QORONEX LTD
Oxford, UK · 2026

BRIEF 2 · 6 MIN READ

FIPS 203 for Automotive Engineers: What Changes, What Stays, What You Need to Order Today

FIPS 203 standardises ML-KEM (Kyber) for key establishment. This paper outlines the practical impact on automotive ECU architecture and planning decisions.

What Actually Changed in August 2024

In August 2024 NIST published three final post-quantum standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). They are final standards, not drafts.

FIPS 203 names ML-KEM for key establishment use cases. FIPS 204 names ML-DSA for digital signatures. FIPS 205 names SLH-DSA for stateless hash-based signatures. This brief focuses on FIPS 203.

Migration planning starts from this baseline publication set. If programme documents still treat these standards as pending, update them now.

What ML-KEM Replaces in Your ECU

ECDH P-256 is the usual baseline for key agreement on connected ECUs. For FIPS 203, NIST lines up ML-KEM-768 as one of the ML-KEM parameter sets for key establishment in FIPS 203, placed next to that legacy curve for programme planning.

- Map ECDH P-256 agreement work to ML-KEM-768 when you trace FIPS 203 through your design.
- Key agreement appears in TLS handshakes, key provisioning, V2X interfaces, and OTA sessions wherever ECDH established a shared secret before.
- Public key material grows from roughly 64 bytes on the ECDH side to roughly 1184 bytes on the ML-KEM-768 side. Buffer and allocation tables need to reflect that step change.
- Treat this change as an interface and memory budget update across handshake and provisioning boundaries.

Why the Size Jump Forces Early Interface Review

The 64-byte versus 1184-byte public key comparison is not a tutorial. It is a reminder that any struct, IPC payload, or bootloader slot sized for classical material will fail silently until someone maps the new maximum into those limits.

Teams own the resize and test plan. This brief stops at the observation: count every place a public key crosses a boundary and check the worst case after ML-KEM.

What FIPS 203 Explicitly Gives You

FIPS 203 gives you a final, published ML-KEM standard with named parameter sets, conformance language, and immediate effectiveness. It does not depend on draft status and can be used now as the baseline for programme planning and cryptographic architecture review.

- Published and effective date: August 13, 2024.
- Parameter sets are explicit: ML-KEM-512, ML-KEM-768, and ML-KEM-1024.
- Implementation can be software, firmware, hardware, or a combination.
- Validation path is defined via NIST CMVP programme references.

What Changes in Planning Artifacts

When key material grows, pressure appears first in design and assurance artifacts. Before implementation details, update the documents that drive interface contracts and test assumptions.

- Interface control documents: update maximum key and ciphertext field sizes where ECDH assumptions were fixed.
- Threat and risk records: add explicit HNDL and CRQC-facing key agreement exposure statements.
- Security architecture packs: map where shared-secret establishment occurs and mark migration dependencies.
- Verification plans: include larger key and message-boundary test cases in protocol and OTA validation suites.

The Timeline to Internalise

- 2024: NIST published final FIPS 203, 204, and 205. If your roadmap still says draft, update it.
- 2025 and 2026: early programmes build PQC prototype ECUs and lab sign-off evidence.
- 2027 and 2028: type-approval and CSMS evidence will increasingly expect post-quantum posture for new vehicle lines.
- 2030: NCSC and BSI treat this window as the credible CRQC threat horizon for planning purposes.
- Model year 2028 and later vehicles need PQC-capable ECUs in design before those dates, not after.

QORONEX can review your current cryptographic footprint and produce a phased migration roadmap that matches your vehicle programme gates.

For enquiries, please contact info@qoronex.co.uk.