Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 13
Thursday May 2, 2013

ICANN KSK Facility@Terremark NCR
18155 Technology Drive, Culpeper, VA 22701-3805

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

- **TEB** = Tamper Evident Bag (AMPAC, item #GCS1013 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large)
- **HSM** = Hardware Security Module
- **IW** = Internal Witness
- **SSC** = Safe Security Controller
- **KSR** = Key Signing Request
- **FD** = Flash Drive
- **CO** = Crypto Officer
- **MC** = Master of Ceremony
- **SKR** = Signed Key Response
- **CA** = Ceremony Administrator
- **SA** = System Administrator
- **IKOS** = ICANN KSK Operations Security
- **RZM** = Root Zone Maintainer

Participants

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

<table>
<thead>
<tr>
<th>Title</th>
<th>Printed Name/Citizenship</th>
<th>Signature</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Mehrmet Akcin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW1</td>
<td>Francisco Arias</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA1</td>
<td>Alexander Kulik</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC1</td>
<td>Julie Hedlund</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSC2</td>
<td>Patrick Jones</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA2</td>
<td>Matt Childs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO3</td>
<td>Olaf Kollman / NL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO4</td>
<td>Robert Seastrom / US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO5</td>
<td>Christopher Griffiths / US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO6</td>
<td>Gaurab Upadhyaya / NP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW1</td>
<td>Alejandro Bolivar / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW2</td>
<td>Sanju Varghese / Verisign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW3</td>
<td>Randy Whitney / Verizon Business</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW4</td>
<td>James Anderson / Neustar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW5</td>
<td>Edward .ewis / Neustar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW6</td>
<td>Russ Hcusley / Vigil Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW7</td>
<td>Mostafa Elghazaly / PricewarehouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW8</td>
<td>Sonia Wong / PricewarehouseCoopers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EW9</td>
<td>Olafur Gudmundsson/Shinkuro</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IW2 IKOS</td>
<td>Tomofumi Okubo</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note: Dual Occupancy enforced. CA leads ceremony. Only CAs, IWs, or SAs can enter ceremony room and/or escort other participants. Only CA+IW can enter safe room and/or escort other participants. CAs, SAs or IWs may let individuals out of the ceremony room but only when CA+IW remain in the ceremony room. No one may leave when CA+IW are in safe room. Participants must sign in and out of ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before completion of the ceremony. The SA starts filming before the participants enter the room.

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

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

Spelling:

- **AL-FAH**
- **BRAH-VOH**
- **CHAR-LEE**
- **DELL-TAH**
- **ECK-OH**
- **FORS-TROT**
- **GOLF**
- **HOH-TEL**
- **IN-DEE-AH**
- **JEW-LEE-ETT**
- **KEY-LOM**
- **LEE-MAH**
- **MIKE**
- **NO-VEM-BER**
- **OSS-CAH**
- **PAH-PAH**
- **KEH-BECK**
- **ROW-ME-OH**
- **SEE-AIR-RAH**
- **TANG-GO**
- **YOU-NEE-FORM**
- **VIK-TAH**
- **WISS-KEY**
- **ECKS-RAY**
- **YANG-KEY**
- **ZOO-LOO**
- **WUN**
- **TOO**
- **TREE**
- **FOW-ER**
- **FIFE**
- **SIX**
- **SEV-EN**
- **AIT**
- **NIN-ER**
- **ZEE-RO**
ICANN DNSSEC Script Exception

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

Instructions: Initial each step that has been completed below, e.g., B'T3. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th></th>
<th>IW notes date and time of key ceremony exception and signs here:</th>
<th>FA</th>
<th>18:02</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Before Step 4, Ixos left the room to bring SA Alex Kulik into the KMF

- End of DNSSEC Script Exception -
Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SA confirms that the videos are recorded and online streaming is live. IW confirms that all participants are signed into the Ceremony Room.</td>
<td>FA</td>
<td>17:56</td>
</tr>
</tbody>
</table>

Emergency Evacuation Procedures

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>CA or IW reviews emergency evacuation procedures with participants.</td>
<td>FA</td>
<td>17:56</td>
</tr>
</tbody>
</table>

Verify Time and Date

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room: Date and time: 2 May 2013 17:56</td>
<td>FA</td>
<td>17:56</td>
</tr>
</tbody>
</table>

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

Open Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>CA and IW1 escort SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.</td>
<td>FA</td>
<td>19:03</td>
</tr>
<tr>
<td>5.</td>
<td>SSC2, while shielding combination from camera, opens Safe #2.</td>
<td>FA</td>
<td>18:04</td>
</tr>
<tr>
<td>6.</td>
<td>SSC2 takes out safe log and prints name, date, time, signature, and reason (i.e. &quot;open safe&quot;) in safe log. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>18:05</td>
</tr>
</tbody>
</table>
COs extract OP Cards from safe deposit boxes

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>One by one, the selected COs checks the SO cards and retrieves the OP cards following the steps shown below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a) With the assistance of CA (and his/her common key), opens her/his safe deposit box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td># Common Key is bottom lock and CO Key is top lock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Returns SO cards, retains OP TEB and locks box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Makes an entry in safe log indicating verification of integrity of contents and OP TEB removal with box #, printed name, date, time and signature.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: if log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeat these steps until all cards are removed. IW1 initials this entry when all CO have finished.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 3: Olaf Kotkman</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box # 1239</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OP TEB # A14365411</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SO TEB # A14377121</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 4: Robert Seastrom</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box # 1260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OP TEB # A14365410</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SO TEB # A14377123</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 5: Christopher Griffiths</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box # 1240</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OP TEB # A15473416</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SO TEB # A14377125</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 6: Gaurab Upadhaya</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box # 1261</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OP TEB # A14365374</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SO TEB # A14377127</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CO 7: Alain Aina</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box # 1262</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OP TEB # BB21359019</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SO TEB # A14377129</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

version 1.7
ICANN DNSSEC Script Exception

Abbreviations

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

Instructions: Initial each step that has been completed below, e.g., BTS. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th></th>
<th>IW notes date and time of key ceremony exception and signs here:</th>
<th>1/4</th>
<th>18:14</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At step 7, COT Alain was not present in the ceremony, therefore his box was not opened.

- End of DNSSEC Script Exception -
ICANN DNSSEC Script Exception

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

Instructions: Initial each step that has been completed below, e.g., BTS. Note time.

Note Exception Time

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here:</td>
</tr>
<tr>
<td></td>
<td>FA</td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
</tr>
</tbody>
</table>

- Step II was not executed as there was no locksmith to escort out

- End of DNSSEC Script Exception -
Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Once all safe deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initial this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>18:14</td>
</tr>
<tr>
<td>9.</td>
<td>SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and card reader indicator is green.</td>
<td>FA</td>
<td>18:15</td>
</tr>
<tr>
<td>10.</td>
<td>IW1, CA, SSC2, and C0s leave safe room, with CP cards in TEBs, closing the door behind them.</td>
<td>FA</td>
<td>18:15</td>
</tr>
<tr>
<td>11.</td>
<td>SA escorts the locksmith out of the key management facility</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Open Equipment Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.</td>
<td>FA</td>
<td>18:18</td>
</tr>
<tr>
<td>13.</td>
<td>SSC1, while shielding combination from camera, opens Safe #1.</td>
<td>FA</td>
<td>18:19</td>
</tr>
<tr>
<td>14.</td>
<td>SSC1 takes out safe log and prints name, date, time, signature and reason (i.e., &quot;opened safe&quot;) in safe log. IW1 initial this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>18:19</td>
</tr>
</tbody>
</table>

Remove Equipment from Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>CA CAREFULLY removes HSM2 (in TEB) from the safe and completes the entry in the safe log indicating HSM Removal, TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initial this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign. HSM2: TEB# A2826763 / serial # K6002013 Verify the integrity of the other HSM that will not be in used this time. HSM1: TEB# BB24049988 / serial # K6002016 (last used)</td>
<td>FA</td>
<td>18:22</td>
</tr>
</tbody>
</table>
### Close Equipment Safe #1 and exit safe room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>SSC1 makes an entry including printed name, date, time and signature into the safe log indicating, &quot;Close safe&quot;. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>18:25</td>
</tr>
<tr>
<td>18.</td>
<td>SSC1 puts log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and door indicator light is green.</td>
<td>FA</td>
<td>18:26</td>
</tr>
<tr>
<td>19.</td>
<td>CA, SSC1 and IW1 leave the safe room with the equipment cart, closing the door to the safe room securely behind them.</td>
<td>FA</td>
<td>18:27</td>
</tr>
</tbody>
</table>
Act 2. Confirm and Sign the Key Signing Request

Set Up Laptop

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. Laptop1 (Dell ATG6400): TEB# A2826764 / serial# 41593712005</td>
<td>FA</td>
<td>18:27</td>
</tr>
<tr>
<td>2.</td>
<td>CA inspects the O/S DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. O/S DVD (Rev600) + HSMFD: TEB# BB21369020</td>
<td>FA</td>
<td>18:29</td>
</tr>
<tr>
<td>3.</td>
<td>CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from O/S DVD.</td>
<td>FA</td>
<td>18:35</td>
</tr>
<tr>
<td>4.</td>
<td>CA presses &quot;CTRL+ALT+F2&quot; to get a console prompt and logs in as root.</td>
<td>FA</td>
<td>18:35</td>
</tr>
</tbody>
</table>
| 5.   | CA enters the commands system-config-display --noui  
and  
killall Xorg  
CA ensures that external display works.                                                                                                            | FA      | 18:35  |
| 6.   | CA logs in as root.                                                                                                                                                                                         | FA      | 18:36  |
| 7.   | CA configures printer as default and prints test page by going to System > Administration > Printing.                                                                                                      | FA      | 18:38  |
| 8.   | CA opens a terminal window and maximizes its size for visibility by going to Applications > Accessories > Terminal.                                                                                             | FA      | 18:38  |
| 9.   | CA checks and fixes date and time on laptop based on wall clock ensuring UTC time zone has been chosen by going to System > Administration > Date and Time.                                                                 | FA      | 18:40  |
| 10.  | CA inserts USB port expander into laptop.                                                                                                                                                                  | FA      | 18:40  |
ICANN DNSSEC Script Exception

Abbreviations

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

Instructions: Initial each step that has been completed below, e.g., BTS. Note time.

Note Exception Time

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW notes date and time of key ceremony exception and signs here: FA 18:50</td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
</tr>
</tbody>
</table>

At step 17 there was no hash in the OS/DVD TEB. ikos got the hash from the publicly available copy of last East Coast Ceremony. The hashes matched.

— End of DNSSEC Script Exception —
### Format and label blank FD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>CA plugs a new FD into the laptop, then waits for it to be recognized by the O/S, closes the file system popup window and formats the drive by executing `dmsetup</td>
<td>grep -A 5 usb-storage<code>to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc).</code>umount /dev/sdal<code>to umounts the drive (change drive letter if necessary).</code>mkfs.vfat -n HSMFD -I /dev/sda` to execute a FAT32 format and label it as HSMFD.</td>
<td>FA</td>
</tr>
<tr>
<td>12.</td>
<td>CA repeats step 11 for the 2nd blank FD</td>
<td>FA</td>
<td>18:43</td>
</tr>
<tr>
<td>13.</td>
<td>CA repeats step 11 for the 3rd blank FD</td>
<td>FA</td>
<td>18:43</td>
</tr>
<tr>
<td>14.</td>
<td>CA repeats step 11 for the 4th blank FD</td>
<td>FA</td>
<td>18:44</td>
</tr>
<tr>
<td>15.</td>
<td>CA repeats step 11 for the 5th blank FD</td>
<td>FA</td>
<td>18:44</td>
</tr>
</tbody>
</table>

### Connect HSMFD

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.</td>
<td>CA plugs HSMFD into free USB slot on the laptop -NOT EXPANDER- and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.</td>
<td>FA</td>
<td>18:46</td>
</tr>
<tr>
<td>17.</td>
<td>Calculate the md5hash of the contents on the copied HSMFD. `find -P /media/HSMFD/ -maxdepth 1 -type f -print</td>
<td>sort</td>
<td>xargs cat</td>
</tr>
</tbody>
</table>

### Start Logging Terminal Session

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td>CA changes the default directory to the HSMFD by executing <code>cd /media/HSMFD</code></td>
<td>FA</td>
<td>18:51</td>
</tr>
<tr>
<td>19.</td>
<td>CA executes <code>script script-20130502.log</code> to start a capture of terminal output.</td>
<td>FA</td>
<td>18:51</td>
</tr>
</tbody>
</table>
Start Logging HSM Output

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.</td>
<td>CA connects a serial to USB null modem cable to laptop.</td>
<td>FA</td>
<td>18:51</td>
</tr>
<tr>
<td>21.</td>
<td>CA opens a second terminal screen and executes <code>cd /media/HSMFD</code> and executes <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port outputs. Note: <strong>DO NOT</strong> unplug USB serial port from laptop as this causes logging to stop.</td>
<td>FA</td>
<td>18:52</td>
</tr>
</tbody>
</table>

Power Up HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. HSM2: TEB# A2825763 / serial # K6002013</td>
<td>FA</td>
<td>18:53</td>
</tr>
<tr>
<td>23.</td>
<td>CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable b the back.</td>
<td>FA</td>
<td>18:54</td>
</tr>
<tr>
<td>24.</td>
<td>CA switches to the ttyaudit terminal window and connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with above. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it since the scripts that does the logging to the laptop adds a timestamp.)</td>
<td>FA</td>
<td>18:55</td>
</tr>
</tbody>
</table>

Enable/Activate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td>CA calls a CO, CO inspects the TEB for tamper evidence, opens the TEB and hands the OP card to the CA who places card in cardholder visible to all.</td>
<td>FA</td>
<td>18:56</td>
</tr>
<tr>
<td>26.</td>
<td>Repeat the step above until all OP cards are placed on the cardholder.</td>
<td>FA</td>
<td>18:58</td>
</tr>
<tr>
<td>27.</td>
<td>CA inserts 3 cards into HSM to activate the unit (via &quot;Set Online&quot; menu item). Type in the default PIN &quot;11223344&quot; when prompted. IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card <em>5</em> of 7 2nd OP card <em>4</em> of 7 3rd OP card <em>3</em> of 7</td>
<td>FA</td>
<td>19:00</td>
</tr>
</tbody>
</table>
April 16th, 2013

To Whom It May Concern:

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

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

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

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

Sincerely,

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

The SHA256 hash of the 2013 Q3 KSR file is:

298c20937ae7c95070fb5854f4e19ee3aa2f92e6839f5c61a24a3eff802ec6f1

The PGP wordlist for the hash above is:

breakup megaton bison molasses keyboard truncated
spearhead embezzle guidance Wichita endorse equation
upshot tolerance quiver torpedo reward combustion
physique trombonist Mohawk opulent escape frequency
rebirth direction concert Yucatan merit coherence
southward vacancy

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer, Cryptographic Business Operations
VeriSign, Inc.
ICANN DNSSEC Script Exception

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

Instructions: Initial each step that has been completed below, e.g., BTS. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th></th>
<th>IW notes date and time of key ceremony exception and signs here:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FA 19:05</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IW Describes exception and action below</td>
<td></td>
</tr>
</tbody>
</table>

- On step 35 the CA asked Russ to click 'Y'
- However there was a typo in the command and it had to be re-run. There were no issues with the re-run.

- End of DNSSEC Script Exception -
## Check Network between Laptop and HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.</td>
<td>CA connects HSM to laptop using Ethernet cable.</td>
<td>FA</td>
<td>19:01</td>
</tr>
<tr>
<td>29.</td>
<td>CA tests network connectivity between laptop and HSM by entering <code>ping 192.168.0.2</code> on the laptop terminal window and looking for responses. Ctrl-C to exit program.</td>
<td>FA</td>
<td>19:01</td>
</tr>
</tbody>
</table>

## Insert Copy of KSR to be signed

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.</td>
<td>The KSR is downloaded to the KSRFD and transferred to the facility by the IKOS. CA plugs FD labeled &quot;KSR&quot; with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA points out the KSR file to be signed then closes the file system window.</td>
<td>FA</td>
<td>19:02</td>
</tr>
</tbody>
</table>

## Execute KSR signer

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.</td>
<td>CA identifies the KSR to be signed and runs, in the terminal window <code>karsigner Kigat7v /media/KSR/kss-root-2013-q3-0.xml</code></td>
<td>FA</td>
<td>19:02</td>
</tr>
<tr>
<td>32.</td>
<td>The KSR signer will ask whether the HSM is activated or not as below. <strong>Activate HSM prior to accepting in the affirmative!!</strong> (y/n) : CA confirms that the HSM is online and then enters &quot;y&quot; to proceed to verification. <strong>Note: DO NOT enter &quot;y&quot; for the &quot;Is this correct y/n?&quot; yet.</strong></td>
<td>FA</td>
<td>19:03</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to identify him/herself, present identification document for IW1 to retain and read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN. IW1 enters RZM representative's name here: <strong>Alejandro Bolivar</strong></td>
<td>FA</td>
<td>19:04</td>
</tr>
<tr>
<td>34.</td>
<td>Participants match the hash read out with that displayed on the terminal. CA asks, &quot;are there are any objections&quot;?</td>
<td>FA</td>
<td>19:05</td>
</tr>
<tr>
<td>35.</td>
<td>CA then enters &quot;y&quot; in response to &quot;Is this correct y/n?&quot; to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in <code>/media/KSR/skr-root-2013-q3-0.xml</code></td>
<td>FA</td>
<td>19:09</td>
</tr>
</tbody>
</table>
$ krsigner K/b grantsv /krs-root-2010-q4-1.xml
Starting: krsigner K/b grantsv /media/KSR/krs-root-2010-q4-1.xml (at Mon Jul 12 22:44:36 2010 UTC)
Use HSM /opt/dnsec/aep.hoonconfig
Activate HSM prior to accepting in the affirmative!! (y/N): y
HSM /opt/dnsec/aep.hoonconfig activated.
[debug] setenv PKCS11_LIBRARY_PATH=/opt/dnsec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyer/PKCS11_GCC4.0.2.so.4.0.07
Found 1 slots on HSM /opt/Keyer/PKCS11_GCC4.0.2.so.4.0.07
HSM slot 0 included
Loaded /opt/Keyer/PKCS11_GCC4.0.2.so.4.0.07 Slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyer Fro 0405
Serial: KG563208

Validating last SKR with HSM...

<table>
<thead>
<tr>
<th>#</th>
<th>Inception</th>
<th>Expired</th>
<th>ZSK Tags</th>
<th>KSK Tag (CKA_LABEL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2010-07-01T00:00:00</td>
<td>2010-07-15T23:59:59</td>
<td>55138,41248</td>
<td>19036</td>
</tr>
<tr>
<td>2</td>
<td>2010-07-31T00:00:00</td>
<td>2010-08-04T23:59:59</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>3</td>
<td>2010-08-04T00:00:00</td>
<td>2010-08-14T23:59:59</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>4</td>
<td>2010-08-06T00:00:00</td>
<td>2010-08-24T23:59:59</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>5</td>
<td>2010-08-09T00:00:00</td>
<td>2010-08-31T23:59:59</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>6</td>
<td>2010-08-29T00:00:00</td>
<td>2010-09-15T23:59:59</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>7</td>
<td>2010-08-30T00:00:00</td>
<td>2010-09-24T00:00:00</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>8</td>
<td>2010-09-04T00:00:00</td>
<td>2010-09-24T00:00:00</td>
<td>41248</td>
<td>19036</td>
</tr>
<tr>
<td>9</td>
<td>2010-09-20T00:00:00</td>
<td>2010-09-30T23:59:59</td>
<td>40288,41248</td>
<td>19036</td>
</tr>
</tbody>
</table>

...VALIDATED.

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

<table>
<thead>
<tr>
<th>#</th>
<th>Inception</th>
<th>Expired</th>
<th>ZSK Tags</th>
<th>KSK Tag (CKA_LABEL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2010-10-01T00:00:00</td>
<td>2010-10-14T23:59:59</td>
<td>40288,41248</td>
<td>19036</td>
</tr>
<tr>
<td>2</td>
<td>2010-10-30T00:00:00</td>
<td>2010-10-30T23:59:59</td>
<td>40288</td>
<td>19036</td>
</tr>
<tr>
<td>3</td>
<td>2010-11-01T00:00:00</td>
<td>2010-11-14T23:59:59</td>
<td>40288</td>
<td>19036</td>
</tr>
<tr>
<td>4</td>
<td>2010-11-27T00:00:00</td>
<td>2010-12-01T23:59:59</td>
<td>40288</td>
<td>19036</td>
</tr>
<tr>
<td>5</td>
<td>2010-12-17T00:00:00</td>
<td>2011-01-05T23:59:59</td>
<td>216539,40288</td>
<td></td>
</tr>
</tbody>
</table>

...PASSED.

SHA256 hash of KSR:
A17653979309261112DCF591A60A4F8FC2821D0EDD71794637D5A0E210C371543
>> ratchet insomniac dwelling mosquito playhouse pioneer fallout Babylon ates reproduce vapor miracle ragtime hamburger upshot Wichita snapshot candidate Belfast tambourine stopwatch bookseller Pluto pyramid highchair specialist robust ultimate assume retraction bombast decimal <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/krs-root-2010-q4-1.xml

<table>
<thead>
<tr>
<th>#</th>
<th>Inception</th>
<th>Expired</th>
<th>ZSK Tags</th>
<th>KSK Tag (CKA_LABEL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2010-10-01T00:00:00</td>
<td>2010-10-14T23:59:59</td>
<td>40288,41248</td>
<td>19036</td>
</tr>
<tr>
<td>2</td>
<td>2010-10-30T00:00:00</td>
<td>2010-10-30T23:59:59</td>
<td>40288</td>
<td>19036</td>
</tr>
<tr>
<td>3</td>
<td>2010-11-01T00:00:00</td>
<td>2010-11-14T23:59:59</td>
<td>40288</td>
<td>19036</td>
</tr>
<tr>
<td>4</td>
<td>2010-11-27T00:00:00</td>
<td>2010-12-01T23:59:59</td>
<td>40288</td>
<td>19036</td>
</tr>
<tr>
<td>5</td>
<td>2010-12-17T00:00:00</td>
<td>2011-01-05T23:59:59</td>
<td>216539,40288</td>
<td></td>
</tr>
</tbody>
</table>

SHA256 hash of SKR:
G0CC741D1B7B363AEE22A6628130A658FDE07F0E24950E95965A6AC67CEFF22134527
>> aardvark revoler chocking brevado kickoff councilmen robust tomorrow tracker: Cherokee Beehive paragon reindeer microscope uncult amusment unearth coherence dechand embezzle treadmill examine tracker parego vibrate quantity kiwi unravel upright hydraulic atlas Eskimo <<
Unloaded /opt/Keyer/PKCS11Provider/pkcs11_GCC4.0.2.so.4.07 Slot=0

********** Log output in /krsigner-2010q4-22-4426.log **********
ICANN DNSSEC Script Exception

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

Instructions: Initial each step that has been completed below, e.g., BTS. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th></th>
<th>IW notes date and time of key ceremony exception and signs here:</th>
<th>FA</th>
<th>19:17</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- At step 36, the printer since we had two log files the printing didn't work. CA had to print each file individually.

-- End of DNSSEC Script Exception --
Starting: krs signer KJqmt7v /media/KSR/krs-root-2013-q3-0.xml (at Thu May 2 19:02:52 2013 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
  Label: ICANNKSK
  ManufacturerID: AEP Networks
  Model: Keyper Pro 0405
  Serial: K6002013

Validating last SKR with HSM...
# Inception    Expiration    ZSK Tags    KSK Tag(CKA_LABEL)
1 2013-04-01T00:00:00 2013-04-15T23:59:59 20580,40323 19036
2 2013-04-11T00:00:00 2013-04-25T23:59:59 20580 19036
3 2013-04-21T00:00:00 2013-05-05T23:59:59 20580 19036
4 2013-05-01T00:00:00 2013-05-15T23:59:59 20580 19036
5 2013-05-11T00:00:00 2013-05-25T23:59:59 20580 19036
6 2013-05-21T00:00:00 2013-06-04T23:59:59 20580 19036
7 2013-06-01T00:00:00 2013-06-14T23:59:59 20580 19036
8 2013-06-10T00:00:00 2013-06-24T23:59:59 20580 19036
9 2013-06-20T00:00:00 2013-07-05T23:59:59 20580,49656 19036
...VALIDATED.

Validate and Process KSR /media/KSR/krs-root-2013-q3-0.xml...
# Inception    Expiration    ZSK Tags    KSK Tag(CKA_LABEL)
1 2013-07-01T00:00:00 2013-07-15T23:59:59 49656,20580
2 2013-07-11T00:00:00 2013-07-25T23:59:59 49656
3 2013-07-21T00:00:00 2013-08-04T23:59:59 49656
4 2013-07-31T00:00:00 2013-08-14T23:59:59 49656
5 2013-08-10T00:00:00 2013-08-24T23:59:59 49656
6 2013-08-20T00:00:00 2013-09-03T23:59:59 49656
7 2013-09-01T00:00:00 2013-09-13T23:59:59 49656
8 2013-09-09T00:00:00 2013-09-24T00:00:00 49656
9 2013-09-20T00:00:00 2013-10-05T23:59:59 59085,49656
...PASSED.

SHA256 hash of KSR:
298c20937ae7c95070fb5854f4e19ee3aa2f92eb6839f5c61a24a3eff802ec6f1
>> breakup megaton bison molasses keyboard truncated spearhead embezzle guidance Wichit
a endorse equation upshot tolerance quiver torpedo reward combustion physique trombonis
t Mohawk opulent escape frequency rebirth direction concert Yucatan merit coherence sou
thward vacancy <<

Can't find requested KSK to sign with
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
Starting: krsigner Kjgmt7v /media/KSR/krs-root-2013-q3-0.xml (at Thu May 2 19:06:33 2
013 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keyper Pro 0405
Serial: K5062013

Validating last SKR with HSM...
# Inception  Expiration  ZSK Tags     KSK Tag(CKA_LABEL)
1 2013-04-01T00:00:00 2013-04-15T23:59:59 20580,40323 19036
2 2013-04-11T00:00:00 2013-04-25T23:59:59 20580 19036
3 2013-04-21T00:00:00 2013-05-05T23:59:59 20580 19036
4 2013-05-01T00:00:00 2013-05-15T23:59:59 20580 19036
5 2013-05-11T00:00:00 2013-05-25T23:59:59 20580 19036
6 2013-05-21T00:00:00 2013-06-04T23:59:59 20580 19036
7 2013-05-31T00:00:00 2013-06-14T23:59:59 20580 19036
8 2013-06-10T00:00:00 2013-06-24T23:59:59 20580 19036
9 2013-06-20T00:00:00 2013-07-05T23:59:59 20580,49656 19036
...VALIDATED.

Validate and Process KSR /media/KSR/krs-root-2013-q3-0.xml...
# Inception  Expiration  ZSK Tags     KSK Tag(CKA_LABEL)
1 2013-07-01T00:00:00 2013-07-15T23:59:59 49656,20580
2 2013-07-11T00:00:00 2013-07-25T23:59:59 49656
3 2013-07-21T00:00:00 2013-08-04T23:59:59 49656
4 2013-07-31T00:00:00 2013-08-14T23:59:59 49656
5 2013-08-10T00:00:00 2013-08-24T23:59:59 49656
6 2013-08-20T00:00:00 2013-09-03T23:59:59 49656
7 2013 00 30T00:00:00 2013-09-13T23:59:59 49656
8 2013-09-09T00:00:00 2013-09-24T00:00:00 49656
9 2013-09-20T00:00:00 2013-10-05T23:59:59 59085,49656
...PASSED.

SHA256 hash of KSR:
298C20937A7C95070FB5854F4E19EE3AA2F92E6839F5C61A24A3EFF802EC6F1
>> breakup meagton bison molasses keyboard truncated spearhead embezzle guidance Wichit
a endorse equation upshot tolerance quiver torpedo reward combustion physique trombonis
tMohawk opulent escape frequency rebirth direction concert Yucatan merit coherence sou
thward vacancy <<<

Generated new SKR in /media/KSR/krs-root-2013-q3-0.xml
# Inception  Expiration  ZSK Tags     KSK Tag(CKA_LABEL)
1 2013-07-01T00:00:00 2013-07-15T23:59:59 20580,49656 19036
2 2013-07-11T00:00:00 2013-07-25T23:59:59 49656 19036
3 2013-07-21T00:00:00 2013-08-04T23:59:59 49656 19036
4 2013-07-31T00:00:00 2013-08-14T23:59:59 49656 19036
5 2013-08-10T00:00:00 2013-08-24T23:59:59 49656 19036
6 2013-08-20T00:00:00 2013-09-03T23:59:59 49656 19036
7 2013-08-30T00:00:00 2013-09-13T23:59:59 49656 19036
8 2013-09-09T00:00:00 2013-09-24T00:00:00 49656 19036
9 2013-09-20T00:00:00 2013-10-05T23:59:59 49656,59085 19036

SHA256 hash of SKR:
0F9D2C42D8A8912D061207CA75CBD23F9D5BA2D75099876B938B20D5AE92062D
>> artist Ohio Burbank December stormy paramount pheasant clergyman afflict backwater a
head revenue indulge revival standard customer quadrant exodus rebirth stethoscope drum
beat nebula Neptune Hamilton playhouse Medusa bison specialist robust misnomer afflict
clergyman <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
## Print Copies of the Operation for Participants

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.</td>
<td>CA prints out a sufficient number of copies for participants using <code>printlog krsigner-20130502-*.log N</code> where <code>krsigner-20130502-*.log</code> is replaced by log output file displayed by program. (This example generates N copies) and hands copies to participants.</td>
<td>FA</td>
<td>19:20</td>
</tr>
<tr>
<td>37.</td>
<td>IW1 attaches a copy to his/her script.</td>
<td>FA</td>
<td>19:20</td>
</tr>
</tbody>
</table>

## Backup Newly Created SKR

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>CA copies the contents of the KSR FD by running <code>cp -p /media/KSR/*</code> for posting back to RZM. Confirm overwrite by entering &quot;y&quot; when prompted.</td>
<td>FA</td>
<td>19:21</td>
</tr>
<tr>
<td>39.</td>
<td>CA lists contents of KSR FD which should now have an SKR by running <code>ls -ltr /media/KSR</code> and then unmounts the KSR FD using <code>umount /media/KSR</code>.</td>
<td>FA</td>
<td>19:22</td>
</tr>
<tr>
<td>40.</td>
<td>CA removes KSR FD containing SKR and gives it to the RZM representative.</td>
<td>FA</td>
<td>19:22</td>
</tr>
</tbody>
</table>

## Disable/Deactivate HSM

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.</td>
<td>CA inserts 3 cards into HSM to deactivate the unit (via &quot;Set Offline&quot; menu item). Type in the default PIN &quot;11223344&quot; when prompted. IW1 records the used cards below. Each card is returned to cardholder after use. CA makes sure the card(s) NOT used to activate are used to deactivate the HSM. 1st OP card of 7 2nd OP card of 7 3rd OP card of 7 Confirm the ready light turns off.</td>
<td>FA</td>
<td>19:24</td>
</tr>
</tbody>
</table>
find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | md5sum
b4ff00825ab2655016adc1b781767cd2a

**Act. 3 Secure Hardware and Close the Ceremony**

Return HSM to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals.</td>
<td>FA</td>
<td>19:26</td>
</tr>
<tr>
<td>2.</td>
<td>CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. HSM2: TEE# BB24049899 / serial # K6002013</td>
<td>FA</td>
<td>19:26</td>
</tr>
<tr>
<td></td>
<td>IW1 initials the TEB and keep the sealing strips for later inventory. CA places item on equipment cart.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stop Recording Serial Port Activity and Logging Terminal Output

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Closing ttyaudit terminal window</td>
<td>FA</td>
<td>19:27</td>
</tr>
<tr>
<td></td>
<td>CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from laptop. CA then exits out of ttyaudit terminal window by typing &quot;exit&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Terminating the logging script</td>
<td>FA</td>
<td>19:27</td>
</tr>
<tr>
<td></td>
<td>CA stops logging terminal output by entering &quot;exit&quot; in the other terminal window. This only stops the script logging and will NOT close window.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Backup HSMFD Contents

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Set dotglob by executing shopt -s dotglob</td>
<td>FA</td>
<td>19:28</td>
</tr>
<tr>
<td></td>
<td>This allows copying everything in the original HSMFD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Calculate the md5hash of the contents on the original HSMFD. find -P /media/HSMFD -type f -print0</td>
<td>sort -z</td>
<td>xargs -0 cat</td>
</tr>
<tr>
<td>7.</td>
<td>Copy and paste the md5Hash and paste it on Text Editor by going to Applications &gt; Accessories &gt; Text Editor</td>
<td>FA</td>
<td>19:30</td>
</tr>
<tr>
<td></td>
<td>Print two copies. One for the audit bundle and the other for the HSMFD package.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>CA displays contents of HSMFD by executing ls -ltr</td>
<td>FA</td>
<td>19:30</td>
</tr>
<tr>
<td>9.</td>
<td>CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the O/S (as HSMFD_), and copies the contents of the HSMFD to the blank drive for backup by executing cp -Rp */media/HSMFD_</td>
<td>FA</td>
<td>19:31</td>
</tr>
</tbody>
</table>
ta endorse equation upshot tolerance quiver torpedo reward combustion physique trombone let Mohawk opulent escape frequency rebirth direction concert Vucutan merit coherence southward vacancy

Is this correct (Y/N)? y

[error] Can't find requested KSG to sign with!
Unloaded /opt/Keypair/PC/SSLProvider/pkcs11.GCC4.0.2.so.4.07 Slot0

---------- Log output in /kser/signer-20130502-192052.log ----------

Starting: kser/signer KJqm7v /media/KSR/kss-root-2013-q-3-0.xml
Use HSM /opt/dnssec/aep.hmcconfig?
Active HSM prior to accepting in the affirmative!! (Y/N): y

HSM /opt/dnssec/aep.hmcconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PC/SSL_LIBRARY_PATH=/opt/Keypair/PC/SSLProvider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keypair/PC/SSLProvider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keypair/PC/SSLProvider/pkcs11.GCC4.0.2.so.4.07 Slot0

HSM Information:
Label: ICANNKSK
ManufacturerID: AEP Networks
Model: Keypair Pro 0405
Serial: X002013

Validating Last KSR with HSM...
# Inception Expiration ZSK Tags KSG Tag(KCA_LABEL)
1 2013-04-31T00:00:00 2013-05-15T23:59:59 20585,40323 1903 1903
2 2013-04-11T00:00:00 2013-05-15T23:59:59 20580 1903 1903
3 2013-04-01T00:00:00 2013-05-15T23:59:59 20580 1903 1903
4 2013-03-31T00:00:00 2013-05-15T23:59:59 20580 1903 1903
5 2013-03-31T00:00:00 2013-05-15T23:59:59 20580 1903 1903
6 2013-03-31T00:00:00 2013-05-15T23:59:59 20580 1903 1903
7 2013-03-31T00:00:00 2013-05-15T23:59:59 20580 1903 1903
8 2013-03-31T00:00:00 2013-05-15T23:59:59 20580 1903 1903
9 2013-03-31T00:00:00 2013-05-15T23:59:59 20580 1903 1903

...VALIDATED.

Validate and Process KSR /media/KSR/kss-root-2013-q-3-0.xml...
# Inception Expiration ZSK Tags KSG Tag(KCA_LABEL)
1 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
2 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
3 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
4 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
5 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
6 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
7 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
8 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0
9 2013-04-01T00:00:00 2013-05-15T23:59:59 49656,20580 1903 0

...PASSED.

SHA256 hash of KSR: 29RZQ93TALK7F07B5854PE819EE3A7AEF2668395C61A24AMEEF62ECE61
"breakup magneton bison molasses keyboard truncated spearhead emblace guidance Which ta endorse equation upshot tolerance quiver torpedo reward combustion physique trombone let Mohawk opulent escape frequency rebirth direction concert Vucutan merit coherence southward vacancy"

Is this correct (Y/N)? y
ttyUSB0 Application Boot Loader - Feb 25 2010 11:08:16
ttyUSB0
ttyUSB0 Battery OK!
ttyUSB0
ttyUSB0 No Temper Counts in BERAM!
ttyUSB0
ttyUSB0 Loading Application (APP)
ttyUSB0
ttyUSB0 Starting loaded code.
ttyUSB0
ttyUSB0 \000Application - Feb 25 2010 11:08:02
ttyUSB0
ttyUSB0 wdog started
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Running DES POST Test
ttyUSB0
ttyUSB0 DES POST Test Passed
ttyUSB0
ttyUSB0 Running Triple DES POST Test
ttyUSB0
ttyUSB0 Triple DES POST Test Passed
ttyUSB0
ttyUSB0 Running AES POST Test
ttyUSB0
ttyUSB0 AES POST Test Passed
ttyUSB0
ttyUSB0 Running SHA1 POST Test
ttyUSB0
ttyUSB0 SHA1 POST Test Passed
ttyUSB0
ttyUSB0 Running SHA2 POST Test
ttyUSB0
ttyUSB0 SHA2 POST Test Passed
ttyUSB0
ttyUSB0 Running RandomGen SHA1 POST Test
ttyUSB0
ttyUSB0 Randomgen SHA1 POST Test Passed
ttyUSB0
ttyUSB0 Running RSA POST Test
ttyUSB0
ttyUSB0 RSA POST Test Passed
ttyUSB0
ttyUSB0 Running DSA POST Test
ttyUSB0
ttyUSB0 DSA POST Test Passed
ttyUSB0
ttyUSB0 Running RandomGen POST Test
ttyUSB0
ttyUSB0 RandomGen POST Test Passed
ttyUSB0
ttyUSB0 Additional RandomGen POST Test Passed
2013-05-02T18:56:49+0000 ttyUSB0 Total Private Memory 4173377
2013-05-02T18:56:49+0000 ttyUSB0 Total Private Memory 4173377
2013-05-02T18:56:49+0000 ttyUSB0 Free Private Memory 4173377
2013-05-02T18:56:49+0000 ttyUSB0 Total Dynamic Memory 14569472
2013-05-02T18:56:49+0000 ttyUSB0 Free Dynamic Memory 14569472
2013-05-02T18:56:49+0000 ttyUSB0 Date and Time: 17:55:04 on 03/05/2011
2013-05-02T18:56:49+0000 ttyUSB0 Created socket 1 on port 5000.
2013-05-02T18:56:49+0000 ttyUSB0 0x100003
2013-05-02T18:56:49+0000 ttyUSB0 0x200023 0800004A7B33296D
2013-05-02T18:56:49+0000 ttyUSB0 0x200023 0800004A83B3296D
2013-05-02T18:56:49+0000 ttyUSB0 Created socket 1 on port 5000.
2013-05-02T18:56:49+0000 ttyUSB0 3/5/2011 at 18:00:04
2013-05-02T18:56:49+0000 ttyUSB0 0x200023 0800004A7B33296D
2013-05-02T18:56:49+0000 ttyUSB0 0x200023 0800004A83B3296D
2013-05-02T18:56:49+0000 ttyUSB0 3/5/2011 at 18:00:27
2013-05-02T18:56:49+0000 ttyUSB0 3/5/2011 at 18:00:29
2013-05-02T18:56:49+0000 ttyUSB0 Accepted connection on address 222.228.192.168.0.1.
2013-05-02T18:56:49+0000 ttyUSB0 Free memory down from 14569472 to 11843072 (last mechanism 0)!
ttyUSB0
2013-05-02T19:03:09+0000
ttyUSB0 18:03:25 on 03-05-2011
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0 Closing connection on address 222.228.192.168.0.1.
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
ttyUSB0
---------------------------------------------------------------------
0x200023 0880004A7B32296D
0x200023 0880004A7B32296D
ICANN DNSSEC Script Exception

Abbreviations

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

Instructions: Initial each step that has been completed below, e.g., B75. Note time.

Note Exception Time

<table>
<thead>
<tr>
<th></th>
<th>IW notes date and time of key ceremony exception and signs here:</th>
<th>FA</th>
<th>19:42</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IW Describes exception and action below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At step 21 we were missing a substep to include the HSMFD Hash. We did include the printout.

— End of DNSSEC Script Exception —
### Step 10. CA displays contents of HSMFD by executing

```
ls -ltr /media/HSMFD_
```

**Activity**: FA

**Time**: 19:31

### Step 11. Calculate the md5hash of the contents on the copied HSMFD.

```
find -P /media/HSMFD_ -type f -print0 | sort -z | xargs -0 cat | md5sum
```

Confirm that it matches the md5hash of the original HSMFD

**Activity**: FA

**Time**: 19:32

### Step 12. CA unmounts new FD using

```
umount /media/HSMFD_
```

**Activity**: FA

**Time**: 19:32

### Step 13. CA removes HSMFD and places on table.

**Activity**: FA

**Time**: 19:32

### Step 14. CA repeats step 9 to 13 for the 2nd copy

**Activity**: FA

**Time**: 19:33

### Step 15. CA repeats step 9 to 13 for the 3rd copy

**Activity**: FA

**Time**: 19:34

### Step 16. CA repeats step 9 to 13 for the 4th copy

**Activity**: FA

**Time**: 19:34

### Step 17. CA repeats step 9 to 13 for the 5th copy

**Activity**: FA

**Time**: 19:35

### Print Logging Information

### Step 18. CA prints out hard copies of logging information by executing

```
enscript -Pc -s 2 script-20130502.log
enscript -Pc -s 2 --font="Courier8" ttysedit-ttyUSB-20130502-*.$log
```

for attachment to IW1 and CA scripts.

*Note: Ignore the error regarding non-printable characters if prompted.*

**Activity**: FA

**Time**: 19:38

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

### Step 19. CA unmounts HSMFD by executing

```
ca /tmp
  then
  umount /media/HSMFD
```

CA removes HSMFD.

**Activity**: FA

**Time**: 19:38

### Step 20. After all print jobs are complete, CA

- a) Turns off the laptop by pressing the power switch
- b) Turns on the laptop by pressing the power switch
- c) Remove the O/S DVD from the drive
- d) Turns off the laptop again by pressing the power switch

**Activity**: FA

**Time**: 19:39

### Step 21. CA places two HSMFDs and OS/DVD in TEB; writes date, time and “HSMFD” in amount field; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below.

**O/S DVD (Rev600) + HSMFD: TEB# BB21368998**

IW1 initials the TEB.
CA places TEB on equipment cart.

**Activity**: FA

**Time**: 19:42
### Distribute HSMFDs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 1 for himself), IKOS(1) to post SKR to RZM, and to review, analyze and improve on procedures.</td>
<td>FA</td>
<td>9:43</td>
</tr>
</tbody>
</table>

### Returning Laptop to a TEB

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.</td>
<td>CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. &lt;br&gt;Laptop1 (Dell ATG6400): TEB# BB24049898 / serial# 41593712005 &lt;br&gt; IW1 initials the TEB and keep the sealing strips for later inventory. CA places TEB on equipment cart.</td>
<td>FA</td>
<td>19:15</td>
</tr>
</tbody>
</table>

### Returning OP Smartcards to TEBs

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td>CA calls each CO to the front of the room one at a time and repeats the steps below &lt;br&gt;a) CA takes a TEB prepared for the CO and reads out the number and description while showing the bag to IW1 and CO. Figure 2 below for an example. &lt;br&gt;b) CA places OP into TEB, seals in front of IW1 and CO then initials bag and strip. &lt;br&gt;c) IW1 inspects the TEB, confirms description in table below and initials TEB and strip. IW1 keeps sealing strips for later inventory. &lt;br&gt;d) CA hands the TEB containing the OP card to the CO. CO inspects and verifies TEB #s and contents then initials his/her bag. &lt;br&gt;e) CO enters completion time and signs for each TEB in the table below in IW1’s script. IW1 initials table entry. &lt;br&gt;f) CO returns to his/her seat with the TEB, being careful not to poke or puncture TEB.</td>
<td>FA</td>
<td>19:51</td>
</tr>
<tr>
<td>CO#</td>
<td>Card Type</td>
<td>TEB #</td>
<td>Printed Name</td>
</tr>
<tr>
<td>-----</td>
<td>-----------</td>
<td>----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>CO 3</td>
<td>OP 3 of 7</td>
<td>BB21368993</td>
<td>Olaf Kolkmann</td>
</tr>
<tr>
<td>CO 4</td>
<td>OP 4 of 7</td>
<td>BB21368994</td>
<td>Robert Seastrom</td>
</tr>
<tr>
<td>CO 5</td>
<td>OP 5 of 7</td>
<td>BB21368999</td>
<td>Christopher Griffiths</td>
</tr>
<tr>
<td>CO 6</td>
<td>OP 6 of 7</td>
<td>BB21368996</td>
<td>Gaurab Upadhaya</td>
</tr>
<tr>
<td>CO 7</td>
<td>OP 7 of 7</td>
<td>BB21368997</td>
<td>Alain Aina</td>
</tr>
</tbody>
</table>
ICANN Root DNSSEC KSK Ceremony 13

SEALING INSTRUCTIONS:
1. Use ball point pen to complete all information BEFORE sealing cap.
2. Remove tear-off receipt and keep with copy of deposit documentation.
3. Remove impregnated peel-off seals from over sealing strip.
4. Press down firmly from center to edges.

DATE: 2 May 2013
SAID TO CONTAIN: OP 3 of 7
1. $ 4. $ 7
2. $ 5. $
3. $ 6. $

FROM: Root DNSSEC KSK Ceremony 13

TO: Olaf Kolkman

Figure 2
## Returning Equipment to Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td>CA, IW1, SSC1 open safe room and enter with equipment cart.</td>
<td>FA</td>
<td>19:32</td>
</tr>
<tr>
<td>26.</td>
<td>SSC1 opens Safe #1 shielding combination from camera.</td>
<td>FA</td>
<td>19:35</td>
</tr>
<tr>
<td>27.</td>
<td>SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>19:36</td>
</tr>
<tr>
<td>28.</td>
<td>CA records return of HSM in next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA CAREFULLY places the HSM into Safe #1 and IW1 initials the entry. HSM2: TEB# BB24049899 / serial # K6002013</td>
<td>FA</td>
<td>19:37</td>
</tr>
<tr>
<td>29.</td>
<td>CA records return of laptop in next entry field of safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry. Laptop1 (Dell ATG#400): TEB# BB24049898 / serial# 4159371205</td>
<td>FA</td>
<td>19:57</td>
</tr>
<tr>
<td>30.</td>
<td>CA records return of O/S DVD + HSMFD in next entry field of safe log with TEB #, printed name, date, time, and signature; places the O/S DVD + HSMFD into Safe #1 and IW1 initials the entry. O/S DVD (Rev600) + HSMFD: TEB# BB21368998</td>
<td>FA</td>
<td>19:58</td>
</tr>
</tbody>
</table>

## Close Equipment Safe #1

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.</td>
<td>SSC1 makes an entry including printed name, date, time, signature and notes “closing safe” in the safe log. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>19:58</td>
</tr>
<tr>
<td>32.</td>
<td>SSC1 places log back in safe and locks Safe #1 (spin dial at least two full revolutions each way, counter clock wise then clock wise). IW1 and CA verify safe is locked and door indicator light is green.</td>
<td>FA</td>
<td>19:58</td>
</tr>
<tr>
<td>33.</td>
<td>IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.</td>
<td>FA</td>
<td>19:59</td>
</tr>
</tbody>
</table>

## Open Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td>After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP card TEB with them.</td>
<td>FA</td>
<td>20:01</td>
</tr>
<tr>
<td>35.</td>
<td>SSC2 opens Safe #2 while shielding combination from camera.</td>
<td>FA</td>
<td>20:03</td>
</tr>
<tr>
<td>36.</td>
<td>SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>20:03</td>
</tr>
</tbody>
</table>
CO returns OP cards to Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
</table>
| 37.  | One by one, each CO along with the CA (using his/her common key):  
|      | a) Open his/her respective safe deposit box and read out box number inside Safe #2.  
|      | b) CO makes an entry into the safe log indicating the return of OP card including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEE and comparing TEB#s and card type to his/her script.  
|      | Note: If log entry is pre-printed, verify the entry, record time of completion and sign.  
|      | c) CO shows the bag to the camera and then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA.  
|      | Repeat the steps above until all cards are returned to the deposit box.                                                                                                                                                                                                                                                                                                                                                           |

<table>
<thead>
<tr>
<th>CO 3: Olaf Kolkman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box # 1239</td>
</tr>
<tr>
<td>OP TEB # B321368993</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CO 4: Robert Seastrom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box # 1260</td>
</tr>
<tr>
<td>OP TEB # B321368994</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CO 5: Christopher Griffiths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box # 1240</td>
</tr>
<tr>
<td>OP TEB # B321368999</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CO 6: Gaurab Upadhaya</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box # 1261</td>
</tr>
<tr>
<td>OP TEB # B821368996</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CO 7: Alain Ana</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box # 1242</td>
</tr>
<tr>
<td>OP TEB # B821368997</td>
</tr>
</tbody>
</table>

FA 20:08
Close Credential Safe #2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes &quot;Close safe&quot; into the safe log. IW1 initials the entry. Note: if log entry is pre-printed, verify the entry, record time of completion and sign.</td>
<td>FA</td>
<td>20:08</td>
</tr>
<tr>
<td>39.</td>
<td>SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). IW1 and CA verify safe is locked and door indicator light is green.</td>
<td>FA</td>
<td>20:09</td>
</tr>
<tr>
<td>40.</td>
<td>CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.</td>
<td>FA</td>
<td>20:09</td>
</tr>
</tbody>
</table>

Participant Signing of IW1’s Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.</td>
<td>All participants enter printed name, date, time, and signature on IW1’s script coversheet.</td>
<td>FA</td>
<td>20:13</td>
</tr>
<tr>
<td>42.</td>
<td>CA reviews W1’s script and signs it.</td>
<td>FA</td>
<td>20:13</td>
</tr>
</tbody>
</table>

Signing out of Ceremony Room

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.</td>
<td>IW2 ensures that all participants sign out of Ceremony Room log and are escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.</td>
<td>FA</td>
<td>20:21</td>
</tr>
</tbody>
</table>

Filming Stops

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td>SA stops filming and makes 2 copies of film, one for on-site and one for off-site storage along with IW1 script copies made below.</td>
<td>FA</td>
<td>20:22</td>
</tr>
</tbody>
</table>
Copying and Storing the Script

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Initial</th>
<th>Time</th>
</tr>
</thead>
</table>
| 45.  | IW1 makes at least 4 copies of his/her script: one for off-site audit bundle, one for IW1, one for IKOS and copies for other participants, as requested. Audit bundles each contain  
1) Output of signer system - HSMFD  
2) Copy of IW1's key ceremony script  
3) Audio-visual recording  
4) Logs from the Physical Access Control and Intrusion Detection System (Range is 11.12.2012 – 05.02.2013)  
5) The IW attestation (A.1 below)  
6) SA attestation (A.2, A.3 below)  
All in a TEB labeled "Key Ceremony 13", dated and signed by IW1 and CA. Off-site audit bundle is delivered to off-site storage. The CA holds the ultimate responsibility for finalizing the audit bundle. | FA     | 23:53 |

All remaining participants sign out of ceremony room log and leave.

Audit Bundle Checklist:

1. **Output of Signer System (CA)**
   One electronic copy (physical flash drive) of the HSMFD in each audit bundle, each placed within a tamper-evident bag, labeled, dated and signed by the CA and the IW1

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

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

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

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

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

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

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

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

Francisco Aleg

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

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

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

Enclosed is also an electronic copy of the event log from the access control system ranging from the last log extraction on [date, time UTC] 1/12/2012 to now.

Alexander Kulik

Date: 2 May 2013
A.3 Firewall Configuration Review (by SA)

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

Enclosed is the configuration extract from the firewall unit.

Alexander Kulik

Date: 2 May 2013
--- JUNOS 10.1R3.7 built 2010-07-10 08:32:02 UTC
matt@srx> show configuration | no-more | except encrypted
## Last commit: 2013-05-03 08:45:30 UTC by alex
version 10.1R3.7;
  system {
    host-name srx;
    domain-name ksk.cjr.dns.icann.org;
    location {
      country-code US;
      postal-code 22701;
      building Terremark-Admin;
      floor 1;
      rack 1;
    }
    ports {
      console {
        log-out-on-disconnect;
        type vt100;
      }
    }
    root-authentication {
    }
    name-server {
      199.4.29.19;
      199.4.29.29;
    }
    login {
      user alex {
        full-name "Alexander Kulik";
        uid 2005;
        class super-user;
        authentication {
          }
        }
      user jsamora {
        full-name "Jesse Samora";
        uid 2001;
        class super-user;
        authentication {
          }
        }
      user matt {
        uid 2006;
        class super-user;
        authentication {
          }
        }
      user reed {

full-name "Reed Quinn";
uid 2003;
class super-user;
authentication {
}
}
services {
  web-management {
    http;
  }
}
syslog {
  archive size 100k files 3;
  user * {
    any emergency;
  }
  host 199.4.29.21 {
    any any;
    match RT_FLOW_SESSION;
    log-prefix SRX-KSK-CJR;
  }
  host 199.4.28.21 {
    any any;
    match RT_FLOW_SESSION;
    log-prefix SRX-KSK-CJR;
  }
  file messages {
    any critical;
    authorization info;
  }
  file interactive-commands {
    interactive-commands error;
  }
  source-address 199.4.29.196;
}
max-configurations-on-flash 5;
max-configuration-rollback 20;
archival {
  configuration {
    transfer-on-commit;
    archive-sites {
      "scp://srxkskcjru199.4.29.21:/home/srxkskcjr" password "#####################################"; ## SECRET-DATA
    }
  }
}
license {
  autoupdate {
    url https://ae1.juniper.net/junos/key_retrieval;
}
}
}

processes {
    idp-policy disable;
}

ntp {
    server 199.4.29.17;
    server 199.4.29.27;
    source-address 10.4.29.1;
}

}

interfaces {
    interface-range interfaces-trust {
        member ge-0/0/1;
        member fe-0/0/2;
        member fe-0/0/3;
        member fe-0/0/4;
        member fe-0/0/5;
        member fe-0/0/6;
        member ge-0/0/0;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/7 {
        speed 100m;
        link-mode full-duplex;
        fastether-options {
            no-auto-negotiation;
        }
        unit 0 {
            family inet {
                address 199.4.29.196/29;
            }
        }
    }
    vlan {
        unit 0 {
            family inet {
                address 10.4.29.1/32;
            }
        }
    }
}

snmp {
    community dnss3c {

clients {
    10.4.29.253/32;
}
trap-options {
    source-address 199.4.29.196;
    agent-address outgoing-interface;
}
trap-group kskeast {
    categories {
        authentication;
        link;
        routing;
        startup;
        configuration;
        services;
    }
    targets {
        199.4.29.21;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 199.4.29.193;
    }
}
security {
    ssh_known-hosts {
        host 199.4.29.21 {
            rsa-key
        }
    }
    nat {
        source {
            rule-set trust-to-untrust {
                from zone trust;
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
}
zones {
  security-zone trust {
    address-book {
      address localnet 10.4.29.0/24;
    }
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
  }
  interfaces {
    vlan.0;
  }
}

security-zone untrust {
  address-book {
    address icannnds 199.4.28.0/22;
    address simplexgrinnell 12.30.47.110/32;
    address simplexgrinnell2 205.145.182.128/32;
  }
  interfaces {
    fe-0/0/7.0 {
      host-inbound-traffic {
        system-services {
          dhcp;
          ping;
        }
      }
    }
  }
}

policies {
  from-zone trust to-zone untrust {
    policy trust-to-untrust {
      match {
        source-address localnet;
        destination-address | icannnds simplexgrinnell simplexgrinnell2 
      }
      application any;
    }
    then {
      permit;
      log {
        session-close;
      }
    }
  }
}
applications {
  application sg {
    protocol udp;
    source-port 3060;
    destination-port 3061;
  }
  application sg2 {
    protocol udp;
    source-port 3065;
    destination-port 3061;
  }
}
vlans {
  vlan-trust {
    vlan-id 3;
    l3-interface vlan.0;
  }
}
matt@srx>