Document version	v2.0	Release R24.1	5 Feb 2024

PQSDK

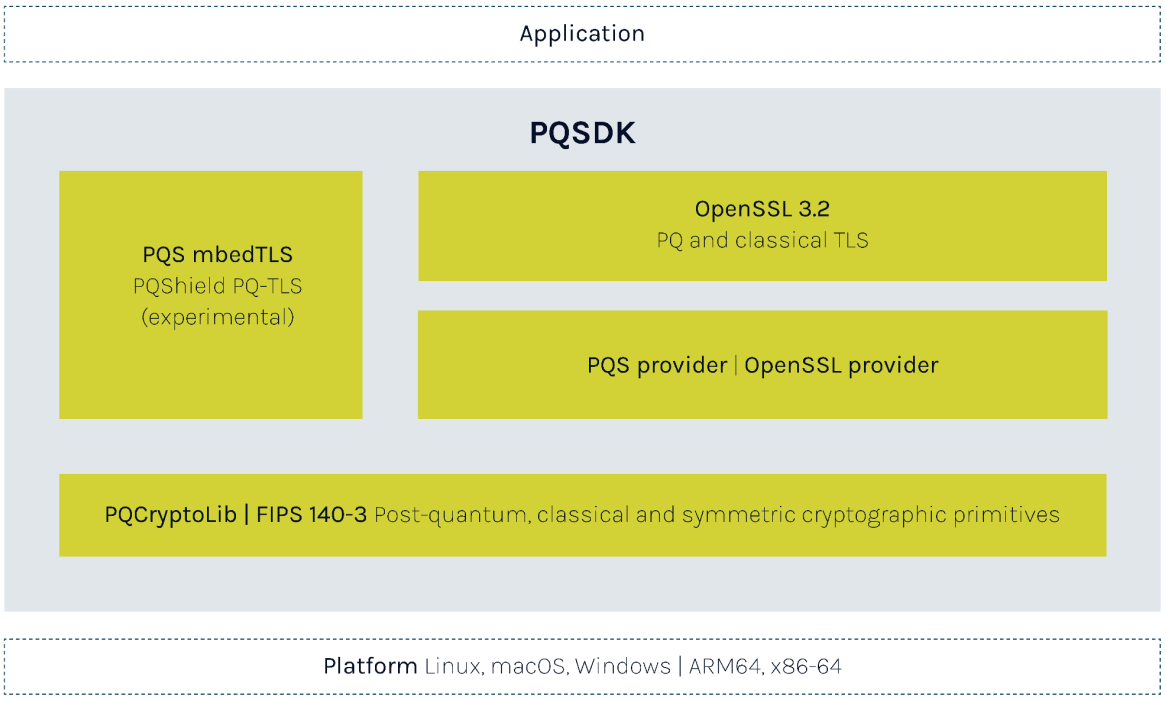
Post-Quantum Software Development Kit (PQS-SW-SDK)

PQSDK provides easy-to-use software implementations of both post-quantum and classical cryptographic primitives. It consists of an integration of PQShield's PQCryptoLib library with two popular high-level cryptography libraries:

- OpenSSL: a widely-adopted secure-communication library.
- mbedTLS: primarily intended for use in embedded system and IoT deployments.

PQSDK enables you to experiment with deployments of PQC (post-quantum cryptography) and to prototype your post-quantum TLS solutions (including TLS X.509) and public key infrastructure management, before progressing to full deployment.

Developers can also use PQSDK's core cryptographic APIs to directly integrate PQC algorithms into their own applications, as shown in the following diagram:



Key Features: PQS Engine and PQS OpenSSL

PQSDK's OpenSSL integration consists of two core PQShield (PQS) components:

- PQS provider - an implementation of the OpenSSL provider API using pure PQC and hybrid (classical plus PQC)
- OpenSSL is v3.2.0+ required as minimum

This enables:

- Post-quantum TLS 1.3
- Post-quantum X.509 PKI support through OpenSSL APIs or binaries
- Further application integrations using OpenSSL's TLS, X.509 and EVP APIs

A complete set of documentation and examples is provided with PQSDK.

Cryptographic primitives

Quantum-resistant primitives are enabled in PQS Provider using the technology in PQCryptoLib, implementing post-quantum key agreement and digital signature algorithms:

- Falcon 512/1024
- FIPS-203 ML-KEM (Kyber) 512/768/1024
- FIPS-204 ML-DSA (Dilithium) 2/3/5

Note: algorithms resistant to time-based side channel attack (with the exception of Falcon)

All existing classical cryptography deployed through OpenSSL continues to be available. Our provider adds to the functionality provided by OpenSSL.

Key Features: PQS mbedTLS

PQSDK includes a direct integration of PQShield's PQCryptoLib into ARM's mbedTLS library version 3.2.1.

This enables:

- Post-quantum TLS 1.3
- Post-quantum X.509 support through mbedTLS's X.509 library

Cryptographic primitives

Quantum-resistant primitives are enabled in PQS mbedTLS using PQCryptoLib technology, implementing post-quantum key agreement and digital signature algorithms:

- Falcon 512/1024
- FIPS-204 ML-DSA (Dilithium) 44/65/87
- FIPS-203 ML-KEM (Kyber) 512/768/1024

Platforms supported (PQS mbedTLS)

- Linux (x86_64 and ARM64)
- macOS
- MS Windows

Use cases: PQSDK

With PQS OpenSSL and the PQS Engine, you can easily integrate PQC support into your applications, developing against existing OpenSSL APIs. Typical PQC migration use cases include:

- Secure communications/TLS
- Public Key Infrastructure/Certificates
- VPN
- Web servers
- User authentication
- Software signing
- Zero Trust architecture (ZTNA)

PQShield has developed a range of demonstration scenarios that illustrate how PQSDK and PQCryptoLib can easily be used to experiment with quantum-resistant solutions. Examples include:

- **Quantum-resistant web browsing**: a modification of the open-source Chromium web browser using PQCryptoLib to support post-quantum and hybrid TLS 1.3 and X.509 certificates.

- **Quantum-resistant web server**: use of PQSDK to develop a quantum-resistant web server using NGINX.

- **Quantum-resistant VPN**: two modifications to popular open-source VPN solutions:

    - OpenVPN: the use of PQSDK to construct a fully-quantum safe TLS-based VPN without having to recompile the VPN library itself. This demonstrator includes a platform security component: the integration of PQCryptoLib into OP-TEE, an open-source Trusted Execution Environment built around ARM's TrustZone technology, providing additional security for the VPN private key.

    - strongSwan: the integration of a PQCryptoLib-based PQC plugin into strongSwan to enable quantum-safe confidentiality using an IPSec-based VPN.

PQShield Software IP

The following table shows how PQSDK compares to PQShield's software security suite.

Software IP	Description
PQSDK / PQS-SW-SDK	**PQShield's software development kit, with interface to TLS (OpenSSL and MbedTLS)**
PQCryptoLib-Embedded / PQS-SW-CLE	Modified cryptography library designed to add PQC capability to microcontrollers, embedded software, or memory-constrained systems.
PQCryptoLib / PQS-SW-CLB	PQShield's generic software library containing post-quantum and classical algorithms