3 cybersecurity technologies every CISO and CTO should know

Latest advancements in key management and cryptographic safeguards

PAYMENT CONNECTIVITY CYBERSECURITY

POSTED ON 10.23.25

As the scale and sophistication of cyberthreats accelerate and as geopolitical tensions intensify the digital risk landscape, cybersecurity needs are surging across all sectors. The looming prospect of Q-day – the moment when Cryptographically Relevant Quantum Computers (CRQCs) could break today's encryption – is further emphasizing the importance for CISO, IT security teams, and software developers to keep strengthening and ensuring the resilience of cryptographic defenses. Let's explore some of the solutions that can give an edge to organizations, offering them the scalable and future-proof data protection they need.

1/ A secure element-based HSM matrix to rethink cryptographic key management

Whether deployed in private data centers or hosted in the cloud, traditional Hardware Security Modules (HSMs) typically rely on a **single, powerful processor**. In this setup, securing the processor and memory of the HSM requires protecting the electronic card in a shield box. This traditional architecture can create hardware bottlenecks, particularly in terms of deployment, operation, and maintenance costs. Besides, relying on a single processor may lead to conflicts between concurrent processes, stemming from the ***software-based* segregation** of keys and cryptographic operations.

Rethinking the HSM architecture around a **matrix of secure elements** provides hardware security by design and strengthens tenant isolation, effectively enabling **the *physical* segregation of cryptographic operations** through dedicated hardware resources and secure enclaves. Another significant advantage of using low-power secure elements, beyond reducing energy consumption[1], is their **ability to support cold storage**. Secure elements eliminate the need for a battery-reliant shielding system, thus avoiding the hassle of reconfiguration in the event of battery failure. This innovative HSM model engineered by IDEMIA Secure Transactions (IST), and already FIPS 140-3 certified, brings a fresh perspective to optimize or ramp-up encryption, authentication and digital signature services.

2/ Quantum-ready libraries to minimize risk, save time, ensure compliance

With quantum computing on the horizon, the clock is ticking to deploy new algorithms and protocols. Today, developers can rely on open-source cryptographic libraries with a reasonable degree of confidence but unlike the time-tested and trusted cryptographic standards we've relied on for decades, post-quantum cryptography is only just emerging. **Few people truly grasp all the nuances of post-quantum migration**, and standards are expected to keep

evolving.

To ensure their Post Quantum Cryptography (PQC) libraries will be maintained over time and at the right pace, organizations may be better off turning to **licensed cryptographic libraries**. Backed by **maintenance contracts**, these also come with guarantees such as code signing, which helps **verify code source** and prevent the inadvertent introduction of vulnerabilities into systems. **Integration support** will also be crucial for organizations without in-house PQC expertise, particularly when deploying libraries within non-standard hardware or software environments.

Replacing the cryptographic libraries of all the devices, software, and services we use every day is no small feat. **It's not just about getting it right. It also isn't something you can simply set and forget.** Proper implementation in every environment, continuous monitoring, rigorous testing, regular updates, and robust compliance processes will be **the very crux of post-quantum resilience**. This is where cryptographic libraries crafted by specialists with proven experience in highly regulated sectors, along with the advisory support they provide, will make the difference. By choosing licensed libraries, organizations will have the assurance to **align with the level of liability required** by new cybersecurity regulations, both in terms of code source content and speed of correction in the event of a flaw.

3/ Crypto-agility to ensure lasting and in-depth cybersecurity

Closely tied to the challenges of post-quantum resilience, cryptographic agility (or crypto-agility) will provide CISOs and IT security teams with **unprecedented capabilities for deep security updates** of devices and systems in the field. **The days of one-off system updates are over**. The banking sector, for instance, has gone through several cryptographic changes over the past decades.[2] As systems become more complex, with more interconnected players, **these upgrades require ever more time and resources**, a luxury that the industry will no longer be able to afford in the post-quantum era. This also holds true for mobile networks, energy infrastructure, healthcare systems, connected cars, and any other system that depends on encryption technologies.

Even without considering the quantum challenge, crypto-agility stands as **a long-term investment in cyber-resilience**. Rather than repeatedly planning and executing large-scale system and device migrations, security professionals will be able to respond swiftly whenever algorithm or protocol updates are needed, **making cryptographic evolution part of regular operations** rather than a recurring overhaul.

Crypto-agility aligns with **modern frameworks and standards** that help organizations manage cybersecurity risks and strengthen cryptographic safeguards across critical sectors, including technical standards like FIPS 140-3 and ISO/IEC cryptography standards, industry frameworks such as PCI DSS, and risk management guidance like the NIST Cybersecurity Framework (CSF).

It also becomes **a compliance asset** as new regulations such as the Cyber Resilience Act (CRA), the Network and Information Security Directive (NIS2) and Directive Digital Operational Resilience Act (DORA) in Europe or the SEC Cybersecurity Disclosure Rules in the United States now require stronger measures to **ensure product and software cybersecurity by design** and to **manage evolving cybersecurity risks**, including prevention, clear reporting, and responding to incidents.

Get your tech stack ready for the quantum count-down

With Q-day around the corner and cyberthreats growing in complexity, it is a critical time to make the right choices to future-proof infrastructures, systems and devices. As part of the cybersecurity toolbox, these **3 tech advances** can help organizations navigate evolving regulatory requirements confidently and ensure their data and assets remain protected well beyond today's standards:

- A **sovereign and secure-by-design HSM** engineered for easy set-up, scalability and cost-effectiveness

- A **quantum-ready cryptographic library** with expert guidance to ensure optimized implementation, standard compliance and timely updates
- **Crypto-agility capabilities** from end-point devices to core systems and the Cloud

Want to dive deeper into these 3 game-changers and see how advanced cryptographic technologies can power your post-quantum journey and beyond?

Contact us

---

[1] With a typical power consumption of 50 W per appliance, IDEMIA Sphere HSM is cutting power consumption by 50% compared to conventional HSMs.

[2] The banking sector has gone through several cryptographic changes over the past decades: The DES standard, used since the 1970s, was replaced in the 1990s by 3DES, followed by the AES standard in the early 2000s, which is still being rolled out. At the same time, RSA key lengths were increased, and the hash functions used with it have been updated several times since the 2000s. Source: https://www.fsisac.com/pqc-crypto-agility

---