EmSPARK™ Security Suite

Evaluation Kit - Getting Started Guide for AAEON BOXER-8251AI Series

Date March 21, 2022 | Version 1.0

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

This **Getting Started Guide** is an overview of the prerequisites to use the **EmSPARK™ Suite Evaluation Kit**, description of the Kit contents, and installation instructions on an Aaeon device. After completing the installation process in this guide, please see the `CORELOCKR_LIBRARIES_GUIDE.pdf` which provides an overview of the CoreLockr™ APIs. The security features of CoreTEE™ in the Secure Domain and the CoreLockr™ APIs in the Rich OS are supported after flashing the device. The installation also includes the root filesystem which has preinstalled the EmSPARK™ components for the Rich OS.

The EmSPARK™ Evaluation Kit demonstrates some of the credentials provisioned on the device. The firmware image in `EmSpark_Xavier-NX-Dev_Eval_[release].tar.gz` has preconfigured keys and certificates that typically a customer would configure in personalization data manifests when building the firmware. Other keys are device-specific generated during the first boot when they are not available.

To demonstrate security scenarios using such credentials for verification, the provided example applications include the private key files associated with public keys provisioned on the device. Client applications using the CoreLockr™ APIs can use the provisioned credentials for operations executed in the Trusted Execution Environment (TEE). In the case of the generated device-specific keys, Device Keys, the example applications illustrate how to use them in the TEE while the Rich OS has not access to the device key private attributes.

Devices flashed with the EmSPARK™ Security Suite are also EmPOWER™ enabled. EmPOWER™ is a SaaS solution that provides the essential cloud services needed to secure, provision, update and manage intelligent edge devices. For information about EmPOWER™ please contact Sequitur Labs.

The secure boot and update processes follow the NVIDIA Jetson flow. Please refer to the NVIDIA Jetson documentation for detail.

1.1. Prerequisites

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

- EmSPARK Suite
  - EmSPARK Development kit: `EmSpark_AAEON_[release].tar.gz`
  - EmSPARK CoreLockr Libraries for client application development: `corelockr_empower_[release].tar.gz`
- AAEON BOXER-8251AI Series device with connected peripherals (keyboard, HDMI and mouse)
- Linux system to extract the Evaluation Kit package, build the example applications and install
- A micro-USB cable to connect the device to the Linux system

1.2. EmSPARK™ Suite Package Contents

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

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

The following directory structure is created under `EmSpark_AAEON`:

- `flash` contains the firmware image ready for flashing. The firmware image has the EmSPARK components and is preconfigured with sample keys and certificates. This image is equivalent to the image that customers would produce with custom components in a development or production environment.
- `corelockr_package` contains the CoreLockr™ APIs, which are C libraries for development of client applications running in the Rich OS (Linux) and work with the Trusted Applications running in the Trusted Execution Environment (CoreTEE™). The Kit includes:
  - `corelockr`, the CoreLockr libraries, TAs, example applications and API documentation
  - `coretee_dev_kit`, the toolchain and the client API for building the example applications
  - `CORELOCKR_LIBRARIES_GUIDE.pdf`, an overview of the CoreLockr libraries and tutorial to build and execute the example applications
  - `COPYRIGHT.txt`, the copyright notice
- `COPYRIGHT.txt`, the copyright notice
- `RELEASE_NOTES.txt`, information about the release
- `GETTING_STARTED.pdf`, this guide

1.3. Terminology

CoreLockr™	Sequitur's native C APIs for development of client applications that execute in the Rich OS and perform security-specific functions in the TEE
CoreTEE™	Sequitur's Trusted Execution Environment (TEE), or secure OS, enabled by ARM's TrustZone™ architecture.
Personalization Manifest	Customer configured data including keys and certificates that are part of the components installed on the device.
SLIP	Encrypted component containing customer personalization data such as keys and certificates. Personalization data is configured in manifests, which after built and encrypted are called SLIPs. They are installed on device along with the device firmware.
TEE	Trusted Execution Environment or secure OS, enabled by ARM's TrustZone™ architecture.

2. INSTALLATION PROCEDURE

The device installation process consists of these steps:

1. Start with the board powered off.
2. Connect the device Micro-USB (labeled OS FLASH) to the host Linux computer.
3. On the device, connect peripherals (optional at this stage).
4. On the device, force USB Recovery Mode by pressing and holding the RECOVERY button (pin in hole) while powering on the board, as explained in the AAEON BOXER-8251AI User's Manual.
5. On the Linux host computer

5.1. When the device is in recovery mode, the `lsusb` command lists

```
ID 0955:7e19 NVidia Corp. APX
```

5.2. Change to the `EmSpark_AAEON/flash` directory and execute

```
sudo ./flash_device.sh
```

5.3. During flashing, the Linux terminal prints messages signifying the process on the device. Flashing the image may take several minutes, and eventually prints messages like these:

```
[ 170.0241 ] Writing partition kernel-dtb with kernel_tegra194-p3668-all-p3509-0000_sigheader.dtb.encry
[ 170.0320 ] [.....] 100%
[ 170.0388 ] Writing partition kernel-dtb_b with kernel_tegra194-p3668-all-p3509-0000_sigheader.dtb.enc
[ 170.0618 ] [.....] 100%
[ 170.0690 ] Writing partition manifest with manifests.img
[ 170.0902 ] [.....] 100%
[ 170.0948 ] Writing partition APP with system.img
[ 170.1155 ] [.....] 100%
[ 409.3812 ]
[ 409.3838 ] tegradevflash_v2 --write BCT br_bct_BR.bct
[ 409.3851 ] Bootloader version 01.00.0000
[ 409.3872 ] Writing partition BCT with br_bct_BR.bct
[ 409.3876 ] [.....] 100%
[ 409.5304 ]
[ 409.5346 ] tegradevflash_v2 --write MB1_BCT mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 409.5357 ] Bootloader version 01.00.0000
[ 409.5380 ] Writing partition MB1_BCT with mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 409.5386 ] [.....] 100%
[ 409.7428 ]
[ 409.7466 ] tegradevflash_v2 --write MB1_BCT_b mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 409.7486 ] Bootloader version 01.00.0000
[ 409.7517 ] Writing partition MB1_BCT_b with mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 409.7531 ] [.....] 100%
[ 409.9565 ]
[ 409.9637 ] tegradevflash_v2 --write MEM_BCT mem_coldboot_sigheader.bct.encrypt
[ 409.9663 ] Bootloader version 01.00.0000
[ 409.9690 ] Writing partition MEM_BCT with mem_coldboot_sigheader.bct.encrypt
[ 409.9709 ] [.....] 100%
[ 411.2293 ]
[ 411.2334 ] tegradevflash_v2 --write MEM_BCT_b mem_coldboot_sigheader.bct.encrypt
[ 411.2357 ] Bootloader version 01.00.0000
[ 411.2388 ] Writing partition MEM_BCT_b with mem_coldboot_sigheader.bct.encrypt
[ 411.2407 ] [.....] 100%
[ 412.4998 ]
[ 412.4999 ] Flashing completed

[ 412.5001 ] Coldbooting the device
[ 412.5036 ] tegrarcm_v2 --ismb2
[ 412.5077 ]
[ 412.5111 ] tegradevflash_v2 --reboot coldboot
[ 412.5127 ] Bootloader version 01.00.0000
[ 412.5151 ]
```

6. When flashing completes, the device will reboot and boot into Linux.

The following are some of the processes that take place during flashing:

- Initialize CoreTEE
- CoreTEE installs personalization data contained in manifests and generates unique device identification
  - Load manifests containing keys and certs
  - Decrypt encrypted manifests
  - Generate device keys and certs
  - Generate OEM Device Key
  - Generate EmPOWER Device Key
  - Generate OEM Device CSR and OEM Device Certificate
  - Generate EmPOWER Device CSR and EmPOWER Device Certificate
- CoreTEE re-encrypts the manifest that contains keys and certs
  - Include in the manifest the newly generated device keys and certificates
  - Write manifests to NVM

In a set up where a serial console is connected to the device, the console prints messages of the process during flashing and booting.

- This is a subset of messages printed in the serial console alluding to processes during flashing:

```
[0216.490] I> Writing manifest partition.
...
[0002.115] I> Initializing CoreTEE...
[0002.118] I> Opening manifest
[0002.121] I> Initializing slip: 1 @ 0x00000000
I/TC:   Initializing slip: 1
I/TC:   Slip 1: SW ver = 0    HW ver = 0
I/TC:   Creating Device Key and Cert
I/TC:   Creating EmPower Device Key and Cert
[0002.364] I> CoreTEE Manifest initialization: 0x00000001
[0002.365] I> Writing Manifests back to NVM
[0002.375] I> Manifest written back to NVM
[0002.375] I> Opening manifest
[0002.376] I> Initializing slip: 2 @ 0x00010400
...
I/TC:   Initializing slip: 2
I/TC:   Slip 2: SW ver = 0    HW ver = 0
I/TC:   Diversifying manifest: 2
[0002.401] I> CoreTEE Manifest initialization: 0x00000001
[0002.402] I> Writing Manifests back to NVM
[0002.413] I> Manifest written back to NVM
[0002.414] starting app coretee_init_app
[0002.415] I> CoreTEE Initialized
```

- This is a subset of messages during device boot, which does not modify the manifests, e.g.

```
[0002.103] I> Initializing CoreTEE...
[0002.106] I> Opening manifest
[0002.109] I> Initializing slip: 1 @ 0x00000000
[0002.114] I> HW Version: 0x00
[0002.128] I> OP: 0xb2000010
I/TC:   Initializing slip: 1


I/TC:   Slip 1: SW ver = 0    HW ver = 0
I/TC:   Device Key and Cert exist
[0002.154] I> CoreTEE Manifest initialization: 0x00000000
[0002.154] I> Manifests not modified
[0002.155] I> Opening manifest
[0002.155] I> Initializing slip: 2 @ 0x00010400
[0002.155] I> HW Version: 0x00
[0002.167] I> OP: 0xb2000010
I/TC:   Initializing slip: 2
I/TC:   Slip 2: SW ver = 0    HW ver = 0
[0002.182] I> CoreTEE Manifest initialization: 0x00000000
[0002.182] I> Manifests not modified
[0002.182] starting app coretee_init_app
[0002.183] I> CoreTEE Initialized
```

3. USING THE SYSTEM

After booting into Linux, on the device with connected peripherals:

- On the HDMI monitor, the user is prompted to enter access credentials
  - User: `seq`
  - Password: `seq`
- The device is configured to acquire an IP address.
- To execute the certificate management operations, the date on the device must be current. If the device is offline, please configure the date.

After installation, the `seq` user has access to the CoreLockr APIs. The filesystem setup has the `coretee` group that has read and write permissions to `/dev/tee0`, e.g.

```
seq@tegra-seqlabs:~$ ll /dev/tee0
crw-rw---- 1 root coretee 244, 0 Mar  5 05:48 /dev/tee0
```

The `seq` user belongs to the `coretee` group, e.g.

```
seq@tegra-seqlabs:~$ groups seq
seq : seq adm sudo audio video gdm lightdm coretee
```

For a user to execute applications using the CoreLockr APIs that communicate with CoreTEE, the user must be in the `coretee` group, or to be `root`. However, any access scheme is acceptable, provided the user calling CoreTEE services has read/write access to `/dev/tee0`.

Note: The CoreLockr Secure Certificates API function that modifies the certificates configured in the personalization manifest is a notable exception that requires `root` privileges. The command updating

these provisioned certificates writes back to the manifest partition. Writing to this partition is restricted to `root`. Additional information is provided in `EMSPARK_KEYS_CERTS.pdf`, part of the EmSPARK Development Kit.

CHANGE HISTORY

DATE	VERSION	RESPONSIBLE	DESCRIPTION
March 21, 2022	1.0	Julia Narvaez	Produced document for release.