

# Juicebox Realm Initialization Ceremony

This document contains instructions for conducting a key ceremony to initialize a Juicebox HSM realm.

The source code for this document is available at <https://github.com/juicebox-systems/ceremony> and identified by the Git commit hash `97cfb88323d58abf3604aa0e227c57dcd0113f7c`.

Identifying bytes of the SHA-256 hash of the PDF file built from that source code:

byte 1		byte 2		byte 3		...	byte 32	

Choose exactly one of the following:	
<input type="radio"/>	Practice ceremony
<input type="radio"/>	Production ceremony

Codename: \_\_\_\_\_

Date: \_\_\_\_\_

Start time: \_\_\_\_\_

Location: \_\_\_\_\_

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

# Contents

1 Introduction .....	3
2 Procedures .....	4
3 Participants .....	5
4 Getting Started .....	6
4.1 Materials .....	6
4.2 Set Up the Computer .....	7
5 Realm Creation .....	15
5.1 Prepare the First HSM .....	15
5.2 Unpack the Smartcards .....	19
5.3 Create the Security World and Sign the Software .....	20
5.4 Destroy the OCS Smartcard .....	24
5.5 Create the Realm Keys .....	25
5.6 Write the Realm DVD .....	28
5.7 Clear the First HSM .....	29
6 HSM Enrollment .....	30
6.1 Set up the First HSM .....	30
6.2 Intermission .....	31
6.3 Set Up the Second HSM .....	33
6.4 Set Up the Third HSM .....	40
6.5 Set Up the Fourth HSM .....	47
6.6 Set Up the Fifth HSM .....	54
7 Conclusion .....	61
A State .....	63
A.1 Boot DVD .....	63
A.2 Vendor DVD .....	64
A.3 Realm DVD .....	65
B HSM Keys .....	66
C Reference .....	67
C.1 NATO Alphabet and Morse Code .....	67
C.2 Windows Keyboard Shortcuts .....	68
C.3 tmux Keyboard Shortcuts .....	68
D Exception Sheet 1 .....	69
E Exception Sheet 2 .....	70
F Exception Sheet 3 .....	71
G Exception Sheet 4 .....	72
H Exception Sheet 5 .....	73

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

# 1 Introduction

The purpose of the ceremony is to create cryptographic keys that may only be accessed within the trust boundaries of a fixed set of *HSMs* (Hardware Security Modules), and only while those HSMs execute a fixed software release. Additionally, the initialization process will create a single NVRAM file on each HSM for only the fixed software release to read and write.

One of the cryptographic keys to be generated is an asymmetric key pair used for encrypted communication with clients. Assuming the private key is indeed restricted to this software release on these HSMs, clients using the public key recorded during this ceremony will have certainty that they are communicating with this software running on the HSMs initialized during this ceremony.

The HSMs used in the ceremony are PCIe expansion cards and thus require a host computer. The HSMs, software, and ceremony are designed so that secrets are never accessible to the host computer. However, the security of the realm depends on the host computer making the correct management requests to the HSMs and presenting the expected HSM software build to the first HSM to be signed. The ceremony will use a brand new computer that is never connected to a network.

The computer's factory Windows OS will be used to verify the hashes of a publicly auditable *boot DVD*, as well as a vendor-proprietary *vendor DVD*. Then, the Linux OS on the boot DVD will be used for the main ceremony. See Appendix A for details on the DVDs and state management.

Each HSM has an external port for a smartcard reader/writer. The HSMs read and write secret keys onto smartcards for administrative operations. The ceremony will utilize two smartcards, referred to as *ACS* and *OCS*. The smartcards must be used only as prescribed and must be destroyed during the ceremony.

The ceremony will involve setting up a computer, then using the first HSM to initialize a *Security World*, write to two smartcards, sign the software, and create the realm keys. The OCS smartcard will be destroyed after it is used to sign the software. The keys reside in encrypted form on the host filesystem (protected by keys that reside on the HSMs and smartcards). As that filesystem is in volatile memory, the signed software and keys will be burned to a *realm DVD* to be accessed later, both during the ceremony and after the ceremony to set up the production environment.

After completing the Security World and realm initialization process on the first HSM, the HSM will be reset. Then, each of the five HSMs (including the first) will be enrolled in the Security World and have its NVRAM file initialized. After the final HSM has been initialized, the ACS smartcard will be destroyed.

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## 2 Procedures

The following roles are defined for participants of the ceremony:

- The *MC* introduces the event, keeps it moving, and is the final decision maker for any exceptions, as explained below.
- The *operator* executes the steps as instructed in this document. The operator should be the only person to approach or access the computer, HSMs, and smartcards during the ceremony. The operator's copy of this document is the official record.
- Any number of *witnesses* observe the ceremony.

A small number of other non-participants may also be present for (parts of) the ceremony, for example to record video.

If, at any point, the instructions are ambiguous, contain an error, fail to instruct the operator in a particular situation, or must be deviated from, the operator should write “exception” in the margin and fill out an *exception sheet*. Several sheets are included at the end of this document (Appendix D through Appendix H). The participants may then discuss concerns and options, but the MC ultimately decides how to proceed.

In this document, a checkbox (☐) denotes a confirmation step that is not optional. If the operator is unable to meet the requirements to check a checkbox, that's an exception. A circle (☐) is used when exactly one of multiple mutually exclusive options is required.

The following conventions apply to dates and times hand-written into this document, unless instructed or annotated otherwise:

- Dates and times should reflect the local time zone.
- Dates should be written as YYYY-MM-DD.
- Times should be written as HH:MM (24-hour local time with minute precision).
- The operator's source of time should be the analog clock visible to all participants.

The ceremony is expected to take about 6 hours. The ceremony instructions include one break at Step 102, about halfway through, allowing (and requiring) the participants to leave the room. If any of the participants need to leave the room at other times, that should be handled as an exception.

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

### 3 Participants

This document is filled out by the following person:

Name: \_\_\_\_\_

Affiliation: \_\_\_\_\_

Ceremony participants:

**Do not initial until the completion of the ceremony. By initialing in this table, you agree that:**

- **You were present for the entire ceremony (excluding breaks).**
- **To the best of your knowledge, the instructions in this document were followed correctly (except as noted elsewhere in this document) and without deception.**
- **To the best of your knowledge, this document is a true and accurate record.**

**If you do not agree, write “do not agree” instead of your initials and record an explanation.**

Role	Name	Affiliation	Initials (see above)
MC			
Operator			
Witness			
Witness			
Witness			
Witness			
Witness			
Witness			
Witness			
Witness			
Witness			
Witness			

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## 4 Getting Started

### 4.1 Materials

Start time: \_\_\_\_\_

Step	Activity	End Time
1	Inspect the operator and the environment. <input type="checkbox"/> There is a prominent analog clock with a second hand. <input type="checkbox"/> The witnesses confirm that the clock is set to the current local time. <input type="checkbox"/> There are two outlets available on the wall or a power strip nearby.	
2	Inspect the materials available to the operator. <input type="checkbox"/> The materials below are available and do not appear tampered with. <input type="checkbox"/> No other materials are available to the operator.	

Materials	
<input type="checkbox"/>	1 antistatic wrist strap
<input type="checkbox"/>	1 pair of scissors
<input type="checkbox"/>	1 Phillips screwdriver
<input type="checkbox"/>	1 rotary tool (to sand through smartcards)
<input type="checkbox"/>	1 table number holder (to display smartcards prominently when not in use)
<input type="checkbox"/>	2 printouts of this document
<input type="checkbox"/>	1 permanent marker
<input type="checkbox"/>	1 roll of masking tape
<input type="checkbox"/>	2 blue ballpoint pens
<input type="checkbox"/>	2 bottles of water
<input type="checkbox"/>	2 juice boxes (preferably apple)
<input type="checkbox"/>	1 sealed pack of 100 tamper-evident bags (ProAmpac GCS0912)
<input type="checkbox"/>	1 pre-burned and finalized boot DVD
<input type="checkbox"/>	1 pre-burned and finalized vendor DVD
<input type="checkbox"/>	1 sealed spindle of blank DVD-Rs (for the realm DVD)
<input type="checkbox"/>	1 computer (Lenovo 90T2000SUS, including a DVD burner and keyboard, with the outer box sealed by the purchaser with tamper-evident tape)
<input type="checkbox"/>	1 VGA video projector (limited to a low resolution so the text is visible to all participants)
<input type="checkbox"/>	1 sealed pack of 10 Entrust smartcards

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

- ☐ At least 5 of the following Entrust HSMs:

Serial Number	ESN	Packaging	Present	Absent	Used As
46-X19834	A114-05E0-D947	[TODO: Bag ID]	<input type="radio"/>	<input type="radio"/>	#____
46-X20349	B216-05E0-D947	[TODO: Bag ID]	<input type="radio"/>	<input type="radio"/>	#____
46-X20517	3B17-05E0-D947	[TODO: Bag ID]	<input type="radio"/>	<input type="radio"/>	#____
46-X21267	341A-05E0-D947	Factory	<input type="radio"/>	<input type="radio"/>	#____
46-X21271	351A-05E0-D947	Factory	<input type="radio"/>	<input type="radio"/>	#____
46-X21323	611A-05E0-D947	Factory	<input type="radio"/>	<input type="radio"/>	#____

The first HSM used in the ceremony should be in factory packaging, which includes a smartcard reader. Fill in the “Used As” column as you unpack the HSMs (“#1”, “#2”, etc). The serial number sometimes contains an additional character after the space (likely A), not included here.

## 4.2 Set Up the Computer

Start time: \_\_\_\_\_

Step	Activity	End Time																												
3	<p>Inspect the computer packaging:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The box does not appear tampered with.</li> <li><input type="checkbox"/> The box ends are sealed with customer-applied tamper-evident tape, on top of somewhat loose Lenovo-branded tape.</li> </ul> <p>Inspect the Lenovo sticker:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The model ((31P) M/T Model) is 90T2000SUS.</li> <li>Serial Number S(SN):</li> </ul> <table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> <ul style="list-style-type: none"> <li>Wi-Fi MAC address (WMAC):</li> </ul> <table border="1"> <tr> <td>byte 1</td><td>byte 2</td><td>byte 3</td><td>byte 4</td><td>byte 5</td><td>byte 6</td></tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> <ul style="list-style-type: none"> <li>Mfg Date (as printed): _____</li> </ul> <p>Inspect the shipping sticker(s):</p> <ul style="list-style-type: none"> <li>SHIP DATE (as printed): _____</li> </ul>	1	2	3	4	5	6	7	8									byte 1	byte 2	byte 3	byte 4	byte 5	byte 6							
1	2	3	4	5	6	7	8																							
byte 1	byte 2	byte 3	byte 4	byte 5	byte 6																									

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

4	<p>Open the computer box from the top with scissors.</p> <p><b>Outer Box:</b></p> <ul style="list-style-type: none"> <li>• Remove the small box containing the mouse and power cord from the outer box.</li> <li>• Remove the long box containing the keyboard from the outer box.</li> <li>• Remove the computer, sandwiched by two large pieces of foam, from the outer box.</li> <li>• Put away the outer box.</li> </ul> <p><b>Desktop:</b></p> <ul style="list-style-type: none"> <li>• Remove the foam from the desktop, and put away the foam.</li> <li>• Remove the plastic bag surrounding the desktop (which is not sealed), and put away the bag.</li> </ul> <p><b>Keyboard Box:</b></p> <ul style="list-style-type: none"> <li>• Open the keyboard box.</li> <li>• Remove the keyboard from its surrounding plastic (which is not sealed).</li> <li>• Inspect the keyboard and the label under it.</li> </ul> <p style="margin-left: 40px;">Date on label under keyboard (MFG, as shown): _____</p> <ul style="list-style-type: none"> <li>• Remove the twist tie on the keyboard's USB cable.</li> <li>• Put away the keyboard box, plastic bag, and twist tie.</li> </ul> <p><b>Mouse and Power Cord Box:</b></p> <ul style="list-style-type: none"> <li>• Open the mouse and power cord box.</li> <li>• Remove the power cable from the box.</li> <li>• Remove the twist tie and plug cover on the power cable, and put away the tie and cover.</li> <li>• Remove the mouse (still in a plastic bag) and paperwork from the box, place them into a tamper-evident bag, and put away the bag. (We don't expect to need the mouse during this ceremony.)</li> </ul> <p style="margin-left: 40px;">Bag ID:</p> <table border="1" style="margin-left: 40px; margin-top: 10px;"> <tr> <td style="width: 20px; text-align: center;">1</td> <td style="width: 20px; text-align: center;">2</td> <td style="width: 20px; text-align: center;">3</td> <td style="width: 20px; text-align: center;">4</td> <td style="width: 20px; text-align: center;">5</td> <td style="width: 20px; text-align: center;">6</td> <td style="width: 20px; text-align: center;">7</td> <td style="width: 20px; text-align: center;">8</td> <td style="width: 20px; text-align: center;">9</td> <td style="width: 20px; text-align: center;">10</td> </tr> <tr> <td style="height: 30px;"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table> <ul style="list-style-type: none"> <li>• Retain the empty box to prop up the DVD drive later.</li> </ul> <p><input type="checkbox"/> The box contents did not appear tampered with or used.</p>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



5	<p>Inspect the computer case. Set it down on its right side to inspect the label on the bottom.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The case does not appear tampered with.</li> <li><input type="checkbox"/> A Windows sticker is present on the left side panel.</li> <li><input type="checkbox"/> An Intel Core i5 sticker is present on the front panel.</li> <li><input type="checkbox"/> The serial number matches the label on the box (<u>Step 3</u>).</li> <li><input type="checkbox"/> The manufacturing date (Mfg Date) matches the label on the box (<u>Step 3</u>).</li> </ul>	
6	<p>Remove the left panel of the case and the front panel:</p> <ul style="list-style-type: none"> <li>• Unscrew the two screws holding the left panel in place using the screwdriver.</li> <li>• Remove the left panel, and put it away.</li> <li>• Ground yourself to the unpainted computer chassis with the antistatic wrist strap. It can be worn on your upper arm or ankle.</li> <li>• Lift up on the three plastic tabs (top, middle, bottom) to get the left side of the front panel off.</li> <li>• Wiggle the front panel off, and put it away.</li> </ul> <p><input type="checkbox"/> The power supply's wattage rating (labeled as Total output continuous shall not exceed) is 260 W.</p>	
7	<p>Remove the SATA drive shelf:</p> <ul style="list-style-type: none"> <li>• Brace the DVD drive and press the black and red tab towards the front of the computer release it. Note: it may eject forcefully.</li> <li>• Unplug the SATA and power cables from the back of the DVD drive.</li> <li>• Set the DVD drive nearby on top of the box that the mouse and power cable came in (since the cables are too short to set the drive down on the table).</li> <li>• Unplug the SATA and power cables from the 3.5" hard drive.</li> <li>• Pull up on the silver and red tab (on the front, left side, middle) to release the SATA drive shelf.</li> <li>• Wiggle the SATA drive shelf off (with the 3.5" hard drive attached), and put away the drive shelf.</li> <li>• Plug the SATA and power cables back into the DVD drive.</li> </ul>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

8	<p>Remove the wireless card and antennas:</p> <ul style="list-style-type: none"><li>• Pull up forcefully on the plastic pin holding the wireless card in place (near where the DC cables come out of the power supply).</li><li>• Remove a small bit of clear plastic that the pin was on.</li><li>• Remove the wireless card from the slot.</li><li>• Gently pry the two antenna cables from the wireless card.</li><li>• Pull forcefully on the front antenna to overcome the adhesive, then remove any tape holding the cable and pull the cable through.</li><li>• Remove the plastic antenna cover on the back of the case by pushing the tab on top (near the case fan) and wiggling the cover off.</li><li>• Pull forcefully on the rear antennas to overcome the adhesive, then remove any tape holding the cable and pull the cable through.</li></ul> <p><input type="checkbox"/> The Wi-Fi MAC address (WFM) on the wireless card's label matches the label on the computer box (Step 3).</p> <p>Place the wireless card, antennas, and plastic bits into a tamper-evident bag for storage.</p> <p>Bag ID:</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
9	<p>Prepare the PCIe x16 slot:</p> <ul style="list-style-type: none"><li>• Pull up on the silver and red tab above the placeholder brackets near the PCIe slots to open the flap.</li><li>• Remove the metal placeholder bracket blocking the PCIe x16 slot and put it away.</li><li>• Close the metal flap.</li></ul>																					
10	<p>Open the projector packaging, and put away the packaging.</p> <p><input type="checkbox"/> The packaging does not appear tampered with.</p> <p><input type="checkbox"/> The projector does not appear tampered with.</p>																					
11	<p>Plug in the projector power and turn on the projector.</p>																					
12	<p>Plug the USB keyboard and VGA projector into the computer.</p>																					
13	<p>Boot into Windows:</p> <ul style="list-style-type: none"><li>• Plug the power cord into the back of the computer.</li><li>• Press the “power button” on the front of the computer.</li><li>• Boot the computer into the pre-installed Windows OS.</li></ul>																					

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

14	<p>When the Windows “Out of Box Experience” prompts for input (asking for your country or region):</p> <ul style="list-style-type: none"> <li>• Press <b>Shift-F10</b> to open a terminal. (Do not use the terminal. Opening it switches focus, which enables more hotkeys.)</li> <li>• Press <b>Win-r</b> to open a Run dialog.</li> <li>• Run <b>powershell</b>.</li> <li>• Press <b>Win-Up</b> to maximize the Powershell window.</li> </ul>	
15	Insert the boot DVD into the DVD drive.	
16	<p>Calculate the SHA-256 hash of the boot DVD image.</p> <pre>\$s = [system.io.file]::open('\\\\.\\e:', 'open', 'read', 'read') get-filehash -inputstream \$s \$s.close()</pre> <p>The <b>get-filehash</b> command should take about 1 minute.</p> <p><input type="checkbox"/> The boot DVD’s SHA-256 digest matches  <b>1603a9418982d1a30bbc3a8c35f3e92cb3093523725bcd95c62a5a3f220a188.</b></p>	
17	<p>Copy the main filesystem image and a small script from the boot DVD onto the NVMe drive.</p> <pre>dir cp -verbose e:\\live\\filesystem.squashfs cp -verbose e:\\entrust.ps1 dir</pre> <p>This will copy the files into <b>C:\\Users\\defaultuser0\\</b>. The first copy command should take about 2 minutes, and the second one should take up to a few seconds.</p>	
18	Eject the boot DVD by pressing the button and insert the vendor DVD into the DVD drive.	
19	<p>Copy the Entrust-provided files from the vendor DVD onto the NVMe drive.</p> <pre>cat entrust.ps1 set-executionpolicy -scope process unrestricted .\\entrust.ps1 dir</pre> <p>Enter <b>Y</b> for yes when setting the policy.</p> <p>The script verifies the hashes of the files and copies them into <b>C:\\Users\\defaultuser0\\</b>. It should take about 10 minutes. During this time, review Appendix A, which discusses the various DVDs and files.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

20	Eject the vendor DVD by pressing the button and insert the boot DVD into the DVD drive.							
21	Power off the computer: <ul style="list-style-type: none"> <li>• Press and release the “power button” on the front of the computer.</li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>							
22	Determine the current date and 24-hour time in UTC. This will be used to set the system time.  <table border="1" style="width: 100%;"> <tr> <td colspan="2">Choose exactly one of the following:</td> </tr> <tr> <td><input type="radio"/></td> <td>Pacific Standard Time (UTC-08:00)</td> </tr> <tr> <td><input type="radio"/></td> <td>Pacific Daylight Time (UTC-07:00)</td> </tr> </table> Local Date (MM/DD/YYYY): _____ Local Time (HH:MM, from analog clock): _____ UTC Date (MM/DD/YYYY): _____ UTC Time (HH:MM): _____	Choose exactly one of the following:		<input type="radio"/>	Pacific Standard Time (UTC-08:00)	<input type="radio"/>	Pacific Daylight Time (UTC-07:00)	
Choose exactly one of the following:								
<input type="radio"/>	Pacific Standard Time (UTC-08:00)							
<input type="radio"/>	Pacific Daylight Time (UTC-07:00)							

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

23	<p>Configure UEFI and boot into the boot DVD:</p> <ol style="list-style-type: none"> <li>1. Plug the power cord into the back of the computer.</li> <li>2. Press the “power button” on the front of the computer.</li> <li>3. Tap <b>F1</b> repeatedly during boot to enter the UEFI setup.</li> <li>4. Press <b>Enter</b> to dismiss the help dialog.</li> <li>5. Press <b>Right</b> to enter the <b>Main</b> settings.</li> <li>6. Press <b>Down</b>, then <b>Enter</b> to enter the <b>Main</b> ▷ <b>System Time &amp; Date</b> settings.</li> <li>7. Set the time and date to UTC. Use the arrows and <b>Enter</b> to navigate, and <b>+</b> and <b>-</b> to adjust the time. Use the time and date calculated in the previous step, adjusted for the minutes that have since passed.</li> <li>8. Press <b>Up</b> repeatedly until highlighting the back arrow, then <b>Enter</b>, then <b>Left</b> to return to the main menu.</li> <li>9. Press <b>Down</b> several times, then <b>Right</b> to enter the <b>Security</b> settings.</li> <li>10. Press <b>Down</b> several times, then <b>Enter</b> to enter the <b>Security</b> ▷ <b>Secure Boot</b> settings.</li> <li>11. Press <b>Enter</b>, then <b>Up</b>, then <b>Enter</b> to disable Secure Boot. (The Linux kernel would refuse to load the vendor’s HSM driver with Secure Boot enabled.)</li> <li>12. Press <b>Up</b>, then <b>Enter</b>, then <b>Left</b> to return to the main menu.</li> <li>13. Press <b>Down</b>, then <b>Right</b> to enter <b>Startup</b> settings.</li> <li>14. Press <b>Enter</b> to enter the <b>Startup</b> ▷ <b>Boot Priority Order</b> settings.</li> <li>15. Except for the SATA DVD-RW drive, press <b>x</b> on each device to exclude it from the boot order. (Skip the DVD-RW drive with <b>Down</b>. You can also un-exclude something with <b>x</b>.)</li> <li>16. Press <b>F10</b>, then <b>Enter</b> to save the changes and reboot.</li> <li>17. The computer should boot into the bootloader on the boot DVD.</li> <li>18. Press <b>Enter</b> at the GRUB menu to boot into Linux.</li> </ol>	
----	--	--

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

24	<p>Display some information about the computer's devices:</p> <pre>lsblk lsusb lspci   nl</pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> <code>lsblk</code> reports <code>loop0</code> (loopback devices), <code>sr0</code> (the DVD drive), <code>nvme0n1</code> with 4 partitions (the Windows disk), and no other block devices.</li> <li><input type="checkbox"/> <code>lsusb</code> reports a "3.0 root hub", a "2.0 root hub", a "Lenovo New Calliope USB Keyboard", and no other USB devices.</li> <li><input type="checkbox"/> <code>lspci</code> reports 24 devices: 22 from Intel, a "Non-Volatile memory controller" from Samsung Electronics, and an "Ethernet controller" from Realtek Semiconductor.</li> </ul>	
25	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li>• <code>ceremony computer shutdown</code></li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## 5 Realm Creation

### 5.1 Prepare the First HSM

Start time: \_\_\_\_\_

Step	Activity	End Time																				
26	<p>This step will process the HSM packaging.</p> <p><input type="checkbox"/> The HSM is in factory packaging.</p> <p>Inspect the outer shipping box:</p> <p><input type="checkbox"/> The box does not appear tampered with.</p> <p>Open the outer shipping box, remove its contents, and put away the box and any extra padding. Inspect the white plastic bag containing this HSM:</p> <p><input type="checkbox"/> The text says “NCIPHER: AN ENTRUST DATACARD COMPANY”, with the first “N” enclosed in a circle.</p> <p><input type="checkbox"/> The bag is sealed and does not appear tampered with.</p> <p>Use scissors to open the end of the bag at the dashed line. Remove the bag and put it away. Inspect the box sleeve:</p> <p><input type="checkbox"/> The text says “ENTRUST: SECURING A WORLD IN MOTION” with the hexagonal “E” logo and “nShield: Hardware Security Modules”.</p> <p><input type="checkbox"/> The box sleeve does not appear tampered with.</p> <p>Remove the box sleeve and put it away. Inspect the box:</p> <p><input type="checkbox"/> The box does not appear tampered with.</p> <p>Inspect the sticker at the end of the box:</p> <p><input type="checkbox"/> The top text says “ENTRUST: nShield Solo XC”.</p> <p><input type="checkbox"/> Only the nC4035E-000 nShield Solo XC F3 model is checked.</p> <p><input type="checkbox"/> Only the Base speed is checked.</p> <p><input type="checkbox"/> The serial number matches an unused HSM listed in Section 4.1.</p> <p>Serial number:</p> <table><tr><td>1</td><td>2</td><td>-</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	-	3	4	5	6	7	8	9											
1	2	-	3	4	5	6	7	8	9													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

27	<p>Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging.</p> <p><input type="checkbox"/> The HSM does not appear tampered with.</p> <p>Inspect the sticker on the side of the HSM:</p> <p><input type="checkbox"/> The serial number (S/N) matches that of the previous step.</p> <p><input type="checkbox"/> The model is nC4035E-000.</p>							
28	<p>Set the mode switch and jumpers on the HSM:</p> <p><input type="checkbox"/> Set the outside-facing physical switch to 0 (the middle position).</p> <p><input type="checkbox"/> Ensure both override jumper switches are set to off.</p>							
29	<p>Note: To fit different computer cases, the HSM may have a low-profile PCI bracket or a full-height PCI bracket attached. Due to a misalignment, the HSM is physically unable to fit into this particular computer when it has either bracket attached, so it will be used without a bracket.</p> <table><tr><td colspan="2">Choose exactly one of the following:</td></tr><tr><td><input type="radio"/></td><td>The HSM currently has no PCI bracket.</td></tr><tr><td><input type="radio"/></td><td>The HSM currently has a low-profile or full-height PCI bracket.</td></tr></table> <p>Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.</p>	Choose exactly one of the following:		<input type="radio"/>	The HSM currently has no PCI bracket.	<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.	
Choose exactly one of the following:								
<input type="radio"/>	The HSM currently has no PCI bracket.							
<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.							
30	<p>Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.</p>							
31	<p>Unpack the card reader. Put away the packaging.</p> <p><input type="checkbox"/> The card reader is etched with “ENTRUST” text and the hexagonal “E” logo.</p> <p><input type="checkbox"/> The card reader does not appear tampered with.</p>							
32	<p>While bracing the HSM, plug the card reader into the HSM’s external port.</p>							
33	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"><li>• Plug the power cord into the back of the computer.</li><li>• Press the “power button” on the front of the computer.</li><li>• The computer should boot into the bootloader on the boot DVD.</li><li>• Press Enter at the GRUB menu to boot into Linux.</li></ul>							
34	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>							

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



35	<p>Print HSM info:</p> <pre>ceremony hsm info</pre> <p>ESN (Module #1 ▷ serial number):</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>7</td><td>8</td><td>-</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <p><input type="checkbox"/> The ESN matches the HSM listed in Section 4.1.</p> <p>Firmware version (Module #1 ▷ version): _____</p> <p><input type="checkbox"/> Module #1 ▷ product name shows all of nC3025E/nC4035E/nC4335N.</p>	1	2	3	4	-	5	6	7	8	-	9	10	11	12															
1	2	3	4	-	5	6	7	8	-	9	10	11	12																	
36	<p>Restart the HSM in maintenance mode:</p> <pre>ceremony hsm restart --mode maintenance</pre> <p>This command should take about 55 seconds.</p>																													
37	<p>Update/overwrite the HSM firmware to version 13.3.1:</p> <pre>ceremony vendor mount firmware ceremony firmware write ceremony vendor unmount firmware</pre> <p>These commands should take about 3 minutes if starting from the same version and may take several more minutes if starting from an earlier version.</p>																													
38	<p>Wait until the HSM is done:</p> <pre>ceremony hsm info</pre> <p><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</p> <p><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</p> <p><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</p> <p>Wait and re-run the command until these conditions are satisfied.</p>																													
39	<p>Power off the computer:</p> <ul style="list-style-type: none"><li><pre>ceremony computer shutdown</pre></li><li>Wait for the computer to turn off.</li><li>Unplug the power cord from the back of the computer.</li><li>Wait a few seconds.</li></ul>																													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

40	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the “power button” on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press <code>Enter</code> at the GRUB menu to boot into Linux.</li> </ul>	
41	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>	
42	<p>Wait until the HSM is ready:</p> <pre>ceremony hsm info</pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</li> <li><input type="checkbox"/> Module #1 ▷ mode shows uninitialized.</li> <li><input type="checkbox"/> Module #1 ▷ serial number matches <a href="#">Step 35</a>.</li> <li><input type="checkbox"/> Module #1 ▷ version shows 13.3.1.</li> <li><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</li> <li><input type="checkbox"/> The HSM LED is blinking in the repeated <code>--</code> pattern.</li> </ul> <p>Wait and re-run the command until these conditions are satisfied.</p> <p>If the module does not appear at all, check <code>dmesg</code> for the error  <code>nfp_open: device &lt;...&gt; failed to open with error: -5</code>. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an <i>exception sheet</i> the first time it occurs.</p>	
43	<p>Restart the HSM in initialization mode:</p> <pre>ceremony hsm restart --mode initialization</pre> <p>This command should take about 55 seconds.</p>	
44	<p>Initialize the HSM with a new module key:</p> <pre>ceremony hsm erase</pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> The output includes the line <code>Initialising Unit 1 (SetNSOPerms)</code>.</li> <li><input type="checkbox"/> Module Key Info ▷ HKM[0] is shows 20 random-looking bytes in hex.</li> </ul> <p>This command should take less than 1 second. This key is temporary, as creating or joining a Security World later will generate a new module key.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

45	<p>Check which features have been activated on the HSM:</p> <pre>ceremony feature info</pre> <p>Active features (excluding SEE): _____</p> <p><input type="checkbox"/> SEE Activation (EU+10) is not activated (shows N).</p>	
46	<p>Activate the SEE (CodeSafe) feature on the HSM:</p> <ul style="list-style-type: none"> <li><pre>ceremony feature activate features/SEEUE_{ESN}.txt</pre> <p>This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.</p> </li> <li>Restart the HSM in initialization mode: <pre>ceremony hsm restart --mode initialization</pre> <p>This command should take about 55 seconds.</p> </li> <li><pre>ceremony feature info</pre> <p><input type="checkbox"/> SEE Activation (EU+10) is activated (shows Y).</p> </li> </ul>	

## 5.2 Unpack the Smartcards

Start time: \_\_\_\_\_

Step	Activity	End Time																				
47	Inspect the smartcard packaging.  <input type="checkbox"/> The packaging does not appear tampered with.																					
48	Open the smartcard packaging. Take out two cards, and put the rest in a tamper-evident bag.  Bag ID: <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

49	<p>Inspect the first smartcard. Label it “OCS”.</p> <p><input type="checkbox"/> The smartcard does not appear tampered with.</p> <p><input type="checkbox"/> The smartcard has nShield and Entrust trademarks.</p> <p>Smartcard ID:</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>-</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	-	5	6	-	7	8	9	10	11	12															
1	2	3	4	-	5	6	-	7	8	9	10	11	12																	
50	<p>Inspect the second smartcard. Label it “ACS”.</p> <p><input type="checkbox"/> The smartcard does not appear tampered with.</p> <p><input type="checkbox"/> The smartcard has nShield and Entrust trademarks.</p> <p>Smartcard ID:</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>-</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	-	5	6	-	7	8	9	10	11	12															
1	2	3	4	-	5	6	-	7	8	9	10	11	12																	
51	Ask a few witnesses to choose a distinctive character or shape, and draw these on the cards.																													
52	Place the ACS smartcard in the card reader and place the OCS smartcard visibly in the stand.																													

### 5.3 Create the Security World and Sign the Software

Start time: \_\_\_\_\_

Step	Activity	End Time																	
53	<p>Create the HSM Security World, enroll the first HSM in it, and write to the ACS smartcard. Enter an empty passphrase when prompted.</p> <pre>ceremony hsm create-world</pre> <p>Identifying bytes of <code>KNS0</code> hash (<code>hkns0</code>):</p> <table><tr><td colspan="2">byte 1</td><td colspan="2">byte 2</td><td colspan="2">byte 3</td><td rowspan="2">...</td><td colspan="2">byte 20</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <p>This command takes about 45 seconds. It writes to the ACS smartcard and creates encrypted keys on the computer's filesystem.</p>	byte 1		byte 2		byte 3		...	byte 20										
byte 1		byte 2		byte 3		...	byte 20												

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

54	<p>Display information about the Security World:</p> <pre>ceremony hsm world-info</pre> <p>Identifying bytes of <code>KMSW</code> Security World key hash (<code>World</code> ▷ <code>hkm</code>):</p> <table><tr><td colspan="2">byte 1</td><td colspan="2">byte 2</td><td colspan="2">byte 3</td><td rowspan="2">...</td><td colspan="2">byte 20</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	byte 1		byte 2		byte 3		...	byte 20										
byte 1		byte 2		byte 3		...	byte 20												
55	<p>Restart the HSM in operational mode:</p> <pre>ceremony hsm restart</pre> <p>This command should take about 55 seconds.</p>																		
56	<p>Remove the ACS smartcard from the card reader. Place the OCS smartcard in the card reader and place the ACS smartcard visibly in the stand.</p>																		
57	<p>Write to the OCS smartcard. Enter an empty passphrase when prompted.</p> <pre>ceremony smartcard write-ocs</pre> <p>This command should take about 12 seconds.</p>																		
58	<p>Create a signing key:</p> <pre>ceremony sign create-key</pre> <p>This command should take about 6 seconds. It writes an encrypted key to the host computer's filesystem.</p>																		
59	<p>Display information about the signing key:</p> <pre>ceremony sign key-info</pre> <p>Identifying bytes of signing key hash (Key AppName seeinteg Ident jbox-signer ▷ hash):</p> <table><tr><td colspan="2">byte 1</td><td colspan="2">byte 2</td><td colspan="2">byte 3</td><td rowspan="2">...</td><td colspan="2">byte 20</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	byte 1		byte 2		byte 3		...	byte 20										
byte 1		byte 2		byte 3		...	byte 20												
60	<p>Install Entrust's compiler, libraries, and header files:</p> <pre>ceremony vendor install codesafe</pre> <p>This command should take about 10 seconds.</p>																		

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

61

Build the `entrust_init` tool:

`ceremony build init`

This command should take about 30 seconds.

☐

 The SHA-256 hash of `entrust_init` encoded as a BIP-39 mnemonic matches:

1	2	3	4
artist	pencil	erode	defy
5	6	7	8
leader	abuse	flat	approve
9	10	11	12
dignity	bag	area	absent
13	14	15	16
mobile	myself	express	economy
17	18	19	20
eight	welcome	dilemma	cup
21	22	23	24
essay	thunder	drastic	parrot

62

Build the HSM software:

`ceremony build hsm`

This command should take about 30 seconds.

☐

 Identifying words of the BIP-39 mnemonic encoding of the SHA-256 hash of `entrust_hsm.elf` match:

word 1	word 2	word 3		word 24
urge	athlete	prevent	...	warfare

The full mnemonic is checked in the next step when this software is signed.

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

63

Sign the HSM software:

`ceremony sign software`

This command should take about 2 seconds. It requires the OCS smartcard. It reads an ELF-format executable from the host computer's filesystem and writes a signed version of that back to the host computer's filesystem.

- ☐ The SHA-256 hash of the input file (`entrust_hsm.elf`) encoded as a BIP-39 mnemonic matches:

1	2	3	4
urge	athlete	prevent	input
5	6	7	8
ribbon	skate	chimney	damage
9	10	11	12
shock	speed	turn	connect
13	14	15	16
strategy	left	economy	foil
17	18	19	20
oppose	taxi	crouch	pill
21	22	23	24
price	olympic	repeat	warfare

Identifying words of the BIP-39 mnemonic encoding of the SHA-256 hash of the signed file (`entrust_hsm.sar`):

word 1	word 2	word 3	...	word 24

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

64

Sign the HSM userdata:

`ceremony sign userdata`

This command should take about 1 second. It requires the OCS smartcard. It reads the string `dummy` from the host computer's filesystem (the content is ignored) and writes a signed version of that back to the host computer's filesystem.

☐ The input file (`userdata.dummy`) SHA-256 hash encoded as a BIP-39 mnemonic matches:

1	2	3	4
remember	bind	flat	patch
5	6	7	8
banana	recall	possible	tourist
9	10	11	12
width	cycle	fringe	next
13	14	15	16
visa	people	private	ready
17	18	19	20
price	tree	comic	glow
21	22	23	24
together	print	annual	cash

Identifying words of the BIP-39 mnemonic encoding of the SHA-256 hash of the signed file (`userdata.sar`):

word 1	word 2	word 3	...	word 24

## 5.4 Destroy the OCS Smartcard

Start time: \_\_\_\_\_

Step	Activity	End Time
------	----------	----------

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



65	Erase the OCS smartcard:  ceremony smartcard erase  This command takes about 30 seconds.	
66	Remove the OCS smartcard from the card reader and physically destroy it. Use a rotary tool to grind the smartcard electronics into a powder. Use scissors to shred the remaining plastic.	

## 5.5 Create the Realm Keys

Start time: \_\_\_\_\_

Step	Activity	End Time
------	----------	----------

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

67	<p>Generate the realm keys:</p> <pre>ceremony realm create-keys</pre> <p>Each key's ACL is the same, except for identifiers, having three permission groups:</p> <ul style="list-style-type: none"> <li>• Permission Group 1 allows reading the ACL itself and allows the key to be duplicated with the same ACL. It should look like: <pre>Action: OpPermissions: DuplicateHandle, GetACL</pre> </li> <li>• Permission Group 2 allows HSM software signed with the signing key to read the key (and associated data, which is not used). It should look like: <pre>Requires Cert: hash: {SIGNING-KEY-HASH} mechanism: Any Flags: certmech_present Action: OpPermissions: ExportAsPlain, GetAppData</pre> </li> <li>• Permission Group 3 allows the key to be saved as a blob on the host filesystem, encrypted by the Security World key (KMSW), only once. It should look like (in two lines, wrapped here): <pre>Use Limit: Global: max: 1 id: {VARYING-40-HEX-CHARS} Action: MakeBlob: Flags: AllowKmOnly, AllowNonKm0, kmhash_present kmhash: {KMSW-HASH}</pre> </li> </ul> <ul style="list-style-type: none"> <li>□ Creating key simple,jbox-mac... ▷ Permission Group 2 ▷ Requires Cert ▷ hash matches the signing key hash in <a href="#">Step 59</a>.</li> <li>□ Creating key simple,jbox-mac... ▷ Permission Group 3 ▷ Action ▷ kmhash matches the Security World key hash in <a href="#">Step 54</a>.</li> <li>□ Creating key simple,jbox-record... ▷ Permission Group 2 ▷ Requires Cert ▷ hash shows the same value as the jbox-mac permissions.</li> <li>□ Creating key simple,jbox-record... ▷ Permission Group 3 ▷ Action ▷ kmhash shows the same value as the jbox-mac permissions.</li> <li>□ Creating key simple,jbox-noise... ▷ Permission Group 2 ▷ Requires Cert ▷ hash shows the same value as the jbox-mac permissions.</li> <li>□ Creating key simple,jbox-noise... ▷ Permission Group 3 ▷ Action ▷ kmhash shows the same value as the jbox-mac permissions.</li> </ul>	
----	---	--

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

68

Verify the ACL on each key no longer allows creating a key blob:

```
ceremony realm print-acl mac
ceremony realm print-acl record
ceremony realm print-acl noise
```

☐ Permission Group 3 is no longer present for the jbox-mac key.
 ☐ Permission Group 3 is no longer present for the jbox-record key.
 ☐ Permission Group 3 is no longer present for the jbox-noise key.

69

Record the public key that clients will use to authenticate this realm.

```
ceremony realm noise-public-key
```

The output Qx is the X25519 public key encoded in hex.

Identifying bytes of Noise public key (Qx):

byte 1	byte 2	byte 3	...	byte 32

Copy and paste the public key into the next command (using the keyboard shortcuts documented in Appendix C.3):

```
ceremony bip39 encode «Qx»
```

Noise public key encoded as a BIP-39 mnemonic phrase:

word 1	word 2	word 3	word 4
word 5	word 6	word 7	word 8
word 9	word 10	word 11	word 12
word 13	word 14	word 15	word 16
word 17	word 18	word 19	word 20
word 21	word 22	word 23	word 24

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## 5.6 Write the Realm DVD

Start time: \_\_\_\_\_

Step	Activity	End Time																				
70	<p>Create the realm DVD image:</p> <pre>ceremony realm-dvd create-iso</pre> <p>This command should take less than 1 second. See Appendix A for details on which files are included on the image.</p> <p>Identifying bytes of SHA-256 hash of the realm DVD image (<code>/root/realm.iso</code>):</p> <table><tr><td>byte 1</td><td>byte 2</td><td>byte 3</td><td>...</td><td>byte 32</td></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table>	byte 1	byte 2	byte 3	...	byte 32																
byte 1	byte 2	byte 3	...	byte 32																		
71	Eject the boot DVD by pressing the button and remove it from the DVD drive.																					
72	<p>Inspect the blank DVD packaging.</p> <p><input type="checkbox"/> The packaging does not appear tampered with.</p>																					
73	<p>Take one blank DVD and label it with:</p> <ul style="list-style-type: none"><li>• “Ceremony Realm DVD”,</li><li>• the local date and time, and</li><li>• the identifying bytes of the SHA-256 hash of the ISO file from <a href="#">Step 70</a>.</li></ul> <p><input type="checkbox"/> The DVD does not appear tampered with and appears blank.</p> <p>Place the remaining spindle in a tamper-evident bag.</p> <p>Bag ID:</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
74	Insert the realm DVD into the DVD drive.																					
75	<p>Write the image to the DVD:</p> <pre>ceremony realm-dvd write</pre> <p>This command should take about 4 minutes and should eject the DVD when completed. Ejecting the DVD is intended to clear any OS or drive caches.</p> <p><input type="checkbox"/> The computer ejected the DVD.</p>																					
76	Insert the realm DVD into the DVD drive.																					

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

77	Verify the files were written to the realm DVD correctly:	
	<code>ceremony realm-dvd verify</code>	

## 5.7 Clear the First HSM

Start time: \_\_\_\_\_

Step	Activity	End Time
78	Restart the HSM in initialization mode:  <code>ceremony hsm restart --mode initialization</code>  This command should take about 55 seconds.	
79	Initialize the HSM with a new module key:  <code>ceremony hsm erase</code>  <input type="checkbox"/> The output includes the line <code>Initialising Unit 1 (SetNSOPerms)</code> . <input type="checkbox"/> <code>Module Key Info &gt; HKM[0]</code> is shows 20 random-looking bytes in hex.  This command should take less than 1 second. This key is temporary, as creating or joining a Security World later will generate a new module key.	
80	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	
81	Power off the computer: <ul style="list-style-type: none"> <li><code>ceremony computer shutdown</code></li> <li>Wait for the computer to turn off.</li> <li>Unplug the power cord from the back of the computer.</li> <li>Wait a few seconds.</li> </ul>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## 6 HSM Enrollment

### 6.1 Set up the First HSM

Start time: \_\_\_\_\_

Step	Activity	End Time
82	Boot into the boot DVD: <ul style="list-style-type: none"><li>• Plug the power cord into the back of the computer.</li><li>• Press the “power button” on the front of the computer.</li><li>• The computer should boot into the bootloader on the boot DVD.</li><li>• Press <code>Enter</code> at the GRUB menu to boot into Linux.</li></ul>	
83	Install Entrust’s tools, daemons, and driver:  <code>ceremony vendor install secworld</code>  This command takes about 80 seconds.	
84	Restart the HSM in initialization mode:  <code>ceremony hsm restart --mode initialization</code>  This command should take about 55 seconds.	
85	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.	
86	Copy the files from the realm DVD:  <code>ceremony realm-dvd restore</code>	
87	Place the ACS smartcard in the card reader.	
88	Enroll the HSM in the Security World:  <code>ceremony hsm join-world</code>  This command takes about 22 seconds and reads from the ACS smartcard.  <input type="checkbox"/> The output <code>hknso</code> matches the one recorded in <a href="#">Step 53</a> .	
89	Restart the HSM in operational mode:  <code>ceremony hsm restart</code>  This command should take about 55 seconds.	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

90	<p>Print the signing key hash from the ACL of a key:</p> <pre>ceremony realm print-acl noise</pre> <p><input type="checkbox"/> key simple,jbox-noise exists... ▷ Permission Group 2 ▷ Requires Cert ▷ hash matches the signing key hash in <a href="#">Step 59</a>.</p>																					
91	<p>Initialize this HSM’s NVRAM file, providing the same signing key hash as the previous step for its ACL:</p> <pre>ceremony realm create-nvram-file --signing-key-hash «HASH»</pre> <p><input type="checkbox"/> Permission Group 2 ▷ Requires Cert ▷ hash matches the signing key hash in <a href="#">Step 59</a>.</p> <p>This command takes about 1 second and reads from the ACS smartcard.</p>																					
92	<p>Remove the ACS smartcard from the card reader and place it visibly in the stand.</p>																					
93	<p>Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.</p>																					
94	<p>Power off the computer:</p> <ul style="list-style-type: none"><li>• <pre>ceremony computer shutdown</pre></li><li>• Wait for the computer to turn off.</li><li>• Unplug the power cord from the back of the computer.</li><li>• Wait a few seconds.</li></ul>																					
95	<p>Unplug the card reader from the HSM.</p>																					
96	<p>Remove the HSM from the computer. Insert it into an antistatic bag and then insert that into a tamper-evident bag (for transport to the production environment).</p> <p>Bag ID:</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													

## 6.2 Intermission

Start time: \_\_\_\_\_

Step	Activity	End Time
97	Detach the operator end of the antistatic wrist strap, leaving it connected to the computer chassis.	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

98	<p>Remove the ACS smartcard from the stand.</p> <p>Wrap the end of the smartcard with masking tape three times over, covering the electronics.</p> <p>Place the ACS smartcard in a tamper-evident bag.</p> <p>Bag ID:</p> <table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
99	<p>Place the card reader in a tamper-evident bag.</p> <p>Bag ID:</p> <table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
100	<p>MC: Decide on an approximate duration for the break.</p> <p>Duration: _____</p> <p>Resume at (time): _____</p>																					
101	<p>Place this document in a tamper-evident bag.</p> <p>Bag ID:</p> <table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
102	<p>The operator must step away from the station. Then, everyone (all participants and anyone else present) should leave the room together.</p> <p><b>No one may enter the room during the break.</b></p> <p>After the break, all participants should reenter the room together. Then, the operator should return to the station and remove this document from its bag.</p> <p><input type="checkbox"/> The bag does not appear tampered with.</p> <p><input type="checkbox"/> The bag ID matches the one recorded above.</p> <p><input type="checkbox"/> By a show of hands, each of the participants agrees that, to the best of their knowledge, no one enter the room during the break.</p> <p>Count: _____</p>																					

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



103	Remove the card reader from its bag.  <input type="checkbox"/> The bag does not appear tampered with. <input type="checkbox"/> The bag ID matches the one recorded above.	
104	Remove the ACS smartcard from the bag, remove the masking tape from it, and place it visibly in the stand.  <input type="checkbox"/> The bag does not appear tampered with. <input type="checkbox"/> The bag ID matches the one recorded above. <input type="checkbox"/> The smartcard ID matches <u>Step 50</u> .	
105	Ground yourself to the unpainted computer chassis with the antistatic wrist strap. It can be worn on your upper arm or ankle.	

### 6.3 Set Up the Second HSM

Start time: \_\_\_\_\_

Step	Activity	End Time
------	----------	----------

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

Choose exactly one of the following:

☐ **The HSM is in factory packaging.**

Choose exactly one of the following:

- ☐ The outer shipping box was opened earlier in the ceremony.
- ☐ The outer shipping box was not opened earlier in the ceremony.  
Inspect the outer shipping box:
- ☐ The box does not appear tampered with.
- Open the outer shipping box, remove its contents, and put away the box and any extra padding.

Inspect the white plastic bag containing this HSM:

- ☐ The text says "NCIPHER: AN ENTRUST DATACARD COMPANY", with the first "N" enclosed in a circle.
- ☐ The bag is sealed and does not appear tampered with.

Use scissors to open the end of the bag at the dashed line. Remove the bag and put it away. Inspect the box sleeve:

- ☐ The text says "ENTRUST: SECURING A WORLD IN MOTION" with the hexagonal "E" logo and "nShield: Hardware Security Modules".
- ☐ The box sleeve does not appear tampered with.

Remove the box sleeve and put it away. Inspect the box:

- ☐ The box does not appear tampered with.

Inspect the sticker at the end of the box:

- ☐ The top text says "ENTRUST: nShield Solo XC".
- ☐ Only the nC4035E-000 nShield Solo XC F3 model is checked.
- ☐ Only the Base speed is checked.
- ☐ The serial number matches an unused HSM listed in Section 4.1.

☐ **The HSM is in an antistatic bag within a tamper-evident bag.**

- ☐ The tamper-evident bag does not appear tampered with.
- ☐ The serial number and bag ID match an unused HSM listed in Section 4.1.

Serial number:

1	2		3	4	5	6	7	8		9
		-								

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

107	<p>Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging.</p> <p><input type="checkbox"/> The HSM does not appear tampered with.</p> <p>Inspect the sticker on the side of the HSM:</p> <p><input type="checkbox"/> The serial number (S/N) matches that of the previous step.</p> <p><input type="checkbox"/> The model is nC4035E-000.</p>																											
108	<p>Set the mode switch and jumpers on the HSM:</p> <p><input type="checkbox"/> Set the outside-facing physical switch to 0 (the middle position).</p> <p><input type="checkbox"/> Ensure both override jumper switches are set to off.</p>																											
109	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>The HSM currently has no PCI bracket.</td> </tr> <tr> <td><input type="radio"/></td> <td>           The HSM currently has a low-profile or full-height PCI bracket.             Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.         </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	The HSM currently has no PCI bracket.	<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																					
Choose exactly one of the following:																												
<input type="radio"/>	The HSM currently has no PCI bracket.																											
<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																											
110	<p>Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.</p>																											
111	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>This HSM did not come with a card reader.</td> </tr> <tr> <td><input type="radio"/></td> <td>           This HSM came with a card reader.             Place the new card reader in a tamper-evident bag for storage.             Bag ID:           <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table> </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	This HSM did not come with a card reader.	<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
Choose exactly one of the following:																												
<input type="radio"/>	This HSM did not come with a card reader.																											
<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table>	1	2	3	4	5	6	7	8	9	10																	
1	2	3	4	5	6	7	8	9	10																			
112	<p>While bracing the HSM, plug the existing card reader into the HSM's external port.</p>																											
113	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the "power button" on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press Enter at the GRUB menu to boot into Linux.</li> </ul>																											

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

114	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>																													
115	<p>Print HSM info:</p> <pre>ceremony hsm info</pre> <p>ESN (Module #1 ▷ serial number):</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>7</td><td>8</td><td>-</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <p><input type="checkbox"/> The ESN matches the HSM listed in Section 4.1.</p> <p>Firmware version (Module #1 ▷ version): _____</p> <p><input type="checkbox"/> Module #1 ▷ product name shows all of nC3025E/nC4035E/nC4335N.</p>	1	2	3	4	-	5	6	7	8	-	9	10	11	12															
1	2	3	4	-	5	6	7	8	-	9	10	11	12																	
116	<p>Restart the HSM in maintenance mode:</p> <pre>ceremony hsm restart --mode maintenance</pre> <p>This command should take about 55 seconds.</p>																													
117	<p>Update/overwrite the HSM firmware to version 13.3.1:</p> <pre>ceremony vendor mount firmware ceremony firmware write ceremony vendor unmount firmware</pre> <p>These commands should take about 3 minutes if starting from the same version and may take several more minutes if starting from an earlier version.</p>																													
118	<p>Wait until the HSM is done:</p> <pre>ceremony hsm info</pre> <p><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</p> <p><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</p> <p><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</p> <p>Wait and re-run the command until these conditions are satisfied.</p>																													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

119	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li>• <code>ceremony</code> computer shutdown</li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>	
120	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the “power button” on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press <code>Enter</code> at the GRUB menu to boot into Linux.</li> </ul>	
121	<p>Install Entrust’s tools, daemons, and driver:</p> <pre><code>ceremony vendor install secworld</code></pre> <p>This command takes about 80 seconds.</p>	
122	<p>Wait until the HSM is ready:</p> <pre><code>ceremony hsm info</code></pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</li> <li><input type="checkbox"/> Module #1 ▷ mode shows uninitialized.</li> <li><input type="checkbox"/> Module #1 ▷ serial number matches <a href="#">Step 115</a>.</li> <li><input type="checkbox"/> Module #1 ▷ version shows 13.3.1.</li> <li><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</li> <li><input type="checkbox"/> The HSM LED is blinking in the repeated <code>--</code> pattern.</li> </ul> <p>Wait and re-run the command until these conditions are satisfied.</p> <p>If the module does not appear at all, check <code>dmesg</code> for the error <code>nfp_open: device &lt;...&gt; failed to open with error: -5</code>. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an <i>exception sheet</i> the first time it occurs.</p>	
123	<p>Restart the HSM in initialization mode:</p> <pre><code>ceremony hsm restart --mode initialization</code></pre> <p>This command should take about 55 seconds.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

124	<p>Initialize the HSM with a new module key:</p> <pre>ceremony hsm erase</pre> <p><input type="checkbox"/> The output includes the line Initialising Unit 1 (SetNS0Perms).</p> <p><input type="checkbox"/> Module Key Info ▷ HKM[0] is shows 20 random-looking bytes in hex.</p> <p>This command should take less than 1 second. This key is temporary, as creating or joining a Security World later will generate a new module key.</p>							
125	<p>Check which features have been activated on the HSM:</p> <pre>ceremony feature info</pre> <p>Active features (excluding SEE): _____</p> <table><tr><th colspan="2">Choose exactly one of the following:</th></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is already activated (shows Y).</td></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is not activated (shows N).</td></tr></table> <p>Activate the SEE (CodeSafe) feature on the HSM:</p> <ul style="list-style-type: none"><li><pre>ceremony feature activate features/SEEUE_⟨ESN⟩.txt</pre><p>This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.</p></li><li>Restart the HSM in initialization mode:<pre>ceremony hsm restart --mode initialization</pre><p>This command should take about 55 seconds.</p></li><li><pre>ceremony feature info</pre><p><input type="checkbox"/> SEE Activation (EU+10) is activated (shows Y).</p></li></ul>	Choose exactly one of the following:		<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).	<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).	
Choose exactly one of the following:								
<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).							
<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).							
126	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.							
127	<p>Copy the files from the realm DVD:</p> <pre>ceremony realm-dvd restore</pre>							
128	Place the ACS smartcard in the card reader.							

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

129	<p>Enroll the HSM in the Security World:</p> <pre>ceremony hsm join-world</pre> <p>This command takes about 22 seconds and reads from the ACS smartcard.</p> <p><input type="checkbox"/> The output <code>hknso</code> matches the one recorded in <a href="#">Step 53</a>.</p>	
130	<p>Restart the HSM in operational mode:</p> <pre>ceremony hsm restart</pre> <p>This command should take about 55 seconds.</p>	
131	<p>Print the signing key hash from the ACL of a key:</p> <pre>ceremony realm print-acl noise</pre> <p><input type="checkbox"/> <code>key simple,jbox-noise exists... ▷ Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p>	
132	<p>Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL:</p> <pre>ceremony realm create-nvram-file --signing-key-hash «HASH»</pre> <p><input type="checkbox"/> <code>Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p> <p>This command takes about 1 second and reads from the ACS smartcard.</p>	
133	Remove the ACS smartcard from the card reader and place it visibly in the stand.	
134	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	
135	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li><code>ceremony computer shutdown</code></li> <li>Wait for the computer to turn off.</li> <li>Unplug the power cord from the back of the computer.</li> <li>Wait a few seconds.</li> </ul>	
136	Unplug the card reader from the HSM.	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

137	<p>Remove the HSM from the computer. Insert it into an antistatic bag and then insert that into a tamper-evident bag (for transport to the production environment).</p> <p>Bag ID:</p> <table border="1" style="margin-left: 40px;"> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">2</td> <td style="text-align: center;">3</td> <td style="text-align: center;">4</td> <td style="text-align: center;">5</td> <td style="text-align: center;">6</td> <td style="text-align: center;">7</td> <td style="text-align: center;">8</td> <td style="text-align: center;">9</td> <td style="text-align: center;">10</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													

## 6.4 Set Up the Third HSM

Start time: \_\_\_\_\_

Step	Activity	End Time
------	----------	----------

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



Choose exactly one of the following:

☐ **The HSM is in factory packaging.**

Choose exactly one of the following:

- ☐ The outer shipping box was opened earlier in the ceremony.
- ☐ The outer shipping box was not opened earlier in the ceremony.  
Inspect the outer shipping box:
- ☐ The box does not appear tampered with.
- Open the outer shipping box, remove its contents, and put away the box and any extra padding.

Inspect the white plastic bag containing this HSM:

- ☐ The text says "NCIPHER: AN ENTRUST DATACARD COMPANY", with the first "N" enclosed in a circle.
- ☐ The bag is sealed and does not appear tampered with.

Use scissors to open the end of the bag at the dashed line. Remove the bag and put it away. Inspect the box sleeve:

- ☐ The text says "ENTRUST: SECURING A WORLD IN MOTION" with the hexagonal "E" logo and "nShield: Hardware Security Modules".
- ☐ The box sleeve does not appear tampered with.

Remove the box sleeve and put it away. Inspect the box:

- ☐ The box does not appear tampered with.

Inspect the sticker at the end of the box:

- ☐ The top text says "ENTRUST: nShield Solo XC".
- ☐ Only the nC4035E-000 nShield Solo XC F3 model is checked.
- ☐ Only the Base speed is checked.
- ☐ The serial number matches an unused HSM listed in Section 4.1.

☐ **The HSM is in an antistatic bag within a tamper-evident bag.**

- ☐ The tamper-evident bag does not appear tampered with.
- ☐ The serial number and bag ID match an unused HSM listed in Section 4.1.

Serial number:

1	2		3	4	5	6	7	8		9
		-								

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

139	<p>Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging.</p> <p><input type="checkbox"/> The HSM does not appear tampered with.</p> <p>Inspect the sticker on the side of the HSM:</p> <p><input type="checkbox"/> The serial number (S/N) matches that of the previous step.</p> <p><input type="checkbox"/> The model is nC4035E-000.</p>																											
140	<p>Set the mode switch and jumpers on the HSM:</p> <p><input type="checkbox"/> Set the outside-facing physical switch to 0 (the middle position).</p> <p><input type="checkbox"/> Ensure both override jumper switches are set to off.</p>																											
141	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>The HSM currently has no PCI bracket.</td> </tr> <tr> <td><input type="radio"/></td> <td>           The HSM currently has a low-profile or full-height PCI bracket.             Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.         </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	The HSM currently has no PCI bracket.	<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																					
Choose exactly one of the following:																												
<input type="radio"/>	The HSM currently has no PCI bracket.																											
<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																											
142	<p>Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.</p>																											
143	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>This HSM did not come with a card reader.</td> </tr> <tr> <td><input type="radio"/></td> <td>           This HSM came with a card reader.             Place the new card reader in a tamper-evident bag for storage.             Bag ID:           <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table> </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	This HSM did not come with a card reader.	<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
Choose exactly one of the following:																												
<input type="radio"/>	This HSM did not come with a card reader.																											
<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10																	
1	2	3	4	5	6	7	8	9	10																			
144	<p>While bracing the HSM, plug the existing card reader into the HSM's external port.</p>																											
145	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the "power button" on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press Enter at the GRUB menu to boot into Linux.</li> </ul>																											

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

146	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>																													
147	<p>Print HSM info:</p> <pre>ceremony hsm info</pre> <p>ESN (Module #1 ▷ serial number):</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>7</td><td>8</td><td>-</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <p><input type="checkbox"/> The ESN matches the HSM listed in Section 4.1.</p> <p>Firmware version (Module #1 ▷ version): _____</p> <p><input type="checkbox"/> Module #1 ▷ product name shows all of nC3025E/nC4035E/nC4335N.</p>	1	2	3	4	-	5	6	7	8	-	9	10	11	12															
1	2	3	4	-	5	6	7	8	-	9	10	11	12																	
148	<p>Restart the HSM in maintenance mode:</p> <pre>ceremony hsm restart --mode maintenance</pre> <p>This command should take about 55 seconds.</p>																													
149	<p>Update/overwrite the HSM firmware to version 13.3.1:</p> <pre>ceremony vendor mount firmware ceremony firmware write ceremony vendor unmount firmware</pre> <p>These commands should take about 3 minutes if starting from the same version and may take several more minutes if starting from an earlier version.</p>																													
150	<p>Wait until the HSM is done:</p> <pre>ceremony hsm info</pre> <p><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</p> <p><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</p> <p><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</p> <p>Wait and re-run the command until these conditions are satisfied.</p>																													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

151	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li>• <code>ceremony</code> computer shutdown</li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>	
152	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the “power button” on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press Enter at the GRUB menu to boot into Linux.</li> </ul>	
153	<p>Install Entrust’s tools, daemons, and driver:</p> <pre><code>ceremony vendor install secworld</code></pre> <p>This command takes about 80 seconds.</p>	
154	<p>Wait until the HSM is ready:</p> <pre><code>ceremony hsm info</code></pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</li> <li><input type="checkbox"/> Module #1 ▷ mode shows uninitialized.</li> <li><input type="checkbox"/> Module #1 ▷ serial number matches <a href="#">Step 147</a>.</li> <li><input type="checkbox"/> Module #1 ▷ version shows 13.3.1.</li> <li><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</li> <li><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</li> </ul> <p>Wait and re-run the command until these conditions are satisfied.</p> <p>If the module does not appear at all, check <code>dmesg</code> for the error <code>nfp_open: device &lt;...&gt; failed to open with error: -5</code>. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an <i>exception sheet</i> the first time it occurs.</p>	
155	<p>Restart the HSM in initialization mode:</p> <pre><code>ceremony hsm restart --mode initialization</code></pre> <p>This command should take about 55 seconds.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

156	<p>Initialize the HSM with a new module key:</p> <pre>ceremony hsm erase</pre> <p><input type="checkbox"/> The output includes the line Initialising Unit 1 (SetNSOPerms).</p> <p><input type="checkbox"/> Module Key Info ▷ HKM[0] is shows 20 random-looking bytes in hex.</p> <p>This command should take less than 1 second. This key is temporary, as creating or joining a Security World later will generate a new module key.</p>							
157	<p>Check which features have been activated on the HSM:</p> <pre>ceremony feature info</pre> <p>Active features (excluding SEE): _____</p> <table><tr><th colspan="2">Choose exactly one of the following:</th></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is already activated (shows Y).</td></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is not activated (shows N).</td></tr></table> <p>Activate the SEE (CodeSafe) feature on the HSM:</p> <ul style="list-style-type: none"><li><pre>ceremony feature activate features/SEEUE_《ESN》.txt</pre><p>This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.</p></li><li>Restart the HSM in initialization mode:<pre>ceremony hsm restart --mode initialization</pre><p>This command should take about 55 seconds.</p><ul style="list-style-type: none"><li><pre>ceremony feature info</pre><p><input type="checkbox"/> SEE Activation (EU+10) is activated (shows Y).</p></li></ul></li></ul>	Choose exactly one of the following:		<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).	<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).	
Choose exactly one of the following:								
<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).							
<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).							
158	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.							
159	Copy the files from the realm DVD: <pre>ceremony realm-dvd restore</pre>							
160	Place the ACS smartcard in the card reader.							

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

161	<p>Enroll the HSM in the Security World:</p> <pre>ceremony hsm join-world</pre> <p>This command takes about 22 seconds and reads from the ACS smartcard.</p> <p><input type="checkbox"/> The output <code>hknso</code> matches the one recorded in <a href="#">Step 53</a>.</p>	
162	<p>Restart the HSM in operational mode:</p> <pre>ceremony hsm restart</pre> <p>This command should take about 55 seconds.</p>	
163	<p>Print the signing key hash from the ACL of a key:</p> <pre>ceremony realm print-acl noise</pre> <p><input type="checkbox"/> <code>key simple,jbox-noise exists... ▷ Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p>	
164	<p>Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL:</p> <pre>ceremony realm create-nvram-file --signing-key-hash «HASH»</pre> <p><input type="checkbox"/> <code>Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p> <p>This command takes about 1 second and reads from the ACS smartcard.</p>	
165	Remove the ACS smartcard from the card reader and place it visibly in the stand.	
166	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	
167	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li><code>ceremony computer shutdown</code></li> <li>Wait for the computer to turn off.</li> <li>Unplug the power cord from the back of the computer.</li> <li>Wait a few seconds.</li> </ul>	
168	Unplug the card reader from the HSM.	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

169	<p>Remove the HSM from the computer. Insert it into an antistatic bag and then insert that into a tamper-evident bag (for transport to the production environment).</p> <p>Bag ID:</p> <table border="1" style="margin-left: 40px;"> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">2</td> <td style="text-align: center;">3</td> <td style="text-align: center;">4</td> <td style="text-align: center;">5</td> <td style="text-align: center;">6</td> <td style="text-align: center;">7</td> <td style="text-align: center;">8</td> <td style="text-align: center;">9</td> <td style="text-align: center;">10</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													

### 6.5 Set Up the Fourth HSM

Start time: \_\_\_\_\_

Step	Activity	End Time
------	----------	----------

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

Choose exactly one of the following:

☐ **The HSM is in factory packaging.**

Choose exactly one of the following:

☐ The outer shipping box was opened earlier in the ceremony.

☐ The outer shipping box was not opened earlier in the ceremony.

Inspect the outer shipping box:

☐ The box does not appear tampered with.

Open the outer shipping box, remove its contents, and put away the box and any extra padding.

Inspect the white plastic bag containing this HSM:

☐ The text says "NCIPHER: AN ENTRUST DATACARD COMPANY", with the first "N" enclosed in a circle.

☐ The bag is sealed and does not appear tampered with.

Use scissors to open the end of the bag at the dashed line. Remove the bag and put it away. Inspect the box sleeve:

☐ The text says "ENTRUST: SECURING A WORLD IN MOTION" with the hexagonal "E" logo and "nShield: Hardware Security Modules".

☐ The box sleeve does not appear tampered with.

Remove the box sleeve and put it away. Inspect the box:

☐ The box does not appear tampered with.

Inspect the sticker at the end of the box:

☐ The top text says "ENTRUST: nShield Solo XC".

☐ Only the nC4035E-000 nShield Solo XC F3 model is checked.

☐ Only the Base speed is checked.

☐ The serial number matches an unused HSM listed in Section 4.1.

☐ **The HSM is in an antistatic bag within a tamper-evident bag.**

☐ The tamper-evident bag does not appear tampered with.

☐ The serial number and bag ID match an unused HSM listed in Section 4.1.

Serial number:

1	2	-	3	4	5	6	7	8		9

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



171	<p>Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging.</p> <p><input type="checkbox"/> The HSM does not appear tampered with.</p> <p>Inspect the sticker on the side of the HSM:</p> <p><input type="checkbox"/> The serial number (S/N) matches that of the previous step.</p> <p><input type="checkbox"/> The model is nC4035E-000.</p>																											
172	<p>Set the mode switch and jumpers on the HSM:</p> <p><input type="checkbox"/> Set the outside-facing physical switch to 0 (the middle position).</p> <p><input type="checkbox"/> Ensure both override jumper switches are set to off.</p>																											
173	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>The HSM currently has no PCI bracket.</td> </tr> <tr> <td><input type="radio"/></td> <td>           The HSM currently has a low-profile or full-height PCI bracket.             Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.         </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	The HSM currently has no PCI bracket.	<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																					
Choose exactly one of the following:																												
<input type="radio"/>	The HSM currently has no PCI bracket.																											
<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																											
174	<p>Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.</p>																											
175	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>This HSM did not come with a card reader.</td> </tr> <tr> <td><input type="radio"/></td> <td>           This HSM came with a card reader.             Place the new card reader in a tamper-evident bag for storage.             Bag ID:           <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table> </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	This HSM did not come with a card reader.	<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
Choose exactly one of the following:																												
<input type="radio"/>	This HSM did not come with a card reader.																											
<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table>	1	2	3	4	5	6	7	8	9	10																	
1	2	3	4	5	6	7	8	9	10																			
176	<p>While bracing the HSM, plug the existing card reader into the HSM's external port.</p>																											
177	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the "power button" on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press Enter at the GRUB menu to boot into Linux.</li> </ul>																											

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

178	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>																													
179	<p>Print HSM info:</p> <pre>ceremony hsm info</pre> <p>ESN (Module #1 ▷ serial number):</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>7</td><td>8</td><td>-</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <p><input type="checkbox"/> The ESN matches the HSM listed in Section 4.1.</p> <p>Firmware version (Module #1 ▷ version): _____</p> <p><input type="checkbox"/> Module #1 ▷ product name shows all of nC3025E/nC4035E/nC4335N.</p>	1	2	3	4	-	5	6	7	8	-	9	10	11	12															
1	2	3	4	-	5	6	7	8	-	9	10	11	12																	
180	<p>Restart the HSM in maintenance mode:</p> <pre>ceremony hsm restart --mode maintenance</pre> <p>This command should take about 55 seconds.</p>																													
181	<p>Update/overwrite the HSM firmware to version 13.3.1:</p> <pre>ceremony vendor mount firmware ceremony firmware write ceremony vendor unmount firmware</pre> <p>These commands should take about 3 minutes if starting from the same version and may take several more minutes if starting from an earlier version.</p>																													
182	<p>Wait until the HSM is done:</p> <pre>ceremony hsm info</pre> <p><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</p> <p><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</p> <p><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</p> <p>Wait and re-run the command until these conditions are satisfied.</p>																													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

183	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li>• <code>ceremony</code> computer shutdown</li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>	
184	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the “power button” on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press <code>Enter</code> at the GRUB menu to boot into Linux.</li> </ul>	
185	<p>Install Entrust’s tools, daemons, and driver:</p> <pre><code>ceremony vendor install secworld</code></pre> <p>This command takes about 80 seconds.</p>	
186	<p>Wait until the HSM is ready:</p> <pre><code>ceremony hsm info</code></pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</li> <li><input type="checkbox"/> Module #1 ▷ mode shows uninitialized.</li> <li><input type="checkbox"/> Module #1 ▷ serial number matches <a href="#">Step 179</a>.</li> <li><input type="checkbox"/> Module #1 ▷ version shows 13.3.1.</li> <li><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</li> <li><input type="checkbox"/> The HSM LED is blinking in the repeated <code>--</code> pattern.</li> </ul> <p>Wait and re-run the command until these conditions are satisfied.</p> <p>If the module does not appear at all, check <code>dmesg</code> for the error <code>nfp_open: device &lt;...&gt; failed to open with error: -5</code>. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an <i>exception sheet</i> the first time it occurs.</p>	
187	<p>Restart the HSM in initialization mode:</p> <pre><code>ceremony hsm restart --mode initialization</code></pre> <p>This command should take about 55 seconds.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

188	<p>Initialize the HSM with a new module key:</p> <pre>ceremony hsm erase</pre> <p><input type="checkbox"/> The output includes the line Initialising Unit 1 (SetNSOPerms).</p> <p><input type="checkbox"/> Module Key Info ▷ HKM[0] is shows 20 random-looking bytes in hex.</p> <p>This command should take less than 1 second. This key is temporary, as creating or joining a Security World later will generate a new module key.</p>							
189	<p>Check which features have been activated on the HSM:</p> <pre>ceremony feature info</pre> <p>Active features (excluding SEE): _____</p> <table><tr><th colspan="2">Choose exactly one of the following:</th></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is already activated (shows Y).</td></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is not activated (shows N).</td></tr></table> <p>Activate the SEE (CodeSafe) feature on the HSM:</p> <ul style="list-style-type: none"><li><pre>ceremony feature activate features/SEEUE_⟨ESN⟩.txt</pre><p>This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.</p></li><li>Restart the HSM in initialization mode:<pre>ceremony hsm restart --mode initialization</pre><p>This command should take about 55 seconds.</p></li><li><pre>ceremony feature info</pre><p><input type="checkbox"/> SEE Activation (EU+10) is activated (shows Y).</p></li></ul>	Choose exactly one of the following:		<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).	<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).	
Choose exactly one of the following:								
<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).							
<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).							
190	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.							
191	<p>Copy the files from the realm DVD:</p> <pre>ceremony realm-dvd restore</pre>							
192	Place the ACS smartcard in the card reader.							

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

193	<p>Enroll the HSM in the Security World:</p> <pre>ceremony hsm join-world</pre> <p>This command takes about 22 seconds and reads from the ACS smartcard.</p> <p><input type="checkbox"/> The output <code>hknso</code> matches the one recorded in <a href="#">Step 53</a>.</p>	
194	<p>Restart the HSM in operational mode:</p> <pre>ceremony hsm restart</pre> <p>This command should take about 55 seconds.</p>	
195	<p>Print the signing key hash from the ACL of a key:</p> <pre>ceremony realm print-acl noise</pre> <p><input type="checkbox"/> <code>key simple,jbox-noise exists... ▷ Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p>	
196	<p>Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL:</p> <pre>ceremony realm create-nvram-file --signing-key-hash «HASH»</pre> <p><input type="checkbox"/> <code>Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p> <p>This command takes about 1 second and reads from the ACS smartcard.</p>	
197	Remove the ACS smartcard from the card reader and place it visibly in the stand.	
198	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	
199	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li>• <pre>ceremony computer shutdown</pre></li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>	
200	Unplug the card reader from the HSM.	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

201	<p>Remove the HSM from the computer. Insert it into an antistatic bag and then insert that into a tamper-evident bag (for transport to the production environment).</p> <p>Bag ID:</p> <table border="1" style="margin-left: 40px;"> <tr> <td style="text-align: center;">1</td><td style="text-align: center;">2</td><td style="text-align: center;">3</td><td style="text-align: center;">4</td><td style="text-align: center;">5</td><td style="text-align: center;">6</td><td style="text-align: center;">7</td><td style="text-align: center;">8</td><td style="text-align: center;">9</td><td style="text-align: center;">10</td></tr> <tr> <td style="height: 20px;"></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													

## 6.6 Set Up the Fifth HSM

Start time: \_\_\_\_\_

Step	Activity	End Time
------	----------	----------

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

Choose exactly one of the following:

☐ **The HSM is in factory packaging.**

Choose exactly one of the following:

☐ The outer shipping box was opened earlier in the ceremony.

☐ The outer shipping box was not opened earlier in the ceremony.

Inspect the outer shipping box:

☐ The box does not appear tampered with.

Open the outer shipping box, remove its contents, and put away the box and any extra padding.

Inspect the white plastic bag containing this HSM:

☐ The text says "NCIPHER: AN ENTRUST DATACARD COMPANY", with the first "N" enclosed in a circle.

☐ The bag is sealed and does not appear tampered with.

Use scissors to open the end of the bag at the dashed line. Remove the bag and put it away. Inspect the box sleeve:

☐ The text says "ENTRUST: SECURING A WORLD IN MOTION" with the hexagonal "E" logo and "nShield: Hardware Security Modules".

☐ The box sleeve does not appear tampered with.

Remove the box sleeve and put it away. Inspect the box:

☐ The box does not appear tampered with.

Inspect the sticker at the end of the box:

☐ The top text says "ENTRUST: nShield Solo XC".

☐ Only the nC4035E-000 nShield Solo XC F3 model is checked.

☐ Only the Base speed is checked.

☐ The serial number matches an unused HSM listed in Section 4.1.

☐ **The HSM is in an antistatic bag within a tamper-evident bag.**

☐ The tamper-evident bag does not appear tampered with.

☐ The serial number and bag ID match an unused HSM listed in Section 4.1.

Serial number:

1	2		3	4	5	6	7	8		9
		-								

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

203	<p>Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging.</p> <p><input type="checkbox"/> The HSM does not appear tampered with.</p> <p>Inspect the sticker on the side of the HSM:</p> <p><input type="checkbox"/> The serial number (S/N) matches that of the previous step.</p> <p><input type="checkbox"/> The model is nC4035E-000.</p>																											
204	<p>Set the mode switch and jumpers on the HSM:</p> <p><input type="checkbox"/> Set the outside-facing physical switch to 0 (the middle position).</p> <p><input type="checkbox"/> Ensure both override jumper switches are set to off.</p>																											
205	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>The HSM currently has no PCI bracket.</td> </tr> <tr> <td><input type="radio"/></td> <td>           The HSM currently has a low-profile or full-height PCI bracket.             Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.         </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	The HSM currently has no PCI bracket.	<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																					
Choose exactly one of the following:																												
<input type="radio"/>	The HSM currently has no PCI bracket.																											
<input type="radio"/>	The HSM currently has a low-profile or full-height PCI bracket.  Remove the two screws holding the bracket from the HSM, then remove the bracket. Put away the bracket and the screws.																											
206	<p>Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.</p>																											
207	<table border="1"> <tr> <th colspan="2">Choose exactly one of the following:</th> </tr> <tr> <td><input type="radio"/></td> <td>This HSM did not come with a card reader.</td> </tr> <tr> <td><input type="radio"/></td> <td>           This HSM came with a card reader.             Place the new card reader in a tamper-evident bag for storage.             Bag ID:           <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table> </td> </tr> </table>	Choose exactly one of the following:		<input type="radio"/>	This HSM did not come with a card reader.	<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10											
Choose exactly one of the following:																												
<input type="radio"/>	This HSM did not come with a card reader.																											
<input type="radio"/>	This HSM came with a card reader.  Place the new card reader in a tamper-evident bag for storage.  Bag ID: <table border="1" style="margin-top: 10px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10																	
1	2	3	4	5	6	7	8	9	10																			
208	<p>While bracing the HSM, plug the existing card reader into the HSM's external port.</p>																											
209	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the "power button" on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press Enter at the GRUB menu to boot into Linux.</li> </ul>																											

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



210	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>																													
211	<p>Print HSM info:</p> <pre>ceremony hsm info</pre> <p>ESN (Module #1 ▷ serial number):</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>-</td><td>5</td><td>6</td><td>7</td><td>8</td><td>-</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <p><input type="checkbox"/> The ESN matches the HSM listed in Section 4.1.</p> <p>Firmware version (Module #1 ▷ version): _____</p> <p><input type="checkbox"/> Module #1 ▷ product name shows all of nC3025E/nC4035E/nC4335N.</p>	1	2	3	4	-	5	6	7	8	-	9	10	11	12															
1	2	3	4	-	5	6	7	8	-	9	10	11	12																	
212	<p>Restart the HSM in maintenance mode:</p> <pre>ceremony hsm restart --mode maintenance</pre> <p>This command should take about 55 seconds.</p>																													
213	<p>Update/overwrite the HSM firmware to version 13.3.1:</p> <pre>ceremony vendor mount firmware ceremony firmware write ceremony vendor unmount firmware</pre> <p>These commands should take about 3 minutes if starting from the same version and may take several more minutes if starting from an earlier version.</p>																													
214	<p>Wait until the HSM is done:</p> <pre>ceremony hsm info</pre> <p><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</p> <p><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</p> <p><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</p> <p>Wait and re-run the command until these conditions are satisfied.</p>																													

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

215	<p>Power off the computer:</p> <ul style="list-style-type: none"> <li>• <code>ceremony</code> computer shutdown</li> <li>• Wait for the computer to turn off.</li> <li>• Unplug the power cord from the back of the computer.</li> <li>• Wait a few seconds.</li> </ul>	
216	<p>Boot into the boot DVD:</p> <ul style="list-style-type: none"> <li>• Plug the power cord into the back of the computer.</li> <li>• Press the “power button” on the front of the computer.</li> <li>• The computer should boot into the bootloader on the boot DVD.</li> <li>• Press Enter at the GRUB menu to boot into Linux.</li> </ul>	
217	<p>Install Entrust’s tools, daemons, and driver:</p> <pre>ceremony vendor install secworld</pre> <p>This command takes about 80 seconds.</p>	
218	<p>Wait until the HSM is ready:</p> <pre>ceremony hsm info</pre> <ul style="list-style-type: none"> <li><input type="checkbox"/> Module #1 ▷ enquiry reply flags shows none (not Offline).</li> <li><input type="checkbox"/> Module #1 ▷ mode shows uninitialized.</li> <li><input type="checkbox"/> Module #1 ▷ serial number matches <a href="#">Step 211</a>.</li> <li><input type="checkbox"/> Module #1 ▷ version shows 13.3.1.</li> <li><input type="checkbox"/> Module #1 ▷ hardware status shows OK.</li> <li><input type="checkbox"/> The HSM LED is blinking in the repeated -- pattern.</li> </ul> <p>Wait and re-run the command until these conditions are satisfied.</p> <p>If the module does not appear at all, check <code>dmesg</code> for the error <code>nfp_open: device &lt;...&gt; failed to open with error: -5</code>. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an <i>exception sheet</i> the first time it occurs.</p>	
219	<p>Restart the HSM in initialization mode:</p> <pre>ceremony hsm restart --mode initialization</pre> <p>This command should take about 55 seconds.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

220	<p>Initialize the HSM with a new module key:</p> <pre>ceremony hsm erase</pre> <div><div><input type="checkbox"/></div><div>The output includes the line Initialising Unit 1 (SetNSOPerms).</div></div> <div><div><input type="checkbox"/></div><div>Module Key Info ▷ HKM[0] is shows 20 random-looking bytes in hex.</div></div> <p>This command should take less than 1 second. This key is temporary, as creating or joining a Security World later will generate a new module key.</p>							
221	<p>Check which features have been activated on the HSM:</p> <pre>ceremony feature info</pre> <p>Active features (excluding SEE): _____</p> <table><tr><th colspan="2">Choose exactly one of the following:</th></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is already activated (shows Y).</td></tr><tr><td><input type="radio"/></td><td>SEE Activation (EU+10) is not activated (shows N).</td></tr></table> <p>Activate the SEE (CodeSafe) feature on the HSM:</p> <div><div><ul style="list-style-type: none"><li><pre>ceremony feature activate features/SEEUE_⟨ESN⟩.txt</pre><p>This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.</p></li><li>Restart the HSM in initialization mode:<pre>ceremony hsm restart --mode initialization</pre><p>This command should take about 55 seconds.</p></li><li><pre>ceremony feature info</pre><div><div><input type="checkbox"/></div><div>SEE Activation (EU+10) is activated (shows Y).</div></div></li></ul></div></div>	Choose exactly one of the following:		<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).	<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).	
Choose exactly one of the following:								
<input type="radio"/>	SEE Activation (EU+10) is already activated (shows Y).							
<input type="radio"/>	SEE Activation (EU+10) is not activated (shows N).							
222	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.							
223	<p>Copy the files from the realm DVD:</p> <pre>ceremony realm-dvd restore</pre>							
224	Place the ACS smartcard in the card reader.							

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

225	<p>Enroll the HSM in the Security World:</p> <pre>ceremony hsm join-world</pre> <p>This command takes about 22 seconds and reads from the ACS smartcard.</p> <p><input type="checkbox"/> The output <code>hkns0</code> matches the one recorded in <a href="#">Step 53</a>.</p>	
226	<p>Restart the HSM in operational mode:</p> <pre>ceremony hsm restart</pre> <p>This command should take about 55 seconds.</p>	
227	<p>Print the signing key hash from the ACL of a key:</p> <pre>ceremony realm print-acl noise</pre> <p><input type="checkbox"/> <code>key simple,jbox-noise exists... ▷ Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p>	
228	<p>Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL:</p> <pre>ceremony realm create-nvram-file --signing-key-hash &lt;HASH&gt;</pre> <p><input type="checkbox"/> <code>Permission Group 2 ▷ Requires Cert ▷ hash</code> matches the signing key hash in <a href="#">Step 59</a>.</p> <p>This command takes about 1 second and reads from the ACS smartcard.</p>	

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## 7 Conclusion

Start time: \_\_\_\_\_

Step	Activity	End Time																				
229	Erase the ACS smartcard: <div>ceremony smartcard erase</div> This command takes about 30 seconds.																					
230	Remove the ACS smartcard from the card reader and physically destroy it. Use a rotary tool to grind the smartcard electronics into a powder. Use scissors to shred the remaining plastic.																					
231	Eject the realm DVD by pressing the button and remove it from the DVD drive.																					
232	Power off the computer: <ul style="list-style-type: none"><li>ceremony computer shutdown</li><li>Wait for the computer to turn off.</li><li>Unplug the power cord from the back of the computer.</li><li>Wait a few seconds.</li></ul>																					
233	Unplug the card reader from the HSM.																					
234	Remove the HSM from the computer. Insert it into an antistatic bag and then insert that into a tamper-evident bag (for transport to the production environment).  Bag ID: <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
235	Place the card reader in a tamper-evident bag.  Bag ID: <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	1	2	3	4	5	6	7	8	9	10											
1	2	3	4	5	6	7	8	9	10													
236	Put away the computer, keyboard, and other materials. Detach both ends of the antistatic wrist strap.																					
237	Close out any unused exception sheets.  Exception sheets used: _____																					

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

238	Collect initials from all ceremony participants.		
	Choose exactly one of the following:		
	<input type="radio"/>	All participants initialed	
	<input type="radio"/>	Not all participants initialed	
239	Display each sheet of this document in sequence to be recorded on video.		

The ceremony is now complete.

The operator should digitize and publish this document as soon as possible. Store the paper copy in a tamper-evident bag.

Bag ID:

1	2	3	4	5	6	7	8	9	10

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix A: State

Other than the computer’s factory-provided firmware and Windows installation, the state entering the ceremony is on the public *boot DVD* (see Appendix A.1) and the Entrust-confidential *vendor DVD* (see Appendix A.2).

In Section 4.2, several files are copied from the DVDs to the NVMe drive, to avoid delays from reading DVDs repeatedly during the ceremony. These files are copied into the primary Windows partition (`C:` or `/dev/nvme0n1p3`, an NTFS filesystem) into `/Users/defaultuser0:`

1. `/live/filesystem.squashfs` from the boot DVD,
2. `/entrust.ps1` from the boot DVD,
3. `/CODESAFE.ZIP` from the vendor DVD,
4. `/FIRMWARE.ZIP` from the vendor DVD, and
5. `/SECWORLD.ZIP` from the vendor DVD.

Subsequently, when booting the boot DVD, the initial ramdisk will attempt to mount the Windows partition in read-only mode, validate the copy of the Squashfs filesystem against the SHA-256 hash found on the boot DVD, and boot into that Squashfs filesystem. If the boot DVD cannot validate this hash, it raises an error.

After booting the boot DVD, the Windows partition remains mounted (at `/run/win`). The ceremony tool verifies the hashes of the copies of the vendor DVD files as found on the Windows partition, then uses those copies instead of reading the vendor DVD.

In Section 5, several new files are produced that are burned to a blank *realm DVD* (see Appendix A.3). The realm DVD is used during the ceremony and must be retained to set up the realm’s production environment.

The HSMs themselves contain some state initialized during the ceremony. Each will contain the `KMSW` key to decrypt the encryption keys found on the realm DVD, and each will have an empty file allocated on its NVRAM. After the ceremony, each HSM’s key and NVRAM file are only accessible within the trust boundary of that HSM.

### A.1 Boot DVD

The boot DVD contains only public content, which can be reviewed and reproduced at <https://github.com/juicebox-systems/ceremony/>. The hash of the ISO 9660 image burned to the DVD is `1603a9418982d1a30bbc3a8c35f3e92cb3093523725bcd95c62a5a3f220a188`. The boot DVD includes:

- a bootable Linux OS based on Debian 12 (Bookworm),
- an official Rust/Cargo toolchain (pre-installed in binary form),
- Rust’s standard library source code (pre-installed in source form),
- Juicebox “ceremony tool” source code (from <https://github.com/juicebox-systems/ceremony/tree/97cfb88323d58abf3604aa0e227c57dcd0113f7c/tool>, at `/root/ceremony/tool`),

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

- Juicebox HSM software and tooling source code (from <https://github.com/juicebox-systems/juicebox-hsm-realm/tree/d09bef2b36199d22877908ec702b047352c26256>, at `/root/juicebox-hsm-realm`),
- source code for Rust dependencies for the above three bullets (at `/root/crates`), and
- CodeSafe feature activation files received from Entrust for these particular HSMs (at `/root/features`).

Most of the boot DVD contents are stored inside a root filesystem in a Squashfs file (`/live/filesystem.squashfs`), while the boot loader, kernel, initial ramdisk, and SHA-256 hashes of all files reside outside of this filesystem. The boot DVD writes all filesystem changes to an in-memory overlay, which is discarded on shutdown.

## A.2 Vendor DVD

The vendor DVD consists of three files that are distributed by Entrust to their nShield HSM customers. We have not found a public location listing these hashes, and we are not authorized to publish these files. See <https://nshielddocs.entrust.com/> and contact [nshield.support@entrust.com](mailto:nshield.support@entrust.com) or [nshield.docs@entrust.com](mailto:nshield.docs@entrust.com) for details.

Path on vendor DVD	<code>/CODESAFE.ZIP</code>
Entrust filename	<code>Codesafe_Lin64-13.4.3.iso.zip</code>
SHA-256 hash	<code>7d6eaff0548d90143d35834f1ea1cf092321e9003e10e14895a01a6f412adadb</code>
Size	586,472,486 bytes
Description	Compiler, libraries, and header files used to build source code to run on the HSM or interface with the HSM

Path on vendor DVD	<code>/FIRMWARE.ZIP</code>
Entrust filename	<code>nShield_HSM_Firmware-13.4.4.iso.zip</code>
SHA-256 hash	<code>035dd8b9841d965c8f048c357ab25e1bf7c11afaa5d616482f1b2a1f8590fdc8</code>
Size	1,856,501,013 bytes
Description	Signed HSM firmware images

Path on vendor DVD	<code>/SECWORLD.ZIP</code>
Entrust filename	<code>SecWorld_Lin64-13.4.4.iso.zip</code>
SHA-256 hash	<code>d05e958b19b26ac4b984cc8e5950c8baa1cd72f1efb7ede2141317b130cb89e7</code>
Size	678,977,000 bytes
Description	Host tools, daemons, and driver to manage HSMs

Note that Linux maps the filenames to lowercase when mounting the vendor DVD.

The overall hash of the vendor DVD ISO 9660 image is

`48f3bebf95d580834d6161fe6d6ec7b2b28106b342869c462b925f0e4989c53`.

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



### A.3 Realm DVD

These files are copied from the root filesystem overlay to the root directory of the realm DVD:

- Host path: `/opt/nfast/kmdata/local/key_simple_jbox-mac`  
A blob of the symmetric key that Juicebox's HSM code uses for HSM-to-HSM authentication, encrypted by `KMSW`.
- Host path: `/opt/nfast/kmdata/local/key_simple_jbox-noise`  
A blob of the asymmetric key used for client-to-HSM communication, encrypted by `KMSW`.
- Host path: `/opt/nfast/kmdata/local/key_simple_jbox-record`  
A blob of the symmetric key that Juicebox's HSM code uses to encrypt its data, encrypted by `KMSW`.
- Host path: `/opt/nfast/kmdata/local/world`  
Contains key blobs for `KMSW` and `KNS0`, encrypted by key(s) encoded in the ACS smartcard(s), as well as other Security World blobs and information.
- Host path:  
`/root/juicebox-hsm-realm/target/powerpc-unknown-linux-gnu/release/entrust_hsm.sar`  
Juicebox's executable program to run within the HSMs, signed by the signing key.
- Host path:  
`/root/juicebox-hsm-realm/target/powerpc-unknown-linux-gnu/release/userdata.sar`  
The string `dummy`, signed by the signing key. This is required to run software on the HSM, but Juicebox's software does not read the contents.
- Host path: `/root/juicebox-hsm-realm/target/release/entrust_init`  
A tool that runs on the host computer to create HSM keys and initialize HSM NVRAM with appropriate ACLs. This is included on the realm DVD to avoid having to compile it repeatedly.

The realm DVD is used during the ceremony and must be retained to set up the realm's production environment. We have chosen not to publish the realm DVD contents because we are not familiar with the exact file formats and cryptography used in these files.

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix B: HSM Keys

This appendix describes relevant keys created by the HSM. The authoritative resource for this information is Entrust (see the Security Manual: <https://nshielddocs.entrust.com/security-world-docs/v13.3/security-manual/intro.html>).

The keys are identified by hashes, encoded as 40 hexadecimal characters. These hashes are labeled using several conventions but are most commonly prefixed with an **h** (for example, **hkns0** for the hash of the **KNS0** key).

Name	Description
<b>KLTU</b>	The key that is encoded in the OCS smartcard(s). Its hash is output when creating a new OCS.
<b>KMSW</b> or <b>KM_sw</b>	<p>The Security World key that is copied to every HSM in the Security World. It is generated when the Security World is created. It encrypts application key blobs in the Security World.</p> <p>The key is stored within the HSMs that are enrolled in the Security World. It is also stored as a blob in <code>/opt/nfast/kmdata/local/world</code>, encrypted by a key that's encoded in the ACS smartcard(s).</p> <p>Although the Security World key is one of multiple "module" keys (<b>KM</b> keys), the hash of <b>KMSW</b> is reported by <code>/opt/nfast/bin/nfkminfo</code> (<code>ceremony hsm world-info</code>) as <b>hkm</b> and in the ACLs as <b>kmhash</b>.</p>
<b>KNS0</b>	<p>A key that is created and its hash is output when creating a Security World. When other HSMs are enrolled in the Security World, they output the same hash.</p> <p>The key blob is stored in <code>/opt/nfast/kmdata/local/world</code>, encrypted by a key that's encoded in the ACS smartcard(s).</p>

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix C: Reference

### C.1 NATO Alphabet and Morse Code

The NATO alphabet should be used to spell out alphanumeric strings, except using normal English number pronunciation.

The HSMs have a blue LED that emits error codes in Morse code. Refer to <https://nshielddocs.entrust.com/1/solo-ug/13.3/morse-code-errors> for the meaning of the error codes. The dashes should have 3 times the duration of a dot, and the word gap should be 7 times the duration of a dot.

Letter	Code Word	Morse Code
A	Alfa	·—
B	Bravo	—···
C	Charlie	—···
D	Delta	—··
E	Echo	·
F	Foxtrot	··—·
G	Golf	—·—
H	Hotel	····
I	India	··
J	Juliett	·—
K	Kilo	—·—
L	Lima	·—··
M	Mike	—
N	November	—·
O	Oscar	—
P	Papa	·—··
Q	Quebec	—··—
R	Romeo	·—·

Letter	Code Word	Morse Code
S	Sierra	···
T	Tango	—
U	Uniform	··—
V	Victor	···—
W	Whiskey	·—
X	Xray	—··—
Y	Yankee	—··—
Z	Zulu	—···
0	Zero	—
1	One	·—
2	Two	··—
3	Three	··—
4	Four	··—
5	Five	···
6	Six	—···
7	Seven	—···
8	Eight	—···
9	Nine	—···

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## C.2 Windows Keyboard Shortcuts

- **Win-R** to open window to launch a program. For example, you can then run **powershell**.
- **Win-Up** to maximize the current window.
- **Win-Down** to un-maximize the current window if maximized, or to minimize it otherwise.
- **Alt-Tab** to switch windows.
- **Alt-F4** to close the current window.

## C.3 tmux Keyboard Shortcuts

The **tmux** terminal multiplexer is used in the boot DVD environment, primarily to provide scrolling and copy-paste. **tmux** is set to **vi** mode and **Ctrl-a** is the prefix key.

- **Ctrl-a ?** for online help (and then **q** or **Enter** to close the help).
- **Ctrl-a [** to enter copy mode.
- **Ctrl-a ]** to paste.

In copy mode (a scroll indicator will appear on the top-right):

- **Space** to start a visual selection.
- **Enter** to copy the current selection and exit copy mode.
- **Esc** to cancel a selection.
- **q** to exit copy mode.
- Move the cursor with **vi**-like keys or arrows.
- **Ctrl-y** to scroll up by one line and **Ctrl-e** to scroll down by one line.
- **PageUp** and **PageDown** to scroll by almost one screen.

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix D: Exception Sheet 1

Choose exactly one of the following:	
<input type="radio"/>	This exception sheet was not needed.
<input type="radio"/>	This exception sheet is used.

Start time: \_\_\_\_\_

Step number: \_\_\_\_\_

☐ The exception was noted in the step margin.

1. What was expected?

---

---

---

---

2. What happened instead?

---

---

---

---

3. What actions and decisions were taken?

---

---

---

---

---

---

---

---

---

---

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix E: Exception Sheet 2

Choose exactly one of the following:	
<input type="radio"/>	This exception sheet was not needed.
<input type="radio"/>	This exception sheet is used.

Start time: \_\_\_\_\_

Step number: \_\_\_\_\_

☐ The exception was noted in the step margin.

1. What was expected?

---

---

---

---

2. What happened instead?

---

---

---

---

3. What actions and decisions were taken?

---

---

---

---

---

---

---

---

---

---

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix F: Exception Sheet 3

Choose exactly one of the following:	
<input type="radio"/>	This exception sheet was not needed.
<input type="radio"/>	This exception sheet is used.

Start time: \_\_\_\_\_

Step number: \_\_\_\_\_

☐ The exception was noted in the step margin.

1. What was expected?

---

---

---

---

2. What happened instead?

---

---

---

---

3. What actions and decisions were taken?

---

---

---

---

---

---

---

---

---

---

Date: \_\_\_\_\_

Initials: \_\_\_\_\_

## Appendix G: Exception Sheet 4

Choose exactly one of the following:	
<input type="radio"/>	This exception sheet was not needed.
<input type="radio"/>	This exception sheet is used.

Start time: \_\_\_\_\_

Step number: \_\_\_\_\_

☐ The exception was noted in the step margin.

1. What was expected?

---

---

---

---

2. What happened instead?

---

---

---

---

3. What actions and decisions were taken?

---

---

---

---

---

---

---

---

---

---

Date: \_\_\_\_\_

Initials: \_\_\_\_\_



## Appendix H: Exception Sheet 5

Choose exactly one of the following:	
<input type="radio"/>	This exception sheet was not needed.
<input type="radio"/>	This exception sheet is used.

Start time: \_\_\_\_\_

Step number: \_\_\_\_\_

☐ The exception was noted in the step margin.

1. What was expected?

---

---

---

---

2. What happened instead?

---

---

---

---

3. What actions and decisions were taken?

---

---

---

---

---

---

---

---

---

---

Date: \_\_\_\_\_

Initials: \_\_\_\_\_