QORONEX LTD
Oxford, UK · 2026

BRIEF 3 · 6 MIN READ

FIPS 204 for Automotive Engineers: What Changes, What Stays, What You Need to Order Today

FIPS 204 standardises ML-DSA (Dilithium) for digital signatures. This paper explains how that change affects automotive ECU verification paths and programme planning.

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

If verification paths still assume classical signature sizes only, treat these published standards as the trigger to update interface and storage assumptions.

What ML-DSA Replaces in Your ECU

ECDSA P-256 is the common choice for firmware signatures, secure-boot verification, and many V2X credential profiles. ML-DSA-65 is one of the ML-DSA parameter sets in FIPS 204 for digital signatures. Signatures appear in secure boot, OTA manifest checks, and certificate chains where ECDSA sat before.

• ECDSA P-256 to ML-DSA-65: use this pairing when you trace FIPS 204 against your signing architecture.

• Any channel that verified an ECDSA signature will need a plan for ML-DSA verification semantics and payload sizes, not only for TLS.

Signature Sizes and Storage Pressure

A compact ECDSA signature is on the order of 64 bytes. ML-DSA-65 signatures are on the order of 3309 bytes. The ratio matters more than the exact byte count: OTA headers, secure-boot verify buffers, and V2X certificate storage were often sized for classical lengths.

The point for programme leads is allocation and interface review, not a step-by-step resize recipe in this brief. If your worst-case buffers assumed 64-byte signatures, those assumptions no longer hold.

What FIPS 204 Explicitly Gives You

FIPS 204 gives you a final, published ML-DSA standard with parameter sets, conformance expectations, and immediate effectiveness. It is a standards anchor you can cite now in design reviews and security case updates.

• Published and effective date: August 13, 2024.

• FIPS 204 defines ML-DSA parameter sets and key/signature encoding rules.

• Implementation can be software, firmware, hardware, or mixed deployment.

• Validation path is defined via NIST CMVP programme references.

What Changes in Planning Artifacts

The first impact of larger signatures is on interfaces, storage, and verification assumptions. Before migration mechanics, make sure baseline programme artifacts reflect ML-DSA realities.

• OTA package schemas: revise signature field maxima and integrity-check staging assumptions.

• Secure-boot verification paths: confirm memory allocation for signature parsing and verification inputs.

• Certificate and credential stores: update sizing assumptions where signatures are persisted or relayed.

• Verification plans: add boundary tests for larger signature payloads in boot, OTA, and V2X flows.

The Timeline to Internalise

• 2024: NIST published final FIPS 203, 204, and 205. Signature migration tracks the same publication line as KEM migration.

• 2025 and 2026: teams that need signed evidence build prototype ECUs and toolchain proofs.

• 2027 and 2028: new programmes face stronger questions on quantum-ready signatures in safety and approval packs.

• 2030: plan against the CRQC window public guidance from NCSC and BSI when you prioritise budget.

• Long-lived vehicles need signing and verification choices locked while the design window for that model year is still open.

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.

QORONEX LTD · Oxford, UK · info@qoronex.co.uk