Factsheet

KUDELSKI LABS

Futureproof your Products Against Quantum Threats

Post-Quantum Cryptography (PQC): Act Now

By 2027, U.S. National Security Systems must adopt post-quantum cryptography, well ahead of EU deadlines set for 2030–2035. Quantum computing is poised to break today's cryptographic standards, putting long-lifecycle products at risk of compromise and non-compliance.

NIST has already selected ML-KEM and ML-DSA as the new PQC standards, making the transition urgent for every organization designing products to last beyond the next decade. Acting now ensures your products remain secure, resilient, and compliant as global regulations evolve, protecting your investments and reputation against tomorrow's quantum threats.

Why PQC Matters Now

Waiting to act risks costly redesigns, compliance failures, and exposure to advanced threats. PQC ensures your security architecture remains robust, agile, and compliant as global standards evolve.

- **Quantum risk is real:** Quantum computers will break today's cryptography, exposing products to future attacks.
- **Long-lifecycle products are vulnerable:** Devices designed now may operate well into the quantum era, risking compromise if not protected.
- **NIST standards are set:** ML-KEM and ML-DSA are the new benchmarks for post-quantum security.
- **Acting now avoids costly redesigns:** Early adoption ensures resilience, compliance, and protects your reputation.

Key Compliance Deadlines

United States: CNSA 2.0 mandates PQC for National Security Systems by 2027; legacy systems must migrate by 2030.

European Union: PQC adoption expected by 2030–2035 for critical infrastructure and regulated industries.

NIST: ML-KEM and ML-DSA selected as standard algorithms for post-quantum security; FIPS 203–205 formalising requirements.

The Kudelski Labs Solution

Integrated PQC in Kudelski Secure Enclave (KSE)

- Embedded ML-KEM and ML-DSA algorithms, with advanced side-channel and fault countermeasures.
- Hardware-software hybrid architecture for performance and upgradeability.
- Secure boot, update, provisioning, and key management, all PQC-ready with included LMS algorithm support.

Hybrid Cryptography & Crypto Agility

- Seamless transition between classical and quantum-resistant algorithms.
- Supports hybrid cryptography for phased migration and crypto agility.
- Enables post-deployment upgrades to meet evolving security requirements.

Benefits at a Glance

End-to-End Trust Chain
Secure provisioning, credential management, and firmware updates across the product lifecycle.

Long-Lifecycle Protection
Designed for products with 5–10+ year lifespans, ensuring resilience against future quantum threats.

Compliance Ready
Aligns with emerging standards (CNSA 2.0, NIST, EU CRA, FIPS, ANSSI).

The transition to PQC is no longer theoretical: it's a strategic imperative for every organisation designing products to last beyond the next decade. Act now to ensure compliance, resilience, and futureproof security.

Strategic Intelligence. Impactful Action.

Our semiconductor security expertise is rooted in more than three decades of hardware, software and cybersecurity experience. We use our expertise and technology to protect all key semiconductor assets - devices, identity, data, decisions, commands and actions throughout the lifetime of the device and its ecosystem.

Contact Us

info@kudelskilabs.com | www.kudelskilabs.com

KUDELSKI LABS