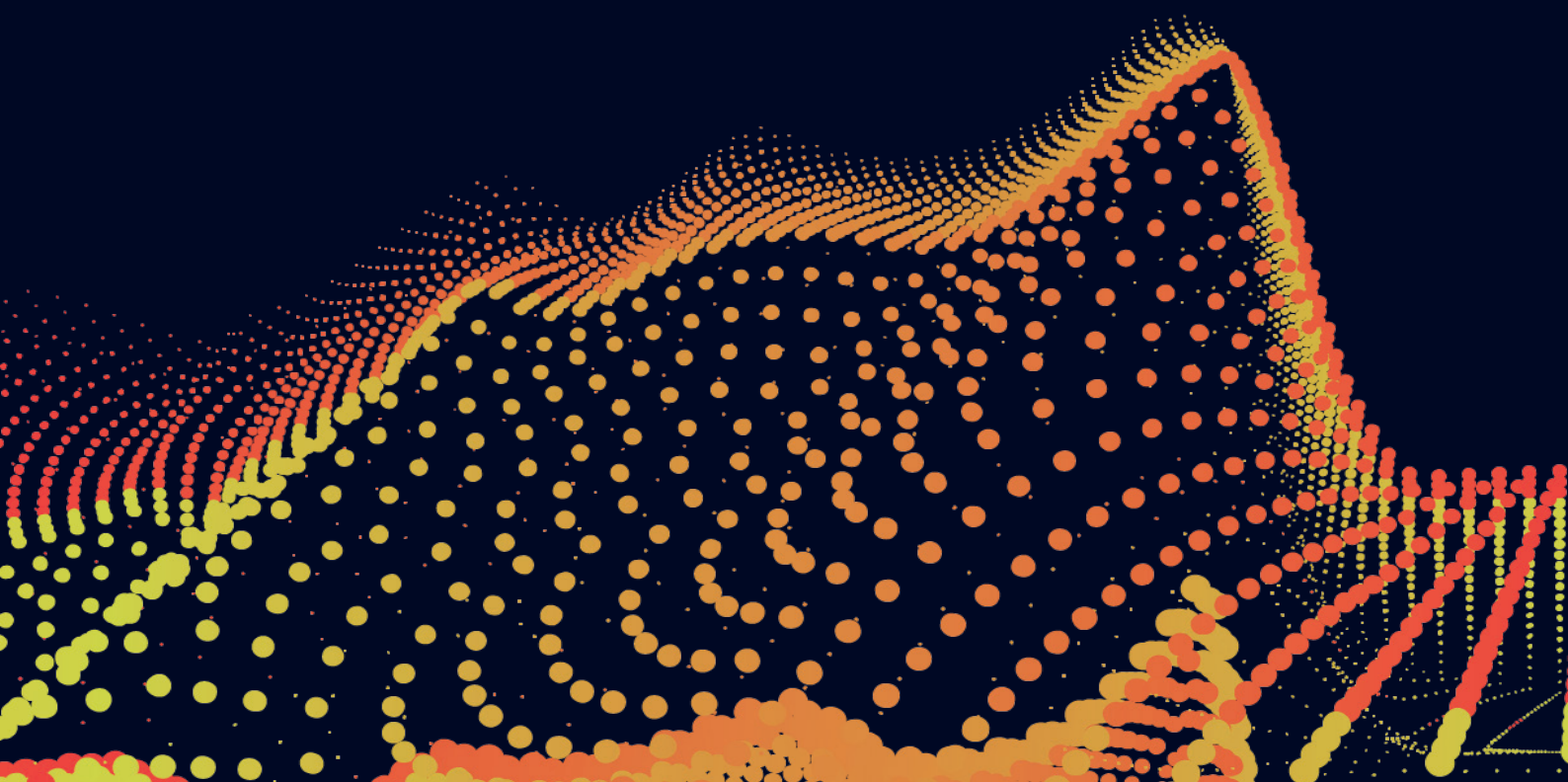


# Securing telecommunications networks against the quantum threat

“In the near future, sufficiently powerful and commercially available quantum computers will undermine current cryptographic standards protecting most digital communications and vast amounts of sensitive data. Mitigating this security risk requires organizations to implement quantum-security technologies that quantum computers cannot break.”<sup>1</sup>



# Post-quantum cryptography

It's no secret that quantum computers will soon pose a threat to the traditional cryptographic methods that keep our information secure. In every industry, the technology that protects data, devices, components and connections will need to be modernized to align with the new global standards, and a new generation of cryptography techniques might be our best defense.

Post-quantum cryptography (PQC), sometimes known as quantum-proof, quantum-safe or quantum-resistant cryptography, refers to cryptographic algorithms (usually public-key algorithms) that have been specifically designed to defend against attacks by quantum computers. For the last few years, a concerted effort has been made to develop and standardize these algorithms, and in telecoms particularly, the adoption of PQC cannot come soon enough.

According to  
GSMA

*"The telecom industry needs to mobilize to define guidelines and processes for the PQC adoption to secure networks, devices and systems, given that this affects the entire telecom supply chain and ecosystem: operators, network and IT vendors, integrators, regulators, standards and open source communities."*<sup>2</sup>

GSMA™

## International PQC Standards

In August 2024, NIST published its Post-Quantum Cryptography standards<sup>3</sup>, as the culmination of a worldwide eight-year project. FIPS 203 ML-KEM (CRYSTALS-Kyber) is now the standard for public-key encryption and key encapsulation mechanisms, while FIPS 204 ML-DSA (CRYSTALS-Dilithium) is the preferred standard for digital signatures, along with FIPS 205 SLH-DSA (SPHINCS+) and FN-DSA (FALCON, FIPS TBD) as alternative standards for digital signatures.

These new quantum-safe cryptography algorithms have been specifically selected with mass-market applicability in mind, as they have very reasonable requirements regarding performance, key size, and ciphertext size.

## The quantum timeline

It's thought that 'Q-Day', the date when quantum computers will be powerful enough to break today's cryptography, will happen within the next decade. For high security systems, the German Federal Office for Information Security (BSI) is predicting that cryptographically relevant quantum computers could become available in the early 2030s.<sup>4</sup>

However, even with this future threat, the time for action is now.

Considering that the adoption and rollout of quantum-safe cryptography could take multiple years for planning, implementation and verification, it's best to think of Q-Day as the point of completion, and consider the timeline between now and then.

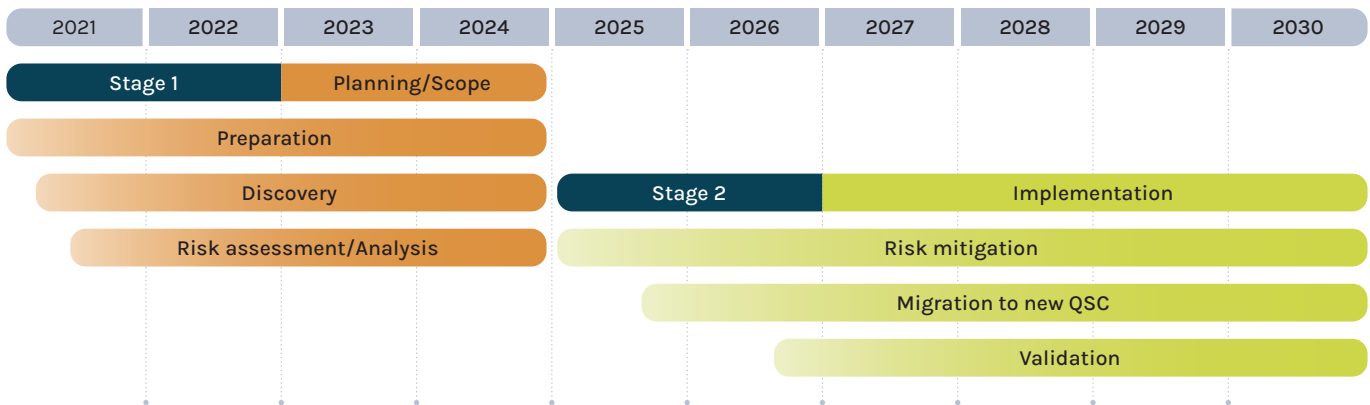
1 [https://www3.weforum.org/docs/WEF\\_Quantum\\_Readiness\\_Toolkit\\_2023.pdf](https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf)

2 <https://www.gsma.com/newsroom/wp-content/uploads/PQ1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version10.pdf>

3 <https://pqshield.com/the-new-nist-pqc-standards-are-here/>

4 [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4)

For example, the recommended timeline of the Canadian National Quantum-Readiness Working Group<sup>5</sup> suggests the following:



What’s more, it’s possible that even now, a potential adversary could steal and harvest sensitive data with a view to decrypting it later, when the technique becomes available. All data, whether historical or current, is at risk unless protected by quantum-safe security.<sup>6</sup>

The quantum era has already begun.

## PQC adoption initiatives around the world

As with all technological advances, the adoption of post-quantum cryptography is necessary not only for security, but also for compatibility. Worldwide, governments and standardization bodies have been working on schedules for the PQC adoption.<sup>7</sup>

In fact, for US government agencies, there is already a mandatory schedule<sup>8</sup> to move to PQC. Additionally, both the French national security agency (ANSSI) and the Canadian Forum for Digital Infrastructure

Region	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2021)	Planning and implementation 2025-2026
Canada	NIST	Cyber Centre (2021)	Implementation 2025+
China	China specific	CACR (2020)	Planning and standard finalization
European Commission	NIST	ENISA (2022)	Planning and mitigation
France	NIST (but not restricted to)	ANSSI (2023)	Implementation 2025+
Germany	NIST (but not restricted to)	BSI (2022)	Implementation 2025+
Japan	NIST (monitoring)	CRYPTREC	Evaluation of standards and planning
New Zealand	NIST	NZISM (2023)	Planning and prioritization
Singapore	NIST (monitoring)	MCI (2022)	No timeline published
South Korea	KpqC	MSIT (2022)	Standards published January 2025
United Kingdom	NIST	NCSC (2020)	Planning and implementation
United States	NIST	NSA (2022)	Implementation 2025+

5 [https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/\\$file/CFDIR-Prati-Tech-Quant-EN.pdf](https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf)

6 <https://www.ibm.com/quantum/quantum-safe>

7 <https://www.gsma.com/newsroom/wp-content/uploads/PQ1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf>

8 [https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA\\_CNSA\\_2.0\\_ALGORITHMS\\_PDF](https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_PDF)

Resilience (CFDIR) recommended the immediate introduction of post-quantum defenses throughout the private sector, and Germany’s BSI has already endorsed the use of post-quantum cryptography.

## How to get started

Thinking about the transition to PQC could be daunting. It involves thinking about systems, components and processes in your organization in depth, and could be a long and complex project, involving a large number of stakeholders. However, there are some things you can do now to make the transition much easier. For example:

- A great first step might be to interview your internal system owners and experts. This will help you understand which vendors and suppliers you need to talk to about PQC, and also ensures that your business is fully aware of the need to migrate.
- Establish a cryptographic inventory: Identify currently used cryptographic algorithms and key-lengths, and systems or vendor products dependent on cryptography.
- Perform a risk assessment of cryptography used in your systems.
- Develop a mitigation strategy
- A Proof-of-Concept will help you in the development and verification of your strategy. PQShield can already help you at this stage.
- Finalize the migration strategy
- Establish a project office for delivery

## Where is your cryptography?

Examples of cryptography applications in telecommunications systems:<sup>9</sup>

Area	Description	Considerations
Secure user provisioning	User identities, machine identities, for example enabling SIM cards. Connection between networks and remote devices	Cryptography is used to authenticate and protect users and machines logging into systems and using networks. It’s essential to consider how these processes might be under threat from a possible quantum attack.
Subscriber identity management	User identity, storage of Personally Identifiable Information (PII), transfer between devices and networks	How is your user identity data stored? What would happen if that encrypted data were extracted and decrypted at a future point in time?
Payment processing	Transfer of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data between remote points and a network, storage of sensitive data	Your organization needs to secure personalized information such as billing details, customer mail addresses and contact details, as well as data relating to transaction records. How is this data stored? How is it managed securely between systems?

Due to the nature of the global supply chain, silicon manufactures will be among the first required to include PQC in their devices. It’s important to note that:

- PQC root security must be implemented into a device’s hardware. It cannot be patched later.
- PQC hardware accelerators and PQC-enabled secure subsystems with telecommunications processors will increase efficiency and performance, and reduce total system costs.

In 2022, the GSM Association formed the GSMA Post-Quantum Telco Network Taskforce<sup>10</sup>, with IBM and Vodafone as initial members, to help define policy, regulation and operator business processes for the transition towards PQC. For more information, we recommend reading the “Guidelines for Quantum Risk Management for Telco” whitepaper,<sup>11</sup> recently released by the taskforce.

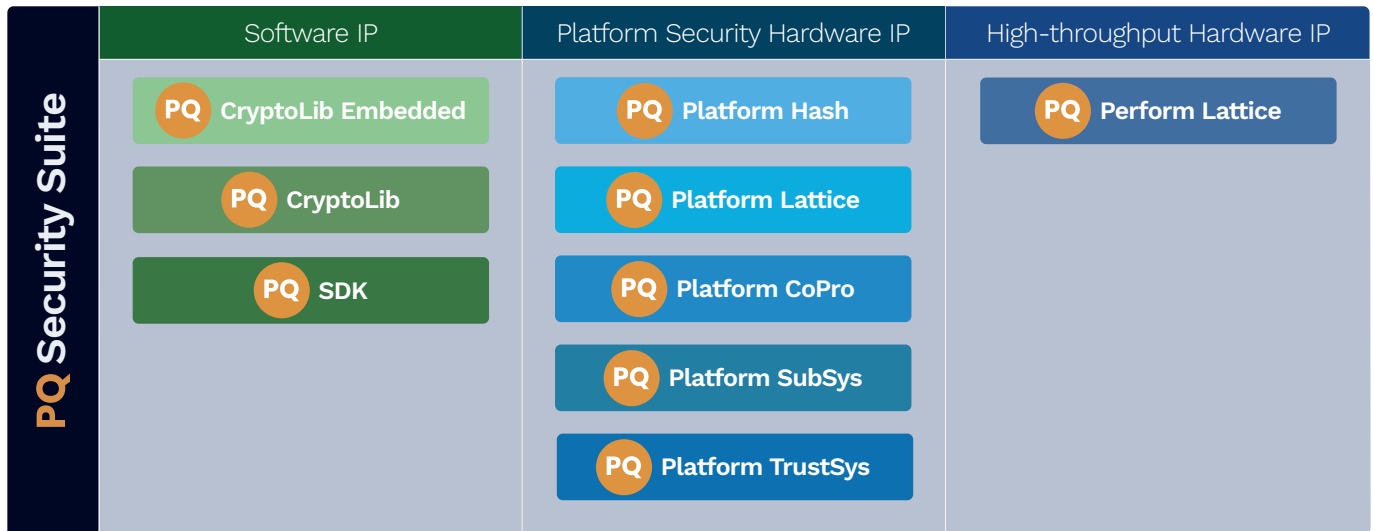
9 <https://content.pqshield.com/cryptography-modernization-part-one>

10 <https://www.gsma.com/newsroom/press-release/gsma-ibm-and-vodafone-establish-post-quantum-telco-network-taskforce/>

11 [https://www.gsma.com/get-involved/working-groups/gsma\\_resources/guidelines-for-quantum-risk-management-for-telco](https://www.gsma.com/get-involved/working-groups/gsma_resources/guidelines-for-quantum-risk-management-for-telco)

# How PQShield Can Help

PQShield comprises a world-leading collaboration of post-quantum cryptographers, researchers and engineers. With headquarters in the UK, we have a team of over 80 specialists in Europe, the US and Japan. We've actively contributed to all of the first international PQC NIST standards and our experts have led multiple projects for the likes of RISC-V, contributing to IETF, ETSI, GlobalPlatform, WEF, GSMA, NCCoE, and other industry associations.



Our PQC solutions are developed for software, FPGA, and ASIC, and are designed and optimized for PQC to deliver exceptional performance, quality, reliability, support, and side-channel resilience (SCA). Our products support PQ/T hybrid and public key cryptography, allowing for simple replacement of existing cryptography IP while meeting the highest security and broadest compliance standards. Our PQC software and hardware solutions are already in the hands of forward-thinking organizations like Microchip, Collins Aerospace, AMD, and many more.



## PQC Software Libraries

**Designed for: software and application developers, systems integrators**

**Use case: update of existing systems or new systems requiring support**

PQCryptoLib is the first cryptographic library in the certification process for FIPS 140-3 CMVP<sup>12</sup>, with further certifications to follow. Meanwhile, the embedded version PQCryptoLib-Embedded requires less than 15 KB of memory and is perfect for updating existing OT and IoT systems with memory-constrained hardware. The TLS-version of PQSDK adds seamless integration with secure communication protocols such as OpenSSL and mbedTLS.

## PQC Hardware IP

**Designed for: silicon and FPGA developers**

**Use case: new processor, Soc and ASIC designs, as well as FPGAs**

PQShield's Platform Security Hardware IP products offer scalable, high security PQC acceleration for processing systems. Our product portfolio ranges from minimum footprint hash accelerators to a fully fledged Root of Trust, and offers flexibility to achieve the ideal combination of low gate count, high-speed processing, and high security.

PQPerform-Lattice, our high-throughput hardware IP, delivers the highest performance and unbeatable resource and power efficiency - the ideal PQC IP solution for HSMs and network processors.

Our hardware IP has been rigorously tested and proven resistant to timing, power, and fault injection attacks. Its crypto-agility has been proven in silicon on our NIST-compliant test chip.

<sup>12</sup> <https://csrc.nist.gov/pubs/fips/140-3/final>



# Ready to learn more?

**Get in touch:** [contact@pqshield.com](mailto:contact@pqshield.com) | [www.pqshield.com](http://www.pqshield.com)

## **PQShield Ltd**

### **Oxford**

Prama House  
267 Banbury Road  
Oxford  
OX2 7HT

### **London**

Office 2.03/4  
51 Moorgate  
London  
EC2R 6BH

## **PQShield SAS**

### **Paris**

WeWork Bercy  
8 Rue des Pirogues  
de Bercy  
Paris  
75012

## **PQShield B.V.**

### **Amsterdam**

Keizersgracht 62  
1015CS  
Amsterdam

## **PQShield Inc.**

### **New York**

228 East 45th Street  
Suite 9E  
New York  
NY 10017

### **California**

900 E Hamilton Ave  
# 100  
Campbell  
CA 95008

