IDEMIA

Cybersecurity: Brace Yourself for the Quantum Leap

The Shift to Post-Quantum Cryptography Marks the Dawn of a New Era

PAYMENT CONNECTIVITY CYBERSECURITY

POSTED ON 05.05.25

For some, the migration to post-quantum cryptography (PQC) is merely a necessary defense against the looming threat of quantum computing. For others, it's a game-changing opportunity to fortify cybersecurity against the very real dangers we already face today. So, which side are you on? Are you ready to embrace post-quantum migration and envision the future of cybersecurity?

The biggest cybersecurity evolution since asymmetric cryptography deployment

The transition to post-quantum cryptography is set to be one of the biggest undertakings of the 21st century. **This global effort involves every industry** that relies on online services or connected devices —meaning, quite simply, every industry today. The cybersecurity world hasn't seen a transformation of this magnitude since the adoption of asymmetric cryptography about 50 years ago.

In the summer of 2024, the White House convened US government and industry leaders to unveil new Post-Quantum Cryptographic standards from the National Institute of Standards and Technology (NIST). With this announcement **the NIST officially kicked off the post-quantum migration**, calling on all digital security stakeholders around the world to implement them without delay. Other standardization bodies and governmental agencies around the world, including in Europe, in South Korea or in China for instance, have also moved forward by selecting their own quantum-resistant algorithms. **The next phases of standardization are now unfolding within major industry organizations** which are set to update their specifications and roadmaps to incorporate post-quantum cryptography— such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the International Organization for Standardization (ISO), the European Telecommunications Standards Institute (ETSI), GlobalPlatform, and the GSMA, to name only a few.

The quantum computers making headlines today, developed by companies like Google, Microsoft, IBM or research teams in Europe or China, **are focused on entirely different applications** than breaking today's cryptographic systems with large number factorization. In fact, these first quantum computers mainly focus on machine learning, medical research and logistics optimization. **Yet, the sense of urgency remains in the cybersecurity community**. As quantum technology advances, and makes these machines more efficient, it could also make them easier to adapt for large-number factorization. At the same time, Shor's algorithm— the algorithm designed for large number factorization with a quantum computer—is being refined to require fewer qubits, lowering the hardware barrier to breaking current cryptographic systems.

Steered by these advances in quantum mathematics and technology—as well as the need to secure certain data for decades to come—**the timeline for migrating to post-quantum cryptography is particularly tight**. The NIST roadmap already indicates that some key sizes currently used in many public-key cryptography systems will be obsolete from 2030 (meaning they can still be used but at the users' risk). **By 2035, many algorithms will be disallowed**[1] —products and systems relying on them will no longer comply with FIPS standards. This not only includes **RSA cryptosystems**, which have been widely used since the 1980s to encrypt and sign documents and emails or authenticate online transactions, **but also cryptosystems based on Elliptic Curves**. The urgency is felt just as strongly in the European Union, where 18 Member States have signed a joint declaration[2] calling for essential security measures to be in place by 2030 to protect the most critical use cases.

The deadlines are tight, and the task is immense—there's no denying that. However, **the benefits of a successful post-quantum migration will be significant**—so much so that the development of a quantum computer designed to break cryptographic keys could ultimately prove largely irrelevant. As systems migrate, the incentive to exploit quantum computing for cryptographic attacks is likely to diminish, even if such machines are still developed for demonstration purposes as the technology becomes more accessible.

PQC migration: Bringing security up to a state-of-the-art level across all sectors

The first major benefit of the post-quantum cryptography migration is the essential step of **taking stock of all cryptographic assets**. This inventory will serve as the foundation for a comprehensive upgrade to the latest security standards.

During the PQC migration, **legacy systems and older protocols will be phased out** in favor of the latest algorithms and protocols. This migration will finally bring years of work on more efficient and secure protocols to fruition through their large-scale deployment. It will also likely speed up the adoption of the latest specifications across various industries.

The migration to post-quantum cryptography will have a major cybersecurity impact because it requires a comprehensive approach. Every part of the chain will need a security upgrade—from HSMs and secure elements to connected devices, operating systems, protocols, and cryptographic libraries, etc. The encompassing scope of the upgrades required was highlighted at Mobile World Congress 2025, where IDEMIA Secure Transactions demonstrated the **migration of an IoT device with an eSIM**—including updates to the chip, the device's TLS protocol, and the server managing eSIM profile updates. PQC algorithms tend to demand greater computational resources, which can potentially impact latency-sensitive applications such as payments and secure authentication. **Taking a comprehensive, use-case-driven approach** is essential to ensure that PQC integrates seamlessly with existing physical and digital infrastructures.

Preparing for the future quantum-safe migration should be taken as an opportunity to make a giant leap forward in **strengthening cybersecurity defenses across all industries** and laying a solid foundation for a safer future.

Crypto-agility: Ensuring continuous and more effective security upgrades

Another opportunity offered by the migration to post-quantum cryptography will be to enable **better management of cryptographic assets in the future** by introducing more agile, frequent, and systematic update mechanisms.

Currently, security maintenance for many devices is difficult to maintain in the long term. The risk remains low once they are installed, as strong cryptography protects them from malware or ransomware installation. However, this barrier could collapse if a quantum computer were to decrypt their cryptographic keys—especially as **cyberattacks become**

more sophisticated and reach a new scale with the use of AI.

Crypto-agility, a key principle of the post-quantum migration, will help keep device cryptographic defenses at the state of the art over time. This new mechanism designed to support the maturation and evolution of post-quantum cryptography will **strengthen cybersecurity in the long run** by enabling more automated security updates that don't require user or technician intervention.

The migration to post-quantum cryptography should also help **extend security more broadly within the IoT sector**, through the use of crypto-agile eSIMs as crypto-processors.[3] This new approach will streamline how cryptography is implemented in connected devices, in contrast to the multiple cryptographic implementations typically found in the embedded Linux systems of these devices. Another key benefit of using quantum-safe eSIMs as crypto-processors and managing cryptographic updates through these crypto-agile elements is that the device or system's security certification won't be impacted and will remain valid. **In terms of certification, this is a significant improvement** over security updates occurring at the Linux system level, which require re-certification of the entire product or system—something that is frequently overlooked.

More consistent cryptographic implementations, easier to deploy and maintain at the state of the art without affecting device certifications, along with **more frequent and efficient security updates—crypto-agility will be a real game-changer** in the face of the ever-growing challenges of cybersecurity.

Post-quantum cryptography: a new chapter in cybersecurity

While the scale and complexity of the task ahead are clear, the **long-term benefits** of post-quantum cryptography migration provide strong motivation to press on. Every organization involved in this journey over the next decade will play a role in **shaping the history of cybersecurity**. At IDEMIA Secure Transactions, we're proud to be part of this journey, working alongside our clients and partners to **make a safer future possible**.

---

[1] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[2] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5
[3] https://www.youtube.com/watch?v=gnVl8fO1xUo
