Quantum Secure Boot (Add-On)

Advanced post quantum solution for IoT secure root of trust, firmware authentication, integrity and safety, and software lifecycle update.

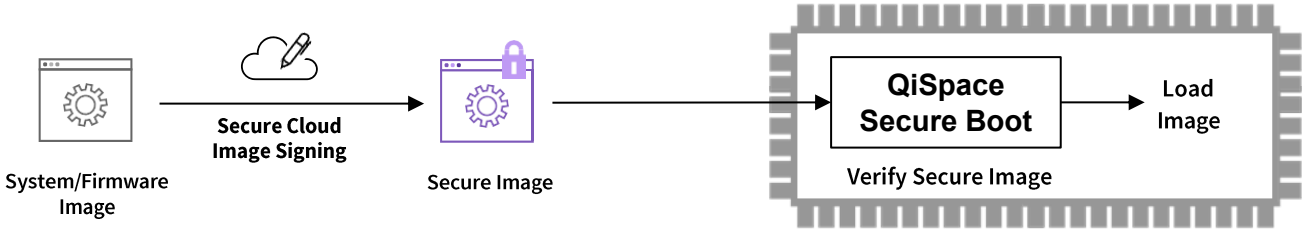
QiSpace™ for IoT Secure Boot Add-on

The QiSpace™ for IoT Secure Boot Add-on provides a quantum-secure Root of Trust that validates system images and prevents unauthorized software execution. Uniquely engineered for resource-constrained embedded systems, it provides the crypto-agility to seamlessly switch algorithms based on your specific security and performance requirements. It is available in 2 formats:

PQC Enhanced MCUboot

A flexible, standalone implementation for standard RTOS environments, providing an easy migration path for existing MCUboot users.

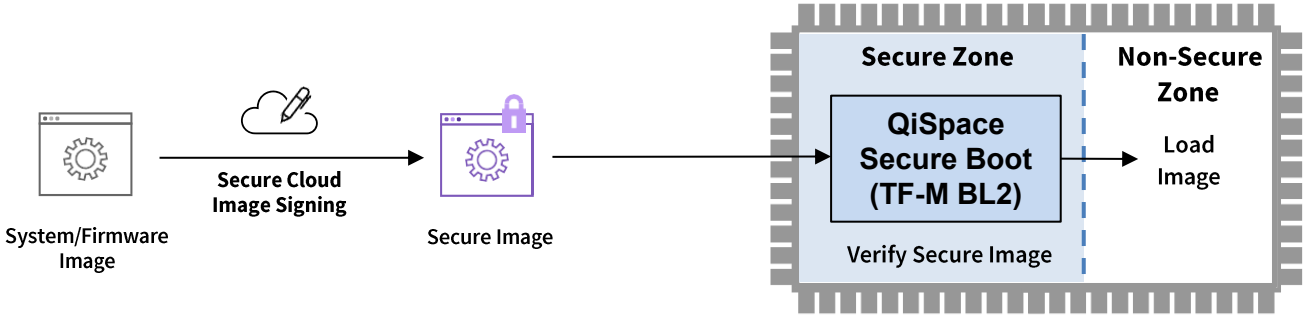
- **Easy Upgrade Path**: Drop-in compatibility for standard MCUboot environments.
- **Universal Compatibility**: Ideal for non-TrustZone or non-TF-M designs that still require NIST-standard PQC.
- **Performance First**: Maintains the familiar MCUboot workflow while adding PQC for image signing/validation.



TF-M Enabled

A hardware-isolated, PSA-supporting implementation for Arm TF-M designs providing an integrated quantum-secure BL2.

- **Integrated BL2**: Acts as the secure handoff between hardware resets and the TF-M Secure Zone
- **TrustZone Isolation:** Shields PQC algorithms and keys in a hardware-protected execution environment.
- **Accelerated PSA Compliance:** Streamlines the path to meeting Arm PSA Root of Trust requirements.



Unified Secure Lifecycle Management

Both formats leverage a common high-security infrastructure to simplify deployment:

- **Supports Secure Cloud Image Signing:** An online service that replaces risky offline tools with automated, audit-ready signing workflows.
- **Secure OTA Updates:** A robust framework to push signed, encrypted firmware updates remotely while maintaining end-to-end integrity.

quantropi

Key Features

- TF-M Enabled and optimized for BL2
- Easy upgrade path for MCUboot implementations
- Full image encryption, authentication, and code signing.
- Quantum-ready with NIST PQC
- High-Performance with Low-Footprint
- Available strong cryptographic keys derived from quantum random numbers

Advantage for Novel Algorithms

- ✓ Quantropi's novel key exchange (HPPK-KEM) is specifically optimized for IoT solutions with an efficient 64-byte ciphertext size and ~8K of memory utilization at NIST L5.
- ✓ Quantropi's novel digital signature (GHPPK-DS) is specifically optimized for IoT solutions with an efficient 264-byte signature size and less than 11K of memory utilization at NIST L5.

Support for leading MCU Platforms

QiSpace™ for IoT supports chipsets from leading vendors ranging from high-performance down to ultra-low-power MCUs. Current supported chipsets include:

- STM32 Cortex M Series MCU
- STM32 Cortex M Series MPU
- Legacy Arm Processors
- SPC5 32-bit Automotive
- Stellar 32-bit Automotive

- RA Cortex M Series MCU
- RL Low Power Series
- RX 32-bit
- RZ 32/64-bit Multicore MPUs
- RH850 Automotive Series MCUs
- RISC-V Processors

- PIC32 Cortex M Series MCU
- SAM Cortex M Series MCU
- Legacy Arm Processors
- RISC-V Processors
- AVR32

Availability and OS Support

The QiSpace™ for IoT Secure Boot Add-on is available for Baseline and Premium SDK packages.

The Baseline Add-on includes:

- NIST PQC standards

The Premium Add-on includes Baseline features and:

- Quantropi novel PQC
- Quantropi TRNG

OS Support includes:

Zephyr, FreeRTOS

Contact Us:
sales@quantropi.com
www.quantropi.com

Try QiSpace™ for IoT