PQ SHIELD

CRYPTOMATHiC

Quantum Secure Key Management: PQShield and Cryptomathic's CrystalKey360

pqshield.com

cryptomathic.com

The urgent evolution of key management

It's clear that the way we handle cryptographic key management is undergoing a seismic shift. In essence, that shift is driven by two powerful forces: first, the imminent threat of quantum computing, and second, the increasing complexity of multi-cloud environments. Organizations are increasingly moving sensitive data to the cloud, relying on providers such as AWS, Microsoft, and Google.

It's a transition that creates significant challenges in security, compliance, and operational complexity, and, with the looming threat of the post-quantum era, is now leading many to focus on the need for cryptoagility - ensuring that systems can update and switch cryptographic algorithms to counter new threats without disruptive overhauls.

Post-quantum imperative

Within the next few years, quantum computers will render public-key cryptography obsolete. But it's not a distant problem. Adversaries can already steal encrypted data with a view to decrypting it with future quantum computers in a so-called 'harvest-now-decrypt-later' attack. With sensitive data on the table, it's an immediate concern for many organizations, and it's led to an acceleration in post-quantum cryptography (PQC).

In 2024, NIST standardized the very first PQC algorithms (ML-KEM, ML-DSA, SLH-DSA) and governments worldwide have been establishing global timelines for their adoption. Meanwhile, cloud providers have already begun integrating these new PQC standards into their cloud key management services and cryptographic libraries.

The complexity of multi-cloud

The second driver of change is of course, the reliance on multi-cloud and hybrid strategies - using a mix of cloud provider KMS, on-prem HSMs and BYOK models. While it's incredibly flexible, it can lead to significant challenges, such as a lack of interoperability, adherence to a complex set of compliance requirements, and an operational burden when it comes to managing a fragmented system of key management. In fact, according to a 2024 report from Entrust, the 2024 State of Zero Trust & Encryption Study, more than half of IT security practitioners state that managing keys already has a 'severe impact' on their organizations.

These trends show that the future of key management, with security and complexity taken into account, requires a holistic, centralized approach to managing policies, governance, and cryptographic agility across the enterprise.

Compliance Requirements

There are a number of requirements now in place regarding the security of sensitive or high-risk systems, many of which apply to the field of key management. The following table outlines some key pieces of regulation and their objectives.

The common theme is that regulators and standard-setters now expect a formal PQC migration strategy. Organizations will certainly be asked to inventory their cryptographic estate and provide plans or evidence of PQC-readiness, and those without a plan risk non-compliance as well as operational risk.

Regulation	Description
Digital Operational Resilience Act (DORA)	Mandates that financial organizations establish formal, written policies for encryption and the entire lifecycle of cryptographic keys
NIS2 Directive	Applies to finance and critical infrastructure. Explicitly requires robust encryption, including PQC in place of RSA and SHA-1
EU Co-ordinated PQC Migration Roadmap	PQC transition by 2035 for EU Member States with high-risk systems including financial infrastructure, PQC ready by 2030
PCI DSS 4.0	Mandates documented procedures for key lifecycle and inventories, plus cryptoagility in place for PQC migration in the near future
NIST Standards	FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA) standardized as of 2024 and now recommended for integration as soon as possible
CNSA 2.0	Constructs a roadmap for US national security systems to adopt PQC by 2035 with specific milestones.

Cryptomathic's CrystalKey 360 and PQShield

The challenges of quantum-safe, regulations-compliant key management solutions in multi-cloud environments aren't just industry trends - they're real-world problems that require next-generation solutions. They're also the reason why solutions such as Cryptomathic's CrystalKey 360 and PQShield's groundbreaking UltraPQ quantum-secure IP have become a platform to solve these exact problems.

CrystalKey 360 is an all-in-one platform that manages policies, algorithms, keys, logging and governance across HSMs, secure cloud enclaves, cloud key stores and applications. It's an ideal solution to the fragmentation and complexity problem.

PQShield builds quantum-safe IP that's designed for everything from hardware, software and the cloud, and its UltraPQ suite is designed for situations that require ultra-fast processing, ultra-secure protection or ultra-small deployment.

In our integration, PQShield Libraries are embedded into CrystalKey 360's Software Security Module (SSM) and Enclave Security Module (ESM) to support PQC key generation and digital signature algorithms. CrystalKey 360 handles key management and distribution and also exposes crypto agile API to consumers, a critical challenge, especially in high availability environments.

This Strategic Technology Alliance partnership between Cryptomathic and PQShield aims to protect digital assets from quantum computing threats by ensuring a combined scalable, secure, and compliant quantum-resistant solution across industries.

Conclusion

The future of enterprise security hinges on centralized, agile cryptographic management. With the threat of quantum computers, that cryptographic management is increasingly required to be quantum-safe, both from a technical perspective and from a compliance angle. Platforms like Cryptomathic's CrystalKey 360 and PQShield's UltraPQ suite aren't just tools but strategic necessities for maintaining security, compliance and enabling future innovation.

Where Crypto-Agility Meets Quantum Resilience

PQ SHIELD

PQShield builds mature PQC for many use cases - where we truly excel is with PQC that is Ultra Fast, Ultra Small or Ultra Secure.

Get in touch: contact@pqshield.com

CRYPTOMATHiC

Simplify your cryptography, strengthen your security and future proof your business with CrystalKey 360.

Get in touch: enquiry@cryptomathic.com