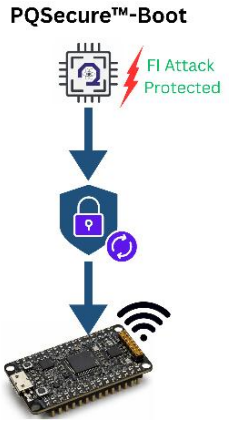
PQSecure™-Boot: Quantum-Safe Secure Boot for Hardware and Software Platforms

PQSecure™-Boot is designed for constrained Root-of-Trust environments, combining verify-only optimization, low footprint, and multi-algorithm quantum-safe authentication and attestation.

✅ Quantum-safe secure boot (ML-DSA, LMS, SLH-DSA) • ✅ SW (C/Rust) and HW implementations • ✅ High-performance, low-latency verification • ✅ Ultra-low footprint (<5KB RAM) • ✅ Fault injection resistant design • ✅ Formally verified

Product Overview



PQSecure™-Boot is PQSecure's quantum-safe secure boot product family, designed for embedded systems, microcontrollers, FPGAs, ASICs, and Root-of-Trust architectures. It is available in both **hardware** and **software** implementations to support a wide range of deployment needs. The PQSecure™-Boot family includes:

- **PQSecure™-Boot-HW**: hardware IP for silicon, FPGA, SoC, and secure enclave integration
- **PQSecure™-Boot-SW**: software libraries for embedded processors, bootloaders, and FW

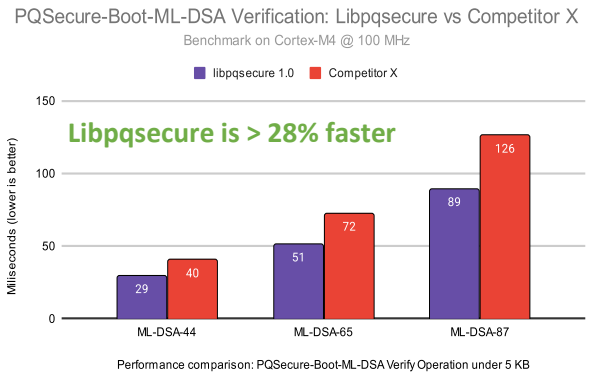
Both offerings support **ML-DSA (FIPS 204), LMS (RFC 8554), and SLH-DSA (FIPS 205)** for quantum-safe authentication of firmware, boot images, and software updates compliant with NIST FIPS and CNSA 2.0.

Secure boot is the foundation of trust in modern connected systems. **PQSecure™-Boot** helps ensure that only authentic and authorized firmware or operating system images are executed during startup. **PQSecure™-Boot** gives device manufacturers and platform integrators a flexible path to deploy post-quantum secure boot in either software or hardware, depending on their system requirements, performance targets, and trust architecture. With support for both **hardware IP** and **software libraries**, PQSecure™-Boot is well suited for embedded devices, IoT products, secure processors, FPGA prototypes, ASIC implementations, and long-lifecycle platforms in defense, aerospace, automotive, and industrial systems.

PQSecure™-Boot-SW

PQSecure™-Boot-SW is a lightweight software implementation for quantum-safe secure boot on embedded processors and constrained devices. It is designed for integration into bootloaders, firmware stacks, and trusted software environments where memory footprint and boot-time latency are critical. Key benefits include:

- Compact implementation available in both **C** and **Rust** under 5KB RAM
- Flexible software deployment on existing processor platforms
- Support for ML-DSA, LMS, and SLH-DSA verification flows
- Well suited for secure boot, firmware verification, and secure update
- NIST ACVP certified and PSA Certified APIs for all the algorithms
- Protection against **fault injection (FI) attacks** to avoid bypass FW verification

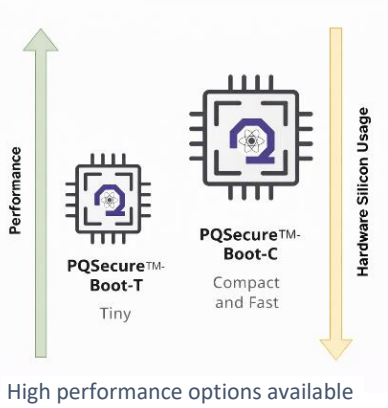


Performance comparison: PQSecure-Boot-ML-DSA Verify Operation under 5 KB

PQSecure™-Boot-HW

PQSecure™-Boot-HW is PQSecure's hardware IP implementation for quantum-safe secure boot in ASICs, FPGAs, SoCs, secure enclaves, and Root-of-Trust subsystems. It provides dedicated hardware-based firmware authentication for customers who need compact area, efficient performance, and strong integration into silicon trust architectures. ML-DSA, LMS, and SLH-DSA are available under the PQSecure™-Boot-HW product family (with SHA2 or SHA3 variants), enabling flexible post-quantum secure boot across a wide range of embedded and silicon platforms.

PQSecure™-Boot-HW delivers compact and efficient quantum-safe secure boot acceleration for hardware Root-of-Trust environments. With support for ML-DSA, LMS, and SLH-DSA, integrated hashing options, flexible memory architectures, and high operating frequency, it is designed for practical post-quantum firmware authentication across ASIC, FPGA, and SoC deployments. A tiny example configuration includes an ML-DSA-87 verify-only accelerator with an integrated SHA3 engine, targeting under 35 kGE (synthesized in 65 nm), supporting 500+ MHz depending on ASIC technology, and offering 32-bit and 64-bit SRAM architectures.



High performance options available

- Supports for ML-DSA, LMS and SLH-DSA compliant with FIPS and certified under ACVP
- **Hardware-based secure boot verification** for Root-of-Trust and secure enclave architecture
- **PQSecure™-Boot-HW Tiny** occupies under 35 kGE target in 65 nm operating above 500 MHz on target technology
- Flexible deployment across ASIC, FPGA, and SoC platforms with major configurations ready
- Optional protections against **fault injection attacks** that could bypass firmware verification

sales@pqsecurity.com