VTT

Preparing for post-quantum cryptography

A playbook for protecting your organisation’s data in the quantum era

beyond the obvious

Introduction

By the end of the decade, some industry estimates suggest that organisations should already have transitioned to post-quantum cryptography – yet most organisations and societies are not prepared for the shift. With major standards bodies such as The National Institute of Standards and Technology (NIST) aiming to phase out current cryptography by the early 2030s, the window to prepare for the quantum era of cybersecurity is already closing.

This marks a fundamental shift in how digital trust is built and maintained. Cybersecurity in the quantum era is not only about replacing current algorithms, but about safeguarding the systems, services and data that modern life depends on before today's protections become vulnerable.

Cryptography operates quietly in the background of almost everything we do, from financial transactions to healthcare systems, software updates and connected infrastructure. This is precisely what makes the transition so challenging. Cryptography is often deeply embedded and poorly documented, making implementing changes complex. To move forward, organisations need a clear understanding of where cryptography exists, how it is used and how it can be updated without disrupting operations.

This playbook helps you take the first step towards post-quantum cryptography. It focuses on understanding how the transition affects your organisation and how to begin moving forward in a structured and manageable way.

About this playbook

This playbook is a practical guide for decision-makers and technology teams navigating the transition to post-quantum cryptography. It translates complex developments in quantum computing and cryptography into clear, actionable steps that organisations can take today.

The content is based on insights from experts of VTT, working at the forefront of cryptography, cybersecurity and emerging technologies. It combines research-based knowledge with practical experience from real-world systems, helping organisations understand both the scale of the challenge and how to approach it in practice.

This playbook offers:

- A clear explanation of what post-quantum cryptography is and why it matters now
- An overview of the technological developments accelerating the transition
- Insight into the key barriers organisations face and how to overcome them
- Practical steps to get started with post-quantum cryptography
- A forward-looking view on how to build long-term resilience in the quantum era

Chapter 1: What is post-quantum cryptography and why does it matter now?

Post-quantum cryptography refers to new cryptographic methods designed to remain secure even in the era of Cryptographically Relevant Quantum Computers (CRQCs). Unlike today's widely used encryption algorithms, these methods are based on different mathematical approaches that are currently considered secure against quantum computers.

This may sound like a niche technical problem, but in reality, it underpins almost every digital interaction.

Today, cryptography secures financial transactions, protects sensitive data, enables software updates and ensures that devices, systems and users can trust each other. In many cases, it operates invisibly in the background – which is precisely why it is often overlooked.

Quantum computing changes this foundation. As the technology advances, it is expected to be able to break many of the cryptographic algorithms currently used to secure digital systems. This foundational change does not happen overnight, but safeguards must be put in place already now to ensure that today's data remains secure in the future. After all, sensitive data can already be harvested and stored for later decryption once more powerful quantum capabilities become available. In the future, quantum attacks could also undermine digital trust by, for example, enabling the forgery of digital signatures and compromising the integrity of digital identities.

This makes the transition to post-quantum cryptography both unavoidable and urgent. And the challenge is not only technological, but also systemic. Cryptography is deeply embedded in software and digital infrastructure, while often being poorly documented, making it difficult for organisations to fully understand where and how it is used within their own systems. As a result, the shift to post-quantum cryptography is not a simple upgrade. It is a large-scale transformation that affects systems, processes and entire ecosystems.

Done right, the transition can deliver more than post-quantum cryptography: it can give organisations better visibility into their systems, such as cryptographic key management, and strengthen trust and resilience across critical digital operations

Harvest now, decrypt later attack

Attackers collect and store encrypted data today, even if they cannot read it yet. Once cryptographically relevant quantum computers become available, attackers can break current encryption methods and reveal sensitive information such as personal data, financial records, confidential communications or intellectual property.

Trust now, forge later attack

In the future, attackers could use cryptographically relevant quantum computers to forge digital signatures, which are used to verify identity and authenticity online. This would allow them to forge software updates, fake identities, impersonate trusted organizations or alter signed documents and transactions, undermining trust in digital systems.

Chapter 2: What is accelerating the shift to post-quantum cryptography?

The shift towards post-quantum cryptography is not driven by a single breakthrough, but by progress across several areas of technology and research, making the overall trajectory difficult to predict. Together, these developments are accelerating both the capabilities of quantum computing and the need to prepare for its impact.

Advances in quantum computing hardware are making quantum systems more reliable by improving qubit stability and reducing errors, allowing these systems to handle increasingly complex calculations. At the same time, advances in quantum algorithms and software are reducing the number of qubits needed to solve complex problems, bringing closer the point at which current cryptographic methods may be broken. Because progress is happening on many fronts at once, the timeline for when quantum computing will have a practical impact on cryptography remains uncertain. What is clear, however, is that this moment is steadily moving closer.

At the same time, significant progress has been made on the defensive side. Over the past decade, new cryptographic standards have been developed specifically to withstand quantum attacks, with organisations such as NIST leading their standardisation. Several of these standards have already been published and are considered ready for deployment, with early adoption underway.

Beyond algorithms, new tools and approaches are also emerging to support the transition. For example, forward-thinking organisations have begun to develop ways to map and manage their cryptographic assets, sometimes referred to as cryptographic inventories or bills of materials. There is also growing interest in using automation and artificial intelligence to support this work, with solutions continuing to mature.

Together, these developments highlight a key reality: the transition is no longer a distant concern. Instead, it is being shaped by technological progress that both increases the urgency to act and makes the transition more achievable.

Chapter 3: Barriers and enablers

As the threat posed by quantum computing becomes clearer, many organisations struggle to move from awareness to action in adopting post-quantum cryptography. By understanding both the challenges and the enablers of the transition, organisations can begin to turn uncertainty into structured action.

At the core of many of these challenges is a lack of visibility. Cryptography is deeply embedded across systems, applications and devices, often without clear documentation. As a result, many organisations do not fully know where cryptography is used, which algorithms are in place or how critical systems depend on them. Without this understanding, planning a transition becomes difficult.

The scale of the task adds another layer of complexity. Unlike previous cryptographic updates, which often focused on replacing a single algorithm, the transition to post-quantum cryptography affects entire digital infrastructures, including systems such as Public Key Infrastructure (PKI).

In practice, the transition to post-quantum cryptography is widely expected to be a multi-year effort. Previous cryptographic migrations have taken more than a decade to complete, and the transition to post-quantum cryptography is expected to be even more demanding in terms of scope and coordination.

The urgency of the transition is shaped by three factors:

1. When will current cryptography become vulnerable?
2. For how long must sensitive data remain confidential?
3. How long will the transition itself take?

There is also uncertainty around standards and implementation. While new cryptographic standards are emerging, organisations may hesitate to act due to concerns about choosing the wrong solutions or investing too early. This can lead to a “wait and see” approach which, in practice, increases risk rather than reduces it.

At the same time, a smooth transition requires a set of core capabilities.

A structured approach to understanding and managing cryptography is a critical first step. Building visibility into where and how cryptography is used allows organisations to assess risks, prioritise actions and plan the transition in a controlled way.

In the quantum era, crypto-agility becomes a necessary operating model for information security. In practice, this means moving towards system architectures where cryptography is managed through dedicated interfaces, rather than embedded directly into application logic. This approach makes it easier to adapt security mechanisms as standards, threats and requirements evolve.

Finally, effective process and governance play a central role. The transition to post-quantum cryptography is not a one-off technical upgrade, but a long-term capability that requires coordination across teams, functions and partners.

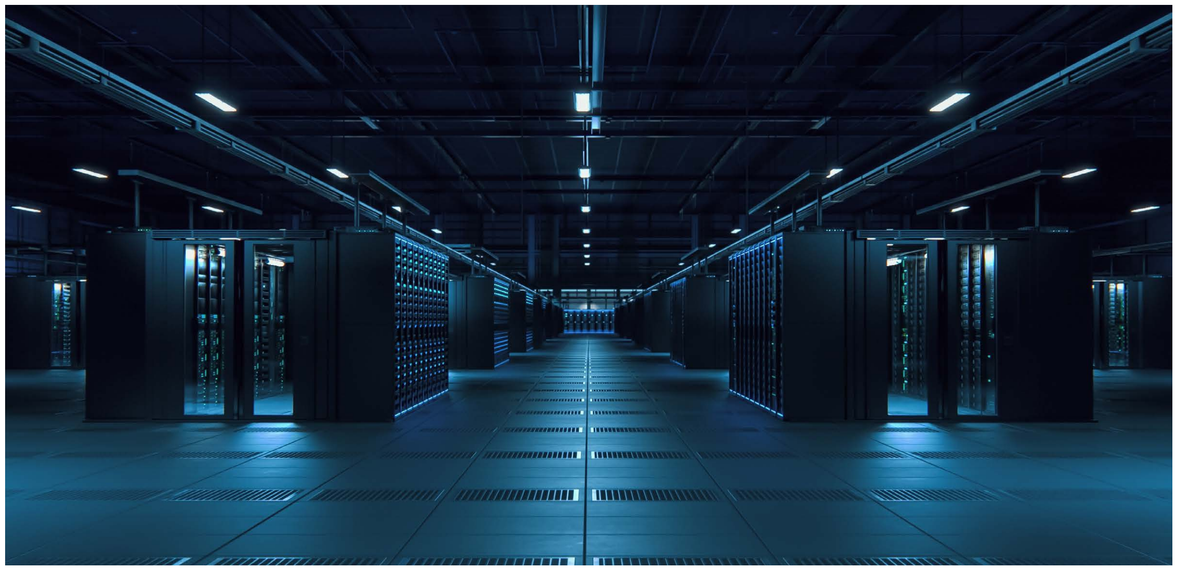
Chapter 4: Navigating the policy landscape

The policy landscape for post-quantum cryptography is evolving, but not yet fully defined. While the risks enabled by quantum computing are increasingly recognised, clear and comprehensive regulatory guidance is still emerging.

In Europe, frameworks such as NIS2 Directive and Digital Operational Resilience Act (DORA) are raising the bar for cybersecurity and resilience. While they do not yet contain comprehensive requirements for transitioning to post-quantum cryptography, discussions around explicit post-quantum cryptography obligations are already underway. This signals a broader regulatory direction in which organisations may increasingly be expected to demonstrate preparedness for the transition to post-quantum cryptography.

At the same time, developments outside Europe are moving faster. In the United States, government-led initiatives and timelines are already pushing organisations, particularly those linked to critical infrastructure, to prepare for the transition. For companies doing business in the US or with US-linked partners, this may translate into concrete requirements, such as the need to demonstrate how post-quantum cryptography has been addressed.

This creates a ripple effect. Organisations may find that post-quantum cryptography becomes a requirement not through direct regulation, but through customers, partners and procurement processes. In critical sectors such as finance, energy and infrastructure, the ability to demonstrate preparedness may become a condition for doing business.



Chapter 5: How to get started with the transition?

Getting started with post-quantum cryptography does not require a complete transformation at once. What matters most is taking the first steps in a structured way.

While every organisation's situation is different, three practical actions help move from awareness to action.

1. Understand how the risk applies to your organisation

The first step is to understand how quantum-related risks affect your organisation, your systems and your data.

For some organisations, the impact may be indirect. If you rely on external software or service providers, the key question is how those providers are preparing for the transition.

As a practical first step, review your key vendors and find out how they are addressing post-quantum cryptography. Larger providers are likely to have plans in place, but for smaller vendors, this may not yet be the case. Ensuring that partners and suppliers can demonstrate their approach is an important part of managing risk.

For organisations that develop their own systems or products, the implications are broader. These organisations need to assess how cryptography is used across applications, infrastructure and devices, and how potential vulnerabilities could affect operations, customers and long-term cybersecurity.

2. Gain visibility through a cryptographic inventory

Once the relevance is understood, the next step is to build visibility.

Many organisations do not have a clear, up-to-date view of where cryptography is used within their systems. Creating a cryptographic inventory helps identify which algorithms, libraries and protocols are in use and where and why they are applied.

This can be done manually as a starting point, but automation and specialised tools can help scale the process.

Establishing this visibility is a critical foundation. Without it, prioritising actions or planning a transition becomes close to impossible.

3. Start the transition in a controlled way

With visibility in place, organisations can begin the transition towards post-quantum cryptography.

This typically involves

- establishing practices for flexible, repeatable cryptographic changes
- adapting (crypto-agile) system architecture
- updating cryptographic components
- thoroughly testing systems

In many cases, this work takes place alongside ongoing operations, making planning and prioritisation essential.

Designing systems to be crypto-agile can help reduce the complexity, risk and effort associated with future cryptographic updates. By separating cryptographic details from application code and managing them through dedicated interfaces, organisations can make future updates more manageable and less disruptive.

The goal is not to complete the transition immediately, but to start building the capability to adapt as standards, technologies and requirements evolve.

Chapter 6: Future outlook

The transition to post-quantum cryptography is not a one-off project. Standards, algorithms and implementation practices will continue to evolve, so organisations need the ability to keep adapting over time.

In the future, crypto-agility should become a core part of information security. Systems should be designed so that cryptographic components can be updated as requirements change, without causing unnecessary disruption to operations. This shift will help organisations respond not only to quantum-related risks, but to future vulnerabilities, implementation flaws and new security expectations.

Acting now helps ensure that today's information remains secure and digital operations remain resilient in the future. By building visibility, strengthening governance and progressing step by step, organisations can reduce risk and build a more resilient foundation.

Instead of trying to predict exactly when quantum computing will change the rules of digital security, focus on ensuring your organisation is ready when it does.

Partner with VTT

The transition to post-quantum cryptography is complex, but you don’t have to navigate it alone. As one of Europe’s leading research, development and innovation partners, VTT helps organisations bring clarity to a complex transition.

VTT can help with:

Understanding the scope and impact of the transition

Gain a clear picture of what post-quantum cryptography means for your organisation, your systems and your business.

Building an inventory of your cryptographic assets

Build visibility into where and how cryptography is used across your systems and what needs to be addressed.

Designing and implementing practical transition paths to post-quantum cryptography

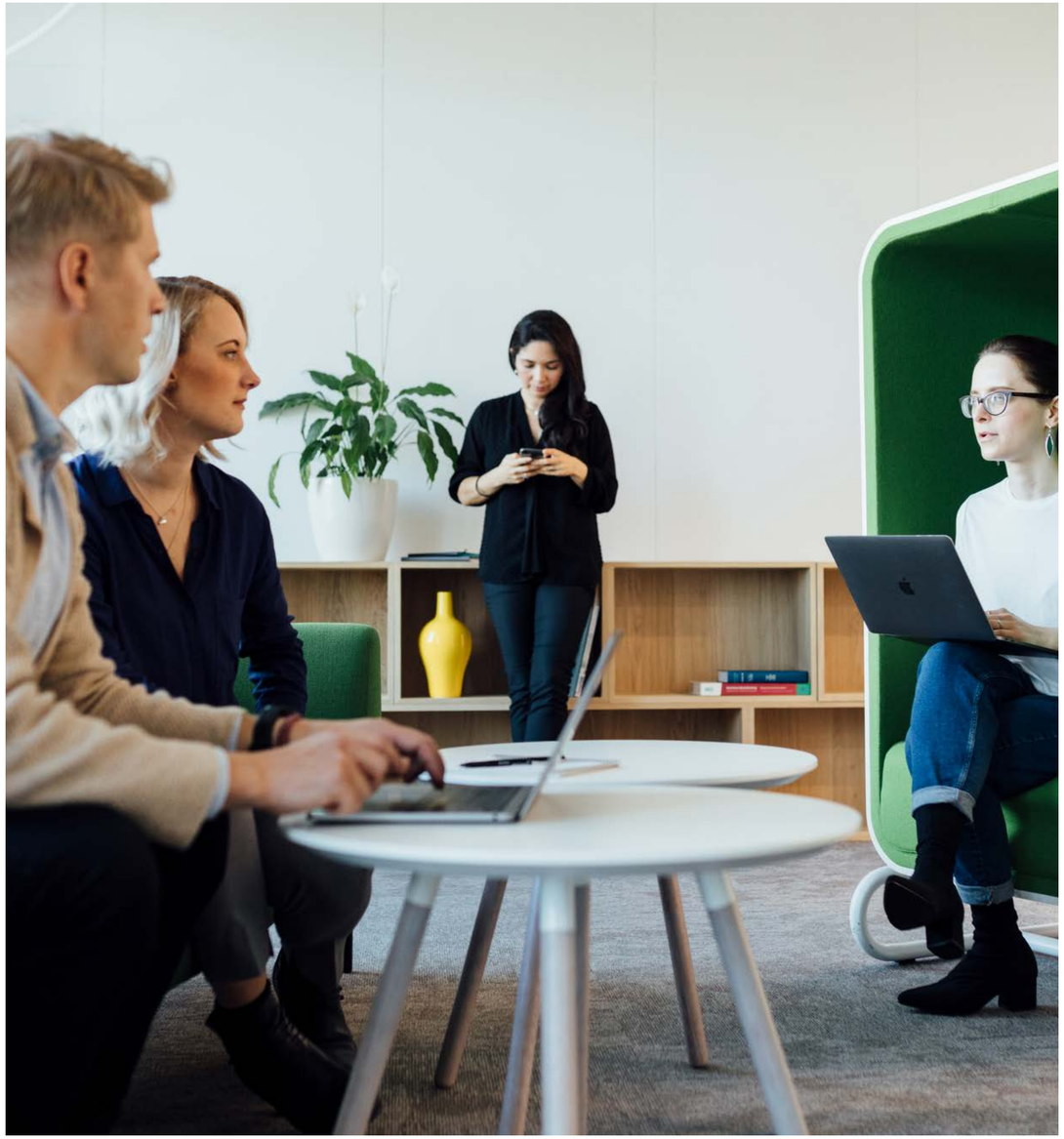
Define and carry out the steps needed to migrate systems towards new cryptographic methods in a controlled and scalable way.

Navigating evolving standards and regulatory expectations

Stay informed about emerging policies and industry requirements and understand how to get started in your specific context.

Get in touch to explore collaboration opportunities.

Mikko Salomaa
Solution Sales Lead
+358405057675
mikko.salomaa@vtt.fi



beyond the obvious

VTT is a visionary research, development and innovation partner for businesses and society and one of the leading technical research organisations in Europe. We have over 80 years of experience in cutting-edge research and science-based results. Our more than 2,000 professionals work to develop systemic and technological solutions that can bring about fundamental transformation.

We promise to always think beyond the obvious.

www.vttresearch.com