td>J0</td>
<td>19.01</td>
</tr>
<tr>
<td></td>
<td><code>ls -ltr /media/KSR</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Copy the contents of the KSRFD to the HSMFD by executing:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cp -pr /media/KSR/*</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: Confirm overwrite by entering &quot;y&quot; if prompted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) List the contents of the HSMFD to verify it has been copied successfully by executing:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ls -ltr</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Unmount the KSRFD by executing:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>umount /media/KSR</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>CA removes the KSRFD containing the SKR files, then gives it to RKOS.</td>
<td>J0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>CA deactivates the HSM by performing the following steps:</td>
<td>J0</td>
<td>19.01</td>
</tr>
<tr>
<td></td>
<td>Note: CA will use OP cards not previously utilized in this ceremony if available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) CA displays the HSM activity logging terminal window</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Select &quot;2.Set Offline&quot;, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) When &quot;Set Offline?&quot; is displayed, press ENT to confirm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) When &quot;Insert Card OP #X?&quot; is displayed, insert the OP card from the card holder.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) When &quot;PIN?&quot; is displayed, enter &quot;11223344&quot;, then press ENT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) When &quot;Remove Card?&quot; is displayed, remove the OP card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) Repeat steps e) to g) for the 2nd and 3rd OP cards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confirm the &quot;READY&quot; LED on the HSM is OFF.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IW records which cards were used below. Each card is returned to its designated card holder after use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1st OP card 4 of 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2nd OP card 5 of 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3rd OP card 6 of 7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: If the card is unreadable, gently wipe its metal contacts and try again.
### 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>28</td>
<td>CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. &lt;br&gt;<strong>Note:</strong> DO NOT unplug the cable connections on the laptop.</td>
<td>JF</td>
<td>19:05</td>
</tr>
<tr>
<td>29</td>
<td>CA places the HSM into a prepared TEB, then seals it.</td>
<td>JP</td>
<td>19:06</td>
</tr>
<tr>
<td>30</td>
<td>CA performs the following steps:&lt;br&gt; a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.&lt;br&gt;b) Confirm with IW that the TEB number and HSM serial number match below.&lt;br&gt;c) Initial the TEB along with IW using a ballpoint pen.&lt;br&gt;d) Give IW the sealing strips for post-ceremony inventory.&lt;br&gt;e) Place the HSM TEB on the cart.</td>
<td>JF</td>
<td>19:08</td>
</tr>
</tbody>
</table>

**HSM5W: TEB # BB51184239 / Serial # H1903017**
Act 4: 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 CO 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 into Tier 5 (Safe Room) to return COs’ 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. | **JF** | **9:10** |
# find -P /media/HSMD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist

SHA-256: c41ebb6f36a4d71797fecedb8e8b0f970059b0771214807c00a061e99eb89682
PGP Words: snowslide Burlington shamrock hemisphere Christmas Pandora stopwatch bookseller preshrunk yesteryear spyglass suspicious orca Medusa artist mosquito aardvark examine ruff led inception atlas belowground merit informant aardvark Orlando fallout ultimate quiver provincial prefer Istanbul
## 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>JD</td>
<td>19:10</td>
</tr>
</tbody>
</table>
| 3    | CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content:  
  a) `lspadmin -p HP -o copies=default=2`  
  b) `hsmfd-hash -p`  
  Note: One copy for audit bundle and one copy for HSMFD package.                                                                                                                                     | JD       | 19:11 |
| 4    | CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltr`                                                                                                    | JD       | 19:12 |
| 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`                                                              | JD       | 19:12 |
| 6    | CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.                                                                                       | JD       | 19:13 |
| 7    | CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: `df`                                                                                      | JD       | 19:13 |
| 8    | CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD:  
  a) `umount /dev/sdc1`  
  b) `mkfs.vfat -n HSMFD -I /dev/sdc1`  
  c) `mount /dev/sdc1 /media/HSMFD1`  
  d) `cp -pR * /media/HSMFD1`                                                                                                           | JD       | 19:15 |
| 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 -m`  
  b) `umount /media/HSMFD1`                                                                                                            | JD       | 19:15 |
| 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.                                                                 | JD       | 19:16 |
| 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.                                                                                      | JD       | 19:18 |
| 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.                                                                                      | JD       | 19:19 |
| 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.                                                                                      | JD       | 19:20 |
| 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.                                                                                    | JD       | 19:21 |
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

2020-04-23T18:29:05+0000
ttyS0

// H1903017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2

// BBL CRC32: 5e1dc989f2

// ttyS0  Running applicationBootLoader at 0x87FDC0000

// ttyS0  H1903017 011403 ABL 030 : Tamper Challenge Response Key

// ttyS0  ABL CRC32: 0xe7b031fa

// ttyS0  #

// ttyS0  ASL tamper record #

// ttyS0  #

// ttyS0  #

// ttyS0  Current Tamper Counts (decimal 0-255):

// ttyS0  -------------------------------

// ttyS0  vnxtoosTamperCount: 0

// ttyS0  vintoolsTamperCount: 5

// ttyS0  vbooosTamperCount: 0

// ttyS0  maxstrtamperCount: 0

// ttyS0  minestrTamperCount: 0

// ttyS0  meshTamperCount: 0

// ttyS0  extampSMKTamperCount: 0

// ttyS0  extampMKTamperCount: 0

// ttyS0  tempdiffTamperCount: 0

// ttyS0  ptTamperCount: 5

// ttyS0  restartTamperCount: 14

// ttyS0  Current tamper bitmaps:

// ttyS0  -------------------------------

// ttyS0  currentTamper bitmap: 0x0000 0b 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111

// ttyS0  currentTamper bitmap: 0x0000 0b 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111

// ttyS0  lastTamper bitmap: 0x0080 0b 11110000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

// EXT_POWER_DOWN
Bitmapped Change Record (most recent first):

Running cryptoApplication at 0xeef00000
Jumping to startup 0 0x001c3784
Board is P2020806
board_mpc_init: 2 cpu
Cpu_clk=1000000000, Sys_clk=100000000, CCBC=500000000
System page at phys:0000b000 user:0000b000 kern:0000b000
Starting next program at v015713c
Starting X-Series Kernel
Copyright Ultra Electronics AW. All Rights Reserved.
Sat Jan  9 04:45:17 1971
Starting auditd v2.0 ... started.
Interface 0 configured for IPv6.
Interface 0 configured for IPv4.
Interface 1 configured for IPv6.
Interface 1 configured for IPv4.
route: writing to routing socket: Network is unreachable
add net default: gateway ::: Network is unreachable
route: writing to routing socket: Network is unreachable
add net default: gateway 0.0.0.0: Network is unreachable
Starting USB driver...
9860 v3.4 Kyeper Application - May 19 2017 15:48:58
2020-04-23T18:29:12+0000  ttyS0 Running DKS POST Test
2020-04-23T18:29:12+0000  ttyS0 DKS POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running Triple DKS POST Test
2020-04-23T18:29:12+0000  ttyS0 Triple DKS POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running ABS POST Test
2020-04-23T18:29:12+0000  ttyS0 ABS POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running SHA1 POST Test
2020-04-23T18:29:12+0000  ttyS0 SHA1 POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running SHA2 POST Test
2020-04-23T18:29:12+0000  ttyS0 SHA2 POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running RandomGen POST Test
2020-04-23T18:29:12+0000  ttyS0 RandomGen POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running RSA POST Test
2020-04-23T18:29:12+0000  ttyS0 RSA POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running DSA POST Test
2020-04-23T18:29:12+0000  ttyS0 DSA POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running SEED POST Test
2020-04-23T18:29:12+0000  ttyS0 SEED POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running RIPemd160 POST Test
2020-04-23T18:29:12+0000  ttyS0 RIPemd160 POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running ECC POST Test
2020-04-23T18:29:12+0000  ttyS0 ECC POST Test Passed
2020-04-23T18:29:12+0000  ttyS0 Running HMAC POST Tests
2020-04-23T18:29:12+0000  ttyS0 HMAC POST Tests Passed
2020-04-23T18:29:12+0000  ttyS0 Audit on 9/1/1971 04:45:23 00100008
2020-04-23T18:29:12+0000  ttyS0
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Keyper 9860-2 Serial Number M1903017</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Memory Usage:</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 RAM (free/total) 19284/52680b</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Flash (free/total) 18896/12896b</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 black store 524b</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 statistics 112b</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 other 116b</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 netStore (free/total) 19784/12896b</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Network Configuration:</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Interface 0:</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Interface 1:</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Interface Address(see): 02:00:6C:00:C4:9A / 192.168.0.2/24 , 2001::2e0:6cfe:ff:fe00:c49a/64</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Interface Address(see): 00:00:6C:00:C4:9B / 192.168.1.2/24 , 2001::1:2e0:6cfe:ff:fe00:c49b/64</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 NIS Port 0: 05000</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 NIS Port 1: 03000</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Default Gateway(see): 0.0.0.0 ::</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 Software Versions:</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 HSL 030 ABL 021 App 034</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 CPLD Version:</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80 1.9</td>
</tr>
<tr>
<td>2020-04-23T18:29:13+0000</td>
<td>tty80</td>
</tr>
</tbody>
</table>
tty80  SCK Firmware Version:
tty80  OSOS-R2.99-N1.20
tty80  McListener: Created IPv4 socket 12 on port 3000.
tty80  McListener: Created IPv6 socket 13 on port 3000.
tty80  McListener: Created IPv4 socket 19 on port 5000.
tty80  McListener: Created IPv6 socket 20 on port 5000.
tty80  McListener: Created IPv4 socket 21 from address 192.168.0.1.
tty80  McListener: Accepted connection on socket 23 from address 192.168.0.1.
tty80  CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
## 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) `lpadmin -p HP -o copies=default=1 -o fit-to-page=default=true`        | JD       | 19:25 |
|      | b) `enscript -2Gr script-202004*.log`                                    |          |       |
|      | c) `enscript -Gr --font="Courier8" ttyaudit-tty*-202004*.log`            |          |       |
|      | 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`                                                            | JD       | 19:25 |
|      | b) `umount /media/HSMFD`                                                |          |       |
|      | 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.                                    | JD       | 19:26 |
|      | b) Turn OFF the laptop by pressing the power button.                      |          |       |
|      | c) Disconnect all connections from the laptop.                           |          |       |
| 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. | JD       | 19:28 |
| 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. | JD       | 19:29 |
|      | b) Confirm with IW that the TEB 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 OS DVD TEB on the cart.                                     |          |       |
|      | **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384**                |          |       |
| 20   | CA distributes the remaining HSMFDs:  
|      | 2 for IW (for audit bundles).                                             | JD       | 19:29 |
|      | 2 for RKOS (for SKR exchange with RZM and process review).                |          |       |
### 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>J9</td>
<td>19:31</td>
</tr>
<tr>
<td>22</td>
<td>CA performs the following steps:</td>
<td>J0</td>
<td>19:32</td>
</tr>
<tr>
<td></td>
<td>a) Read aloud the TEB number and laptop serial number, then show it to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the audit camera above for participants to see.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Confirm with IW that the TEB number and laptop serial number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>matches with the information below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Initial the TEB along with IW using a ballpoint pen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Give IW the sealing strips for post-ceremony inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Place the laptop TEB on the cart.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Laptop3: TEB # BB81420121 / Service Tag # C3SVSG2

### Place Crypto Officer Credentials into TEBs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>CA perform the following steps sequentially for the COs listed below:</td>
<td>J0</td>
<td>19:41</td>
</tr>
<tr>
<td></td>
<td>a) Gather the OP TEB and plastic case prepared for the CO.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Take the CO's OP card from the card holder and place it inside of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>plastic case.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Place the plastic case into the prepared TEB, read aloud the TFR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>number and description, then seal it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Initial the TEB with a ballpoint pen, and give IW the sealing strips</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>for post-ceremony inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) IW inspects the TEB, confirms the TEB number with the list below,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>then initials it with a ballpoint pen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) IW writes the date and time, then signs the tale of IW's script, then</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA initials the entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) IW places the TEBs on the ceremony table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h) Repeat steps for the remaining COs' credentials on the list.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CO4: Carlos Martínez  
OP TEB # BB91951363

CO5: Olafur Gudmundsson  
OP TEB # BB91951362

CO6: Nicholas Antoniello  
OP TEB # BB91951361
<table>
<thead>
<tr>
<th>CO</th>
<th>Card Type</th>
<th>TEB #</th>
<th>Printed Name</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
<th>CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO4</td>
<td>OP 4 of 7</td>
<td>OP TEB #</td>
<td>Jonathan Denison</td>
<td></td>
<td>2020 Apr 23</td>
<td>19:36</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BB91951363</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 #</td>
<td>Jonathan Denison</td>
<td></td>
<td>2020 Apr 23</td>
<td>19:39</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BB91951362</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 #</td>
<td>Jonathan Denison</td>
<td></td>
<td>2020 Apr 23</td>
<td>19:41</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BB91951361</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>JD</td>
<td>19:42</td>
</tr>
<tr>
<td>25</td>
<td>SSC1 opens Safe #1 while shielding the combination from the camera.</td>
<td>JD</td>
<td>19:43</td>
</tr>
<tr>
<td></td>
<td>Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.</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 &quot;Open Safe&quot; 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>JD</td>
<td>19:49</td>
</tr>
<tr>
<td>27</td>
<td>CA performs the following steps to return each piece of equipment to the safe:</td>
<td>JD</td>
<td>19:47</td>
</tr>
<tr>
<td></td>
<td>a) CAREFULLY remove the equipment TEB from the cart.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Write the date, time, and signature on the safe log where &quot;Return&quot; is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW verifies the safe log entry, then initials it.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HSM5W: TEB # BB51184239  
Laptop3: TEB # BB81420121  
OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384

## 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 &quot;Close Safe&quot; is indicated. IW verifies the entry, then initials it.</td>
<td>JD</td>
<td>19:47</td>
</tr>
<tr>
<td>29</td>
<td>SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked 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>JD</td>
<td>19:48</td>
</tr>
<tr>
<td>30</td>
<td>CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).</td>
<td>JD</td>
<td>19:48</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 into Tier 5 (Safe Room.)</td>
<td>JD</td>
<td>19:49</td>
</tr>
<tr>
<td>32</td>
<td>SSC2 opens Safe #2 while shielding the combination from the camera.</td>
<td>JD</td>
<td>19:51</td>
</tr>
<tr>
<td></td>
<td>Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.</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 &quot;Open Safe&quot; 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>JD</td>
<td>19:51</td>
</tr>
</tbody>
</table>
### Return Crypto Officer 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>IW performs the following steps sequentially to return the required TEBs:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) IW reads aloud the TEB number, then verifies the integrity of the</td>
<td>J0</td>
<td>19:59</td>
</tr>
<tr>
<td></td>
<td>TEB while showing it to the audit camera above</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) After the CA operates the guard key in the bottom lock, IW uses</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the CO's tenant key to operate the top lock and opens the CO's</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) IW reads aloud the safe deposit box number, places the TEB inside,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>then closes and locks the safe deposit box with assistance from the CA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) IW writes the date and time, then signs the safe log where &quot;Return&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is indicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) CA verifies the completed safe log entry, then initial it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO4: Carlos Martinez</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1068</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB91951363</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO5: Olafur Gudmundsson</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1789</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB91951362</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CO6: Nicolas Antoniello</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Box # 1073</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP TEB # BB91951361</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 safe deposit boxes are closed and locked, SSC2 writes the date</td>
<td>J0</td>
<td>19:54</td>
</tr>
<tr>
<td></td>
<td>and time, then signs the safe log where &quot;Close Safe&quot; is indicated. IW</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>verifies the safe log entry, then initial it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>SSC2 returns the safe log back to Safe #2, closes the safe door, pulls</td>
<td>J0</td>
<td>20:00</td>
</tr>
<tr>
<td></td>
<td>up on the handle, and ensures it's locked by spinning the dial at least</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>two full revolutions each way, counter-clockwise then clockwise. CA and IW</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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, and SSC2 leave Tier 5 (Safe Room) returning to Tier 4 (Key</td>
<td>J0</td>
<td>20:00</td>
</tr>
<tr>
<td></td>
<td>Ceremony Room).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Place Crypto Officer Keys into TEBs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
</table>
| 38   | CA performs the following steps sequentially for the COs key listed below:  
  a) Gather the CO key TEB and envelope prepared for the CO.  
  b) IW gives the CO key to CA who then places it inside of the envelope.  
  c) Place the envelope into the prepared TEB, read aloud the TEB number and description, then seal it.  
  d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory.  
  e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.  
  f) Repeat steps for remaining COs' keys on the list. | Jd | 20.11 |

**CO4: Carlos Martinez**  
Key TEB # BB91951358

**CO5: Olafur Gudmundsson**  
Key TEB # BB91951359

**CO6: Nicolas Antoniello**  
Key TEB # BB91951360

Note: The COs' keys will be promptly returned to the COs who will sign a second key declaration form confirming receipt. The completed declaration forms will be available on the IANA web page along with the standard post-ceremony materials.
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Carlos Martínez hereby attest that my safe deposit box key for safe deposit box #1068 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in TEB #BB91951284 before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into TEB #BB91951358 before the key was returned to me.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name  CARLOS MARTÍNEZ  
Signature  

Date  29/04/2020  (April 25, 2020)
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Olafur Gudmundsson hereby attest that my safe deposit box key for safe deposit box #1789 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in TEB #BB91951277 before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into TEB #BB91951359 before the key was returned to me.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name Olafur Gudmundsson

Signature

Date 2020/4/27
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Nicolas Antoniello hereby attest that my safe deposit box key for safe deposit box #1073 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in TEB #BB91951289 before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into TEB #BB91951360 before the key was returned to me.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name
Nicolas Antoniello

Signature

Date 4/27/2020
Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Joao Luis Silva Damas hereby attest that my safe deposit box key for safe deposit box #1068 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in TEB #BB91951281 before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into TEB #NULL before the key was returned to me. AS MY KEY WAS NOT USED IN THIS KSK CEREMONY IT WAS RETURNED TO ME IN THE SAME ORIGINAL TEB BAG THAT IT WAS TRANSFERRED TO ME IN.

I attest the safe deposit box key was returned to me with no indication of temper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name ______________  Joao Luis Silva Damas ______________________

Signature ______________  [Signature] ______________________

Date ______________  27 - April - 2020 ______________________
Act 5: Close the Key Signing Ceremony

The CA will finish the ceremony by performing the following steps:

- Read any exceptions that occurred during the ceremony
- Call the ceremony participants to sign the IW’s script
- Stop the online streaming and video recording
- Ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Prepare the audit bundle materials

Participants Sign 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>JG</td>
<td>20:59</td>
</tr>
<tr>
<td>2</td>
<td>CA asks any COs who are participating remotely if they have any concerns pertaining to the</td>
<td>JG</td>
<td>20:12</td>
</tr>
<tr>
<td></td>
<td>ceremony or exceptions which may have occurred.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CA calls each attendee on the participants list to proceed to the ceremony table and sign</td>
<td>JG</td>
<td>20:13</td>
</tr>
<tr>
<td></td>
<td>IW’s participants list. All signatories declare that this script is a true and accurate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>record of the ceremony.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CA reviews IW’s script, then signs the participants list.</td>
<td>JG</td>
<td>20:14</td>
</tr>
<tr>
<td>5</td>
<td>IW signs the list and records the completion time.</td>
<td>JG</td>
<td>20:16</td>
</tr>
</tbody>
</table>

Stop Online Streaming and 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 acknowledges the participation of the online participants, then notifies the SA to stop</td>
<td>JG</td>
<td>20:17</td>
</tr>
<tr>
<td></td>
<td>the online streaming.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>CA informs onsite participants of post ceremony activities.</td>
<td>JG</td>
<td>20:17</td>
</tr>
<tr>
<td>8</td>
<td>Ceremony participants take a group photo.</td>
<td>JG</td>
<td>20:20</td>
</tr>
<tr>
<td>9</td>
<td>CA acknowledges the participation of the COs, RZM, and Auditors in the call, then stops the</td>
<td>JG</td>
<td>20:21</td>
</tr>
<tr>
<td></td>
<td>call.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sign Out of Tier 4 (Key Ceremony Room) and Stop Recording

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initials</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room), SA, IW, and</td>
<td>JG</td>
<td>20:31</td>
</tr>
<tr>
<td></td>
<td>CA must remain in Tier 4 (Key Ceremony Room).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>CA requests that an SA stop the audit camera video recording.</td>
<td>JG</td>
<td>20:31</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>12</td>
<td>IW makes a copy of their script for off-site audit bundle containing:</td>
<td></td>
<td></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: <strong>20200216 00:00:00 to 20200424 00:00:00 UTC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) IW's attestation (See Appendix C on page 32).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) SA's attestation (See Appendix D on page 33 and Appendix E on page 34).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All TEBs are labeled **Root DNSSEC KSK Ceremony 41**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.
Appendix A: References

The numeric items listed below have 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/lana-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/lana-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-255 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 HSMFDe

The following is the main command invoked by this script:
find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist
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/lana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb∗

[5] ttyaudit: Is a perl script used to capture and logging the HSM output. The source code is available at https://github.com/lana-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/lana-org/dnssec-keytools

[8] printlog: Is a bash script used to print the Key Signing Log output from ksrsigner application. The source code is available at https://github.com/lana-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 -xvzf 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 pre-labeled 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 on page 32.

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 on page 33.

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 on page 34. 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: Jonathan Denison

Signature: [Signature]

Date: 2020 Apr 23
Appendix D: Access Control System Configuration Review (by SA)

In my review of the KMF'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: 20200216 00:00:00 to 20200424 00:00:00 UTC.

SA: [Signature]

Signature: [Signature]

Date: 2020 Apr 23
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 5th Edition (2020-04-07). There are no part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA:  Patrick Tudor

Signature: [Signature]

Date: 2020 Apr 23
Appendix F: CO4 Safe Deposit Box Key Chain of Custody

The following photo contains the CO4 Carlos Martinez Safe Deposit Box Key TEB # BB91951284 dispatched from the CO.
Appendix G: CO5 Safe Deposit Box Key Chain of Custody

The following photo contains the CO5 Olafur Gudmundsson Safe Deposit Box Key TEB # BB91951277 dispatched from the CO.
Appendix H: CO6 Safe Deposit Box Key Chain of Custody

The following photo contains the CO6 Nicolas Antoniello Safe Deposit Box Key TEB # BB91951289 dispatched from the CO.
Appendix I: CO3 Safe Deposit Box Key Chain of Custody

The following photo contains the CO3 Joao Damas Safe Deposit Box Key TEB # BB91951281 dispatched from the CO.

This key has been designated as a backup. The TEB will remain sealed in the courier envelope unless the situation dictates its use. It will be sent back to the CO after the ceremony in its sealed state post-ceremony.
ptudor@srx> show configuration
## Last commit: 2020-01-17 18:22:39 UTC by jjenkins
version 15.1X49-D170.4;
system {
    host-name srx;
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "XXXXXXXX"; ## SECRET-DATA
    }
    name-server {
        192.0.42.53;
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
class super-user;
authentication {
    encrypted-password "XXXXXXXX"; ## SECRET-DATA
}
}
user sfreeark {
    uid 2002;
    class super-user;
    authentication {
        encrypted-password "XXXXXXXX"; ## SECRET-DATA
    }
}
password {
    format sha512;
}
}
services {
    ssh {
        root-login deny;
    }
}
syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    file messages {
        any critical;
        authorization info;
    }
    file interactive-commands {
        interactive-commands error;
    }
    max-configurations-on-flash 5;
    max-configuration-rollback 20;
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
chassis {
    config-button no-rescue no-clear;
    aggregated-devices {
        ethernet {
            device-count 2;
        }
}
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
security {
    pki {
        ca-profile root-ca {
            ca-identity "ICANN Root CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
        }
        administrator {
            email-address "cbo-team@iana.org";
        }
    }
    ca-profile intermediate-ca {
ca-identity "ICANN SSL CA";
revocation-check {
  crl { 
    disable on-download-failure;
  }
}
ike {
  proposal ike-proposal-KMF {
    authentication-method rsa-signatures;
    dh-group group24;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
  }
  policy ike-policy-KMF {
    proposals ike-proposal-KMF;
    certificate {
      local-certificate ksk-lax;
    }
  }
  gateway Gateway-to-KMF-East {
    ike-policy ike-policy-KMF;
    address 64.124.6.5;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface ge-0/0/15;
    version v2-only;
  }
}
ipsec {
  proposal IPSecProposal {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 7200;
  }
  policy defaultPolicy {
    perfect-forward-secrecy {
      keys group5;
    }
    proposals IPSecProposal;
  }
  vpn vpn-to-KMF-East {
    bind-interface st0.1;
    ike {
      gateway Gateway-to-KMF-East;
      ipsec-policy defaultPolicy;
    }
    establish-tunnels immediately;
  }
}
screen {
  ids-option external-screen {
    icmp {
      ping-death;
    }
    ip {
      source-route-option;
      tear-drop;
    }
    tcp {
      syn-flood {
        alarm-threshold 1024;
        attack-threshold 200;
        source-threshold 1024;
        destination-threshold 2048;
        timeout 20;
      }
    }
  }
}
nat {
    source {
        rule-set internal-to-external {
            from zone [ access guest wifi ];
            to zone untrust;
            rule source-nat-rule {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
    policies {
        from-zone access to-zone untrust {
            policy allow-mail {
                match {
                    source-address [ ACC ACS EVM IMS ];
                    destination-address icann;
                    application junos-smtp;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
            policy allow-dns {
                match {
                    source-address [ ACC ACS EVM IMS ];
                    destination-address [ icann-dns google-dns ];
                    application [ junos-dns-udp junos-dns-tcp ];
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
            policy allow-simplex {
                match {
                    source-address IDP;
                    destination-address simplex;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
        from-zone access to-zone video {
            policy access-to-video {
                match {
                }
            }
        }
    }
}
source-address IMS;
   destination-address kmf_west_video;
application junos-icmp-all;
} 
then { 
   permit;
} 
} 
from-zone access to-zone ipsec {
   policy allow-access-to-ipsec {
      match {
         source-address [ ACS ACC ];
         destination-address [ kmf_east_acs kmf_east_acc ];
         application any;
      }
      then {
         permit;
         log {
            session-close;
         }
      }
   }
   policy allow-icmp {
      match {
         source-address any;
         destination-address any;
         application junos-icmp-ping;
      }
      then {
         permit;
      }
   }
   policy allow-access-access {
      match {
         source-address kmf_west_access;
         destination-address kmf_east_access;
         application any;
      }
      then {
         permit;
      }
   }
}
from-zone ipsec to-zone access {
   policy allow-ipsec-to-access {
      match {
         source-address [ kmf_east_acs kmf_east_acc ];
         destination-address [ ACS ACC ];
         application any;
      }
      then {
         permit;
         log {
            session-close;
         }
      }
   }
   policy allow-icmp {
      match {
         source-address any;
         destination-address any;
         application junos-icmp-ping;
      }
      then {
         permit;
      }
   }
}
policy allow-access-access {
    match {
        source-address kmf_east_access;
        destination-address kmf_west_access;
        application any;
    }
    then {
        permit;
    }
}

from-zone video to-zone ipsec {
    policy allow-video-to-ipsec {
        match {
            source-address VSS;
            destination-address kmf_east_vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_west_video;
            destination-address kmf_east_video;
            application any;
        }
        then {
            permit;
        }
    }
}

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

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

from-zone ipsec to-zone video {
    policy allow-ipsec-to-video {
        match {
            source-address kmf_east_vss;
            destination-address VSS;
            application any;
        }
        then {
        }
    }
}
permit;
log {
  session-close;
}
}
policy allow-icmp {
  match {
    source-address any;
    destination-address any;
    application any;
  }
  then {
    permit;
  }
}
policy allow-access-video {
  match {
    source-address kmf_east_video;
    destination-address kmf_west_video;
    application any;
  }
  then {
    permit;
  }
}
from-zone access to-zone access {
  policy allow-access {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone video to-zone untrust {
  policy allow-mail {
    match {
      source-address VSS;
      destination-address icann;
      application junos-smtp;
    }
    then {
      permit;
      log {
        session-close;
      }
    }
  }
}
default-policy {
  deny-all;
}
}
zones {
  security-zone access {
    address-book {
      address ACS 10.4.28.203/32;
      address ACC 10.4.28.202/32;
      address IDP 10.4.28.201/32;
      address EVM 10.4.28.200/32;
      address IMS 10.4.28.204/32;
      address E1 10.4.28.210/32;
      address E3 10.4.28.212/32;
    }
  }
  security-zone video {
    address-book {
      address ACS 10.4.28.203/32;
      address ACC 10.4.28.202/32;
      address IDP 10.4.28.201/32;
      address EVM 10.4.28.200/32;
      address IMS 10.4.28.204/32;
      address E1 10.4.28.210/32;
      address E3 10.4.28.212/32;
    }
  }
  security-zone untrust {
    address-book {
      address ACS 10.4.28.203/32;
      address ACC 10.4.28.202/32;
      address IDP 10.4.28.201/32;
      address EVM 10.4.28.200/32;
      address IMS 10.4.28.204/32;
      address E1 10.4.28.210/32;
      address E3 10.4.28.212/32;
    }
  }
}
address E4 10.4.28.213/32;
address kmf_west_access 10.4.28.192/26;
address localnet 10.4.28.0/24;
address-set iris-scanners {
    address E1;
    address E3;
    address E4;
}
}
}
}
}
}
security-zone untrust {
    address-book {
        address icann 192.0.32.0/20;
        address icann-dns 192.0.42.53/32;
        address googledns1 8.8.8.8/32;
        address googledns2 8.8.4.4/32;
        address simplex1 216.224.218.31/32;
        address simplex2 216.224.218.32/32;
        address simplex3 216.224.218.33/32;
        address simplex4 216.224.218.34/32;
        address-set google-dns {
            address googledns1;
            address googledns2;
        }
        address-set simplex {
            address simplex1;
            address simplex2;
            address simplex3;
            address simplex4;
        }
    }
    screen external-screen;
    interfaces {
        ge-0/0/15.0 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
}
security-zone video {
    address-book {
        address kmf_west_video 10.4.28.128/26;
        address VSS 10.4.28.150/32;
        address C1 10.4.28.151/32;
        address C2 10.4.28.152/32;
        address C3 10.4.28.153/32;
        address-set cameras {
            address C1;
            address C2;
            address C3;
        }
    }
    interfaces {
        irb.1 {
host-inbound-traffic {
    system-services {
        ping;
    }
}

security-zone guest {
    address-book {
        address STR 10.4.28.20/32;
        address VCC 10.4.28.22/32;
        address kmf_west_guest 10.4.28.0/25;
    }
    interfaces {
        irb.2 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}

security-zone ipsec {
    address-book {
        address kmf_east_access 10.4.29.192/26;
        address kmf_east_video 10.4.29.128/26;
        address kmf_east_acs 10.4.29.204/32;
        address kmf_east_acc 10.4.29.202/32;
        address kmf_east_idp 10.4.29.201/32;
        address kmf_east_evm 10.4.29.200/32;
        address kmf_east_ims 10.4.29.203/32;
        address kmf_east_E1 10.4.29.210/32;
        address kmf_east_E2 10.4.29.211/32;
        address kmf_east_E3 10.4.29.212/32;
        address kmf_east_E4 10.4.29.213/32;
        address kmf_east_vss 10.4.29.150/32;
        address kmf_east_C1 10.4.29.151/32;
        address kmf_east_C2 10.4.29.152/32;
        address kmf_east_C3 10.4.29.153/32;
    }
    interfaces {
        st0.1 {
            host-inbound-traffic {
                system-services {
                    ping;
                    ike;
                }
            }
        }
    }
}

security-zone wifi {
    address-book {
        address kmf_west_wifi 10.100.1.0/24;
    }
    interfaces {
        irb.3 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
}
interfaces {
  ge-0/0/6 {
    ether-options {
      802.3ad ae0;
    }
  }
  ge-0/0/7 {
    ether-options {
      802.3ad ae0;
    }
  }
  ge-0/0/15 {
    unit 0 {
      family inet {
        address 192.0.35.202/26;
      }
    }
  }
  ae0 {
    aggregated-ether-options {
      lacp {
        active;
      }
    }
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members [ vlan-access vlan-guest vlan-video vlan-wifi ];
        }
      }
    }
  }
  irb {
    unit 0 {
      description "access vlan";
      family inet {
        address 10.4.28.193/26;
      }
    }
    unit 1 {
      description "video vlan";
      family inet {
        address 10.4.28.129/26;
      }
    }
    unit 2 {
      description "guest vlan";
      family inet {
        address 10.4.28.1/25;
      }
    }
    unit 3 {
      description "wifi vlan";
      family inet {
        address 10.100.1.1/24;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        filter {
          input route-engine-filter;
        }
      }
    }
  }
}
st0 {
  unit 1 {
    description "IPSec KMF-West";
    family inet;
  }
}

routing-options {
  static {
    route 0.0.0.0/0 next-hop 192.0.35.201;
    route 10.4.29.0/24 next-hop st0.1;
    route 64.124.6.5/32 next-hop 192.0.35.201;
  }
}

policy-options {
  prefix-list resolver-servers {
    apply-path "system name-server <*>";
  }
  prefix-list local-prefixes {
    10.4.28.0/24;
  }
  prefix-list ntp-servers {
    129.6.15.28/32;
    129.6.15.29/32;
  }
  prefix-list remote-ike-peers {
    apply-path "security ike gateway <*> address <*>";
  }
}

firewall {
  family inet {
    filter route-engine-filter {
      term deny-icmp-redirects {
        from {
          protocol icmp;
          icmp-type redirect;
        }
        then {
          discard;
        }
      }
      term allow-icmp {
        from {
          protocol icmp;
          icmp-type [ echo-request echo-reply unreachable time-exceeded ];
        }
        then {
          policer small-bw-limit;
          accept;
        }
      }
      term allow-traceroute {
        from {
          protocol udp;
          port 33434-33534;
        }
        then {
          policer small-bw-limit;
          accept;
        }
      }
      term allow-dns {
        from {
          source-prefix-list {
            resolver-servers;
          }
          protocol udp;
          source-port domain;
        }
        then {
          accept;
        }
      }
    }
  }
}
then {  
  policer small-bw-limit;
  accept;
}

}  

}  

}  

term allow-ntp {  
  from {  
    source-prefix-list {  
      local-prefixes;
      ntp-servers;
    }  
    protocol udp;
    port ntp;
  }  
  then {  
    policer small-bw-limit;
    accept;
  }  
}

term allow-establish {  
  from {  
    protocol tcp;
    tcp-established;
  }  
  then accept;
}

}  

}  

term allow-ipsec-esp {  
  from {  
    source-prefix-list {  
      remote-ike-peers;
    }  
    protocol esp;
  }  
  then accept;
}

term allow-ipsec-udp {  
  from {  
    source-prefix-list {  
      remote-ike-peers;
    }  
    protocol udp;
    port 500;
  }  
  then accept;
}

term allow-ike-fragments {  
  from {  
    source-prefix-list {  
      remote-ike-peers;
    }  
    is-fragment;
    protocol udp;
  }  
  then {  
    policer small-bw-limit;
    accept;
  }  
}

term allow-ssh {  
  from {  
    source-address {  
      10.4.29.193/32;
    }  
    protocol tcp;
    destination-port ssh;
  }  
  then accept;
term LAST {
    then {
        discard;
    }
}
policer small-bw-limit {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
vlangs {
    vlan-access {
        vlan-id 10;
        l3-interface irb.0;
    }
    vlan-guest {
        vlan-id 12;
        l3-interface irb.2;
    }
    vlan-video {
        vlan-id 11;
        l3-interface irb.1;
    }
    vlan-wifi {
        vlan-id 13;
        l3-interface irb.3;
    }
}

ptudor@srx>