EmSPARK™ Security Suite

for the

MICROCHIP SAMA5D2 MICROPROCESSOR WITH ARM® TRUSTZONE®

www.sequiturlabs.com

SEQUITUR LABS

All Your IoT Security Needs in One Easy-to-Use Package

Sequitur Labs' EmSPARK™ Security Suite is an integrated software suite that makes it easy to use advanced hardware security and build trustworthy products using the Microchip SAMA5D2 microprocessor with Arm® TrustZone®.

Hardened Security. Simplified.

The EmSPARK™ Security Suite enables rapid and easy use of advanced hardware security technologies, such as Arm® TrustZone® and cryptography, without developers having to undergo a long learning curve. The Suite covers the most common security requirements facing IoT device manufacturers in a single, easy-to-use package.

EmSPARK™ SECURITY SUITE FEATURES

- **Trusted Boot –** Root of trust verified initial startup code, Linux and other embedded software
- **IP Protection –** Encryption of embedded firmware and execution of authenticated firmware
- **Trusted Device ID –** Unique device certificate tied to root of trust for strong identity authentication
- **Secure Storage –** TrustZone-secured cryptography, storage of keys, certificates and in-system data
- **Secure Communications –** Authenticated device pairing and IoT cloud communications (OpenSSL, TLS)
- **Secure Firmware Update –** Remotely upgrade MPU firmware safely and securely

Secure by Design.

IoT products must be secure by design in order to assure device integrity and data fidelity through the life of the device. The ability to isolate and protect critical data is fundamental to securing devices over their lifespan. The EmSPARK™ Security Suite provides the necessary underpinnings to execute critical processes such as storing, encrypting, decrypting, and exchanging keys between devices and applications. It is pre-configured to use available cryptographic resources and provides easy-to-use APIs for application developers; thereby, saving time and labor associated with making use of hardware security.

ACHIEVE SECURE-BY-DESIGN GOALS

- Isolate and protect critical data and functions
- Pre-configured to support hardware security components
- Reduce learning curve with simple APIs
- Reduce cost and time to market for secure products

Solution Capabilities

HARDWARE

Arm® TrustZone®

Hardware Crypto Engines

TRNG

Secure Fuses

Secure SRAM

SOFTWARE

Device Integrity and Firmware Protection

Streamlined Provisioning for IoT Cloud Authentication

Device Pairing and Mutual Authentication

Protect Data at Rest and In Transit

Getting Started

Sequitur Labs gives you multiple options to get you started quickly on the path to building secure devices and applications. The various options are listed below:

LEARN

Evaluation Kit

Evaluation version of EmSPARK™ Security Suite. Write trial applications for:

Secure storage

Secure communications

Payload verification

OpenSSL keystore in TrustZone

Pre-sales support & consultation

DEVELOP

Development Kit

Develop firmware using the EmSPARK™ Security Suite:

Use any Linux environment including peripheral drivers

Build firmware on development board

Enhanced development support – Email support included. Telephone hotline support available for purchase

MANUFACTURE

Production Kit

Final production-ready, fully functional software kit with all the features of the EmSPARK™ Security Suite.

Enterprise license for ONE commercial project with UNLIMITED volumes

Production level support – Email support included. Telephone hotline support available for purchase

SEQUITUR SERVICES

Take advantage of Sequitur Labs' security expertise. From design to implementation, Sequitur's professional services works with you and your team to achieve a secure architecture for your product. Contact us to learn more.

Case Study

PROVISIONING FOR IOT CLOUD AUTHENTICATION

Device Industrial control systems (ICS).

Scenario The ICS collects data from sensors and sends it to a cloud application for analysis.

Threat Hackers can obtain device ID and public cloud certificates to impersonate the device or the cloud.

Requirements

Device credentials and public cloud certificates need to be provisioned and stored securely.

+ Device must contain the proper credentials
+ Credentials must be protected from compromise
+ Device-to-cloud connection must always be secure

What EmSPARK™ Security Suite Does

+ Stores a signed, unique device certificate in the secure enclave (TrustZone) at time of manufacture
+ Stores a public cloud certificate in the secure enclave
+ Isolates crypto engine and key material in secure enclave
+ Presents trusted device cerificate as identity to the cloud
+ Uses TLS to communicate securely to the IoT cloud

The Result

Enables trustworthy provisioning and authentication of devices by the IoT cloud.

SEQUITUR LABS

Sequitur Labs is developing seminal technologies to improve trust in a connected world, reducing the cost and complexity to build secure embedded and IoT devices. Sequitur's products span a range of disciplines required for trusted computing, from boot through the full device lifecycle. Sequitur's security solutions provide real business value to device makers, such as reducing BoM costs, protecting revenue by thwarting IP theft, improving product reliability and reducing liability, and improving device lifecycle management processes. To learn more about Sequitur's security platform, visit us at www.sequiturlabs.com.

Sequitur Labs Inc.,
PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com

MPBEm-0002-Rev B. Printed in the U.S.A.