SEQUITUR LABS

# Sequitur Labs Inc.

# IoT Security Suite Kit Descriptions

*For Microchip SAMA5D2*

 | PO Box 1127 | Issaquah, WA 98027 USA | p: +1 425 654 2048 | f: +1 425 654 2051 | www.sequiturlabs.com

# Introduction

Sequitur provides two types of software kits to help customers learn about and implement IoT Security Suite in their products.

1. Software Evaluation Kit for pre-purchase evaluation of the IoT Security Suite
2. Commercial Kit for product development and commercial production

This document describes each of the kits in detail.

# Licenses Associated with the Kits

Sequitur provides two kinds of licenses associated with kits mentioned above. The Software Evaluation Kit has a web based click-through license. The Commercial Kit (sometimes referred to as the Production kit) is covered by a commercial license. See table below:

| Evaluation License | Commercial License |
|---|---|
| Software Evaluation Kit | Production/Commercial Kit |
| Registration required.<br>Free of charge | Registration and payment required. |

# Kit Descriptions

## Software Evaluation Kit

The Software Evaluation Kit includes all components necessary to build a fully functional Linux system on a SAMA5D2 Xplained Ultra rev.B board. Evaluation Kit allows OEMs to do the following:

- Flash the kit to the SAMA5D2 Xplained Ultra rev.B development boards via Secure SAM-BA Loader
- Build Linux applications and use the included security features
- Run examples described in the User Guide that make use of the security features and preloaded keys and certificates
- Test TLS/MQTT connectivity and authentication to Amazon AWS IoT using the generated device certificate

The Software Evaluation Kit includes the following:

- A compressed file containing
  - Assets to load the SAMA5D2 Xplained board with the Evaluation Kit
    - Secure SAM-BA encrypted files (.cip) containing the firmware, bootstrap and Customer Key (Sequitur Lab's Customer Key)
    - Scripts/applets for the Secure Sam-BA Loader needed to flash the test boards
    - Instructions on how to flash the development board using Microchip's Secure SAM-BA Loader (Secure SAM-BA Cypher is not needed)
  - Development Kit – Sequitur's CoreLockr libraries
- Keys and certificates supporting the example applications are included as part of the package. These can also be used to support the development of other test applications. Note that all keys are the same in all evaluation kits and will not provide adequate protection of secrets; they are for evaluation purposes only. The following keys are included:
  - 1 OEM root certificate preloaded (associated private key provided as a file)
  - 1 AWS IoT root certificate
  - 1 OEM private key
  - Key pairs associated with all the preloaded certificates
  - 1 device certificate signed with the OEM root private key and the associated private key needed for TLS mutual authentication with AWS IoT. This certificate is regenerated with a new key every time.

    ***Note:*** *The Kit includes instructions on how to create this device certificate supporting the AWS IoT example. In the Production version of the IoT Security Suite this device certificate is created on the fly at in-system provisioning.*
- A User Guide that includes a detailed description of all the components, examples and how to enable all features of the kit.
- Example applications.

## Commercial Kit

The Production Kit contains:

- Full version of the Packaging Tool
- The first part of bootloader code and documentation regarding its completion
- Encrypted CoreTEE and trusted applications in a package
- Linux libraries that the developer needs to include in their own version of Linux to enable CoreTEE
- OpenSSL version and engine plus documentation detailing how to enable the CoreTEE-based OpenSSL engine
- Complete version of Linux (Ubuntu based on Microchip Linux for SAM kernel) + libraries + OpenSSL (as included in the Evaluation Kit). This is intended for customers that do not want to build a different Linux version of their own.
- A User Guide and example applications
- Firmware Update API
- Production provisioning

# Summary Comparison of Capabilities

Table 1 - IoT Security Suite Kit Comparison

| | | Eval Kit | Commercial Kit |
|---|---|---|---|
| Setup | Program the SAMA5D2 Xplained board | ● | |
| | Program on custom SAMA5D2-based board | | ● |
| | Use Linux kernel of choice | | ● |
| | Burn fuses of the SAMA5D2 | | ● |
| Capabilities | Use CoreLockr APIs | ● | ● |
| | Use demo applications | ● | ● |
| | Use TLS mutual authentication with AWS IoT Cloud | ● | ● |
| | Use TLS mutual authentication with the IoT cloud (server) of choice | | ● |
| Application Development | Develop applications in Linux | ● | ● |
| | Use OpenSSL with TrustZone based cryptographic functions | ● | ● |
| | Use hardware-based cryptographic functions | ● | ● |
| Keys & Certificates | Preprogrammed (fixed) keys and certificates | ● | |
| | Inject and use OEM Root Certificate | | ● |
| | Use unique Device Certificate created and signed at programming | | ● |
| | Inject 4 additional symmetric/asymmetric keys | | ● |
| Lifecycle Management | Securely upgrade firmware | | ● |