EmSPARK Suite

Evaluation Kit - Getting Started Guide

Date June 2, 2020 | Version 2.0

CONFIDENTIAL AND PROPRIETARY

THIS DOCUMENT IS PROVIDED BY SEQUITUR LABS INC. THIS DOCUMENT, ITS CONTENTS, AND THE SECURITY SYSTEM DESCRIBED SHALL REMAIN THE EXCLUSIVE PROPERTY OF SEQUITUR LABS, ARE CONFIDENTIAL AND PROPRIETARY TO SEQUITUR LABS, AND SHALL NOT BE DISCLOSED TO OTHERS.

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 SDCARD and start the system. After completing this guide, see the `USER_GUIDE.pdf` tutorial for a complete description of the Evaluation Kit and instructions to build and run the provided example applications.

1.1. Prerequisites

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

- SAMA5D2 (Rev. C) Xplained Ultra development board.
- Linux System to extract the Evaluation Kit package and build the example applications
- Windows system or Linux system to flash the Secure Bootloader
- SDCARD to install the filesystem
- FTDI UART cable such as FTDI TTL-232R-3V3 (optional) to connect to the serial terminal and to be able to see programming progress

Note: SAMA5D2 (Rev. B) Xplained Ultra development boards support the execution of applications using the CoreLockr APIs. Please see note in the installation procedure section of this document.

1.2. EmSPARK Suite Package Contents

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

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 SDCARD
- Set up the board connections. See **Appendix A: Board Connections** for instructions.
- Flash the secure bootloader, CoreTEE and Linux Kernel on the Microchip SAMA5D2 board
- Start the console
- Start the system

2.1. Installing the filesystem on SDCARD

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: The SAMA5D2 Xplained development board includes a supercapacitor as a backup battery that supplies power for the Secure RAM. After flashing the board with the EmSPARK Suite Evaluation Kit, it is recommended to keep the board powered up. If the board is unpowered for several hours, the supercapacitor will be discharged and the backup memory will be erased, and as a result the board will need to be re-flashed. 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 B: Installation Instructions for Windows** for step-by-step guide.
  - Linux environment: see **Appendix C: Installation Instructions for Linux**. To flash the board, use a Linux native machine, not a virtual machine.

2.3. Starting the Console

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

- Connect a TTL to USB Serial Converter to the J1 (DEBUG) header on the SAMA5D2. An appropriate cable would be the FTDI TTL-232R-3V3.
- Connect the host machine to the serial port
  - 115200 bps
  - No parity
  - 8 bits
  - 1 stop bit
  - No flow control
- Power the board using the A5-USB-A port

2.4. Secure Boot Mode - Starting and Using the System

To start and use the system on the board:

- Insert the SDCARD on the board (the SDCARD may be inserted while the "reset" button is pressed and the power is off)
- Ensure that the BOOT_DIS jumper is open
- 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 through the RJ45 port

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 through the RJ45 port. 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.

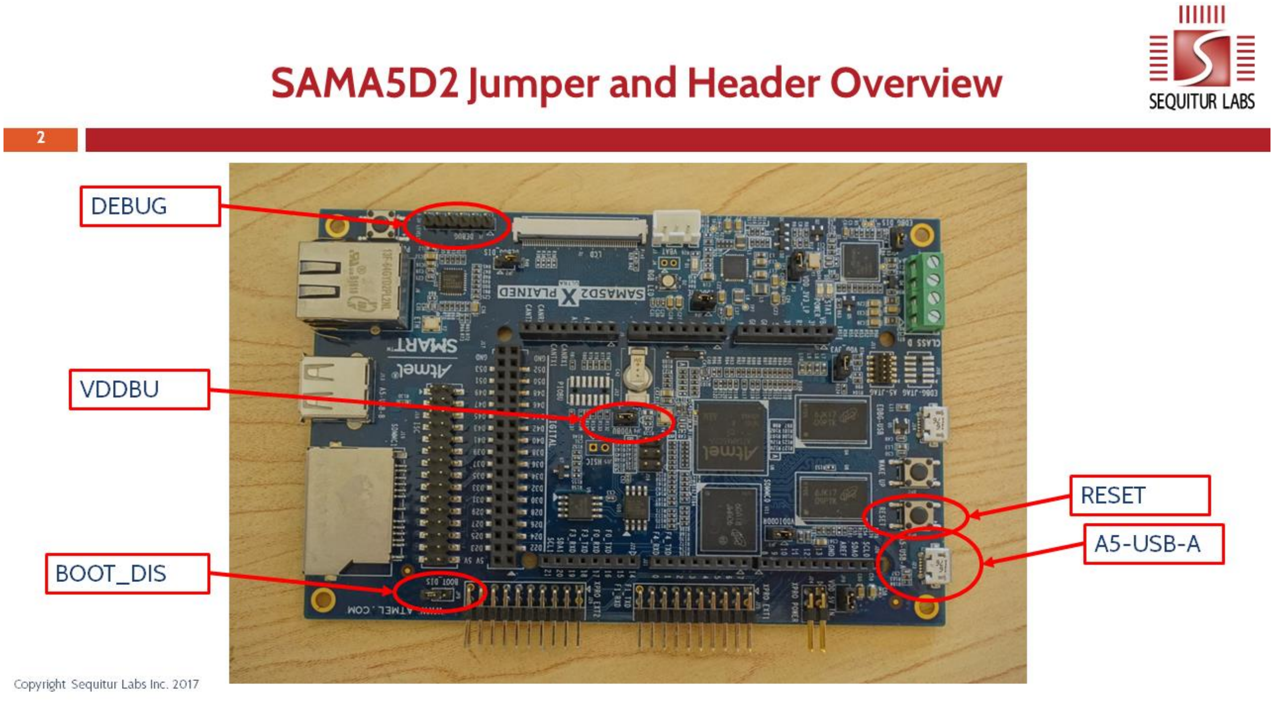
2.5. Re-flashing a Board Already in Secure Mode

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

- Remove power from the board
- Pull the 'VDDBU' jumper located near the center of the board
- Replace the jumper
- 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.**

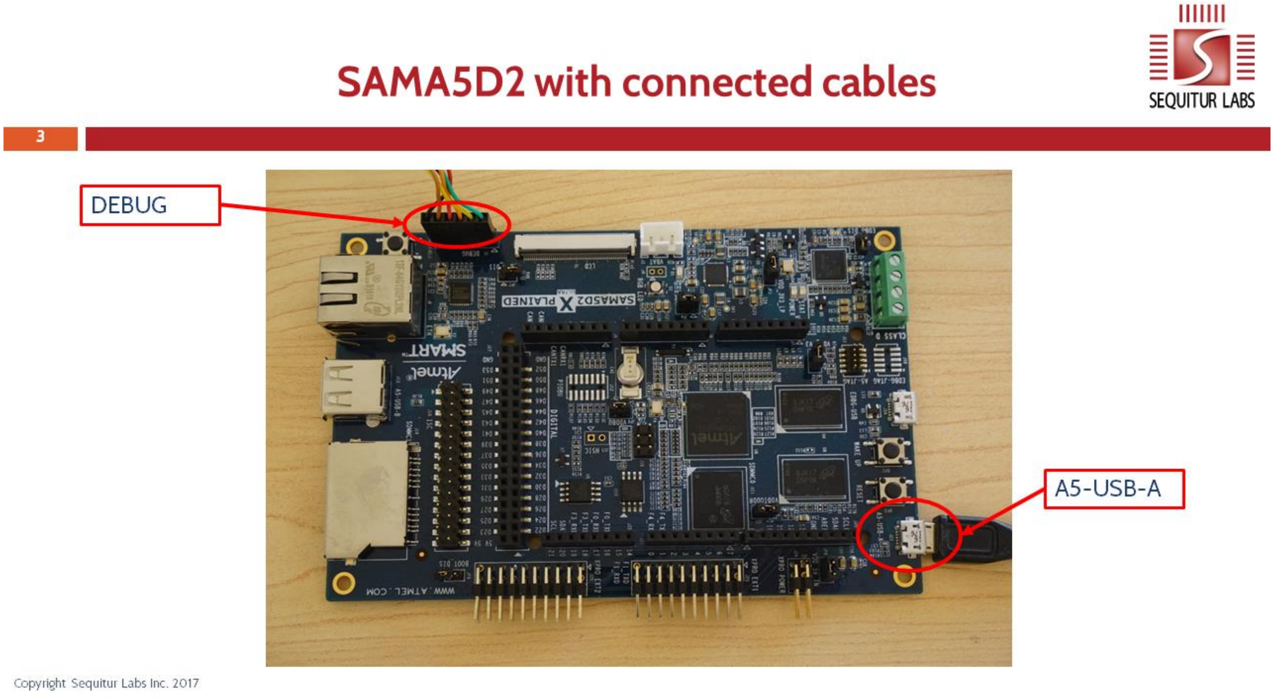
APPENDIX A: BOARD CONNECTIONS



SAMA5D2 Jumper and Header Overview

2

Copyright Sequitur Labs Inc. 2017



SAMA5D2 with connected cables

3

Copyright Sequitur Labs Inc. 2017

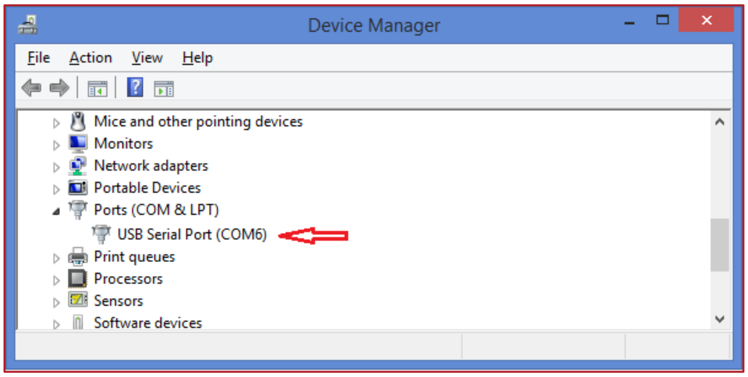
APPENDIX B: INSTALLATION INSTRUCTIONS FOR WINDOWS

Board set up

- Remove the SDCARD
- Remove power from the board
- Pull the 'VDDBU' jumper located near the center of the board
- Replace the 'VDDBU' jumper

Step 1

- Open Windows Device Manager.
- Attach an FTDI UART cable from the “DEBUG” header on the device to USB of host computer.
- Look on the Device Manager for the Serial COM port associated with this cable.
- This will be used to see the programming progress of the chip, e.g.



Step 2

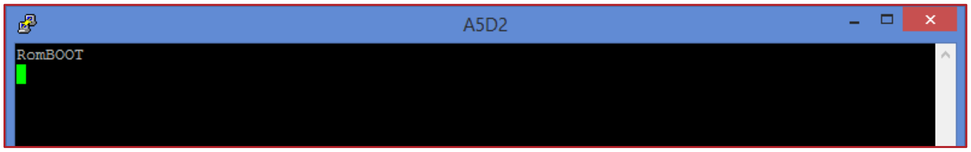
- Open Putty or another serial communication program.
- Connect to the corresponding COM port with the following parameters
  - 115200 bps
  - No parity
  - 8 bits
  - 1 stop bit
  - No flow control

Step 3

- Close the 'BOOT_DIS' jumper on the board.
- Attach the micro-USB (labeled “A5-USB-A”) from the device to a USB port of the host computer. Device Manager will list a new COM port that will be used to program the board.

Step 4

- ‘RomBOOT’ should appear on the serial terminal.



```
RomBOOT
```

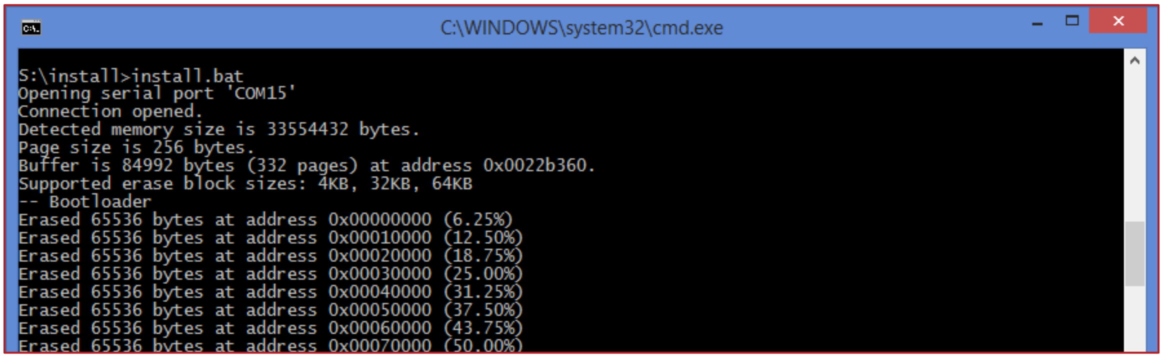
- Open the 'BOOT_DIS' jumper on the board.

Step 5

- Open a windows command prompt and change to the `install` directory
- Run the script to put board into secure mode and to load the firmware to the board, and follow its instructions:

  ```
  > install.bat
  ```

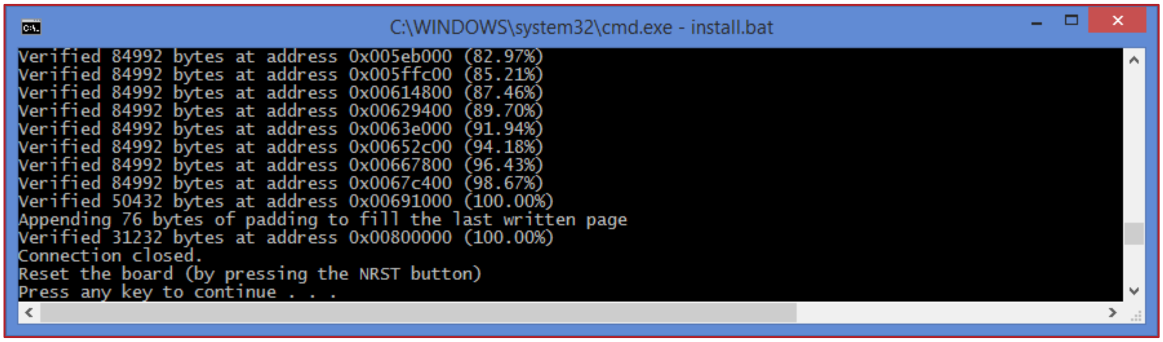
  The script will identify the correct port attached to the host computer and start the programming process.



```
S:\install>install.bat
Opening serial port 'COM15'
Connection opened.
Detected memory size is 33554432 bytes.
Page size is 256 bytes.
Buffer is 84992 bytes (332 pages) at address 0x0022b360.
Supported erase block sizes: 4KB, 32KB, 64KB
-- Bootloader
Erased 65536 bytes at address 0x00000000 (6.25%)
Erased 65536 bytes at address 0x00010000 (12.50%)
Erased 65536 bytes at address 0x00020000 (18.75%)
Erased 65536 bytes at address 0x00030000 (25.00%)
Erased 65536 bytes at address 0x00040000 (31.25%)
Erased 65536 bytes at address 0x00050000 (37.50%)
Erased 65536 bytes at address 0x00060000 (43.75%)
Erased 65536 bytes at address 0x00070000 (50.00%)
```

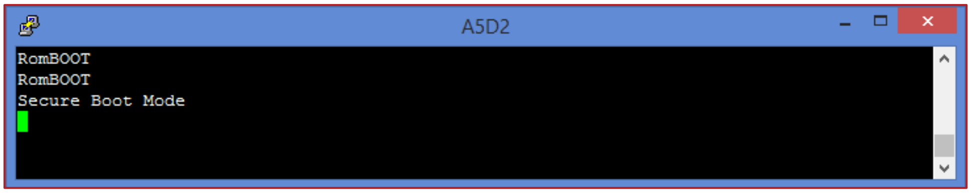
Step 7

- When instructed press the 'RESET' button.



```
Verified 84992 bytes at address 0x005eb000 (82.97%)
Verified 84992 bytes at address 0x005ffc00 (85.21%)
Verified 84992 bytes at address 0x00614800 (87.46%)
Verified 84992 bytes at address 0x00629400 (89.70%)
Verified 84992 bytes at address 0x0063e000 (91.94%)
Verified 84992 bytes at address 0x00652c00 (94.18%)
Verified 84992 bytes at address 0x00667800 (96.43%)
Verified 84992 bytes at address 0x0067c400 (98.67%)
Verified 50432 bytes at address 0x00691000 (100.00%)
Appending 76 bytes of padding to fill the last written page
Verified 31232 bytes at address 0x00800000 (100.00%)
Connection closed.
Reset the board (by pressing the NRST button)
Press any key to continue . . .
```

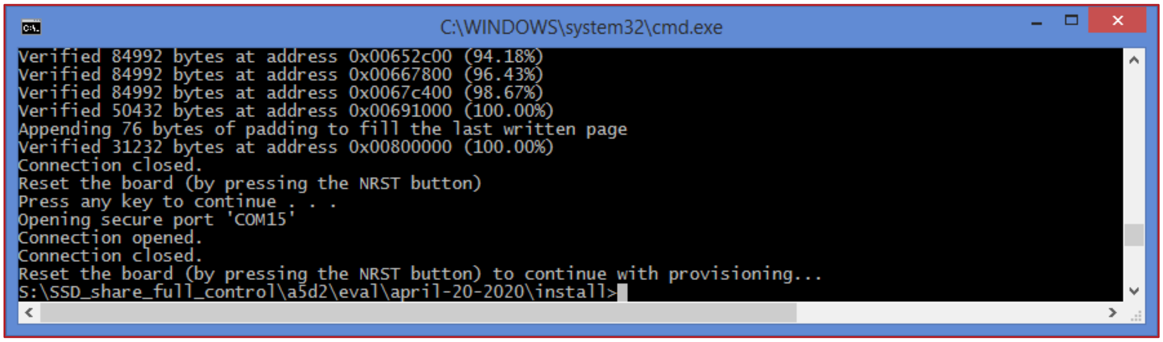
- 'Secure Boot Mode' should be printed on the console.



```
RomBOOT
RomBOOT
Secure Boot Mode
```

Step 7

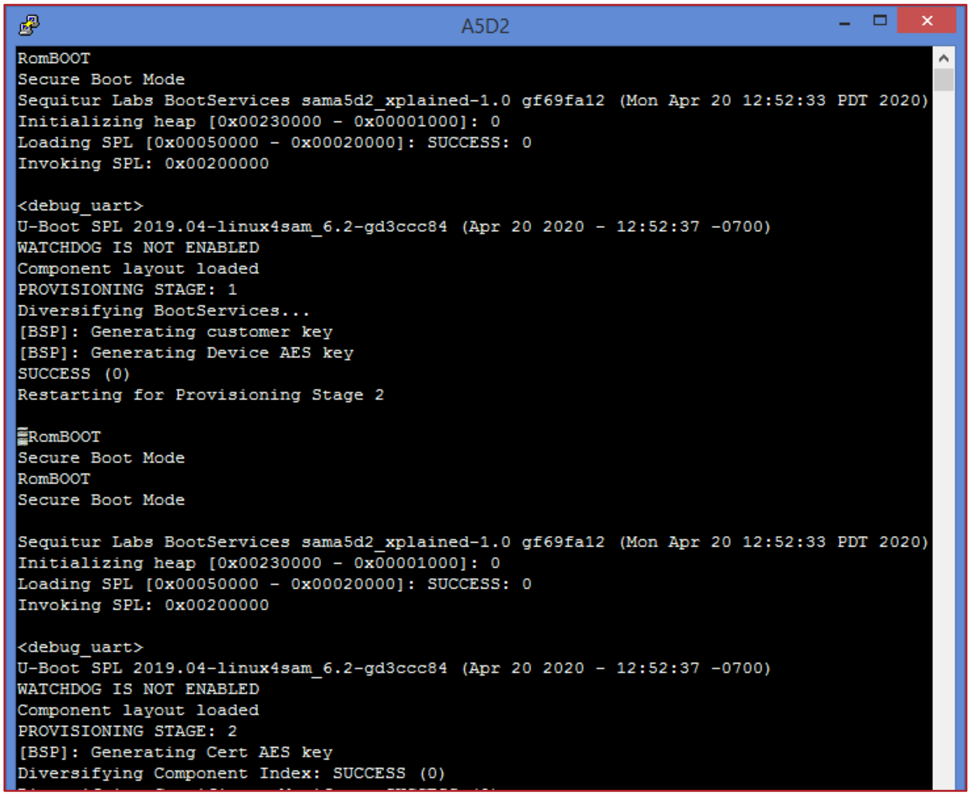
- On the Windows command line, press any key to write the customer key.
- The programming process on the Windows command line will complete.



```
Verified 84992 bytes at address 0x00652c00 (94.18%)
Verified 84992 bytes at address 0x00667800 (96.43%)
Verified 84992 bytes at address 0x0067c400 (98.67%)
Verified 50432 bytes at address 0x00691000 (100.00%)
Appending 76 bytes of padding to fill the last written page
Verified 31232 bytes at address 0x00800000 (100.00%)
Connection closed.
Reset the board (by pressing the NRST button)
Press any key to continue . . .
Opening secure port 'COM15'
Connection opened.
Connection closed.
Reset the board (by pressing the NRST button) to continue with provisioning...
S:\SSD_share_full_control\a5d2\eval\april-20-2020\install>
```

Step 8

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



```
RomBOOT
Secure Boot Mode
Sequitur Labs BootServices sama5d2_xplained-1.0 gf69fa12 (Mon Apr 20 12:52:33 PDT 2020)
Initializing heap [0x00230000 - 0x00001000]: 0
Loading SPL [0x00050000 - 0x00020000]: SUCCESS: 0
Invoking SPL: 0x00200000

<debug_uart>
U-Boot SPL 2019.04-linux4sam_6.2-gd3ccc84 (Apr 20 2020 - 12:52:37 -0700)
WATCHDOG IS NOT ENABLED
Component layout loaded
PROVISIONING STAGE: 1
Diversifying BootServices...
[BSP]: Generating customer key
[BSP]: Generating Device AES key
SUCCESS (0)
Restarting for Provisioning Stage 2

RomBOOT
Secure Boot Mode
RomBOOT
Secure Boot Mode

Sequitur Labs BootServices sama5d2_xplained-1.0 gf69fa12 (Mon Apr 20 12:52:33 PDT 2020)
Initializing heap [0x00230000 - 0x00001000]: 0
Loading SPL [0x00050000 - 0x00020000]: SUCCESS: 0
Invoking SPL: 0x00200000

<debug_uart>
U-Boot SPL 2019.04-linux4sam_6.2-gd3ccc84 (Apr 20 2020 - 12:52:37 -0700)
WATCHDOG IS NOT ENABLED
Component layout loaded
PROVISIONING STAGE: 2
[BSP]: Generating Cert AES key
Diversifying Component Index: SUCCESS (0)
```

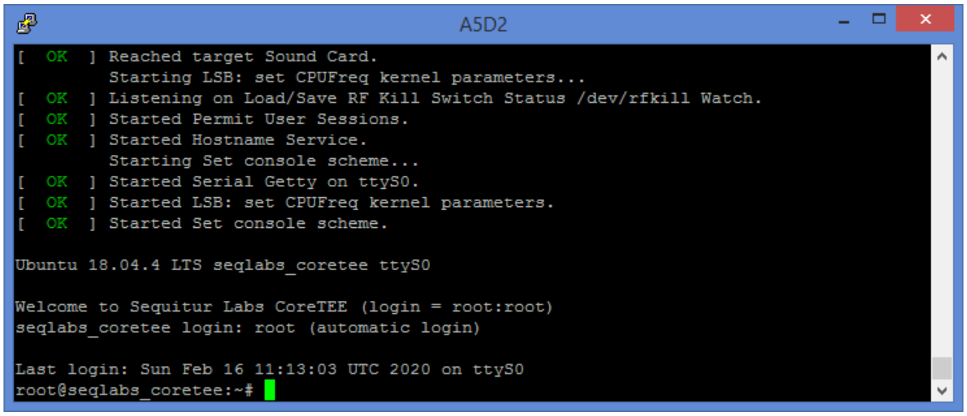
NOTE:

If using a Rev. B board, the board will not auto-reboot during provisioning. Please press the "RESET" button when the terminal prints these lines and waits for a reset:

```
RomBOOT
Secure Boot Mode
```

Step 9

- When provisioning concludes, the board will boot.
- Insert the SD card with the file system and press the "RESET" button.
- The board will boot and auto-login.



```
[  OK  ] Reached target Sound Card.
         Starting LSB: set CPUFreq kernel parameters...
[  OK  ] Listening on Load/Save RF Kill Switch Status /dev/rfkill Watch.
[  OK  ] Started Permit User Sessions.
[  OK  ] Started Hostname Service.
         Starting Set console scheme...
[  OK  ] Started Serial Getty on ttyS0.
[  OK  ] Started LSB: set CPUFreq kernel parameters.
[  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: Sun Feb 16 11:13:03 UTC 2020 on ttyS0
root@seqlabs_coretee:~#
```

APPENDIX C: INSTALLATION INSTRUCTIONS FOR LINUX

1. Board set up
   - Remove the SDCARD
   - Remove power from the board
   - Pull the 'VDDBU' jumper located near the center of the board
   - Replace the 'VDDBU' jumper

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

3. Attach an FTDI UART cable from the “DEBUG” header on the device to USB of host computer. This will be used to see the programming progress of the chip.

4. Use a serial communication program to observe the Secure World console. Connect the serial terminal with the following parameters:

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

5. Close the 'BOOT_DIS' jumper on the board.

6. Attach the micro-USB (labeled “A5-USB-A”) from the device to a USB port of the host computer. `/dev/ttyACM0` will be used to program the board.

7. ‘RomBOOT’ will appear on the serial terminal.

8. Open the 'BOOT_DIS' jumper on the board.

9. 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%)...
   ```

10. When instructed, press the "RESET" button to reset the board

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

11. 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...
    ```

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

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

    ```
    Sequitur Labs BootServices sama5d2_xplained-1.0 g2efbe0c
    ...
    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)
    ...
    ```

    NOTE:
    If using a Rev. B board, the board will not auto-reboot during provisioning. Please press the "RESET" button when the terminal prints these lines and waits for a reset:

    ```
    RomBOOT
    Secure Boot Mode
    ```

13. When provisioning concludes, the board will boot.

14. Insert the SD card with the file system and press the "RESET" 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
April 30, 2018	1.0	Julia Narvaez	Produced document for release.
June 19, 2018	1.0	Julia Narvaez	Updated troubleshooting information
June 2, 2020	2.0	Julia Narvaez	Updated Kit information for SAMA5D2 Xplained Rev. C.