Five Years Out

Shield96

Advanced Hardware Security for IoT – At Scale

IoT developers are very concerned with the security and data privacy of IoT solutions. In conjunction with security as a priority, skills gaps are highlighted as a struggle and having a security platform where security has been baked in from the beginning to make it more accessible and easier to implement is critical.

The “Shield96” Board based on Microchip silicon available preloaded 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.

EmSPARK is the essential software companion suite complementing the Microchip hardware providing a cost-effective solution appropriate for every connected device built with the ATSAMA5D2 processor. Engineers can leverage this solution for digital transformation built on trust extracting the full value of the advanced embedded security features of the ATSAMA5D2 MPU.

Out of the box the firmware implements a secure boot chain from ROM to the Linux kernel, diversified devices and a secure enclave using TrustZone/TEE abstracted through an easy to use SDK.

Firmware includes example code, applications and documentation.

Features/Benefits

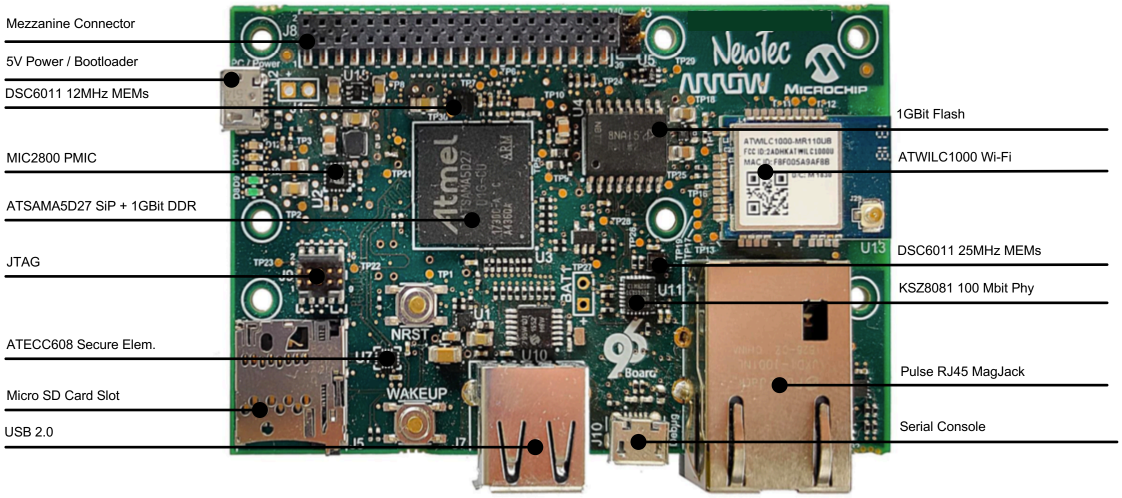
> Secure firmware update
> Secure storage
> Tamper detection
> Managed key store and certified authority store
> Unique device ID, immutable, bound to the Hardware Root of Trust (HWRoT)
> Crypto engine in secure domain with OpenSSL adaptor

Firmware Management as a Service

> Hosted on cloud platform
> Secure provisioning
> Secure updates
> Secure decommissioning

Firmware Management as a Service

> AWS IoT Core ready
> Pre-provisioned credentials
> Arm® Mbed™ TLS with secure crypto



MICROCHIP

SEQUITUR LABS

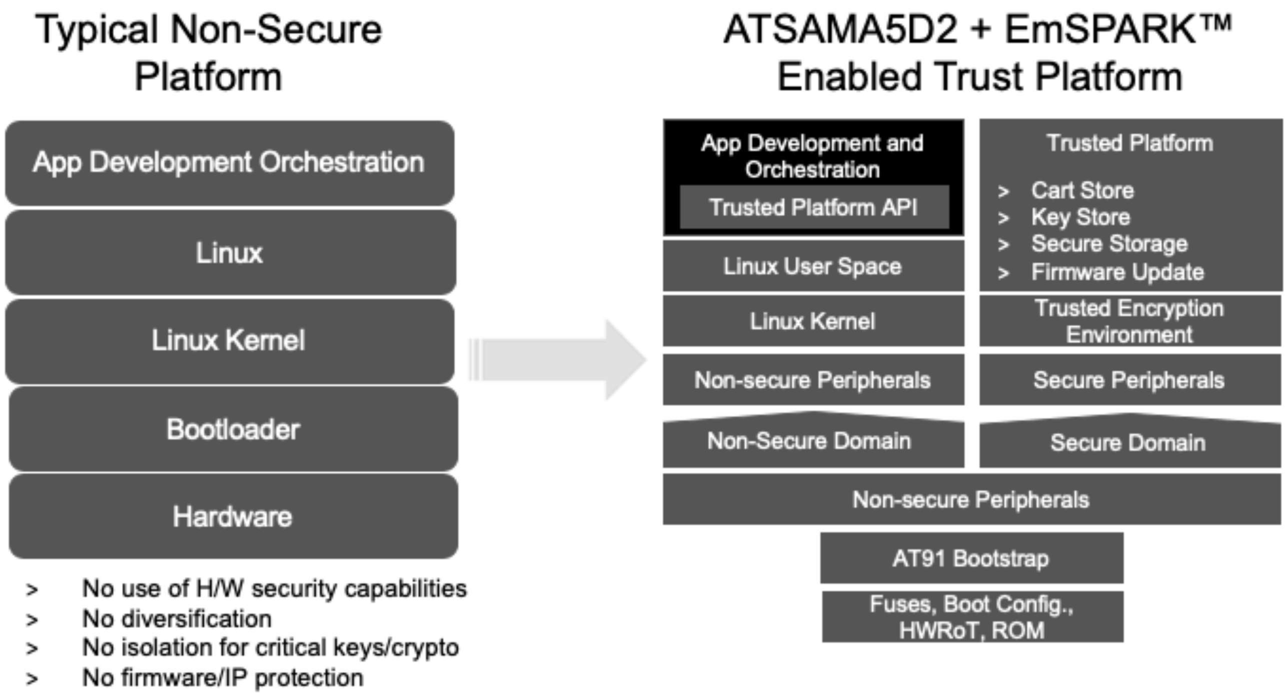
NewTec
System-Entwicklung und Beratung

96Boards

Five Years Out

Purchase Now GitHub Page

Shield96


Typical Non-Secure Platform

App Development Orchestration

Linux

Linux Kernel

Bootloader

Hardware

- > No use of H/W security capabilities
- > No diversification
- > No isolation for critical keys/crypto
- > No firmware/IP protection

ATSAMA5D2 + EmSPARK™ Enabled Trust Platform

App Development and Orchestration

Trusted Platform API

Linux User Space

Linux Kernel

Non-secure Peripherals

Non-Secure Domain

Trusted Platform

- > Cart Store
- > Key Store
- > Secure Storage
- > Firmware Update

Trusted Encryption Environment

Secure Peripherals

Secure Domain

Non-secure Peripherals

AT91 Bootstrap

Fuses, Boot Config., HWRoT, ROM

Customization Services

Shield96 is designed for pre-production purposes and can be used for proof-of-concept development and testing. Arrow can help create customized production-ready systems, with the following services:

- > Preload “Custom TA” trusted application
- > Customized hardware/software to meet security needs and environmental requirements
- > Bespoke application development for mobile, desktop or web
- > Scalable cloud or self-hosted analytics and dashboard development
- > Automated Secure Provisioning Service at scale

Current Security Obstacles for Customers

Introducing embedded security comes with challenges such as skill and experience gaps. Taking to market a product with security onboarded requires firmware to be provisioned securely in volume, fuses to be burned, keys to be managed for the lifecycle of the product. EmSPARK Suite covers the gaps, streamlines the transformation and cuts the time to market by at least 6 months.

Market Demands and Trends

The current focus for strong security in the Internet of Things (IoT) industry is the use of hardware security or embedded security. Keeping cost under control is crucial for the success of all businesses, therefore selecting the proper MPU/board and fully utilizing its capabilities is critical. The ATSAMA5D2 incorporates all the needed security features for applications like electronic payments to all IoT verticals. To utilize its full capabilities the ATSAMA5D2 requires well designed software that addresses the entire lifecycle from development through manufacturing and into operation.

ORDERING INFORMATION:

- Preloaded with EmSPARK Security Suite HD96_Trusted_Platform
- Virgin board HD96_Standard