WHITEPAPER

NIST Post-Quantum Cryptography Standards Explained

A plain-English guide to FIPS 203, 204, 205 and 206 — what each standard replaces, how they differ, and how other national bodies align with them.

Why NIST, and Why These Four

The US National Institute of Standards and Technology ran a multi-year, open, international competition to select the algorithms that would become the first generation of standardised post-quantum cryptography. That process — public submissions, years of cryptanalysis by researchers worldwide, multiple elimination rounds — is precisely why these standards carry the weight they do: they weren't chosen behind closed doors, they survived sustained attempts to break them.

Four algorithms have resulted from that process so far, each solving a different cryptographic problem.

ML-KEM (FIPS 203) — Key Establishment

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) replaces the key-exchange role that RSA and Diffie-Hellman/ECDH play today — the mechanism two parties use to agree on a shared secret key at the start of a secure connection, such as a TLS handshake. It's a lattice-based algorithm, meaning its security rests on the hardness of certain problems in high-dimensional lattices, a mathematical structure quantum algorithms don't have an efficient attack against.

ML-DSA (FIPS 204) — General-Purpose Digital Signatures

ML-DSA (Module-Lattice-Based Digital Signature Algorithm) is the primary replacement for RSA and ECDSA signatures — used for authenticating certificates, signing software, and

verifying identity across countless protocols. Also lattice-based, it's expected to become the default signature choice for most general-purpose use cases where signature and key size are a practical concern.

SLH-DSA (FIPS 205) — Hash-Based Signatures

SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) takes a fundamentally different mathematical approach — its security rests on the properties of cryptographic hash functions rather than lattice problems. Hash-based signatures have a long history of conservative, well-understood security, which makes SLH-DSA an attractive choice precisely where long-term trust matters more than signature size: firmware validation, code-signing roots of trust, and other scenarios where a signature made today needs to remain trustworthy for a very long time. The trade-off is larger keys and signatures than ML-DSA.

FN-DSA (FIPS 206, in progress) — A Compact Alternative

A further signature scheme, based on the algorithm known as Falcon during the standardisation process, is expected to be published as FIPS 206. It offers notably compact signatures compared with ML-DSA, which matters in bandwidth- or storage-constrained environments, at the cost of a more complex implementation. As a draft standard, it should be tracked but not yet treated as a settled default the way FIPS 203–205 can be.

Why Multiple Algorithms, Not Just One

Having more than one standardised approach is a deliberate hedge, not redundancy for its own sake. Lattice-based cryptography (ML-KEM, ML-DSA) is efficient and well-suited to most deployments, but it's a comparatively newer mathematical foundation for cryptography at this scale. Hash-based cryptography (SLH-DSA) is mathematically conservative with decades of scrutiny behind the underlying primitives, trading efficiency for that extra assurance. Should an unexpected weakness ever be found in one mathematical family, having a standardised alternative built on entirely different foundations is exactly the kind of resilience a global cryptographic transition needs.

Beyond NIST: A Converging Global Picture

NIST's standards are not operating in isolation. National cybersecurity bodies including France's ANSSI, Germany's BSI, and the UK's NCSC track and generally align their own guidance with the same algorithm choices, and the US National Security Agency's CNSA 2.0 suite sets its own timeline for national security systems built on this same standards foundation. For an international organisation, this convergence is good news: it means adopting the NIST standards is very unlikely to be a wrong bet against a competing regional standard.