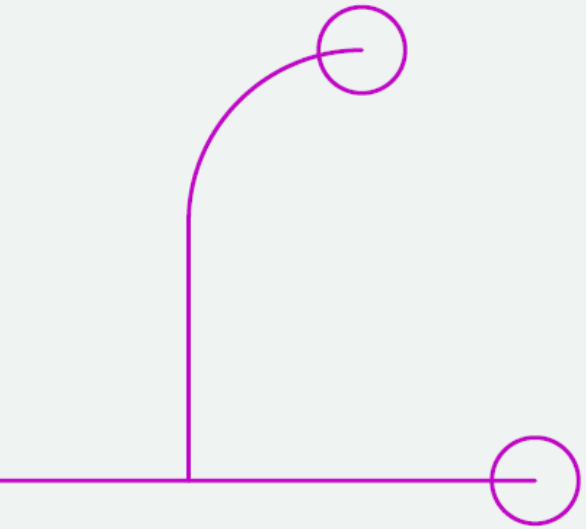
WHITE PAPER

PREPARING FOR THE QUANTUM ERA

A Practical Guide to Post-Quantum Cryptography

Quantum?

Outline



Introduction

Understanding the quantum threat

Understanding post-quantum cryptography

Taking first steps towards post-quantum readiness

Sector-specific use cases

Conclusions

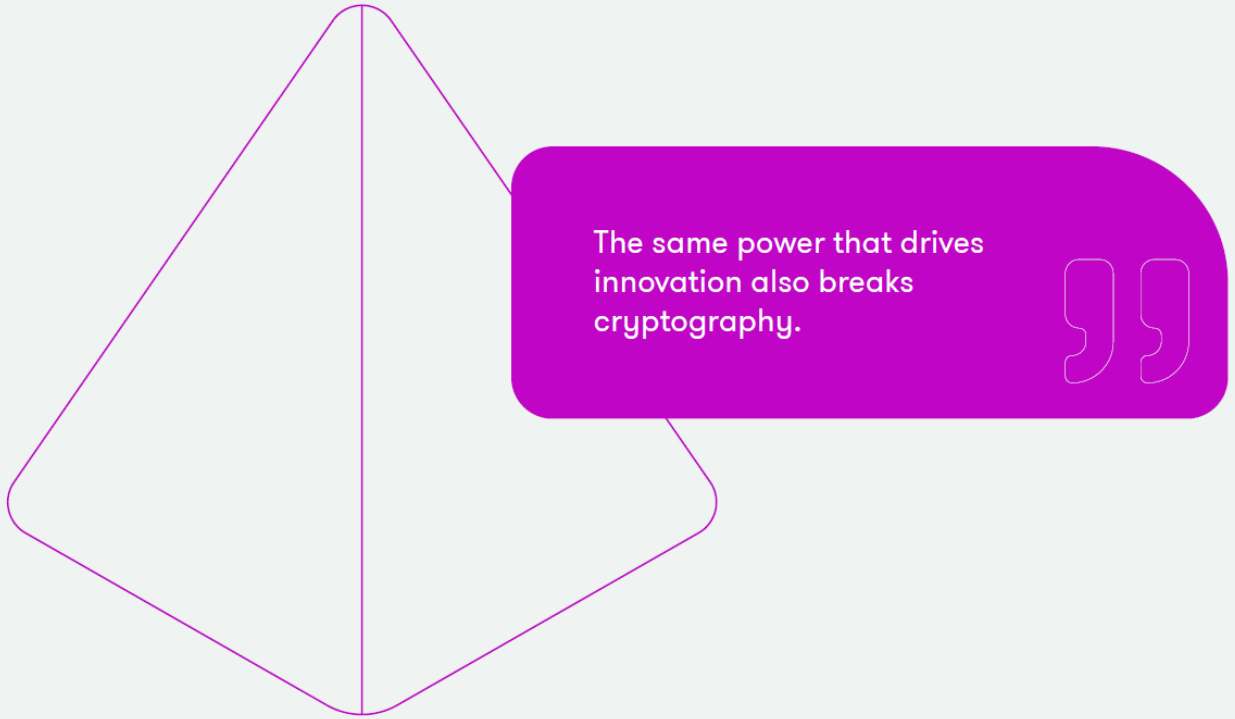
What is quantum?

Quantum computing principles

Quantum computers use superposition and entanglement to process information differently than classical computers.

Transformative applications

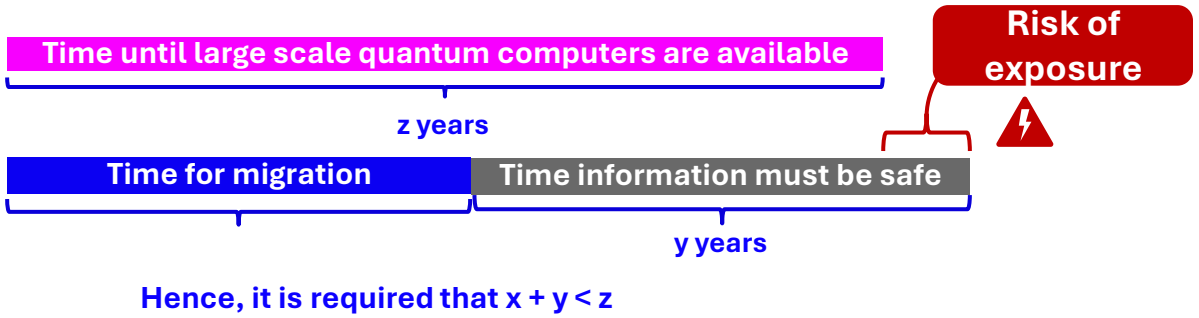
Quantum computing can solve complex problems in materials science, logistics, and artificial intelligence rapidly.



Understanding the quantum threat

The Quantum threat – Why act now?

Data Confidentiality: Harvest Now, Decrypt Later



Hence, it is required that x + y < z

Data Authentication

Depends on the lifetime of a product and the possibility to update it:

Hardware in production sites has a long lifetime and often can't be updated quickly so the same signature might be used in 20 years.

Risk of exposure

Software can be updated quickly and thus there is a possibility to adapt things later on.

No immediate risk of exposure

Understanding the quantum threat

The uncertain timeline

Emergency probability of strong quantum computers

Experts estimate a 19% to 34% chance of cryptographically relevant quantum computers emerging within ten years, rising to 50% by 2039.

Quantum Risk Timeline

Urgency of proactive security

Due to rapid quantum advances, organizations must proactively secure cryptographic infrastructure without waiting for breakthroughs.

But there is a solution:

Post-quantum cryptography (PQC)

Quantum-resistant algorithms

PQC algorithms are designed to resist attacks from both classical and quantum computers using complex mathematical problems.

Key PQC families

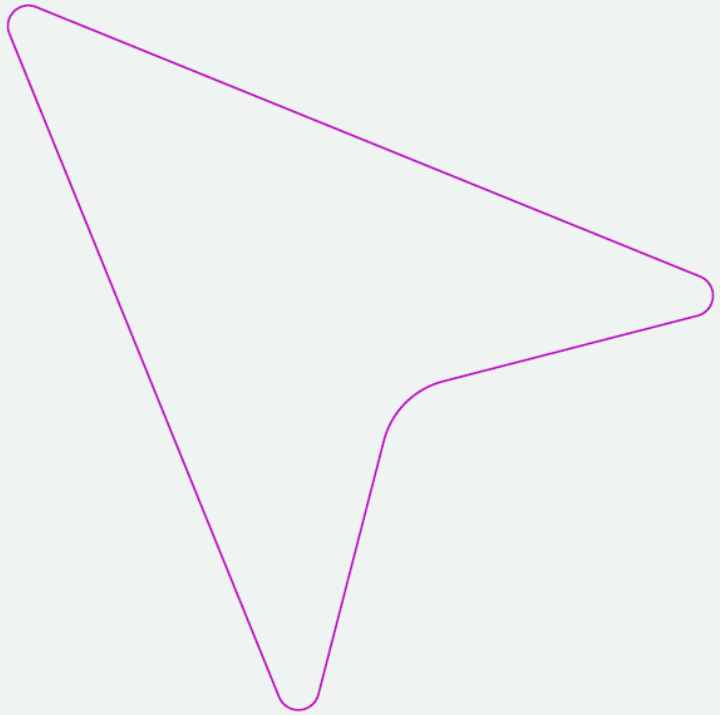
Main PQC types include code-based, lattice-based, multivariate, and hash-based cryptography protecting future communications.

NIST PQC standards

NIST has selected promising PQC standards such as Kyber, Dilithium, SPHINCS+, and Falcon to secure digital systems.

Ongoing challenges

Advanced cryptographic functions like zero-knowledge proofs lack efficient PQC versions, requiring further research.



Taking first steps towards post-quantum readiness

Phase 1: Awareness and assessment

Building awareness

Educate IT, security, and leadership teams on quantum computing and its security implications.

Data sensitivity evaluation

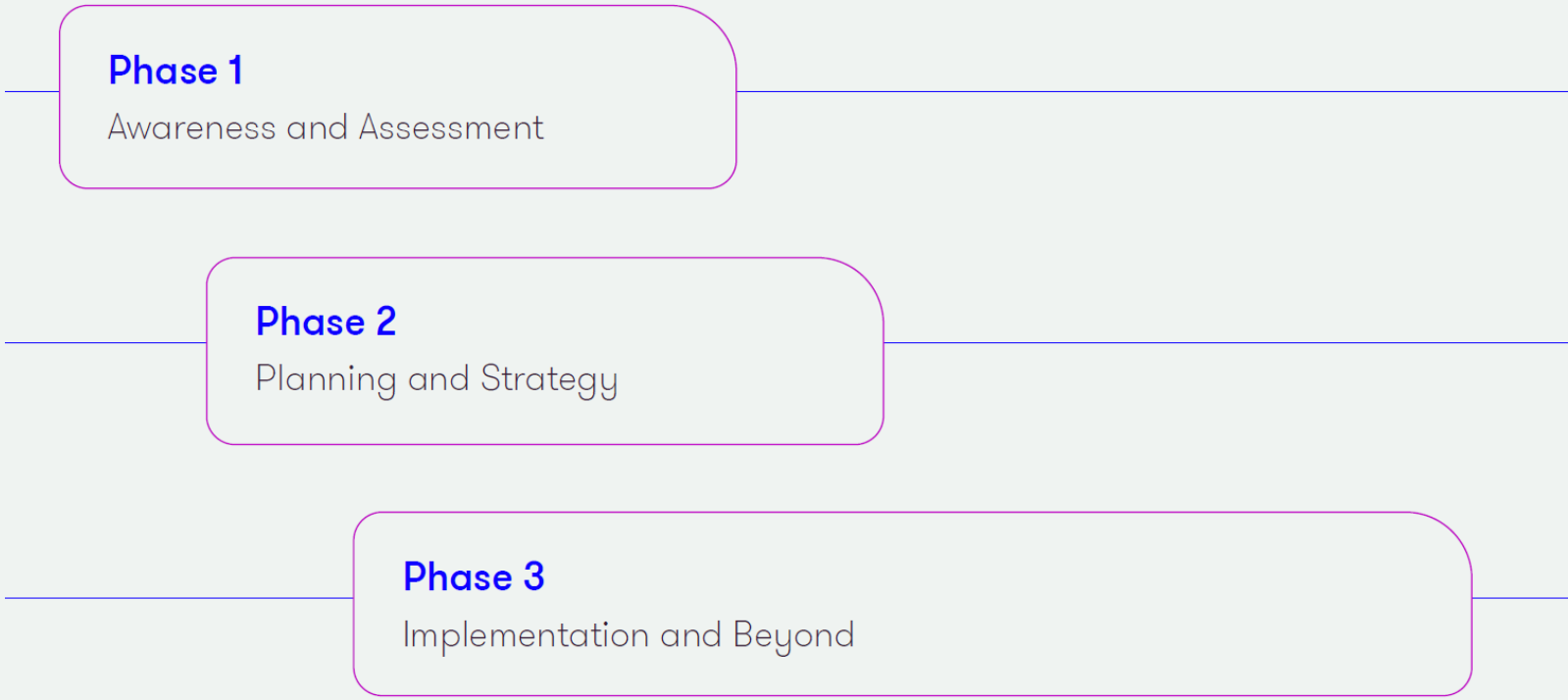
Assess sensitivity, retention, and migration effort to prioritize data for post-quantum cryptography migration.

Cryptographic asset inventory

Compile a detailed inventory of algorithms, libraries, hardware, and vendor dependencies in use.

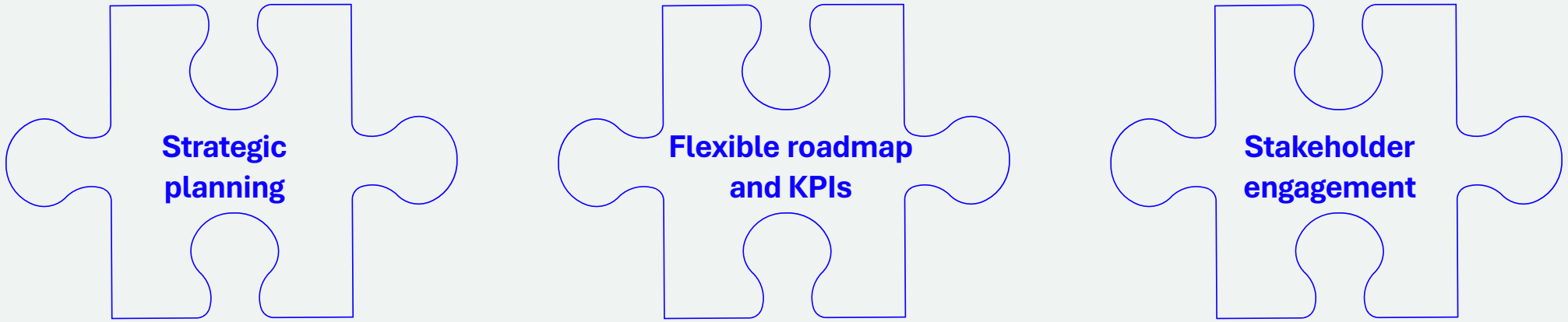
Flagging legacy systems

Identify and mark legacy systems that cannot be upgraded for eventual phaseout.



Taking first steps towards post-quantum readiness

Phase 2: Planning and strategy



Levels	Confidentiality	Transition effort and impact	Asset lifetime
Low	Not significant	< 8 years	< 10 years
Medium	< 10 years	> 8 years low impact	> 10 years low impact
High	>= 10 years	> 8 years high impact	> 10 years high impact

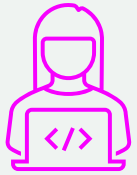
Quantum Risk Levels

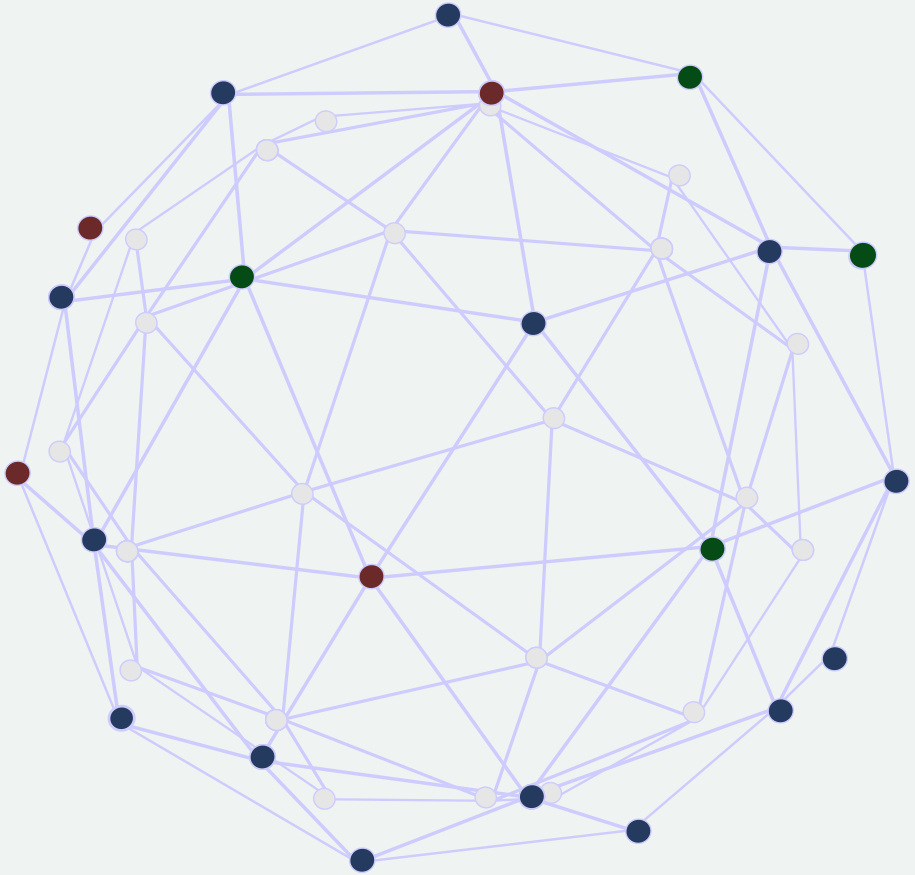
Taking first steps towards post-quantum readiness

Phase 3: Implementation and beyond

Continuous monitoring and adaptation

PQC deployment and prioritization



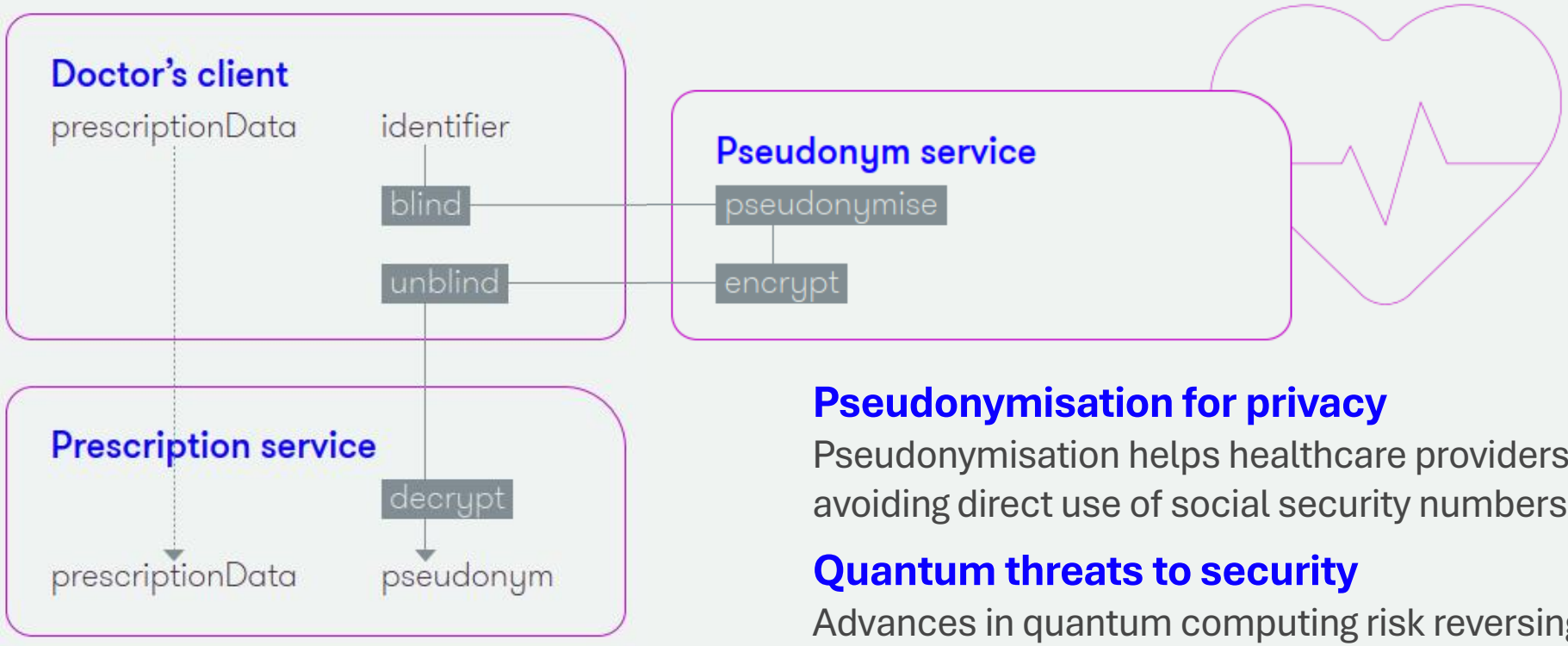


Collaboration and resilience

Crypto-agility and regulatory alignment

Sector-specific use case

Healthcare: Blind identifier pseudonymization



Pseudonymisation for privacy

Pseudonymisation helps healthcare providers protect patient data by avoiding direct use of social security numbers.

Quantum threats to security

Advances in quantum computing risk reversing pseudonymisation, challenging current cryptographic protections.

Roadmap to quantum readiness

Healthcare providers plan to migrate to post-quantum cryptography, design quantum-resistant algorithms, and adopt crypto-agility.

Conclusion

Call to action

Quantum threat to cryptography and Necessity of strategic migration

Quantum computing poses a **significant risk** by potentially breaking current cryptographic systems, creating urgent cybersecurity challenges.
Migrating to post-quantum cryptography requires **organization-wide planning**, vendor cooperation, and strong leadership.

Benefits of early action

Early adoption safeguards data, builds trust with stakeholders, and positions organizations for future success.
Leading in quantum readiness demonstrates **resilience** and foresight in a rapidly evolving digital world.

By 2026
National strategies and awareness campaigns established by Member States.

By 2030
Critical infrastructure and high-risk use cases protected with PQC.

By 2035
Broad adoption across all sectors and lower-risk use systems completed.

Questions?

Thank you!