EmSPARK Suite

Evaluation Kit - Getting Started Guide

Date May 22, 2020 | Version 1.2

TABLE OF CONTENTS

1. INTRODUCTION

The **EmSPARK Suite – Evaluation Kit**, **Getting Started** guide provides an overview of the prerequisites to use the Evaluation Kit and the Kit package contents. It also provides information to flash the secure bootloader on the board, install the file system on SD Card and start the system. After completing this guide, see the `USER_GUIDE.pdf` tutorial for a description of the Evaluation Kit and the `CORELOCKR_LIBRARIES_GUIDE.pdf` for instructions to build and run the provided example applications.

1.1. Prerequisites

The guide assumes that the following hardware and software are available:

- Shield96 board. Note: Jumper for J3 must be in place.
- Linux system to extract the Evaluation Kit package and build the example applications
- Windows system or Linux system to flash the Secure Bootloader
- SD Card to install the filesystem (U1 and U3 cards should NOT be used due to HW Limitations)
- Two micro USB cables to connect the board a computer

1.2. EmSPARK Suite Package Contents

Download the Evaluation Kit package. Expand the package in a Linux environment:

```
tar -zxvf security_suite_eval_[release].tar.gz
```

Extracting the tar file creates the following file structure:

- `corelockr`, the CoreLockr libraries, example applications and API documentation
- `coretee_dev_kit`, the toolchain and the client API for building the example applications
- `install`, the Secure SAM-BA Loader and firmware
- `filesystem`, the filesystem for installation on the SD Card
- `USER_GUIDE.pdf`, an overview of the Evaluation Kit
- `CORELOCKR_LIBRARIES_GUIDE.pdf`, an overview of the CoreLockr libraries and tutorial to build and execute the example applications
- `COPYRIGHT.txt`, the copyright notice
- `RELEASE_NOTES.txt`, information about the release
- `GETTING_STARTED.pdf`, this guide

2. INSTALLATION PROCEDURE

The process consists of these steps, which will be detailed in the following sections:

- Install the filesystem on an SD Card
- Flash the secure bootloader, CoreTEE and Linux Kernel on the Shield96 board
- Start the console
- Start the system

2.1. Installing the filesystem on SD Card

To install the board's Normal World filesystem on an SD Card, partition and create two partitions:

- First partition, an ext4 filesystem minimum of 3GB.

- Second partition, a Linux swap partition, minimum 512 MB.

Then extract the filesystem in `filesystem/seqlabs_ubuntu_[release].tar.gz` directly into the first partition.

The following steps are one way to install the filesystem on the SD Card (tested on 16.04.2):

- Identify the card device in the system and unmount it.
- Create the partitions:

```
fdisk /dev/<device>
```

- Create an ext4 filesystem on the SD Card first partition:

```
mkfs -t ext4 /dev/sd[x]1
```

  where `/dev/sd[x]1` is the card device in the system, partition `1`.

- Mount the empty card, usually in a mount-point:

```
mount /dev/sd[x]1 /mnt/sdcard/
```

  where `/mnt/sdcard/` is a mount-point previously created in the system.

- Change to the mount-point and extract there `seqlabs_ubuntu_[release].tar.gz`. To preserve permissions, execute this step as root:

```
cd /mnt/sdcard

tar -zxvf /security_suite_eval_[release]/filesystem/
seqlabs_ubuntu_[release].tar.gz
```

- After the tar file is extracted, execute "`sync`". This step can take from a few seconds to a few minutes.
- Unmount and eject the SD Card from the Linux system.
- The SD Card is now ready to be inserted on the board.

2.2. Flashing the Secure Bootloader

Note: After flashing the board with the EmSPARK Suite Evaluation Kit, because the Evaluation Kit uses emulated fuses stored on the chip SRAM, in order to maintain their values, it is recommended to keep the board powered up. If the board is unpowered, the provisioning data will be erased and as a result the board will need to be provisioned again. This will not affect the SD Card data.

If the memory is erased, the behavior during boot will return to the default boot configuration.

The Secure Bootloader can be flashed on the board in either Windows or Linux environments. The `install` directory contains everything necessary to flash the bootloader, including the necessary scripts for Windows and Linux environments, the loader, and documentation:

- `linux/sam-ba_3.3.1` and `windows/sam-ba_3.3.1` are the Secure SAM-BA Loader tools for Linux and Windows environments.
- `install.sh`, in Linux environment, flashes the firmware to the device.
- `install.bat`, in Windows environment, flashes the firmware to the device.

To flash the bootloader:

- The flashing procedure does not require pre-installation of software.
- Follow the board flashing steps for your work environment:
  - Windows environment: see **Appendix A: Installation Instructions for Windows** for step-by-step guide.
  - Linux environment: see **Appendix B: Installation Instructions for Linux** for instructions.

NOTE: To flash the board, please use a native Windows or Linux machine, not a virtual machine.

Flashing the board on a virtual machine may fail.

2.3. Starting the Console

To start the serial console which is the TEE console where occasionally the Secure World prints output messages:

- Connect a micro USB cable to J10 (debug) micro USB port on the board
- Connect the host machine to the serial port
  - 115200 bps
  - No parity
  - 8 bits
  - 1 stop bit
  - No flow control
- Connect a micro USB cable to the PC/power micro USB port on the board

2.4. Secure Boot Mode – Starting and Using the System

To start and use the system on the board:

- Insert the SD Card on the board (the SD Card may be inserted while the power is off)
- Start the console

After the board starts up:

- The console prints these messages

```
Welcome to Sequitur Labs CoreTEE (login = root:root)
seqlabs_coretee login: root (automatic login)
...
root@seqlabs_coretee:~#
```

- The board is configured to acquire an IP address using DHCP

The board is ready for your configuration:

- Required configuration:
  - The date on the board must be current for certificate management. When the board is used offline, the date must be configured. When the board is configured for remote access, verify that the date is current.
- Optional configuration:
  - Configure additional user(s). In addition to `root`, users in the `coretee` group have access to the TEE clients and can execute applications using the CoreLockr APIs. If users are created to execute the example applications, then create the `coretee` group if not already created and add users to this group.
  - Configure the board for remote access. The board is configured to acquire an IP address using DHCP. SSH is set up in the filesystem.

The board set up is complete. You can transfer to the board and execute example applications that use the EmSPARK Suite APIs.

2.5. Re-flashing a Board Already in Secure Mode

To re-flash a board that had been previously flashed and it is already in secure mode:

- Remove power from the board
- Wait for at least 30 seconds
- Reapply power the board

This clears any memory and the secure state of the board. The board should now be ready to be re-flashed using the steps in Section **2.2 Flashing the Secure Bootloader.**

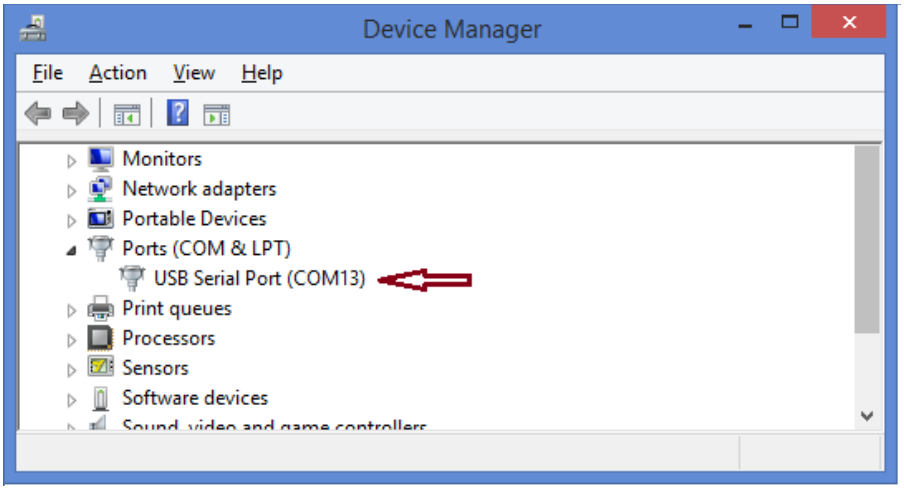
APPENDIX A: INSTALLATION INSTRUCTIONS FOR WINDOWS

Board set up

- Remove power from the board and wait at least 30 seconds

Step 1

- Open Windows Device Manager.
- Connect a micro USB cable to J10 (debug) micro USB port on the board.
- Look on the Device Manager for the Serial COM port associated with this cable.
- This port will be used to see the programming progress of the chip.



Step 2

- Open a serial communication program, such as "putty"
- Connect to the corresponding COM port with the following parameters
  - 115200 bps
  - No parity
  - 8 bits
  - 1 stop bit
  - No flow control
- 'RomBOOT' should appear on the serial terminal.

Step 3

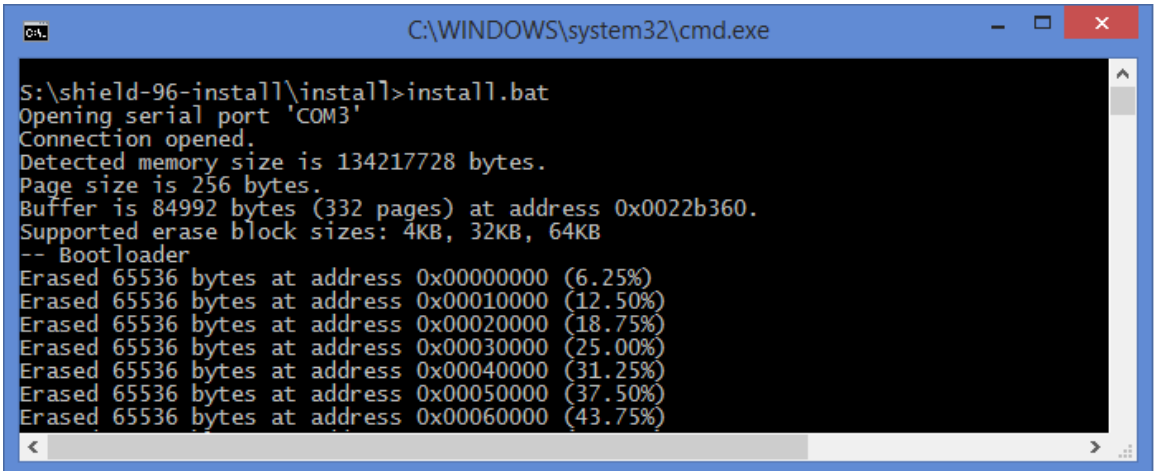
- Connect a micro USB cable to the PC/power micro USB port on the board.
  - This port will be used to program the board.

Step 4

- Open a Windows command prompt and change to the Secure SAM-BA loader directory, `install`
- Run the script to load the firmware to the board, and follow its instructions:

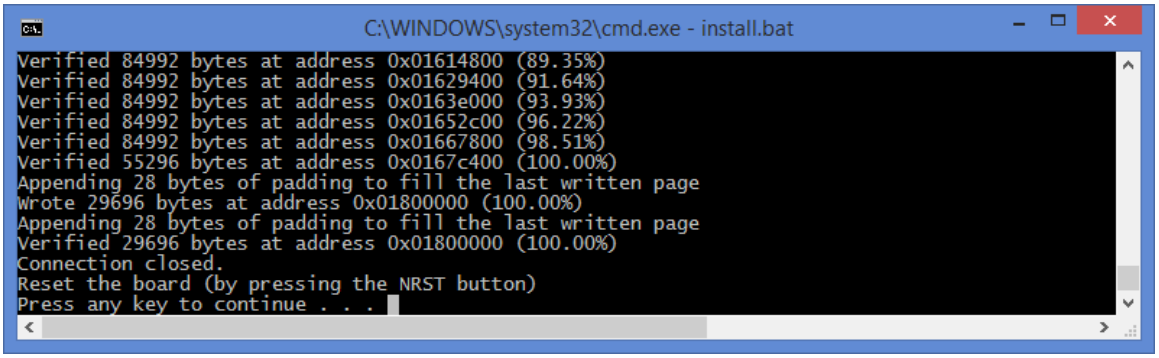
```
> install.bat
```

The script will identify the correct port attached to the host computer and start the programming process.



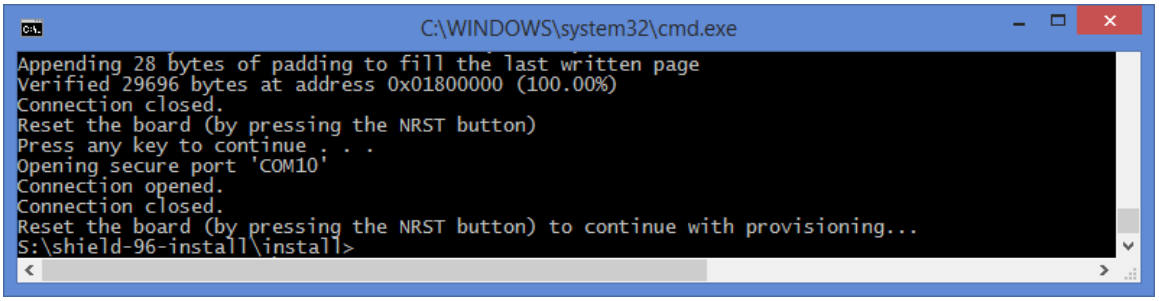
Step 5

- When instructed on the Windows terminal, reset the board (do not power it off, use the NRST button to reset).



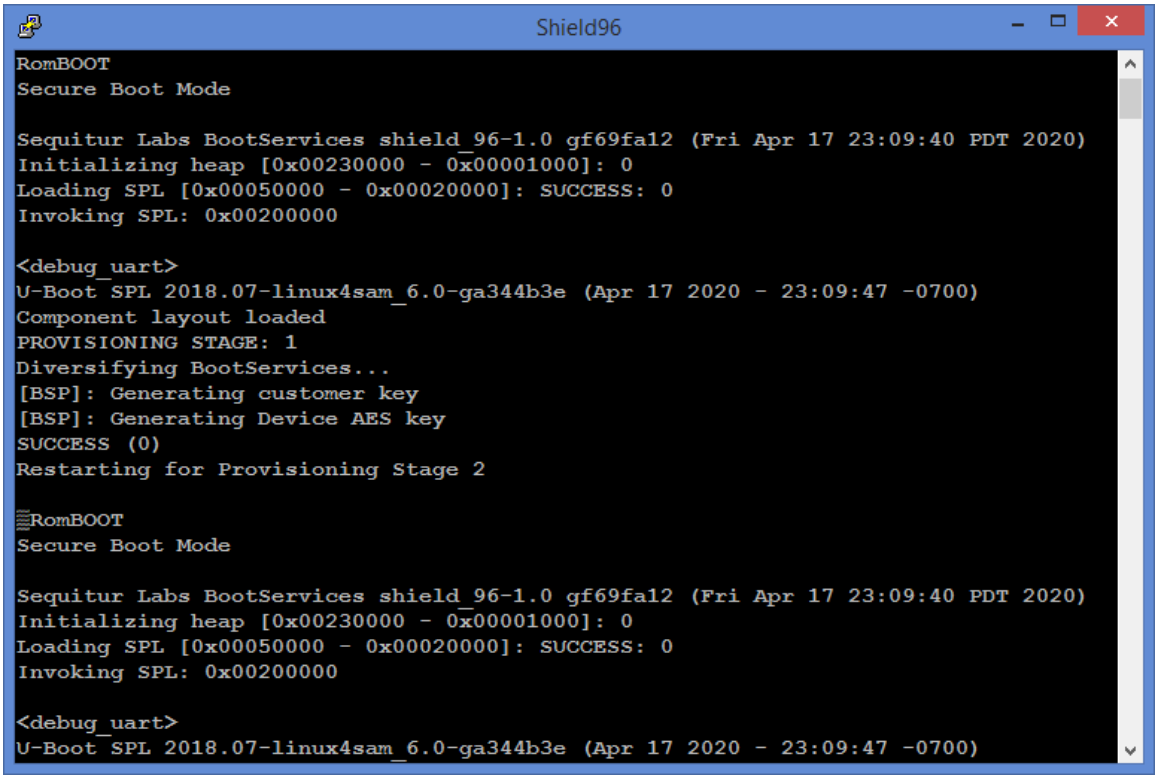
- 'Secure Boot Mode' is displayed on the serial terminal.

- On the Windows command line, press any key to write the customer key.
- The programming process on the Windows command line will complete.

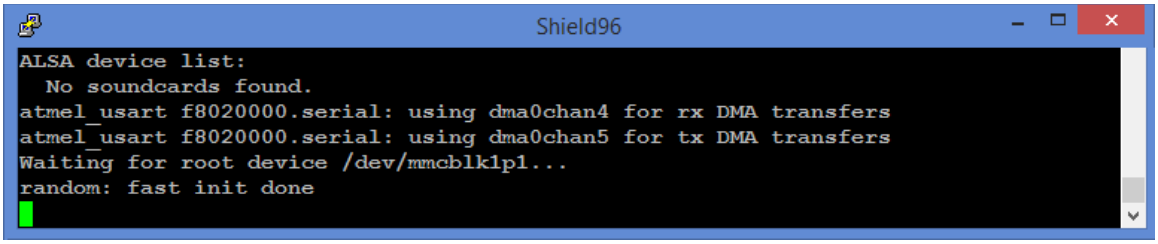


Step 6

- Reset the board once more to start provisioning the board.
- The serial terminal will print the provisioning messages.

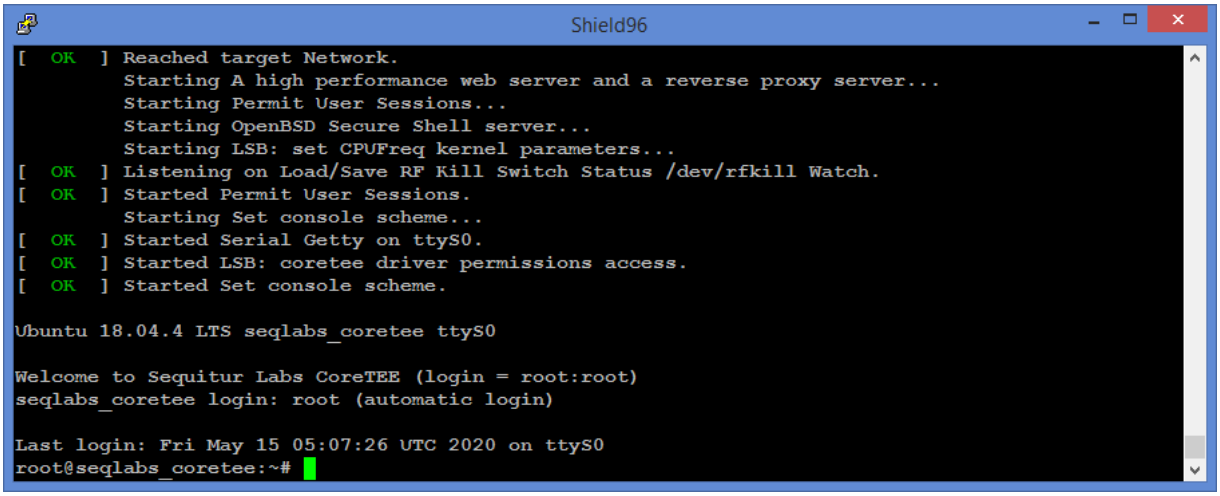


- When provisioning concludes, the board will boot.



Step 7

- Insert the SD card with the file system and press the NRST button.
- The board will begin booting.


Shield96
[OK] Reached target Network.
Starting A high performance web server and a reverse proxy server...
Starting Permit User Sessions...
Starting OpenBSD Secure Shell server...
Starting LSB: set CPUFreq kernel parameters...
[OK] Listening on Load/Save RF Kill Switch Status /dev/rfkill Watch.
[OK] Started Permit User Sessions.
Starting Set console scheme...
[OK] Started Serial Getty on ttyS0.
[OK] Started LSB: coretee driver permissions access.
[OK] Started Set console scheme.
Ubuntu 18.04.4 LTS seqlabs_coretee ttyS0
Welcome to Sequitur Labs CoreTEE (login = root:root)
seqlabs_coretee login: root (automatic login)
Last login: Fri May 15 05:07:26 UTC 2020 on ttyS0
root@seqlabs_coretee:~#

APPENDIX B: INSTALLATION INSTRUCTIONS FOR LINUX

1. Board set up. Remove power from the board and wait at least 30 seconds.

2. On the Linux host computer, make sure the user has permissions to access /dev/ttyACM0 and /dev/ttyUSB0.

3. Connect a micro USB cable to J10 (debug) micro USB port on the board.

4. Use a serial communication program to observe the Secure World console. For example, open "minicom". Connect the serial terminal with the following parameters:

   - 115200 bps
   - No parity
   - 8 bits
   - 1 stop bit
   - No flow control

   'RomBOOT' will appear on the serial terminal.

5. Connect a micro USB cable to the PC/power micro USB port on the board. `/dev/ttyACM0` will be used to program the board.

6. Open a second terminal to program the board and change to the `install` directory. Run the script to load the firmware to the board, and follow its instructions.

   ```
   $ ./install.sh
   ```

   The programming process starts and prints messages, e.g.

   ```
   Opening serial port 'ttyACM0'
   Connection opened.
   Detected memory size is ...
   Page size is 256 bytes.
   Buffer is 84992 bytes (332 pages) at address ...
   Supported erase block sizes: 4KB, 32KB, 64KB
   -- Bootloader
   Erased 65536 bytes at address 0x00000000 (6.25%)...
   ```

7. When instructed, reset the board (do not power it off, use the NRST button to reset).

   '`Secure Boot Mode`' will be displayed on the serial terminal.

8. On the Linux terminal, press any key to write the customer key.

   The programming process on the Linux command line will complete.

   ```
   Connection closed.
   Reset the board (by pressing the NRST button), then press any key to
   continue...Opening secure port 'ttyACM0'
   Connection opened.
   ```

```
Connection closed.
Reset the board (by pressing the NRST button) to continue with
provisioning...
```

9. Reset the board once more to start the provisioning process.

   The serial terminal will print the provisioning messages, e.g.

```
Sequitur Labs BootServices shield_96-1.0 gf69fa12
...
PROVISIONING STAGE: 1
Diversifying BootServices...
[BSP]: Generating customer key
[BSP]: Generating Device AES key
SUCCESS (0)
Restarting for Provisioning Stage 2
...
PROVISIONING STAGE: 2
[BSP]: Generating Cert AES key
Diversifying Component Index: SUCCESS (0)
Diversifying Certificate Manifest: SUCCESS (0)
Diversifying SPL: SUCCESS (0)
...
```

10. When provisioning concludes, the board will boot.
11. Insert the SD card with the file system and press the NRST button. The board will boot and auto-login in Linux, e.g.

```
Ubuntu 18.04.4 LTS seqlabs_coretee ttyS0

Welcome to Sequitur Labs CoreTEE (login = root:root)
seqlabs_coretee login: root (automatic login)
...
root@seqlabs_coretee:~#
```

CHANGE HISTORY

DATE	VERSION	RESPONSIBLE	DESCRIPTION
November 15, 2019	1.0	Julia Narvaez	Produced document for release.
February 24, 2020	1.1	Julia Narvaez	Updated SD Card requirments
May 22, 2020	1.2	Julia Narvaez	Aligned script names with package contents.