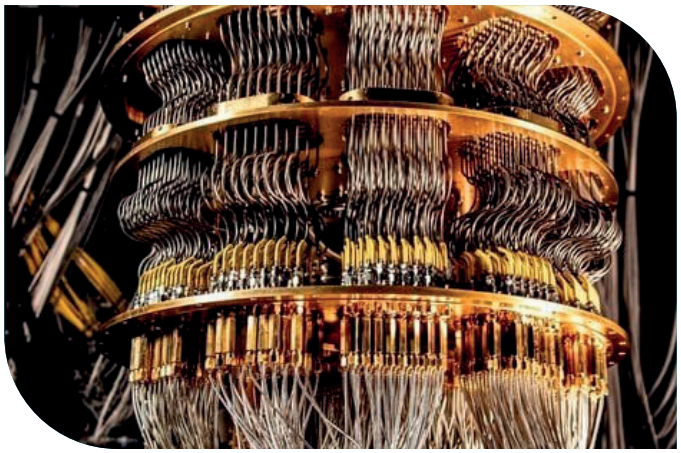
Post-Quantum Cryptography

Not If. When.

Quantum computing introduces a long-term risk to today's public-key cryptography.

Organisations must begin preparing now for the transition to quantum-resistant algorithms.

The OpenSSL Library integrates classical algorithms, post-quantum algorithms and hybrid cryptographic modes to support this transition.



OpenSSL CORPORATION

OpenSSL Library PQC Integration in OpenSSL 3.5

ML-KEM (FIPS 203)

A key encapsulation mechanism designed to establish shared secrets for secure communications.

ML-DSA (FIPS 204)

A digital signature algorithm designed for authentication and software integrity.

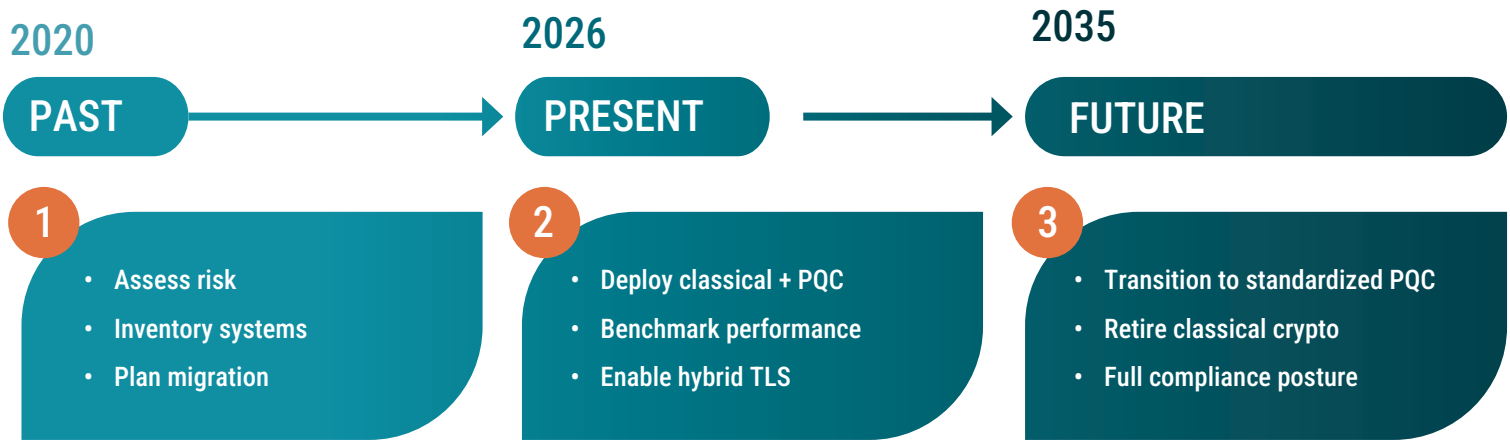
SLH-DSA (FIPS 205)

A hash-based signature scheme designed for long-term cryptographic resilience.

Hybrid TLS (Classical + PQC)

Allows existing systems to combine current cryptographic algorithms with post-quantum algorithms while maintaining compatibility with today's infrastructure.

PQC Adoption Timeline



Talk to us to help accelerate the process of upgrading your applications and infrastructure to remain safe in a post-quantum world.

openSSL CORPORATION

OpenSSL Software Services Inc.
40 E Main St, Suite 744 · Newark, DE 19711
sales@openssl.org · www.openssl-corporation.org

openssl.to/icmc2026