SEC eDGE™
Digital Security to the Edge

EMSPARK™ MICROEDGE™ EVALUATION KIT

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

April 4, 2024 | Version 2.1

1. TABLE OF CONTENTS

2. INTRODUCTION

This guide is specific for Tata.

The EmSPARK™ MicroEdge™ 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 the secure boot components and start the system on a VAR-SOM-MX8M-PLUS or a or DART-MX8M-PLUS device.

After the device is up and running, this guide instructs how to set up MicroEdge to enable secure connectivity with

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 firmware 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!

2.1. 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

2.2. 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

3. 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 README.txt located at the root of the package.

   1.2. Flash the secure components on the SD Card

   Please follow the steps described in the “Flash the encrypted EmSPARK components” section of README.txt located at the root of the package.

   Note: To facilitate debugging, the new package includes In the gold blobs there is now a "loud" and a "quiet" coretee (tee-pager_loud.bin.blob, tee-pager_quiet.bin.blob). And a prov.sdx to go with them. The flash/README.txt talks about these.

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 firmware 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

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

4. 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.

5. MICROEDGE

The instructions in this section are executed on the device that has EmSPARK installed. The MicroEdge configuration is done on a device during runtime.

5.1. SECeDGE SERVICE PLATFORM

MicroEdge™ is a middleware component which provides zero-touch security provisioning, secure end-to-end data in motion and at rest for Internet of Things and Operational Technology on embedded devices. The solution can be deployed to a variety of devices. It is installed on devices equipped with Linux OS. It has been tested on diverse hardware including devices with Variscite SOM modules. Some examples of implementations are vending machines, automotive modules, IoT gateways, set-top boxes, smart locks, perimeter security, and smart city infrastructure.

A single MicroEdge instance on a device enables multi-tunnel connectivity to different CloudEdge servers enabling more secure services and/or new monetization options for the owners of the IoT/Edge devices, depicted in Figure 1.

CloudEdge™ is the cloud termination endpoint for MicroEdge device tunnels. Endpoint devices can be anchored to one or more peer endpoints on an external network, but residing on the same administrative span of control as the MicroEdge endpoint. This peer endpoint is referred to as the CloudEdge. All external network flows will be securely tunneled to CloudEdge where the flows can be subjected to additional security analysis before being routed to their ultimate destination.

Customers deploy one instance of CloudEdge in their backend to connect securely all IoT/Edge devices to their backend application server.

ControlEdge™ administers all edges (IoT devices equipped with MicroEdge and CloudEdge) within the SecEdge ecosystem. ControlEdge performs all the heavy lifting functions to set, configure and manage the security of the entire deployment. All this connectivity and provisioning is managed by ControlEdge services which allow for the deployment of IPsec tunnels facilitating secure communications between instances.

ControlEdge is available as a SecEdge managed service and is accessed by customers via simple APIs.

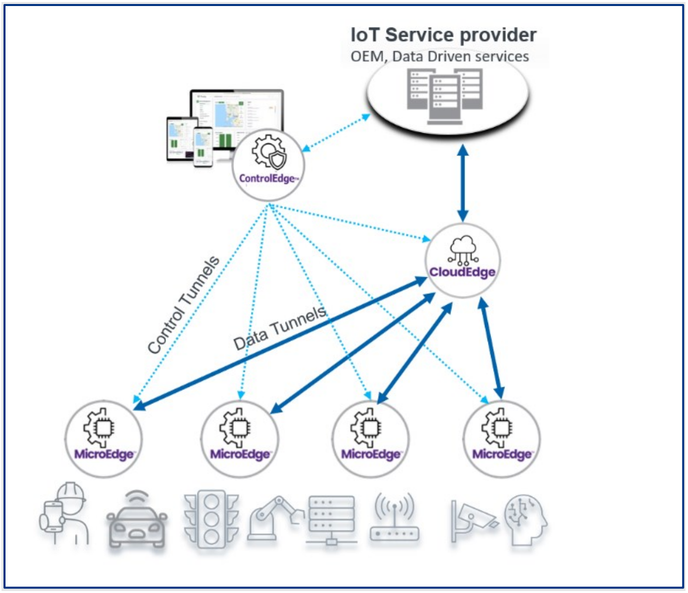

Figure 1 SecEdge Service Platform Architecture

5.2. TATA ARTIFACTS AND CONFIGURATION

The objective of the artifacts supplied in the Evaluation Kit is to demonstrate that Tata can get IPSec tunnels up and running.

+ MicroEdge
    - MicroEdge components are supplied in the Evaluation Kit
    - The b4cd0e9c-66c6-4bb1-a707-afd2efa21a63.tar tarball in the kit contains a key and certs for one device (Day0 credential).
    - The filesystem installed on the SDCard has some configuration ready.
    - The MicroEdge Reference Manual r7.pdf is supplied as a reference of the functional and operational views.
+ CloudEdge anchor point for the MicroEdge device tunnel
    - The CloudEdge is already configured for Tata in the SecEdge cloud infrastructure.
    - The certs in b4cd0e9c-66c6-4bb1-a707-afd2efa21a63.tar are specific for the CloudEdge configured for Tata.
    - The traffic from CloudEdge is redirected to Tata’s backend.
+ ControlEdge
    - ControlEdge is transparent to Tata with the current Eval Kit.

5.3. SETTING UP MICROEDGE ON DEVICE

Clean up filesystem: this step is not part of the normal installation and should be done only once before installing MicroEdge for the first time. The filesystem has some content under /data/tee/storage. It is recommended to start with this section clean.

On the device, execute `rm -rf /data/tee/storage`

This deletes all data stored in the secure storage.

MicroEdge setup:

1. Create

   ```
   mkdir -p /etc/softse.d/day0
   ```

2. Add the following IPs and domains to /etc/hosts:

   ```
   35.230.164.12 register.regression.dev.me.secedge.com
   35.245.199.234 cloud.regression.dev.me.secedge.com
   ```

3. Transfer Day0 credentials and command key to the device

   Transfer ~/Tata_MicroEdge_Test_Cert/b4cd0e9c-66c6-4bb1-a707-afd2efa21a63.tar and ~/Tata_MicroEdge_Test_Cert/clrsc_example_command_key.pem to the device to a directory of your choice.

4. Extract contents of ~/Tata_MicroEdge_Test_Cert/b4cd0e9c-66c6-4bb1-a707-afd2efa21a63.tar

   The tarball contains:

   ```
   net-edge.cert
   net-edge.key
   nex-cloud-tc.cert
   endpoint
   ```

   Notes: endpoint uses port 8882

5. Provision MicroEdge

   On the device, on the directory where the contents of b4cd0e9c-66c6-4bb1-a707-afd2efa21a63.tar and clrsc_example_command_key.pem are located, run the following command:

   ```
   emspark_meprovision -i 683a6d68-eb56-4c44-8ccb-db107a45f24b -c net-edge.cert -k net-edge.key -e endpoint -p publicKey.pem
   ```

where

- b4cd0e9c-66c6-4bb1-a707-afd2efa21a63 is the Device Id and corresponds to the Common Name (CN) in net-edge.cert.
- net-edge.cert is the Day0 x509 certificate file.
- net-edge.key is a key to store in the TEE.
- net-edge.key is the Day0 key file.
- publicKey.pem is an output file used to register the MicroEdge device in the SecEdge cloud.

And then, run the following command:

```
emspark_meprovision -m add-ca -c nex-cloud-tc.cert -k clrsc_example_command_key.pem
```

6. Send publicKey.pem to SecEdge contacts

   At this point, the device public key (publicKey.pem) generated in the previous step for the MicroEdge device needs to be added to the SecEdge cloud backend. Usually, customer adds it on the backend using the user's enterprise access to the backend.

   To simplify the step, please send the publicKey.pem to Julia Narvaez <julia.narvaez@SecEdge.com> or Mike Hendrick mike.hendrick@SecEdge.com to add the device.

   Julia Narvaez or Mike Hendrick will send confirmation when the device is registered in the SecEdge cloud backend. Upon receiving confirmation, please to continue with the next step, 5.4.

5.4. RUNNING MICROEDGE

1. Run MicroEdge

   Execute the following commands to export an environment variable to print log to the console and run MicroEdge:

```
export LOG_FILE_CONSOLE=true

microedge --foreground --nosslvalidate --loglevel 6 &
```

The loglevel can take values from 0 to 7.

2. Observe the IPSec tunnel

When MicroEdge connects to day1, check tunnel on device. For example, executing ifconfig or ip a , notice the xfrm interface created by the MicroEdge is listed, e.g.

```
x168034310 Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
      inet addr:10.4.0.6  Mask:255.255.0.0
      inet6 addr: fe80::44fe:9ee0:6d52:17e6/64 Scope:Link
      UP RUNNING NOARP  MTU:1400  Metric:1
      RX packets:1 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1 errors:0 dropped:1 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:84 (84.0 B)  TX bytes:84 (84.0 B)
```

6. TROUBLESHOOTING

Issue: After successful firmware 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	DESCRIPTION
September 23, 2021	1.0	Produced document for release.
October 21, 2021	1.1	Added the STARTING AND USING THE SYSTEM and Troubleshooting sections.
March 4, 2024	2.0	Added MicroEdge content.
April 4, 2024	2.1	Updated MicroEdge installation procedure.