

White Paper Executive Summary

Sovereign by Design

How Europe Can Secure its Digital Future in the Post-Quantum Age

Europe stands on the brink of a new technological frontier – one that challenges not only its cybersecurity posture but its digital sovereignty as a whole. The advent of quantum computing is forcing every government, enterprise, and critical infrastructure provider to rethink how trust is built, maintained, and protected.

At the heart of the analysis lies the coming cryptographic revolution. Quantum computers promise extraordinary computational power but simultaneously threaten the encryption schemes that underpin the modern economy. Algorithms such as RSA and ECC, once unbreakable, will become vulnerable within the foreseeable future. The immediate danger lies in the harvest-now, decrypt-later strategy, where attackers capture encrypted data today to exploit it once quantum capabilities mature.

To meet this challenge, migration to post-quantum cryptography (PQC) has already begun. The U.S. National Institute of Standards and Technology (NIST) finalized its first three PQC standards in 2024 – ML-KEM, ML-DSA, and SLH-DSA – providing the global baseline for implementation. In parallel, the European Commission's Coordinated Implementation Roadmap for PQC (June 2025) defines mandatory milestones: national migration plans by 2026, transition of high-risk systems by 2030, and completion for medium-risk environments by 2035. These timelines make cryptographic modernization a regulatory and strategic imperative.

The document offers a pragmatic migration framework: establish governance early, map dependencies,

pilot hybrid deployments combining classical and post-quantum algorithms, and embed crypto-agility into every product and update process. This evolution will take years and must align with broader European legislation such as the Cyber Resilience Act (CRA), NIS2, and DORA, which make secure-by-design architectures a condition for market access. Compliance and competitiveness are now inseparable.

Beyond technology, Europe is pursuing digital sovereignty – the ability to act independently and responsibly within the global digital ecosystem. The EU's regulatory power – GDPR, the AI Act, eIDAS 2.0, and the Digital Product Passport – provides the legal scaffold for that independence. Yet regulation alone is insufficient; it must be matched by industrial capacity through initiatives such as the European Chips Act, Gaia-X, and EuroQCI, ensuring Europe retains control over both data and hardware supply chains.

Small and medium-sized enterprises (SMEs) play a critical role in sustaining that sovereignty. Without shared certification services, simplified compliance paths, and funding mechanisms to offset regulatory costs, Europe risks a "sovereignty gap" where only large incumbents can afford to participate. True sovereignty must be inclusive – built on harmonized standards, accessible security frameworks, and open innovation.

The conclusion is clear: quantum computing does not only disrupt encryption – it redefines sovereignty. Europe's future competitiveness will depend on its ability to coordinate regulation, investment, and innovation around a shared vision of secure independence.

Download the complete white paper