PostClassicalSecurity

NIST PQC Cheat Sheet

Choosing the right NIST PQC standard

● PQC Reference

The NIST PQC Standards

NIST has established multiple post-quantum standards for key establishment, and additional standards are in draft status. Selecting the correct algorithm for a use case is important for compatibility, performance and long-term security.

Algorithm	Purpose	Replaces	Advantages	Use Case
ML-KEM FIPS 203	Key establishment	RSA key transport, DH/ECDH	Quantum secure key establishment	Establishing shared symmetric key
ML-DSA FIPS 204	Digital signatures	RSA signatures, ECDSA/EdDSA	Smaller signatures Faster signing	Code signing Document signing General authentication TLS certificates
SLH-DSA FIPS 205	Digital signatures	RSA signatures, ECDSA/EdDSA	Stronger security	Root CA operations Long-term trust anchors Software supply chain code signing
FN-DSA FIPS 206 draft	Digital signatures	RSA signatures, ECDSA/EdDSA	Smallest signatures Fastest signing	Wait for official standard