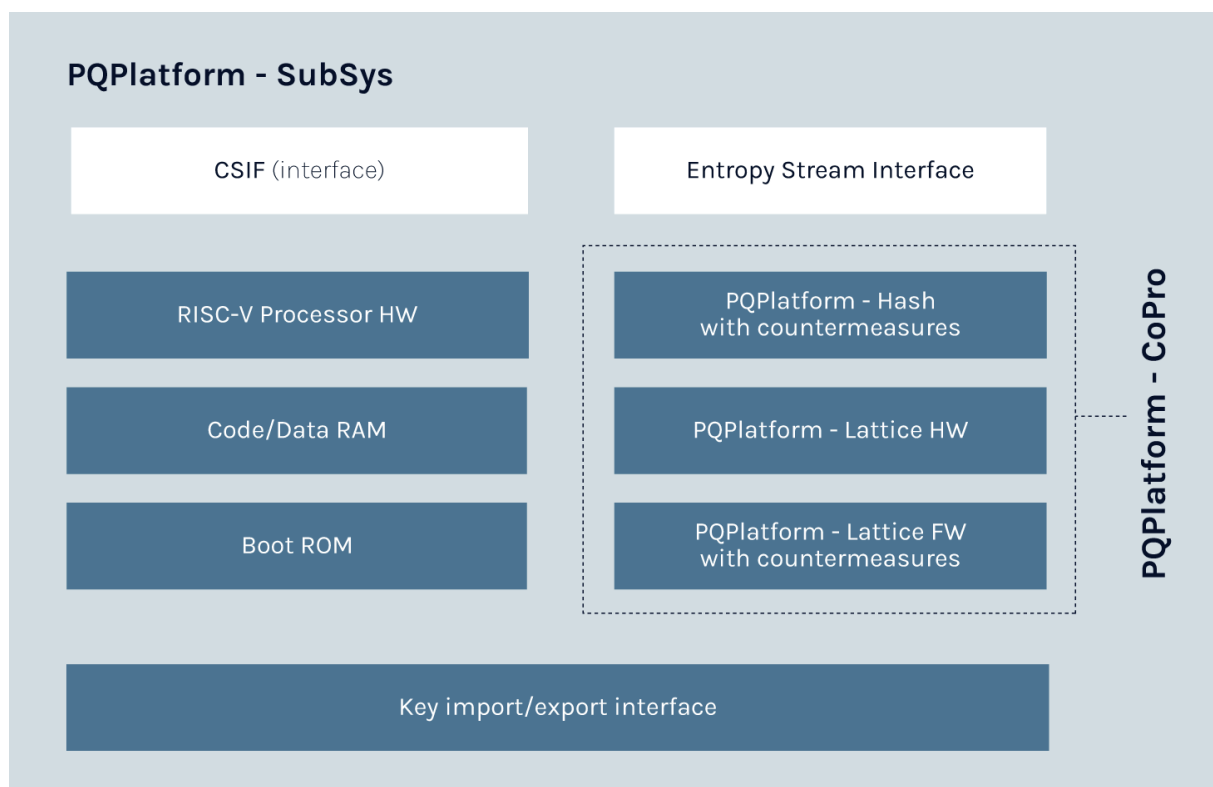


PQPlatform-SubSys

Post-Quantum Security Subsystem

PQPlatform-SubSys is a complete cryptographic subsystem, providing services including post-quantum signature generation, verification, and secure key establishment. It combines the power of lattice-based and hash-based cryptography, deployed in a self-contained system with a built-in RISC-V processor, allowing cryptographic services to be offloaded and handled by PQPlatform-SubSys.

- Optional side-channel security (SCA) for post quantum cryptographic algorithms
- Hardware interfaces for secure key import/export
- PQShield’s supplied firmware, running inside PQPlatform-SubSys
- Firmware driver running on customer CPU (delivered as C source code)



Key Features and Parameters: PQPlatform-Subsys

- Key Encapsulation
 - NIST FIPS 203 ML-KEM (512, 768, 1024)
 - NIST SP 800-56A
- Digital Signatures
 - NIST FIPS 204 ML-DSA (44,65,87)
- HASH Algorithm support including
 - AES and Advanced SHA ongoing
 - XMSS (verification)
 - LMS (verification)
 - SHA-2 HW support
 - NIST FIPS 180-4
 - NIST FIPS-202 SHA3-256/384/512
 - NIST FIPS-202 SHAKE128 and SHAKE256
- NIST FIPS 186-4 and 186-5 compliant
- ANSSI X9.142-2020 compliant
- Key Management
 - Secure Key Import and Export
- Firmware Update
 - Support for Secure Firmware download to update functionality
- All cryptographic algorithms are timing side-channel resistant
- Optional non-invasive side-channel (power, EM) attack countermeasures for PQC (post-quantum cryptography) algorithms
- Ease of Integration : PQPlatform-SubSys uses industry-standard AXI interfaces allowing simple integration in typical systems

Size Requirements

Config Information	IP Area
Typical configuration (GF12LP)	~320Kgte

Performance Expectations

Algorithm	Security Level	Max Performance (cycles)
ML-KEM Key generation	ML-KEM-512	500K
ML-KEM Encapsulation	ML-KEM 512	700K
ML-KEM Decapsulation	ML-KEM 512	1M
ML-DSA Key generation	ML-DSA 44	1.2M
ML-DSA Signing	ML-DSA 44	5.25M
ML-DSA Verification	ML-DSA 44	270K

PQS RISC-V Processor HW

The RISC-V CPU controls the operation of PQPlatform-SubSys.

Entropy Stream Interface

The Entropy Stream Interface is the hardware interface through which entropy (random number generation) is delivered to the subsystem. This entropy is used in cryptographic operations, such as key generation.

PQS Coprocessor

PQPlatform-CoPro is PQShield's post-quantum cryptographic coprocessor. It is used within PQPlatform-SubSys to perform post-quantum cryptographic operations.

Working memory is accessed via the PQRAM AXI4-Lite memory interface.

PQS Cryptographic Service Interface (CSIF)

The Cryptographic Service Interface (CSIF) is the interface used by the host system to control PQPlatform-SubSys and to request cryptographic services.

PQPlatform-Subsys Memories

The Boot ROM contains the initial set of services, including standard firmware verification functions. PQPlatform-SubSys also contains private instruction and data RAM, which is used by the control CPU.

PQShield Hardware IP

The following table shows how PQPlatform-SubSys compares to PQShield’s security suite.

Hardware IP		Description
PQP-HW-SUB	PQPlatform-SubSys	Self-contained cryptographic subsystem designed for PQC + classical, minimal integration effort, with SCA protection
PQP-HW-LAT	PQPlatform-Lattice	Lattice-based post-quantum Processing Engine
PQP-HW-HBS	PQPlatform-Hash	Hash-based post-quantum hardware accelerator
PQP-HW-COP	PQPlatform-CoPro	Post-Quantum Cryptography Processor, combining Lattice and Hash
PQF-HW-LAT	PQPerform-Lattice	High capacity post-quantum cryptography, designed for high throughput and high speed