# Product Brief

PQ CryptoLib Core

## Highly configurable SW PQC Library for Classical, PQC and PQ/T Hybrid on Linux, Windows and Mac

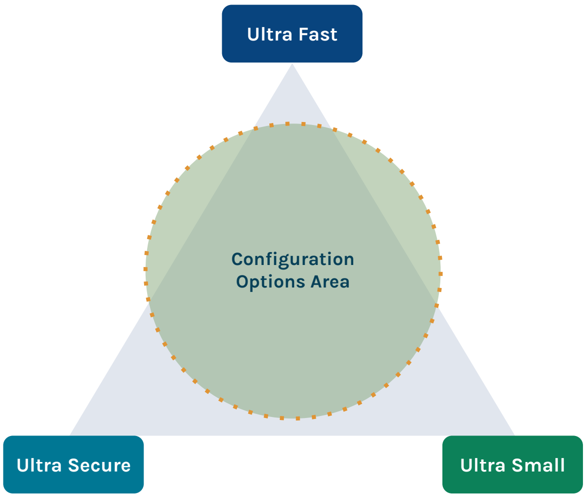
## Overview

**PQCryptoLib-Core** is a FIPS 140-3 CMVP Certified / CAVP Compliant general-purpose cryptographic library, designed for a wide variety of applications.

It provides the latest NIST-standardized post-quantum and PQ/T Hybrid algorithms in a software environment. With a configurable, secure and easy-to-use API, PQCryptoLib-Core is optimized for crypto-agility, particularly when it comes to FIPS-compliant PQ/T Hybrid solutions - built to protect against the threat of 'Harvest Now Decrypt Later' attacks.

PQCryptoLib-Core helps organizations transition smoothly and securely to quantum resistance in a manageable, easy-to-integrate solution.

## Design Space



## Key Benefits

- Plug and play
- Extensions leverage hardware accelerators on mainstream devices
- Documented API - leverages existing hardware accelerators
- Extensive functional and security validation
- Support for CAVP/CMVP compliance paths
- Technical assistance for library integration
- Operation on several OS platforms with a C compiler

## Common Use Cases

- Migration from traditional cryptography to PQC
- Device, app, and user authentication
- Remote attestation
- TLS, SSL, OpenSSL
- Secure key exchange
- Data at rest encryption, integrity and authenticity
- Secure app configuration management
- App personalization
- Secure key provisioning

Contact our experts

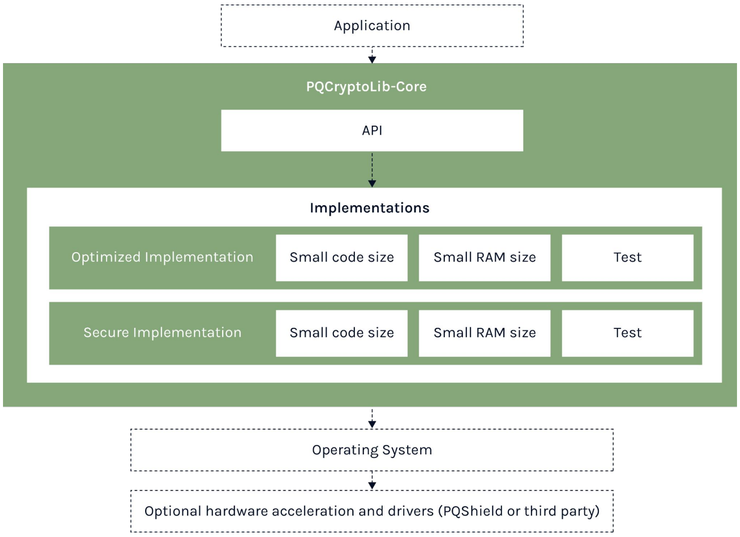
# Product Brief

PQ CryptoLib Core

## Technical Specification

**PQCryptoLib-Core** provides software implementations of PQC algorithms, alongside traditional algorithms. The library supports multiple OS platforms such as Windows, MacOS and Linux, and has been designed for brownfield applications in high assurance systems - cloud infrastructure, networking equipment, and secure applications where either PQ-readiness is required on the field, or where modifying hardware is not an option.

The library exposes a clean, minimal C API that can be integrated with existing implementations of SSL, TLS or custom/standard high-level protocols. PQCryptoLib-Core integrates easily into existing toolchains, accelerating migration to PQC, enabling faster certification and time-to-market for quantum secure applications.



PQShield is a global leader in Post-Quantum Cryptography, with a team of around 90 experts across 11 countries who co-authored the first NIST PQC standards and continue to be major contributors to the industry at large. As a leading authority on real-world PQC implementation who has filed more than 40 patents, PQShield provides high-quality software and hardware IP to the global secure products supply chain.

## Main Features

**Cryptographic algorithms:**

- ML-DSA (FIPS 203)
- ML-KEM (FIPS 204)
- SLH-DSA (FIPS 205)
- XMSS/LMS
- SHA2, SHA3, SHAKE
- ECDH, ECDSA
- Falcon
- FrodoKEM
- HKDF
- HMAC
- HSS

**APIs:**

- Simple API
- Streaming API
- HW acceleration API (for SHA-2 and SHA-3)

## Deliverables

- Documentation
- Sample code
- Prebuilt binary and source code
- Performance benchmark
- Functional test report (includes CAVP execution log)
- Security evaluation reports
  - Constant time
  - Fuzzing

## See also

- PQCryptoLib-SDK OpenSSL integration
- PQMicroLib-Core baremetal PQC library for embedded systems
- Certification and FIPS 140-3
- Discover the UltraPQ-Suite in full
- Visit PQShield's website
- Listen to our Podcast

Contact our experts