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:	
◯	Practice ceremony
◯	Production ceremony

Codename: _____

Date: _____

Start time: _____

Location: _____

Date: _____

Initials: _____

Contents

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: 0h00m

Step	Activity	End Time
1	Inspect the operator and the environment. □ There is a prominent analog clock with a second hand. □ The witnesses confirm that the clock is set to the current local time. □ There are two outlets available on the wall or a power strip nearby.	+1m20s =0h01m
2	Inspect the materials available to the operator. □ The materials below are available and do not appear tampered with. □ No other materials are available to the operator.	+5m20s =0h06m

Materials	
□	1 antistatic wrist strap
□	1 pair of scissors
□	1 Phillips screwdriver
□	1 rotary tool (to sand through smartcards)
□	1 table number holder (to display smartcards prominently when not in use)
□	2 printouts of this document
□	1 permanent marker
□	1 roll of masking tape
□	2 blue ballpoint pens
□	2 bottles of water
□	2 juice boxes (preferably apple)
□	1 sealed pack of 100 tamper-evident bags (ProAmpac GCS0912)
□	1 pre-burned and finalized boot DVD
□	1 pre-burned and finalized vendor DVD
□	1 sealed spindle of blank DVD-Rs (for the realm DVD)
□	1 computer (Lenovo 90T2000SUS, including a DVD burner and keyboard, with the outer box sealed by the purchaser with tamper-evident tape)
□	1 VGA video projector (limited to a low resolution so the text is visible to all participants)
□	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]	◯	◯	#____
`46-X20349`	`B216-05E0-D947`	[TODO: Bag ID]	◯	◯	#____
`46-X20517`	`3B17-05E0-D947`	[TODO: Bag ID]	◯	◯	#____
`46-X21267`	`341A-05E0-D947`	Factory	◯	◯	#____
`46-X21271`	`351A-05E0-D947`	Factory	◯	◯	#____
`46-X21323`	`611A-05E0-D947`	Factory	◯	◯	#____	 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: 0h06m

Step	Activity	End Time
3	Inspect the computer packaging: □ The box does not appear tampered with. □ The box ends are sealed with customer-applied tamper-evident tape, on top of somewhat loose Lenovo-branded tape. Inspect the Lenovo sticker: • □ The model (`(31P) M/T Model`) is `90T2000SUS`. • Serial Number `S(SN)`: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |---|---|---|---|---|---|---|---| | | | | | | | | | • Wi-Fi MAC address (`WMAC`): | byte 1 | byte 2 | byte 3 | byte 4 | byte 5 | byte 6 | |---|---|---|---|---|---| | | | | | | | | | | | | | • `Mfg Date` (as printed): _____ Inspect the shipping sticker(s): • `SHIP DATE` (as printed): _____	+5m20s =0h12m

Date: _____

Initials: _____

4	Open the computer box from the top with scissors. **Outer Box:** • Remove the small box containing the mouse and power cord from the outer box. • Remove the long box containing the keyboard from the outer box. • Remove the computer, sandwiched by two large pieces of foam, from the outer box. • Put away the outer box. **Desktop:** • Remove the foam from the desktop, and put away the foam. • Remove the plastic bag surrounding the desktop (which is not sealed), and put away the bag. **Keyboard Box:** • Open the keyboard box. • Remove the keyboard from its surrounding plastic (which is not sealed). • Inspect the keyboard and the label under it. Date on label under keyboard (`MFG`, as shown): _____ • Remove the twist tie on the keyboard's USB cable. • Put away the keyboard box, plastic bag, and twist tie. **Mouse and Power Cord Box:** • Open the mouse and power cord box. • Remove the power cable from the box. • Remove the twist tie and plug cover on the power cable, and put away the tie and cover. • 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.) Bag ID: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | • Retain the empty box to prop up the DVD drive later. ☐ The box contents did not appear tampered with or used.	+4m50s =0h16m

Date: _____

Initials: _____

5	Inspect the computer case. Set it down on its right side to inspect the label on the bottom. ☐ The case does not appear tampered with. ☐ A Windows sticker is present on the left side panel. ☐ An Intel Core i5 sticker is present on the front panel. ☐ The serial number matches the label on the box (Step 3). ☐ The manufacturing date (`Mfg Date`) matches the label on the box (Step 3).	+3m20s =0h20m
6	Remove the left panel of the case and the front panel: • Unscrew the two screws holding the left panel in place using the screwdriver. • Remove the left panel, and put it away. • Ground yourself to the unpainted computer chassis with the antistatic wrist strap. It can be worn on your upper arm or ankle. • Lift up on the three plastic tabs (top, middle, bottom) to get the left side of the front panel off. • Wiggle the front panel off, and put it away. ☐ The power supply's wattage rating (labeled as `Total output continuous shall not exceed`) is 260 W.	+2m50s =0h23m
7	Remove the SATA drive shelf: • Brace the DVD drive and press the black and red tab towards the front of the computer release it. Note: it may eject forcefully. • Unplug the SATA and power cables from the back of the DVD drive. • 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). • Unplug the SATA and power cables from the 3.5″ hard drive. • Pull up on the silver and red tab (on the front, left side, middle) to release the SATA drive shelf. • Wiggle the SATA drive shelf off (with the 3.5″ hard drive attached), and put away the drive shelf. • Plug the SATA and power cables back into the DVD drive.	+2m50s =0h25m

Date: _____

Initials: _____

8	Remove the wireless card and antennas: • Pull up forcefully on the plastic pin holding the wireless card in place (near where the DC cables come out of the power supply). • Remove a small bit of clear plastic that the pin was on. • Remove the wireless card from the slot. • Gently pry the two antenna cables from the wireless card. • Pull forcefully on the front antenna to overcome the adhesive, then remove any tape holding the cable and pull the cable through. • 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. • Pull forcefully on the rear antennas to overcome the adhesive, then remove any tape holding the cable and pull the cable through. □ The Wi-Fi MAC address (`WFM`) on the wireless card's label matches the label on the computer box (Step 3). Place the wireless card, antennas, and plastic bits into a tamper-evident bag for storage. Bag ID: 1 2 3 4 5 6 7 8 9 10	+3m50s =0h29m
9	Prepare the PCIe x16 slot: • Pull up on the silver and red tab above the placeholder brackets near the PCIe slots to open the flap. • Remove the metal placeholder bracket blocking the PCIe x16 slot and put it away. • Close the metal flap.	+1m20s =0h31m
10	Open the projector packaging, and put away the packaging. □ The packaging does not appear tampered with. □ The projector does not appear tampered with.	+3m20s =0h34m
11	Plug in the projector power and turn on the projector.	+0m50s =0h35m
12	Plug the USB keyboard and VGA projector into the computer.	+0m50s =0h36m
13	Boot into Windows: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • Boot the computer into the pre-installed Windows OS.	+2m10s =0h38m

Date: _____

Initials: _____

14	When the Windows "Out of Box Experience" prompts for input (asking for your country or region): • Press `Shift-F10` to open a terminal. (Do not use the terminal. Opening it switches focus, which enables more hotkeys.) • Press `Win-r` to open a Run dialog. • Run `powershell`. • Press `Win-Up` to maximize the Powershell window.	+1m20s =0h39m
15	Insert the boot DVD into the DVD drive.	+0m30s =0h40m

16	Calculate the SHA-256 hash of the boot DVD image.
	`$s = [system.io.file]::open('\\.\e:', 'open', 'read', 'read')`
	`get-filehash -inputstream $s`
	`$s.close()`
	The `get-filehash` command should take about 1 minute.
	☐ The boot DVD's SHA-256 digest matches `1603a9418982d1a30bbc3a8c35f3e92cb3093523725bcdb95c62a5a3f220a188`.
		+1m50s
		=0h41m

17	Copy the main filesystem image and a small script from the boot DVD onto the NVMe drive.
	`dir`
	`cp -verbose e:\live\filesystem.squashfs`
	`cp -verbose e:\entrust.ps1`
	`dir`
	This will copy the files into `C:\Users\defaultuser0\`. The first copy command should take about 2 minutes, and the second one should take up to a few seconds.
		+3m20s
		=0h45m

18	Eject the boot DVD by pressing the button and insert the vendor DVD into the DVD drive.	+0m30s =0h45m

Date: _____

Initials: _____

19	Copy the Entrust-provided files from the vendor DVD onto the NVMe drive.
	
	`cat entrust.ps1`
	`set-executionpolicy -scope process unrestricted`
	`.\entrust.ps1`
	`dir`
	
	Enter `Y` for yes when setting the policy.
	
	The script verifies the hashes of the files and copies them into `C:\Users\defaultuser0\`. It should take about 10 minutes. During this time, review Appendix A, which discusses the various DVDs and files.
		+10m20s
		=0h56m

20	Eject the vendor DVD by pressing the button and insert the boot DVD into the DVD drive.	+0m30s =0h56m
21	Power off the computer: • Press and release the “power button” on the front of the computer. • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =0h57m
22	Determine the current date and 24-hour time in UTC. This will be used to set the system time. Choose exactly one of the following: ◯ Pacific Standard Time (UTC−08:00) ◯ Pacific Daylight Time (UTC−07:00) Local Date (`MM/DD/YYYY`): _____ Local Time (`HH:MM`, from analog clock): _____ UTC Date (`MM/DD/YYYY`): _____ UTC Time (`HH:MM`): _____	+0m50s =0h58m

Date: _____

Initials: _____

23	Configure UEFI and boot into the boot DVD: 1. Plug the power cord into the back of the computer. 2. Press the "power button" on the front of the computer. 3. Tap `F1` repeatedly during boot to enter the UEFI setup. 4. Press `Enter` to dismiss the help dialog. 5. Press `Right` to enter the `Main` settings. 6. Press `Down`, then `Enter` to enter the `Main` ▷ `System Time & Date` settings. 7. Set the time and date to UTC. Use the arrows and `Enter` to navigate, and `+` and `-` to adjust the time. Use the time and date calculated in the previous step, adjusted for the minutes that have since passed. 8. Press `Up` repeatedly until highlighting the back arrow, then `Enter`, then `Left` to return to the main menu. 9. Press `Down` several times, then `Right` to enter the `Security` settings. 10. Press `Down` several times, then `Enter` to enter the `Security` ▷ `Secure Boot` settings. 11. Press `Enter`, then `Up`, then `Enter` to disable Secure Boot. (The Linux kernel would refuse to load the vendor's HSM driver with Secure Boot enabled.) 12. Press `Up`, then `Enter`, then `Left` to return to the main menu. 13. Press `Down`, then `Right` to enter `Startup` settings. 14. Press `Enter` to enter the `Startup` ▷ `Boot Priority Order` settings. 15. Except for the SATA DVD-RW drive, press `x` on each device to exclude it from the boot order. (Skip the DVD-RW drive with `Down`. You can also un-exclude something with `x`.) 16. Press `F10`, then `Enter` to save the changes and reboot. 17. The computer should boot into the bootloader on the boot DVD. 18. Press `Enter` at the GRUB menu to boot into Linux.	+4m00s =1h02m

Date: _____

Initials: _____

24	Display some information about the computer's devices:
	
	`lsblk`
	`lsusb`
	`lspci | nl`
	
	☐ `lsblk` reports `loop0` (loopback devices), `sr0` (the DVD drive), `nvme0n1` with 4 partitions (the Windows disk), and no other block devices.
	
	☐ `lsusb` reports a "3.0 root hub", a "2.0 root hub", a "Lenovo New Calliope USB Keyboard", and no other USB devices.
	
	☐ `lspci` reports 24 devices: 22 from Intel, a "Non-Volatile memory controller" from Samsung Electronics, and an "Ethernet controller" from Realtek Semiconductor.
		+2m20s
		=1h04m

25	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =1h05m

Date: _____

Initials: _____

5 Realm Creation

5.1 Prepare the First HSM

Start time: 1h05m

Step	Activity	End Time
26	This step will process the HSM packaging. ☐ The HSM is in factory packaging. 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. Serial number: 1 2 - 3 4 5 6 7 8 9	+2m20s =1h07m

Date: _____

Initials: _____

27	Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging. ☐ The HSM does not appear tampered with. Inspect the sticker on the side of the HSM: ☐ The serial number (`S/N`) matches that of the previous step. ☐ The model is `nC4035E-000`.	+1m20s =1h08m
28	Set the mode switch and jumpers on the HSM: ☐ Set the outside-facing physical switch to `0` (the middle position). ☐ Ensure both override jumper switches are set to off.	+0m30s =1h09m
29	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. Choose exactly one of the following: ◯ The HSM currently has no PCI bracket. ◯ 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.	+1m50s =1h11m
30	Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.	+1m20s =1h12m
31	Unpack the card reader. Put away the packaging. ☐ The card reader is etched with "ENTRUST" text and the hexagonal "E" logo. ☐ The card reader does not appear tampered with.	+1m20s =1h13m
32	While bracing the HSM, plug the card reader into the HSM's external port.	+0m35s =1h14m
33	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =1h15m

Date: _____

Initials: _____

34	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =1h16m
35	Print HSM info: `ceremony hsm info` ESN (`Module #1` ▷ `serial number`): 1 2 3 4 - 5 6 7 8 - 9 10 11 12 ☐ The ESN matches the HSM listed in Section 4.1. Firmware version (`Module #1` ▷ `version`): _____ ☐ `Module #1` ▷ `product name` shows all of `nC3025E/nC4035E/nC4335N`.	+2m00s =1h18m
36	Restart the HSM in maintenance mode: `ceremony hsm restart --mode maintenance` This command should take about 55 seconds.	+1m15s =1h20m

37	Update/overwrite the HSM firmware to version 13.3.1:
	
	`ceremony vendor mount firmware`
	`ceremony firmware write`
	`ceremony vendor unmount firmware`
	
	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.
		+3m20s
		=1h23m

38	Wait until the HSM is done: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `--` pattern. Wait and re-run the command until these conditions are satisfied.	+0m50s =1h24m

Date: _____

Initials: _____

39	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =1h25m
40	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =1h26m
41	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =1h27m
42	Wait until the HSM is ready: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `mode` shows `uninitialized`. ☐ `Module #1` ▷ `serial number` matches Step 35. ☐ `Module #1` ▷ `version` shows `13.3.1`. ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `–·–` pattern. Wait and re-run the command until these conditions are satisfied. If the module does not appear at all, check `dmesg` for the error `nfp_open: device ❮...❯ failed to open with error: -5`. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an *exception sheet* the first time it occurs.	+0m50s =1h28m
43	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =1h29m

Date: _____

Initials: _____

44	Initialize the HSM with a new module key: `ceremony hsm erase` ☐ The output includes the line `Initialising Unit 1 (SetNSOPerms)`. ☐ `Module Key Info` ▷ `HKM[0] 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.	+0m50s =1h30m
45	Check which features have been activated on the HSM: `ceremony feature info` Active features (excluding SEE): _____ ☐ `SEE Activation (EU+10)` is not activated (shows `N`).	+2m20s =1h32m
46	Activate the SEE (CodeSafe) feature on the HSM: • `ceremony feature activate features/SEEUE_❮ESN❯.txt` This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode. • Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds. • `ceremony feature info` ☐ `SEE Activation (EU+10)` is activated (shows `Y`).	+0m20s =1h33m

5.2 Unpack the Smartcards

Start time: 1h33m

Step	Activity	End Time
47	Inspect the smartcard packaging. ☐ The packaging does not appear tampered with.	+0m50s =1h34m

Date: _____

Initials: _____

48	Open the smartcard packaging. Take out two cards, and put the rest in a tamper-evident bag. Bag ID: 1 2 3 4 5 6 7 8 9 10	+1m20s =1h35m
49	Inspect the first smartcard. Label it “OCS”. ☐ The smartcard does not appear tampered with. ☐ The smartcard has nShield and Entrust trademarks. Smartcard ID: 1 2 3 4 - 5 6 - 7 8 9 10 11 12	+1m40s =1h37m
50	Inspect the second smartcard. Label it “ACS”. ☐ The smartcard does not appear tampered with. ☐ The smartcard has nShield and Entrust trademarks. Smartcard ID: 1 2 3 4 - 5 6 - 7 8 9 10 11 12	+1m40s =1h38m
51	Ask a few witnesses to choose a distinctive character or shape, and draw these on the cards.	+2m20s =1h41m
52	Place the ACS smartcard in the card reader and place the OCS smartcard visibly in the stand.	+0m35s =1h41m

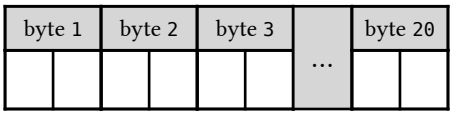
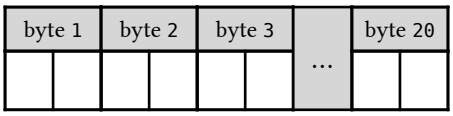
5.3 Create the Security World and Sign the Software

Start time: 1h41m

Step	Activity	End Time

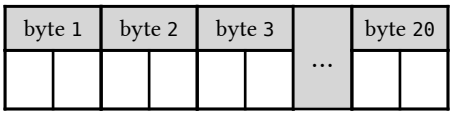
Date: _____

Initials: _____

53	Create the HSM Security World, enroll the first HSM in it, and write to the ACS smartcard. Enter an empty passphrase when prompted. `ceremony hsm create-world` Identifying bytes of `KNSO` hash (`hknso`):  This command takes about 45 seconds. It writes to the ACS smartcard and creates encrypted keys on the computer's filesystem.	+2m20s =1h44m
54	Display information about the Security World: `ceremony hsm world-info` Identifying bytes of `KMSW` Security World key hash (`World` ▷ `hkm`): 	+1m20s =1h45m
55	Restart the HSM in operational mode: `ceremony hsm restart` This command should take about 55 seconds.	+1m15s =1h46m
56	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.	+0m30s =1h47m
57	Write to the OCS smartcard. Enter an empty passphrase when prompted. `ceremony smartcard write-ocs` This command should take about 12 seconds.	+0m40s =1h47m
58	Create a signing key: `ceremony sign create-key` This command should take about 6 seconds. It writes an encrypted key to the host computer's filesystem.	+0m30s =1h48m

Date: _____

Initials: _____

59	Display information about the signing key: `ceremony sign key-info` Identifying bytes of signing key hash (`Key AppName seeinteg Ident jbox-signer` ▷ `hash`): 	+1m20s =1h49m
60	Install Entrust's compiler, libraries, and header files: `ceremony vendor install codesafe` This command should take about 10 seconds.	+0m30s =1h50m
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		+1m00s =1h51m

Date: _____

Initials: _____

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.	+1m00s =1h52m

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 | | --- | --- | --- | --- | --- | | | | | | |	+1m20s =1h53m

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: Identifying words of the BIP-39 mnemonic encoding of the SHA-256 hash of the signed file (`userdata.sar`):	+1m20s =1h54m

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

word 1	word 2	word 3	…	word 24

5.4 Destroy the OCS Smartcard

Start time: 1h54m

Step	Activity	End Time

Date: _____

Initials: _____

65	Erase the OCS smartcard: `ceremony smartcard erase` This command takes about 30 seconds.	+0m50s =1h55m
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.	+2m20s =1h57m

5.5 Create the Realm Keys

Start time: 1h57m

Step	Activity	End Time

Date: _____

Initials: _____

67	Generate the realm keys:
	
	`ceremony realm create-keys`
	
	Each key's ACL is the same, except for identifiers, having three permission groups:
	
	• Permission Group 1 allows reading the ACL itself and allows the key to be duplicated with the same ACL. It should look like:
	
	`Action: OpPermissions: DuplicateHandle, GetACL`
	
	• 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:
	
	`Requires Cert: hash: ⟪SIGNING-KEY-HASH⟫ mechanism: Any`
	`Flags: certmech_present`
	`Action: OpPermissions: ExportAsPlain, GetAppData`
	
	• 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):
	
	`Use Limit: Global: max: 1 id: ⟪VARYING-40-HEX-CHARS⟫`
	`Action: MakeBlob: Flags: AllowKmOnly, AllowNonKm0,`
	`kmhash_present kmhash: ⟪KMSW-HASH⟫`
	
	☐ `Creating key simple,jbox-mac`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59.
	
	☐ `Creating key simple,jbox-mac`… ▷ `Permission Group 3` ▷ `Action` ▷ `kmhash` matches the Security World key hash in Step 54.
	
	☐ `Creating key simple,jbox-record`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` shows the same value as the `jbox-mac` permissions.
	
	☐ `Creating key simple,jbox-record`… ▷ `Permission Group 3` ▷ `Action` ▷ `kmhash` shows the same value as the `jbox-mac` permissions.
	
	☐ `Creating key simple,jbox-noise`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` shows the same value as the `jbox-mac` permissions.
	
	☐ `Creating key simple,jbox-noise`… ▷ `Permission Group 3` ▷ `Action` ▷ `kmhash` shows the same value as the `jbox-mac` permissions.
		+3m20s
		=2h01m

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.
		+1m20s
		=2h02m

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
		+3m20s
		=2h05m

Date: _____

Initials: _____

5.6 Write the Realm DVD

Start time: 2h05m

Step	Activity	End Time
70	Create the realm DVD image: `ceremony realm-dvd create-iso` This command should take less than 1 second. See Appendix A for details on which files are included on the image. Identifying bytes of SHA-256 hash of the realm DVD image (`/root/realm.iso`): byte 1 | byte 2 | byte 3 | … | byte 32	+0m20s =2h06m
71	Eject the boot DVD by pressing the button and remove it from the DVD drive.	+0m30s =2h06m
72	Inspect the blank DVD packaging. ☐ The packaging does not appear tampered with.	+0m50s =2h07m
73	Take one blank DVD and label it with: • "Ceremony Realm DVD", • the local date and time, and • the identifying bytes of the SHA-256 hash of the ISO file from Step 70. ☐ The DVD does not appear tampered with and appears blank. Place the remaining spindle in a tamper-evident bag. Bag ID: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10	+2m20s =2h09m
74	Insert the realm DVD into the DVD drive.	+0m30s =2h10m
75	Write the image to the DVD: `ceremony realm-dvd write` 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. ☐ The computer ejected the DVD.	+4m20s =2h14m

Date: _____

Initials: _____

76	Insert the realm DVD into the DVD drive.	+0m30s =2h15m
77	Verify the files were written to the realm DVD correctly: `ceremony realm-dvd verify`	+1m20s =2h16m

5.7 Clear the First HSM

Start time: 2h16m

Step	Activity	End Time
78	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =2h17m
79	Initialize the HSM with a new module key: `ceremony hsm erase` ☐ The output includes the line `Initialising Unit 1 (SetNSOPerms)`. ☐ `Module Key Info` ▷ `HKM[0] 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.	+0m50s =2h18m
80	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	+0m30s =2h19m
81	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =2h19m

Date: _____

Initials: _____

6 HSM Enrollment

6.1 Set up the First HSM

Start time: 2h19m

Step	Activity	End Time
82	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =2h20m
83	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =2h22m
84	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =2h23m
85	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.	+0m30s =2h24m
86	Copy the files from the realm DVD: `ceremony realm-dvd restore`	+0m50s =2h25m
87	Place the ACS smartcard in the card reader.	+0m20s =2h25m
88	Enroll the HSM in the Security World: `ceremony hsm join-world` This command takes about 22 seconds and reads from the ACS smartcard. ☐ The output `hknso` matches the one recorded in Step 53.	+1m10s =2h26m
89	Restart the HSM in operational mode: `ceremony hsm restart` This command should take about 55 seconds.	+1m15s =2h27m

Date: _____

Initials: _____

90	Print the signing key hash from the ACL of a key: `ceremony realm print-acl noise` ☐ `key simple,jbox-noise exists…` ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59.	+1m00s =2h28m
91	Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL: `ceremony realm create-nvram-file --signing-key-hash ⟨HASH⟩` ☐ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59. This command takes about 1 second and reads from the ACS smartcard.	+1m10s =2h30m
92	Remove the ACS smartcard from the card reader and place it visibly in the stand.	+0m50s =2h30m
93	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	+0m30s =2h31m
94	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =2h32m
95	Unplug the card reader from the HSM.	+0m20s =2h32m
96	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: 1 2 3 4 5 6 7 8 9 10	+2m20s =2h34m

6.2 Intermission

Start time: 2h34m

Step	Activity	End Time
97	Detach the operator end of the antistatic wrist strap, leaving it connected to the computer chassis.	+0m35s =2h35m

Date: _____

Initials: _____

98	Remove the ACS smartcard from the stand. Wrap the end of the smartcard with masking tape three times over, covering the electronics. Place the ACS smartcard in a tamper-evident bag. Bag ID: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | |	+1m20s =2h36m
99	Place the card reader in a tamper-evident bag. Bag ID: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | |	+1m20s =2h37m
100	*MC:* Decide on an approximate duration for the break. Duration: _____ Resume at (time): _____	+0m50s =2h38m
101	Place this document in a tamper-evident bag. Bag ID: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | |	+1m20s =2h40m
102	The operator must step away from the station. Then, everyone (all participants and anyone else present) should leave the room together. **No one may enter the room during the break.** 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. □ The bag does not appear tampered with. □ The bag ID matches the one recorded above. □ 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. Count: _____	+30m20s =3h10m

Date: _____

Initials: _____

103	Remove the card reader from its bag. ☐ The bag does not appear tampered with. ☐ The bag ID matches the one recorded above.	+0m50s =3h11m
104	Remove the ACS smartcard from the bag, remove the masking tape from it, and place it visibly in the stand. ☐ The bag does not appear tampered with. ☐ The bag ID matches the one recorded above. ☐ The smartcard ID matches Step 50.	+0m50s =3h12m
105	Ground yourself to the unpainted computer chassis with the antistatic wrist strap. It can be worn on your upper arm or ankle.	+0m35s =3h12m

6.3 Set Up the Second HSM

Start time: 3h12m

Step	Activity	End Time

Date: _____

Initials: _____

106

+1m20s
=3h14m

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	Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging. ☐ The HSM does not appear tampered with. Inspect the sticker on the side of the HSM: ☐ The serial number (`S/N`) matches that of the previous step. ☐ The model is `nC4035E-000`.	+1m20s =3h15m
108	Set the mode switch and jumpers on the HSM: ☐ Set the outside-facing physical switch to `0` (the middle position). ☐ Ensure both override jumper switches are set to off.	+0m30s =3h15m
109	Choose exactly one of the following: ◯ The HSM currently has no PCI bracket. ◯ 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.	+1m50s =3h17m
110	Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.	+1m20s =3h19m
111	Choose exactly one of the following: ◯ This HSM did not come with a card reader. ◯ This HSM came with a card reader. Place the new card reader in a tamper-evident bag for storage. Bag ID: 1 2 3 4 5 6 7 8 9 10	+1m20s =3h20m
112	While bracing the HSM, plug the existing card reader into the HSM's external port.	+0m35s =3h20m
113	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =3h21m

Date: _____

Initials: _____

114	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =3h23m
115	Print HSM info: `ceremony hsm info` ESN (`Module #1` ▷ `serial number`): 1 2 3 4 - 5 6 7 8 - 9 10 11 12 ☐ The ESN matches the HSM listed in Section 4.1. Firmware version (`Module #1` ▷ `version`): _____ ☐ `Module #1` ▷ `product name` shows all of `nC3025E/nC4035E/nC4335N`.	+2m00s =3h25m
116	Restart the HSM in maintenance mode: `ceremony hsm restart --mode maintenance` This command should take about 55 seconds.	+1m15s =3h26m

117	Update/overwrite the HSM firmware to version 13.3.1:
	
	`ceremony vendor mount firmware`
	`ceremony firmware write`
	`ceremony vendor unmount firmware`
	
	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.
		+3m20s
		=3h30m

118	Wait until the HSM is done: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `--` pattern. Wait and re-run the command until these conditions are satisfied.	+0m50s =3h31m

Date: _____

Initials: _____

119	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =3h31m
120	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =3h32m
121	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =3h34m
122	Wait until the HSM is ready: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `mode` shows `uninitialized`. ☐ `Module #1` ▷ `serial number` matches Step 115. ☐ `Module #1` ▷ `version` shows `13.3.1`. ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `–·–` pattern. Wait and re-run the command until these conditions are satisfied. If the module does not appear at all, check `dmesg` for the error `nfp_open: device ❮...❯ failed to open with error: -5`. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an *exception sheet* the first time it occurs.	+0m50s =3h35m
123	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =3h36m

Date: _____

Initials: _____

124	Initialize the HSM with a new module key: `ceremony hsm erase` ☐ The output includes the line `Initialising Unit 1 (SetNSOPerms)`. ☐ `Module Key Info` ▷ `HKM[0] 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.	+0m50s =3h37m

125	Check which features have been activated on the HSM:
	`ceremony feature info`
	Active features (excluding SEE): _____
	Choose exactly one of the following:
	◯ `SEE Activation (EU+10)` is already activated (shows `Y`).
	◯ `SEE Activation (EU+10)` is not activated (shows `N`).
	Activate the SEE (CodeSafe) feature on the HSM:
	• `ceremony feature activate features/SEEUE_⟨ESN⟩.txt`
	This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.
	• Restart the HSM in initialization mode:
	`ceremony hsm restart --mode initialization`
	This command should take about 55 seconds.
	• `ceremony feature info`
	☐ `SEE Activation (EU+10)` is activated (shows `Y`).
		+2m20s
		=3h39m

126	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.	+0m30s =3h40m
127	Copy the files from the realm DVD: `ceremony realm-dvd restore`	+0m50s =3h40m
128	Place the ACS smartcard in the card reader.	+0m20s =3h41m

Date: _____

Initials: _____

129	Enroll the HSM in the Security World: `ceremony hsm join-world` This command takes about 22 seconds and reads from the ACS smartcard. ☐ The output `hknso` matches the one recorded in Step 53.	+1m10s =3h42m
130	Restart the HSM in operational mode: `ceremony hsm restart` This command should take about 55 seconds.	+1m15s =3h43m
131	Print the signing key hash from the ACL of a key: `ceremony realm print-acl noise` ☐ `key simple,jbox-noise exists`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59.	+1m00s =3h44m
132	Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL: `ceremony realm create-nvram-file --signing-key-hash ⟪HASH⟫` ☐ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59. This command takes about 1 second and reads from the ACS smartcard.	+1m10s =3h45m
133	Remove the ACS smartcard from the card reader and place it visibly in the stand.	+0m50s =3h46m
134	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	+0m30s =3h47m
135	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =3h47m
136	Unplug the card reader from the HSM.	+0m20s =3h48m

Date: _____

Initials: _____

137	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: 1 2 3 4 5 6 7 8 9 10	+2m20s =3h50m

6.4 Set Up the Third HSM

Start time: 3h50m

Step	Activity	End Time

Date: _____

Initials: _____

138

+1m20s
=3h51m

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	Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging. ☐ The HSM does not appear tampered with. Inspect the sticker on the side of the HSM: ☐ The serial number (`S/N`) matches that of the previous step. ☐ The model is `nC4035E-000`.	+1m20s =3h53m
140	Set the mode switch and jumpers on the HSM: ☐ Set the outside-facing physical switch to `0` (the middle position). ☐ Ensure both override jumper switches are set to off.	+0m30s =3h53m
141	Choose exactly one of the following: ◯ The HSM currently has no PCI bracket. ◯ 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.	+1m50s =3h55m
142	Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.	+1m20s =3h56m
143	Choose exactly one of the following: ◯ This HSM did not come with a card reader. ◯ This HSM came with a card reader. Place the new card reader in a tamper-evident bag for storage. Bag ID: 1 2 3 4 5 6 7 8 9 10	+1m20s =3h58m
144	While bracing the HSM, plug the existing card reader into the HSM's external port.	+0m35s =3h58m
145	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =3h59m

Date: _____

Initials: _____

146	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =4h01m
147	Print HSM info: `ceremony hsm info` ESN (`Module #1` ▷ `serial number`): 1 2 3 4 - 5 6 7 8 - 9 10 11 12 ☐ The ESN matches the HSM listed in Section 4.1. Firmware version (`Module #1` ▷ `version`): _____ ☐ `Module #1` ▷ `product name` shows all of `nC3025E/nC4035E/nC4335N`.	+2m00s =4h03m
148	Restart the HSM in maintenance mode: `ceremony hsm restart --mode maintenance` This command should take about 55 seconds.	+1m15s =4h04m

149	Update/overwrite the HSM firmware to version 13.3.1:
	`ceremony vendor mount firmware`
	`ceremony firmware write`
	`ceremony vendor unmount firmware`
	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.
		+3m20s
		=4h08m

150	Wait until the HSM is done: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `--` pattern. Wait and re-run the command until these conditions are satisfied.	+0m50s =4h08m

Date: _____

Initials: _____

151	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =4h09m
152	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =4h10m
153	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =4h12m
154	Wait until the HSM is ready: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `mode` shows `uninitialized`. ☐ `Module #1` ▷ `serial number` matches Step 147. ☐ `Module #1` ▷ `version` shows `13.3.1`. ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `−·−` pattern. Wait and re-run the command until these conditions are satisfied. If the module does not appear at all, check `dmesg` for the error `nfp_open: device ❮...❯ failed to open with error: -5`. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an *exception sheet* the first time it occurs.	+0m50s =4h13m
155	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =4h14m

Date: _____

Initials: _____

156	Initialize the HSM with a new module key: `ceremony hsm erase` ☐ The output includes the line `Initialising Unit 1 (SetNSOPerms)`. ☐ `Module Key Info` ▷ `HKM[0] 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.	+0m50s =4h15m

157	Check which features have been activated on the HSM:
	`ceremony feature info`
	Active features (excluding SEE): _____
	Choose exactly one of the following:
	◯ `SEE Activation (EU+10)` is already activated (shows `Y`).
	◯ `SEE Activation (EU+10)` is not activated (shows `N`).
	Activate the SEE (CodeSafe) feature on the HSM:
	• `ceremony feature activate features/SEEUE_⟨ESN⟩.txt`
	This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.
	• Restart the HSM in initialization mode:
	`ceremony hsm restart --mode initialization`
	This command should take about 55 seconds.
	• `ceremony feature info`
	☐ `SEE Activation (EU+10)` is activated (shows `Y`).
		+2m20s
		=4h17m

158	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.	+0m30s =4h17m
159	Copy the files from the realm DVD: `ceremony realm-dvd restore`	+0m50s =4h18m
160	Place the ACS smartcard in the card reader.	+0m20s =4h19m

Date: _____

Initials: _____

161	Enroll the HSM in the Security World: `ceremony hsm join-world` This command takes about 22 seconds and reads from the ACS smartcard. ☐ The output `hknso` matches the one recorded in Step 53.	+1m10s =4h20m
162	Restart the HSM in operational mode: `ceremony hsm restart` This command should take about 55 seconds.	+1m15s =4h21m
163	Print the signing key hash from the ACL of a key: `ceremony realm print-acl noise` ☐ `key simple,jbox-noise exists`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59.	+1m00s =4h22m
164	Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL: `ceremony realm create-nvram-file --signing-key-hash ⟪HASH⟫` ☐ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59. This command takes about 1 second and reads from the ACS smartcard.	+1m10s =4h23m
165	Remove the ACS smartcard from the card reader and place it visibly in the stand.	+0m50s =4h24m
166	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	+0m30s =4h25m
167	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =4h25m
168	Unplug the card reader from the HSM.	+0m20s =4h26m

Date: _____

Initials: _____

169	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: 1 2 3 4 5 6 7 8 9 10	+2m20s =4h28m

6.5 Set Up the Fourth HSM

Start time: 4h28m

Step	Activity	End Time

Date: _____

Initials: _____

170

+1m20s
=4h29m

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	Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging. ☐ The HSM does not appear tampered with. Inspect the sticker on the side of the HSM: ☐ The serial number (`S/N`) matches that of the previous step. ☐ The model is `nC4035E-000`.	+1m20s =4h31m
172	Set the mode switch and jumpers on the HSM: ☐ Set the outside-facing physical switch to `O` (the middle position). ☐ Ensure both override jumper switches are set to off.	+0m30s =4h31m
173	Choose exactly one of the following: ◯ The HSM currently has no PCI bracket. ◯ 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.	+1m50s =4h33m
174	Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.	+1m20s =4h34m
175	Choose exactly one of the following: ◯ This HSM did not come with a card reader. ◯ This HSM came with a card reader. Place the new card reader in a tamper-evident bag for storage. Bag ID: 1 2 3 4 5 6 7 8 9 10	+1m20s =4h36m
176	While bracing the HSM, plug the existing card reader into the HSM's external port.	+0m35s =4h36m
177	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =4h37m

Date: _____

Initials: _____

178	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =4h39m
179	Print HSM info: `ceremony hsm info` ESN (`Module #1` ▷ `serial number`): 1 2 3 4 - 5 6 7 8 - 9 10 11 12 ☐ The ESN matches the HSM listed in Section 4.1. Firmware version (`Module #1` ▷ `version`): _____ ☐ `Module #1` ▷ `product name` shows all of `nC3025E/nC4035E/nC4335N`.	+2m00s =4h41m
180	Restart the HSM in maintenance mode: `ceremony hsm restart --mode maintenance` This command should take about 55 seconds.	+1m15s =4h42m

181	Update/overwrite the HSM firmware to version 13.3.1:
	
	`ceremony vendor mount firmware`
	`ceremony firmware write`
	`ceremony vendor unmount firmware`
	
	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.
		+3m20s
		=4h45m

182	Wait until the HSM is done: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `--` pattern. Wait and re-run the command until these conditions are satisfied.	+0m50s =4h46m

Date: _____

Initials: _____

183	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =4h47m
184	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =4h48m
185	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =4h50m
186	Wait until the HSM is ready: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `mode` shows `uninitialized`. ☐ `Module #1` ▷ `serial number` matches Step 179. ☐ `Module #1` ▷ `version` shows `13.3.1`. ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `–·–` pattern. Wait and re-run the command until these conditions are satisfied. If the module does not appear at all, check `dmesg` for the error `nfp_open: device ❮...❯ failed to open with error: -5`. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an *exception sheet* the first time it occurs.	+0m50s =4h50m
187	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =4h52m

Date: _____

Initials: _____

188	Initialize the HSM with a new module key: `ceremony hsm erase` ☐ The output includes the line `Initialising Unit 1 (SetNSOPerms)`. ☐ `Module Key Info` ▷ `HKM[0] 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.	+0m50s =4h52m

189	Check which features have been activated on the HSM:
	`ceremony feature info`
	Active features (excluding SEE): _____
	Choose exactly one of the following:
	◯ `SEE Activation (EU+10)` is already activated (shows `Y`).
	◯ `SEE Activation (EU+10)` is not activated (shows `N`).
	Activate the SEE (CodeSafe) feature on the HSM:
	• `ceremony feature activate features/SEEUE_⟨ESN⟩.txt`
	This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.
	• Restart the HSM in initialization mode:
	`ceremony hsm restart --mode initialization`
	This command should take about 55 seconds.
	• `ceremony feature info`
	☐ `SEE Activation (EU+10)` is activated (shows `Y`).
		+2m20s
		=4h55m

190	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.	+0m30s =4h55m
191	Copy the files from the realm DVD: `ceremony realm-dvd restore`	+0m50s =4h56m
192	Place the ACS smartcard in the card reader.	+0m20s =4h56m

Date: _____

Initials: _____

193	Enroll the HSM in the Security World: `ceremony hsm join-world` This command takes about 22 seconds and reads from the ACS smartcard. ☐ The output `hknso` matches the one recorded in Step 53.	+1m10s =4h58m
194	Restart the HSM in operational mode: `ceremony hsm restart` This command should take about 55 seconds.	+1m15s =4h59m
195	Print the signing key hash from the ACL of a key: `ceremony realm print-acl noise` ☐ `key simple,jbox-noise exists`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59.	+1m00s =5h00m
196	Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL: `ceremony realm create-nvram-file --signing-key-hash ⟪HASH⟫` ☐ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59. This command takes about 1 second and reads from the ACS smartcard.	+1m10s =5h01m
197	Remove the ACS smartcard from the card reader and place it visibly in the stand.	+0m50s =5h02m
198	Eject the realm DVD by pressing the button and insert the boot DVD into the DVD drive.	+0m30s =5h02m
199	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =5h03m
200	Unplug the card reader from the HSM.	+0m20s =5h03m

Date: _____

Initials: _____

201	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: 1 2 3 4 5 6 7 8 9 10	+2m20s =5h06m

6.6 Set Up the Fifth HSM

Start time: 5h06m

Step	Activity	End Time

Date: _____

Initials: _____

202

+1m20s
=5h07m

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	Unpack and inspect the HSM. Retain the antistatic bag and put away the other packaging. ☐ The HSM does not appear tampered with. Inspect the sticker on the side of the HSM: ☐ The serial number (`S/N`) matches that of the previous step. ☐ The model is `nC4035E-000`.	+1m20s =5h08m
204	Set the mode switch and jumpers on the HSM: ☐ Set the outside-facing physical switch to `0` (the middle position). ☐ Ensure both override jumper switches are set to off.	+0m30s =5h09m
205	Choose exactly one of the following: ◯ The HSM currently has no PCI bracket. ◯ 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.	+1m50s =5h11m
206	Insert the HSM (without an attached bracket) into the PCIe x16 slot in the computer.	+1m20s =5h12m
207	Choose exactly one of the following: ◯ This HSM did not come with a card reader. ◯ This HSM came with a card reader. Place the new card reader in a tamper-evident bag for storage. Bag ID: 1 2 3 4 5 6 7 8 9 10	+1m20s =5h13m
208	While bracing the HSM, plug the existing card reader into the HSM's external port.	+0m35s =5h14m
209	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =5h15m

Date: _____

Initials: _____

210	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =5h17m
211	Print HSM info: `ceremony hsm info` ESN (`Module #1` ▷ `serial number`): 1 2 3 4 - 5 6 7 8 - 9 10 11 12 ☐ The ESN matches the HSM listed in Section 4.1. Firmware version (`Module #1` ▷ `version`): _____ ☐ `Module #1` ▷ `product name` shows all of `nC3025E/nC4035E/nC4335N`.	+2m00s =5h19m
212	Restart the HSM in maintenance mode: `ceremony hsm restart --mode maintenance` This command should take about 55 seconds.	+1m15s =5h20m

213	Update/overwrite the HSM firmware to version 13.3.1:
	
	`ceremony vendor mount firmware`
	`ceremony firmware write`
	`ceremony vendor unmount firmware`
	
	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.
		+3m20s
		=5h23m

214	Wait until the HSM is done: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `--` pattern. Wait and re-run the command until these conditions are satisfied.	+0m50s =5h24m

Date: _____

Initials: _____

215	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =5h25m
216	Boot into the boot DVD: • Plug the power cord into the back of the computer. • Press the "power button" on the front of the computer. • The computer should boot into the bootloader on the boot DVD. • Press `Enter` at the GRUB menu to boot into Linux.	+1m00s =5h26m
217	Install Entrust's tools, daemons, and driver: `ceremony vendor install secworld` This command takes about 80 seconds.	+1m40s =5h27m
218	Wait until the HSM is ready: `ceremony hsm info` ☐ `Module #1` ▷ `enquiry reply flags` shows `none` (not `Offline`). ☐ `Module #1` ▷ `mode` shows `uninitialized`. ☐ `Module #1` ▷ `serial number` matches Step 211. ☐ `Module #1` ▷ `version` shows `13.3.1`. ☐ `Module #1` ▷ `hardware status` shows `OK`. ☐ The HSM LED is blinking in the repeated `–·–` pattern. Wait and re-run the command until these conditions are satisfied. If the module does not appear at all, check `dmesg` for the error `nfp_open: device ❮...❯ failed to open with error: -5`. Powering the computer off and on should resolve this. While this problem is somewhat anticipated, use an *exception sheet* the first time it occurs.	+0m50s =5h28m
219	Restart the HSM in initialization mode: `ceremony hsm restart --mode initialization` This command should take about 55 seconds.	+1m15s =5h29m

Date: _____

Initials: _____

220	Initialize the HSM with a new module key: `ceremony hsm erase` □ The output includes the line `Initialising Unit 1 (SetNSOPerms)`. □ `Module Key Info` ▷ `HKM[0] 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.	+0m50s =5h30m

221	Check which features have been activated on the HSM:
	`ceremony feature info`
	Active features (excluding SEE): _____
	Choose exactly one of the following:
	◯ `SEE Activation (EU+10)` is already activated (shows `Y`).
	◯ `SEE Activation (EU+10)` is not activated (shows `N`).
	Activate the SEE (CodeSafe) feature on the HSM:
	• `ceremony feature activate features/SEEUE_⟨ESN⟩.txt`
	This command takes about 55 seconds. It has a side effect of leaving the HSM in operational mode.
	• Restart the HSM in initialization mode:
	`ceremony hsm restart --mode initialization`
	This command should take about 55 seconds.
	• `ceremony feature info`
	□ `SEE Activation (EU+10)` is activated (shows `Y`).
		+2m20s
		=5h33m

222	Eject the boot DVD by pressing the button and insert the realm DVD into the DVD drive.	+0m30s =5h33m
223	Copy the files from the realm DVD: `ceremony realm-dvd restore`	+0m50s =5h34m
224	Place the ACS smartcard in the card reader.	+0m20s =5h34m

Date: _____

Initials: _____

225	Enroll the HSM in the Security World: `ceremony hsm join-world` This command takes about 22 seconds and reads from the ACS smartcard. ☐ The output `hknso` matches the one recorded in Step 53.	+1m10s =5h35m
226	Restart the HSM in operational mode: `ceremony hsm restart` This command should take about 55 seconds.	+1m15s =5h37m
227	Print the signing key hash from the ACL of a key: `ceremony realm print-acl noise` ☐ `key simple,jbox-noise exists`… ▷ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59.	+1m00s =5h38m
228	Initialize this HSM's NVRAM file, providing the same signing key hash as the previous step for its ACL: `ceremony realm create-nvram-file --signing-key-hash ⟪HASH⟫` ☐ `Permission Group 2` ▷ `Requires Cert` ▷ `hash` matches the signing key hash in Step 59. This command takes about 1 second and reads from the ACS smartcard.	+1m10s =5h39m

Date: _____

Initials: _____

7 Conclusion

Start time: 5h39m

Step	Activity	End Time
229	Erase the ACS smartcard: `ceremony smartcard erase` This command takes about 30 seconds.	+0m50s =5h40m
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.	+2m20s =5h42m
231	Eject the realm DVD by pressing the button and remove it from the DVD drive.	+0m30s =5h43m
232	Power off the computer: • `ceremony computer shutdown` • Wait for the computer to turn off. • Unplug the power cord from the back of the computer. • Wait a few seconds.	+0m40s =5h43m
233	Unplug the card reader from the HSM.	+0m20s =5h44m
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: 1 2 3 4 5 6 7 8 9 10	+2m20s =5h46m
235	Place the card reader in a tamper-evident bag. Bag ID: 1 2 3 4 5 6 7 8 9 10	+1m20s =5h47m
236	Put away the computer, keyboard, and other materials. Detach both ends of the antistatic wrist strap.	+2m20s =5h50m
237	Close out any unused exception sheets. Exception sheets used: _____	+3m20s =5h53m

Date: _____

Initials: _____

238	Collect initials from all ceremony participants. Choose exactly one of the following: ◯ All participants initialed ◯ Not all participants initialed	+5m20s =5h58m
239	Display each sheet of this document in sequence to be recorded on video.	+5m20s =6h04m

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 `1603a9418982d1a30bbc3a8c35f3e92cb3093523725bcdb95c62a5a3f220a188`. 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 or nshield.docs@entrust.com for details.

Path on vendor DVD	`/CODESAFE.ZIP`
Entrust filename	`Codesafe_Lin64-13.4.3.iso.zip`
SHA-256 hash	`7d6eaff0548d90143d35834f1ea1cf092321e9003e10e14895a01a6f412adadb`
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	`/FIRMWARE.ZIP`
Entrust filename	`nShield_HSM_Firmware-13.4.4.iso.zip`
SHA-256 hash	`035dd8b9841d965c8f048c357ab25e1bf7c11afaa5d616482f1b2a1f8590fdc8`
Size	`1,856,501,013` bytes
Description	Signed HSM firmware images

Path on vendor DVD	`/SECWORLD.ZIP`
Entrust filename	`SecWorld_Lin64-13.4.4.iso.zip`
SHA-256 hash	`d05e958b19b26ac4b984cc8e5950c8baa1cd72f1efb7ede2141317b130cb89e7`
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 `48f3bebfb95d580834d6161fe6d6ec7b2b28106b342869c462b925f0e4989c53`.

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 `KNSO`, 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, `hknso` for the hash of the `KNSO` key).

Name	Description
`KLTU`	The key that is encoded in the OCS smartcard(s). Its hash is output when creating a new OCS.
`KMSW` or `KM_sw`	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. The key is stored within the HSMs that are enrolled in the Security World. It is also stored as a blob in `/opt/nfast/kmdata/local/world`, encrypted by a key that's encoded in the ACS smartcard(s). Although the Security World key is one of multiple "module" keys (`KM` keys), the hash of `KMSW` is reported by `/opt/nfast/bin/nfkminfo` (`ceremony hsm world-info`) as `hkm` and in the ACLs as `kmhash`.
`KNSO`	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. The key blob is stored in `/opt/nfast/kmdata/local/world`, encrypted by a key that's encoded in the ACS smartcard(s).

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:	
◯	This exception sheet was not needed.
◯	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:	
◯	This exception sheet was not needed.
◯	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:	
◯	This exception sheet was not needed.
◯	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:	
◯	This exception sheet was not needed.
◯	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:	
◯	This exception sheet was not needed.
◯	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: _____