Product Brief

R25.1.1 Feb 21, 2025

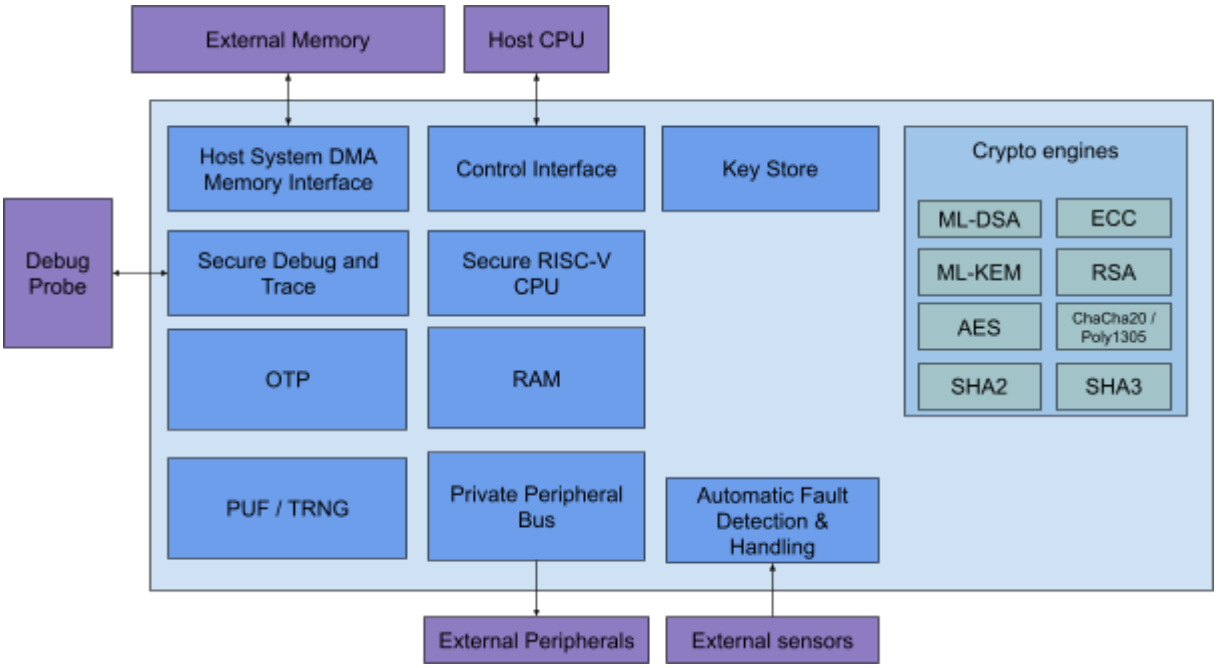
PQPlatform-TrustSys

Post-quantum secure root of trust subsystem

PQPlatform-TrustSys provides a complete Root of Trust solution, providing architects with everything needed to secure systems during, and beyond post-quantum cryptography transition. It is a fully programmable subsystem containing advanced post-quantum cryptography co-processors, bulk encryption and hashing accelerators, together with support for legacy classical cryptography based on ECC and RSA.

PQPlatform-TrustSys can be configured with advanced fault tolerance and power/EM side-channel attack countermeasures.

- Industry leading support for the NIST standardized FIPS 203 ML-KEM and FIPS 204 ML-DSA algorithms, including best-in-class secure and efficient side-channel countermeasures.
- Support for ECC and RSA cryptography, essential for supporting hybrid and legacy protocols during PQC transition.
- Advanced accelerators for symmetric cryptography, including AES, SHA2, SHA3, HMAC, and other bulk operations.
- Integrates with third-party OTP, PUF and Entropy Source components, with pre-validated support provided by PQShield.



Key Features

Easy integration:

- Industry standard hardware interfaces for control, debugging, data I/O, and secure key delivery.
- Compatible with multiple OTP, Entropy Source and PUF providers:
  - Allows for reuse of existing licenced components or selection of best available components for specific technology nodes.
  - Pre-verified integrations are supported by PQShield.

Comprehensive Cryptography:

- Post-Quantum Secure Asymmetric Primitives
  - ML-DSA
  - ML-KEM
  - LMS Verification
- Classical Asymmetric Primitives
  - ECDH
  - ECDSA
  - EdDSA
  - RSA
- Symmetric Primitives
  - AES
  - SHA2
  - SHA3 / SHAKE
  - ChaCha20 / Poly1305
  - HKDF
  - HMAC
  - DRBG

Advanced Security:

- Secure key management features
- Configurable power-side channel countermeasures.
- Configurable fault-tolerance countermeasures.
- Hardware level protection of all secrets.
- Physically Unclonable Function (PUF) support for secure root key derivation.

Use Cases

- Device identification and attestation
- Device provisioning
- Secure boot
- Secure firmware update
- Secure product configuration management
- Key storage and management
- Bulk encryption & hashing acceleration
- Secure Debug
- User Authentication/authorization
- User data confidentiality and integrity protection
- Random number generation
- Cryptographic primitives acceleration

How It Works

PQPlatform-TrustSys works as a secure 'island', providing services to the wider system while ensuring that key material is safely stored inside it. Applications use a PQShield provided firmware driver to interface with PQPlatform-TrustSys and perform operations such as key generation, encryption and signature verification. Secrets within the Root of Trust are hardware-protected against logical, timing, and physical attacks.

The firmware API is designed for simplicity and ease of use within customer applications, while the industry-standard hardware interfaces allow quick and easy integration for a faster time to market.

Deliverables

Complete Documentation:

- Hardware Integration Guide
- Firmware User Manual
- Reference Manuals

Source Code Delivery:

- SystemVerilog RTL
- RoT internal firmware
- External driver

Integration Support:

- Hardware Integration Testbench
- System-level Integration Tests
- Standard test vectors for all cryptographic algorithms
- Scripts for running with standard EDA flows
- Tooling for working with the delivered product

PQShield Hardware IP

The following table shows how PQPlatform-TrustSys compares to PQShield's hardware security suite.

Hardware IP		Description
PQP-HW-ROT	**PQPlatform-TrustSys**	**PQC-first, root-of-trust subsystem for foundational security including post-quantum, hash acceleration, bulk encryption and classical support**
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