Spartan: AWS IoT

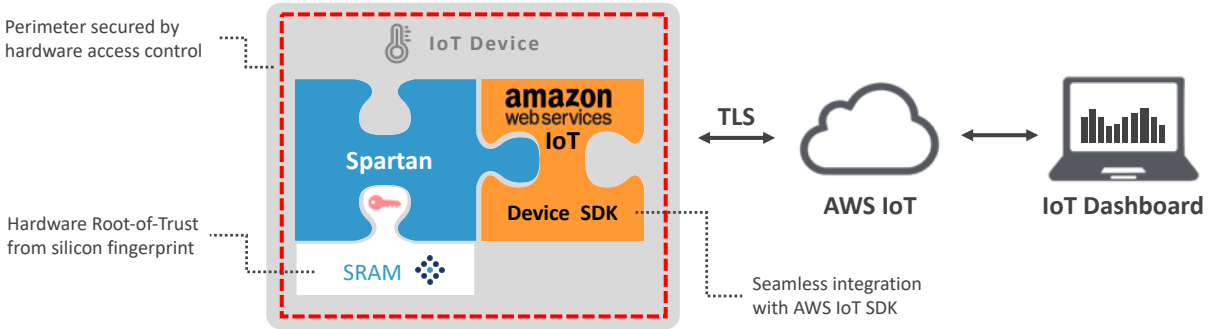
In the vastly growing Internet of Things it is increasingly important that devices and data can be trusted. Spartan is a family of software modules for authenticating chips to each other and to networked services. The Spartan products extract device-unique unclonable keys from the uniqueness that is inherent to every piece of silicon. These keys give microcontrollers and other semiconductors device-unique unclonable identities which serve as root-of-trust in the ecosystem.

Intrinsic ID's Spartan is the world's first security software for IoT devices that combines SRAM Physical Unclonable Function (PUF) technology with elliptic curve key agreement.

SRAM PUF-based Authentication SW Module for IoT devices

Intrinsic ID's Spartan is a security software for IoT devices that combines SRAM Physical Unclonable Function (PUF) technology with elliptic curve key agreement. It allows IoT designers to provision their products with secure keys and platform-compliant certificates in a scalable and cost-efficient way. These assets are needed to set up a mutual authentication session upon connection with the cloud platforms like AWS IoT. Authentication requires generation of a device-unique private key that must remain private and secured for the entire life of the device, from manufacturing to end-of-life. By using Spartan, the unclonable private key is generated on the device and reconstructed when needed. It is never stored nor exposed and not visible when the device is powered off.

The Spartan AWS-IoT embedded software module can be added to IoT devices at any stage in the production process and is portable to any CPU or operating system. No hardware customization is needed and retrofitting existing devices is possible.



SRAM PUF Benefits

- Uses standard SRAM
- Device-unique, unclonable keys
- No secrets reside on the chip

Ideal for the IoT

- Industrial
- Automotive
- Health
- Wearables
- Smart grid
- Home

Benefits

- Seamless integration of security into any IoT product – More flexible than adding a SE
- Lower TCO: no need for a separate crypto chip on the device
- Internally generates private keys – solves the sensitive key handling problem
- Tamper-resistant, device-unique unclonable keys that are not stored and never exposed
- Hardware-based security – In line with the strategic principles of the U.S. Department of Homeland Security for securing the IoT
- No human intervention required; automatic onboarding to the web service upon initial connection
- Portable to virtually all CPUs, operating systems, and platforms

Embedded Authentication Module

The Spartan embedded authentication module enables mutual authentication upon connection with AWS IoT. It contains a crypto library and an SRAM PUF key generation module that generates a device-unique private key (ECC NIST P256 curve) from the SRAM in the chip. The Spartan library provides an API to applications in conjunction with the cloud service connection library. Running Spartan on the CPU of a device sets up an authenticated TLS connection with the cloud platform based on its device-unique key. The private key never leaves the security perimeter and is not visible when the device is powered off.

Key Features

- Seamless integration with Amazon Web Services IoT SDK
- Keeps private key secure
- Strong authentication based on an unclonable device-unique key established from SRAM PUF
- Well-defined security boundary within the chip
- Connects to third-party TLS library (e.g. embed TLS)

Use Cases

- Strong IoT Node Security and ID – Device-unique authentication of IoT end-node to the web service
- Anti-Counterfeiting – Ensures only OEM/licensed nodes (and accessories) work
- Anti-Cloning – Prevents building with identical BOM or stolen code
- Message Security – Authentication, message integrity and confidentiality of network nodes)

Deliverables

- Spartan authentication library (embedded SW): compiled for a specific target CPU and specific connected TLS library
- Intrinsic ID's BroadKey-Pro for device-unique key generation and secure storage, based on SRAM PUF technology
- Certificate generation tool that can be run on Windows/Linux server for setting up device identity certificates. Optionally it connects to an external Certificate Authority such as GlobalSign
- Cloud Authentication Control Tool (Operator/Service Provider) - Optional

Requirements

- 2KB of uninitialized SRAM memory available on the chip
- The ability to run cloud connection software (e.g. MQTT or Pub/Sub) with supporting TLS security library

* Operation with other clouds like Microsoft Azure IoT Hub, and the Google Cloud Platform available upon request.