EmSPARK™ Security Suite

Embedded Security Software Platform

The EmSPARK™ Security Suite is a software solution that makes it easy for IoT device OEMs to develop, manufacture, and maintain secure and trustworthy products.

Device Security is simply not optional any longer. IoT Device developers need to ensure their products are:

- Protected from attacks (supporting secure and known firmware, encryption, and protection of critical intellectual property)
- Safe and secure through the process of manufacturing, software provisioning, and device delivery
- Able to be upgraded, managed, and monitored securely throughout the life of the product

Sequitur's products span a range of disciplines required for IoT devices, from boot through the full device lifecycle.

FEATURES

- Protection of Critical IP (AI/ML Algorithms) at the Edge
- Secure OTA Device Firmware Updates
- Integration of Devices and Security Metrics with Cloud Platforms
- Secure Application Development
- Key and Certificate Management
- Secure Boot
- Secure Manufacturing and Device Provisioning
- Device Resiliency and Failover Protection
- Secure Device Management
- Robust API's for Easy Implementation
- Firmware Packaging Tools

APPLICATIONS

- Secure Gateways
- Building Management Systems
- Industrial Automation & Control
- Medical Devices
- Biometric Readers
- Consumer Products
- Machine Vision
- Voice Recognition
- Video Surveillance
- Process Control
- Energy Management

Secure Update

Firmware and payload authentication

Secure Enclave

secure / non-secure system partitioning TEE included

Piracy/Cloning Protection

Firmware and applications locked to each board

Secure Boot

Encrypted and signed boot from ROM to Linux Kernel

Secure Provisioning

Arrow provisioning service

- **Protect** device-resident software including ML/AI assets at the edge
- **Isolate, protect** security credentials to prevent device compromise
- **Prevent** supply chain compromises with EmSPARK Provisioning Tool and Arrow Provisioning Services
- **Accelerate** time-to-market
- **Reduce** security implementation labor and cost

EmSPARK™ Security Suite Components

CoreTEE™

Sequitur's Trusted Execution Environment (Secure OS) which is required to utilize Arm® TrustZone® and TrustZone secured resources.

Easy to use API's

Easily implements security functions. Allows developers to focus on their application and not on the intricacies of hardware or TrustZone security.

Packaging Tool

Step by step tool that simplifies firmware development and IP protection, abstracting the complexity of secure boot and TrustZone.

Hardware Crypto Engines

TrustZone integrated crypto engine and OpenSSL plugin, accessible in Linux.

In-system Provisioning Procedure and Toolset

Includes anti-replay measures and IP protection.

Get Started

EmSPARK™ is supporting on NXP (i.MX and Layerscape), Microchip (SAMA5D2/SAM-A5D2-SOM1, NVIDIA (Jetson Xavier/Nano/Orin), and ST Micro STM32MP1 platforms. To get started, the evaluation board below is recommended.

Arrow Shield96 Evaluation Kit

Includes:

- 96Board IoT Extended form factor (54mm x 85mm)
- SoC independent open platform specifications
- Microchip SAMA5D27 MPU
- **EmSPARK™ Embedded Security Suite – Preloaded!**

Where to Buy:

- AWS Partner Device Catalog
- www.arrow.com
- SKU Number: HD96_Trusted_Platform

A **FREE** EmSPARK™ Security Suite Evaluation Kit is available at: https://www.sequiturlabs.com/emspark/free-eval-kit/.

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.

PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com