EmSPARK™ Security Suite

Evaluation Kit - Getting Started Guide for Variscite VAR-SOM-MX8M-PLUS and DART-MX8M-PLUS Devices

Date October 21, 2021 | Version 1.1

SEQUITUR LABS

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** is an overview of the prerequisites to use the Evaluation Kit, description of the Kit contents, and installation instructions on an SD Card. The components installed on the SD Card will provision and start the system on a VAR-SOM-MX8M-PLUS or a or DART-MX8M-PLUS device. After completing this guide, please see the `EMSPARK_SECURE_BOOT.pdf` and `CORELOCKR_LIBRARIES_GUIDE.pdf` documents included with the Kit:

- `EMSPARK_SECURE_BOOT.pdf` describes the provisioning process and secure boot.
- `CORELOCKR_LIBRARIES_GUIDE.pdf` provides an overview of the CoreLockr™ APIs for development of client applications that run in the Rich OS (Linux) and work with the Trusted Applications that run in the Trusted Execution Environment (CoreTEE™), and instructions to build and run the example applications.

NOTE: As explained in `EMSPARK_SECURE_BOOT.pdf`, booting the board from the SD Card created with the installation instructions will program the fuses on the board!

1.1. Prerequisites

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

- Variscite VAR-SOM-MX8M-PLUS or DART-MX8M-PLUS device based on NXP i.MX 8M Plus
- Linux system to extract the Evaluation Kit package, build the example applications and open a serial terminal to interact with the device
- SD Card to install the system, minimum 8GB
- A micro USB cable to connect the USB Debug (J29) on the board to the Linux system

1.2. EmSPARK™ Suite Package Contents

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

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

Expanding the tar file creates the following file structure:

- `README.txt`, installation instructions
- `corelockr`, expanding `corelockr_empower.tar.gz`, the CoreLockr libraries, example applications and API documentation
- `coretee_dev_kit`, the toolchain and the client API for building the example applications
- `flash/flash_gold_[release].tar.gz`, the encrypted EmSPARK components for installation on the SD Card
- `filesystem/variscite_eval_filesystem.tar.gz`, the filesystem for installation on the SD Card
- `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 device installation process consists of these steps:

1. On the Linux machine:

1.1. Install the filesystem on an SD Card
Please follow the steps described in the “Create SD card with correct partitions” section of `security_suite_eval_variscite_[release]/README.txt`.

1.2. Flash the secure components on the SD Card
Please follow the steps described in the “Flash the encrypted EmSPARK components” section of `security_suite_eval_variscite_[release]/README.txt`.

2. On the Linux machine, start a serial terminal

2.1. Connect the USB Debug (J29) on the board to the Linux machine

2.2. Open a serial terminal on the Linux machine to see the messages during provisioning and secure boot

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

3. On the device, prepare to boot from the SD Card

   - Insert the SD Card
   - Set the DIP switch SW3 to 'SD' to boot from the SD card

4. Power on the board to start the following processes

4.1. **Provisioning**, follows the process explained in `EMSPARK_SECURE_BOOT.pdf`, note the fuse programming and additional messages printed in the serial console

4.2. **Secure boot**, follows the process explained in `EMSPARK_SECURE_BOOT.pdf`

3. STARTING AND USING THE SYSTEM

After the board starts up:

- The user is prompted to enter access credentials: `root` : `root`.
- The board is configured to acquire an IP address.
- To execute the certificate management operations, the date on the board must be current. If the board is offline, please configure the date.

Optional configuration: to allow execution of applications using the CoreLockr APIs to users different than `root`, create a group that has read and write permissions to `/dev/tee0` and add users to it.

4. TROUBLESHOOTING

Issue: After successful provisioning, during the first boot, the board console prints Kernel panic messages such as the following:

```
[    3.415143] ---[ end Kernel panic - not syncing: No working init found.
Try passing init= option to kernel. See Linux Documentation/admin-
guide/init.rst for guidance. ]---
 -0700)
```

Procedure: These errors occur when the filesystem installation on the SD Card did not succeed. To resolve the issue, please repeat the filesystem installation procedure on the SD Card as instructed in `security_suite_eval_variscite_[release]/README.txt`. If the error persists, please repeat the entire SD Card installation procedure.

CHANGE HISTORY

DATE	VERSION	RESPONSIBLE	DESCRIPTION
September 23, 2021	1.0	Julia Narvaez	Produced document for release.
October 21, 2021	1.1	Julia Narvaez	Added the STARTING AND USING THE SYSTEM and Troubleshooting sections.