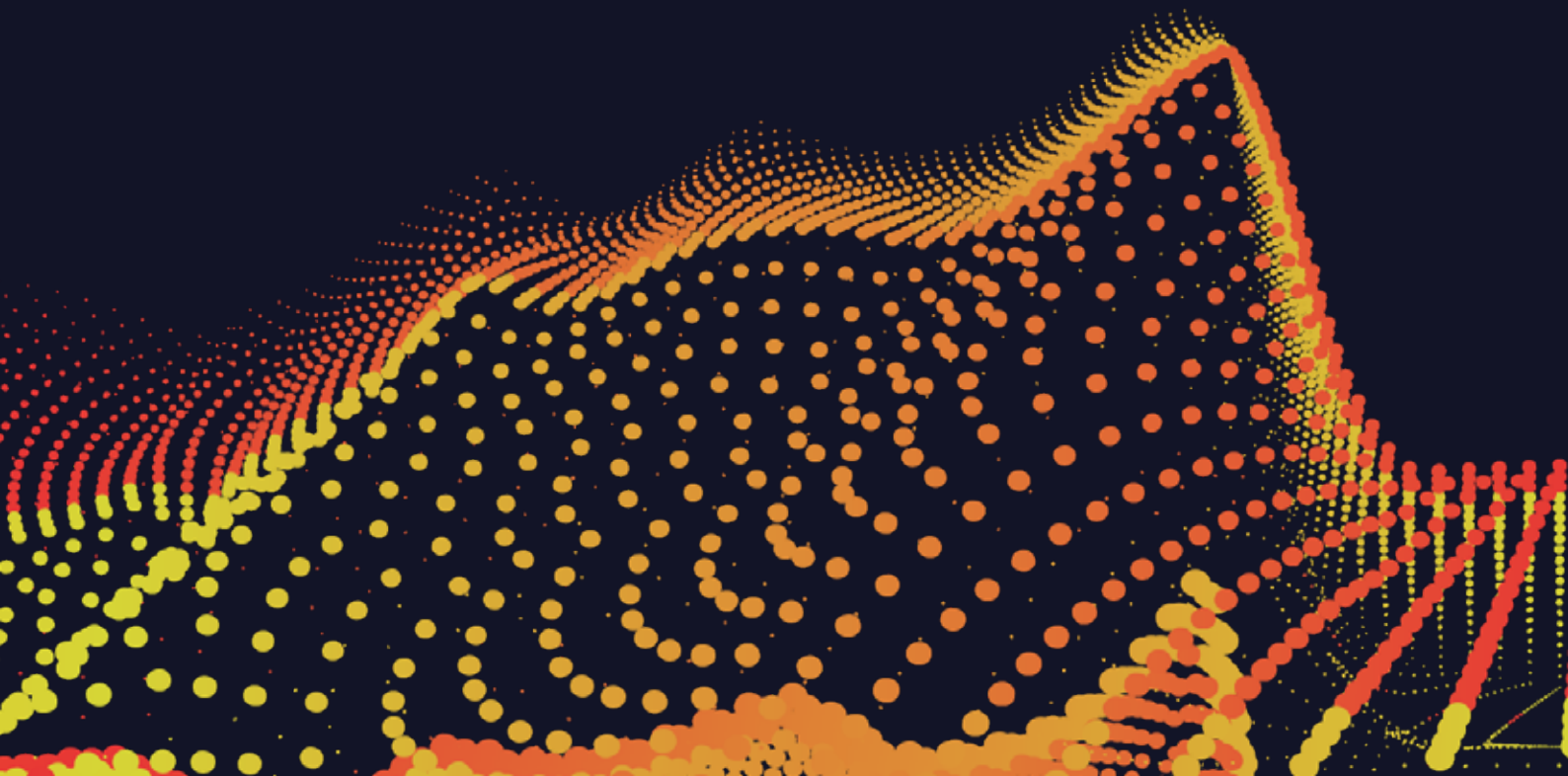
PQ SHIELD

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." [1]



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."[2]

GSMA

NIST standardization

Since 2016, the **NIST Post-Quantum Cryptography Project**[3] has been working towards the standardization of multiple PQC algorithms.

For example, CRYSTALS-Kyber (FIPS 203) is now the draft **standard for public-key encryption** and key encapsulation mechanisms, while CRYSTALS-Dilithium (FIPS 204) has been selected as the preferred **standard for digital signatures** (with Falcon and SPHINCS+ (FIPS 205) as alternative standards for digital signatures). These standards are currently in Draft stage, with the final standards expected by summer 2024.

These algorithms have explicitly been selected with an eye on mass-market applicability, as they have very reasonable requirements regarding computing performance, key size and cybertext size.

The quantum timeline

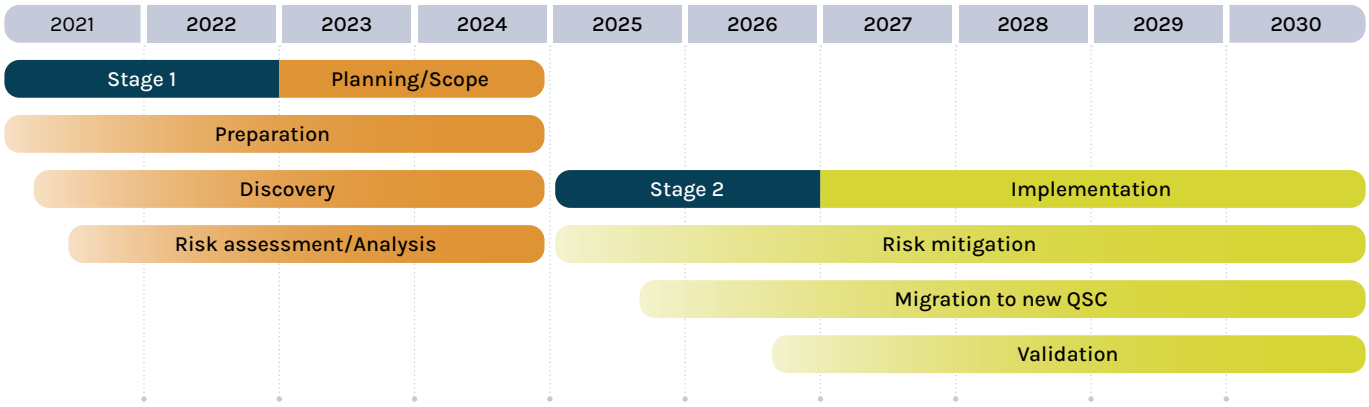
It's thought that 'Q-Day', the date when quantum computers will be powerful enough to break today's cryptography, will happen within the next decade. For high security systems, the German Federal Office for Information Security (BSI) is predicting that cryptographically relevant quantum computers will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

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
2 https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf
3 https://csrc.nist.gov/projects/post-quantum-cryptography
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[5] 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.[6]

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. [7]

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

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2021)	Start planning; early implementation 2025-2026
Canada	NIST	Cyber Centre (2021)	Start planning; impl. from 2025
China	China Specific	CACR (2020)	Start Planning
European Commission	NIST	ENISA (2022)	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022)	Start planning; Transition from 2025
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
New Zealand	NIST	NZISM (2022)	Start planning
Singapore	Monitoring NIST	MCI (2022)	No timeline available
South Korea	KpqC	MSIT (2022)	Start competition First round (Nov.'22-Nov.'23)
United Kingdom	NIST	NCSC (2020)	Start planning
United States	NIST	NSA (2022)	Implementation 2023-2033

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
6 https://www.ibm.com/quantum/quantum-safe
7 https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-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

(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: Identity 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:[9]

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:

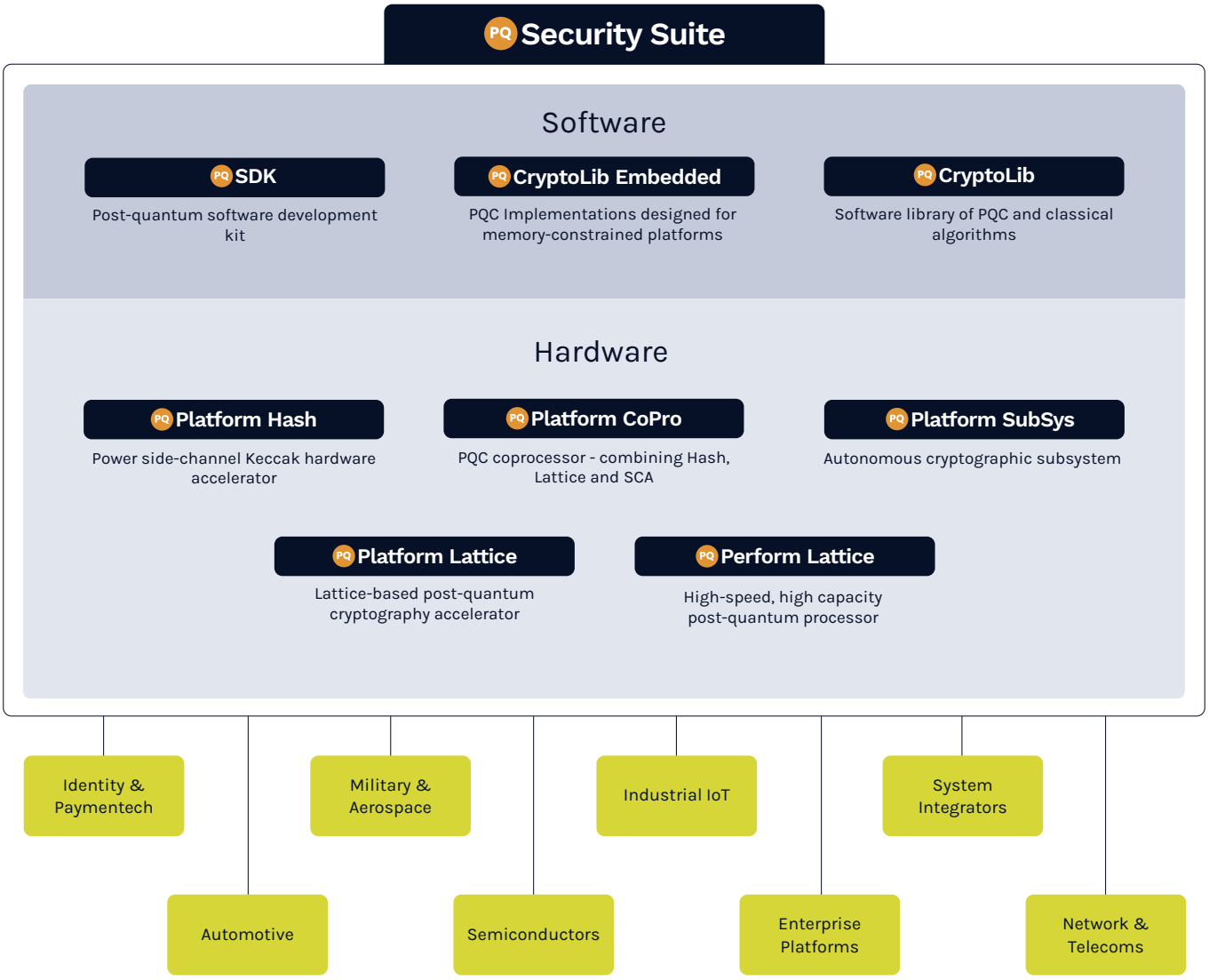
- PQC root security must be implemented into a device's hardware. It cannot be patched later.
- PQC hardware accelerators and PQC-enabled secure subsystems with telecommunications processors will increase efficiency and performance, and reduce total system costs.

In 2022, the GSM Association formed the GSMA Post-Quantum Telco Network Taskforce[10], 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,[11] recently released by the taskforce.

9 PQShield white paper "Cryptography Modernization Part 1: Where is your Cryptography? 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

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 60 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 software and hardware solutions are already in the hands of forward-thinking organizations like Microchip, Collins Aerospace, AMD, and many more.



PQCryptoLib is the first cryptographic library that is already in the certification process for FIPS140-3[12], with further certifications to follow. In addition, PQCryptoLib-Embedded is designed to deploy PQC in situations where memory is constrained, and PQSDK provides a full software development kit to enable PQC in secure communication protocols such as TLS.

PQShield's products excel in performance, quality, reliability, support, and side channel attack (SCA) resilience.

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

PQSHIELD

Ready to learn more?

Get in touch: contact@pqshield.com | www.pqshield.com

PQShield Ltd
Oxford
Prama House
267 Banbury Road
Oxford
OX2 7HT

PQShield SAS
Paris
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

London
City Tower
40 Basinghall Street
London
EC2V 5DE