SEQUITUR LABS

EmSPARK™ Security Suite

Data Sheet

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.

By implementing the EmSPARK™ IoT Security suite, enabled by industry-leading processors, device OEMs can:

- Isolate, protect security credentials to prevent device compromise by implementing end-to-end secure boot process, isolating secure functions from normal world assets (ex. Linux Kernel), and managing keys/certificates, sensitive data, and mission-critical applications
- Protect device-resident software including ML/AI assets at the edge
- Prevent supply chain compromises with secure software provisioning and updates
- Accelerate time-to-market while reducing implementation cost

The EmSPARK™ Security Suite supports a range of disciplines required for IoT devices, from boot through the full device lifecycle.

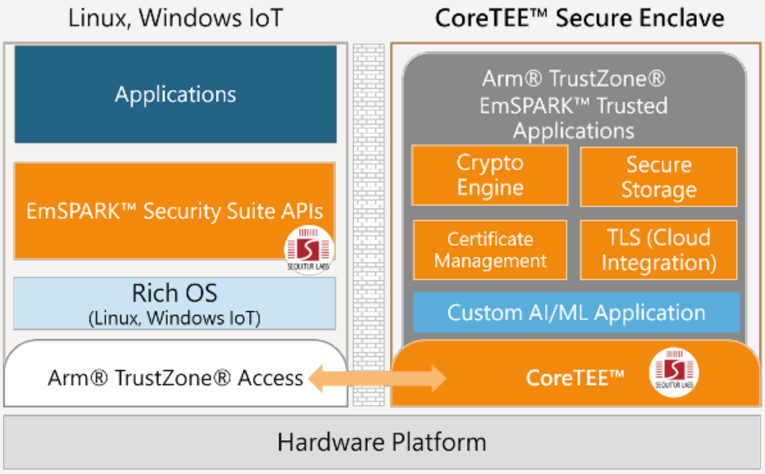
FEATURES

- 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

THE EmSPARK™ SECURITY SUITE

EmSPARK™ uses the ARM® TrustZone architecture to create a safe and secure environment for critical device data and applications. Supporting security functions for encryption, storage, data transmission and key/certificate management are delivered by EmSPARK™ and housed in the secure environment.

EmSPARK™ Enables Trusted Execution of Critical Processes



EmSPARK™ SECURITY SUITE LICENSE PACKAGES

		BASE	ADVANCED
FEATURES	Secure Bootloader	●	●
	Secure Updates Tool	●	●
	Firmware Packaging & Software Provisioning Tool	●	●
	Crypto, Key Mgmt, Storage, OpenSSL APIs		●
	Crypto, Storage & Certificate Mgmt Trusted Applications		●
	Cloud Integration Tools (TLS TA & API, Opaque keys and payloads, AWS & Azure Client Examples)		●
	Normal World IP Protection Trusted Application		●
BENEFITS	End-to-End Secure Boot	●	●
	Secure Over-the-Air Firmware Updates	●	●
	Secure Device Failure Recovery	●	●
	Secure Software Provisioning during Manufacturing	●	●
	Application Access Control		●
	Application Encryption		●
	Secure Data Storage		●
	AI/ML Protection		●
	Support for Custom Application Development		●
	Access to Deep Device Metrics		●
	Pre-loaded Cloud Integration		●

EmSPARK™ SECURITY SUITE TOOLBOX

COMPONENT	DESCRIPTION
CoreTEE™ SECURE OPERATING SYSTEM	Trusted Execution Environment (TEE), utilizing ARM® Trustzone® and Trustzone Secured Resources.
CoreLockr™ SECURITY ASSETS	**Trusted Applications** with pre-packaged security functions + **Crypto** (robust suite of encryption engines) + **Certificate Management** (Generation and maintenance of keys and certificates) + **Storage** (Encryption and restricted access to critical data) + **Transport Layer Security (TLS)** for secure chip-to-cloud mutual authentication data transfer **APIs** for easy integration + **Crypto** + **Certificate Management** + **Storage** + **Transport Layer Security (TLS)** + **OpenSSL Integration** + **Payload Verification** **Code Examples** for accelerated software development. Includes Linux patches for CoreTEE™.
SECURE BOOT LOADER	Complete secure boot process from power on through loading, verification, and decryption of all device applications.
FIRMWARE PACKAGING TOOL	Server-based utility for combining firmware components into a single payload for provisioning and updates.

EmSPARK™ SECURITY SUITE SDK

Software Developer's Kit for integration of customer-developed Trusted Applications (ex. AI/ML Algorithms).

EmSPARK™ SECURITY SUITE SUPPORT

Maintenance releases, bug fixes and technical support.

TECHNICAL SPECIFICATIONS

MEMORY REQUIREMENTS	PROCESSING REQUIREMENTS	OTHER REQUIREMENTS
RAM	**NVM (FLASH)**	**CRYPTOGRAPHY ALGORITHMS**
Minimum: 10MB (8MB Secure, 2MB shared)	**1MB** For Boot, CoreTEE™, U-Boot (Per Stack)	AES RSA DES ECDSA ECDH DH DSA HMAC
Typical: 40MB (32MB Secure, 8MB Shared)	**32-64 MB** Linux Kernel (Per Stack)	

HARDWARE DEVELOPMENT PLATFORMS

PLATFORMS & PRODUCT/ORDERING INFO

ARROW SHIELD96 TRUSTED BOARD

The Shield96 Board, based on Microchip silicon, available pre-loaded with the EmSPARK™ Security Suite by Sequitur Labs, provides a secure platform applicable across all IoT verticals to enable secure devices and protect firmware, keys and data throughout the lifecycle of a product.

AVAILABLE ON

Arrow.com: HD96_TRUSTED_PLATFORM

SUPPORTED SoC & SOM PLATFORMS

PARTNERS & PLATFORMS

NXP SEMICONDUCTORS	MICROCHIP	NVIDIA	ST MICRO
i.MX (6/7/8) Layerscape	SAMA5D2 / SAMA5D2 SOM	Jetson Xavier Jetson AGX Orin	STM32MP1 Series

SUPPORTED CLOUD PLATFORMS

PARTNERS & PLATFORMS

AMAZON WEB SERVICES	MICROSOFT
AWS IoT Core	Azure IoT

EMSPARK™ SECURITY SUITE

EVAL KITS & PRICING

FREE EVALUATION KIT	PRICING
Available HERE	Contact Us