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.

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.

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

EmSPARK™ Security Suite APIs

<table>
<thead>
<tr>
<th>Linux, Windows IoT</th>
<th>CoreTEE™ Secure Enclave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Arm® TrustZone®</td>
</tr>
<tr>
<td>Open SSL</td>
<td>EmSPARK™ Trusted Applications</td>
</tr>
<tr>
<td>Rich OS (Linux, Windows IoT)</td>
<td>Secure Storage</td>
</tr>
<tr>
<td>Arm® TrustZone® Access</td>
<td>Certificate Management</td>
</tr>
<tr>
<td></td>
<td>CoreTEE™ (TLS, Cloud Integration)</td>
</tr>
<tr>
<td></td>
<td>Custom AI/ML Application</td>
</tr>
</tbody>
</table>
### COMPONENT

<table>
<thead>
<tr>
<th>CoreTEE™ SECURE OPERATING SYSTEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Execution Environment (TEE), utilizing ARM® Trustzone® and Trustzone Secured Resources.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CoreLockr™ SECURITY ASSETS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Applications with pre-packaged security functions</td>
<td></td>
</tr>
<tr>
<td>+ Crypto (robust suite of encryption engines)</td>
<td></td>
</tr>
<tr>
<td>+ Certificate Management (Generation and maintenance of keys and certificates)</td>
<td></td>
</tr>
<tr>
<td>+ Storage (Encryption and restricted access to critical data)</td>
<td></td>
</tr>
<tr>
<td>+ Transport Layer Security (TLS) for secure chip-to-cloud mutual authentication data transfer</td>
<td></td>
</tr>
<tr>
<td>APIs for easy integration</td>
<td></td>
</tr>
<tr>
<td>+ Crypto</td>
<td></td>
</tr>
<tr>
<td>+ Certificate Management</td>
<td></td>
</tr>
<tr>
<td>+ Storage</td>
<td></td>
</tr>
<tr>
<td>+ Transport Layer Security (TLS)</td>
<td></td>
</tr>
<tr>
<td>+ OpenSSL Integration</td>
<td></td>
</tr>
<tr>
<td>+ Payload Verification</td>
<td></td>
</tr>
<tr>
<td>Code Examples for accelerated software development. Includes Linux patches for CoreTEE™.</td>
<td></td>
</tr>
</tbody>
</table>

### 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

RAM
Minimum:
10MB
(8MB Secure, 2MB shared)

Typical:
40MB
(32MB Secure, 8MB Shared)

PROCESSING REQUIREMENTS

NVM (FLASH)
1MB
For Boot, CoreTEE™,
U-Boot (Per Stack)

32-64 MB
Linux Kernel (Per Stack)

OTHER REQUIREMENTS

CRYPTOGRAPHY ALGORITHMS

AES
RSA
DES
ECDSA
ECDH
DH
DSA
HMAC

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
i.MX (6/7/8)
Layerscape

MICROCHIP
SAMA5D2 /
SAMA5D2 SOM

NVIDIA
Jetson Xavier

SUPPORTED CLOUD PLATFORMS

PARTNERS & PLATFORMS

AMAZON WEB SERVICES
AWS IoT Core

MICROSOFT
Azure IoT

EMSPARK™ SECURITY SUITE

EVAL KITS & PRICING

FREE EVALUATION KIT
Available HERE

PRICING
Contact Us