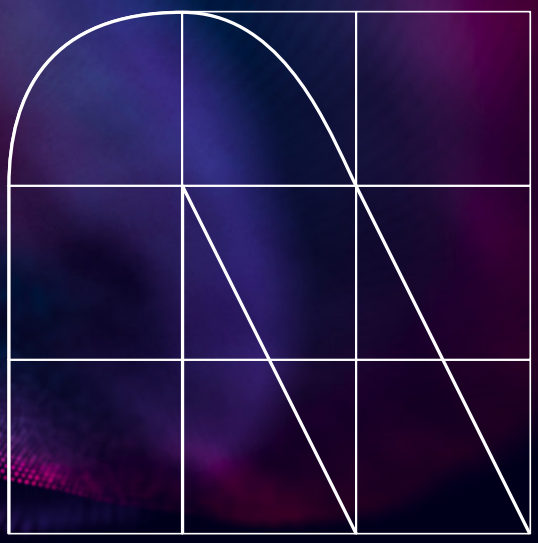
NTT DATA

July 2025

Are you ready for Q-Day? Prepare now for post-quantum cryptography

A guide to the post-quantum era in the European public sector



Making sense of a post-quantum world

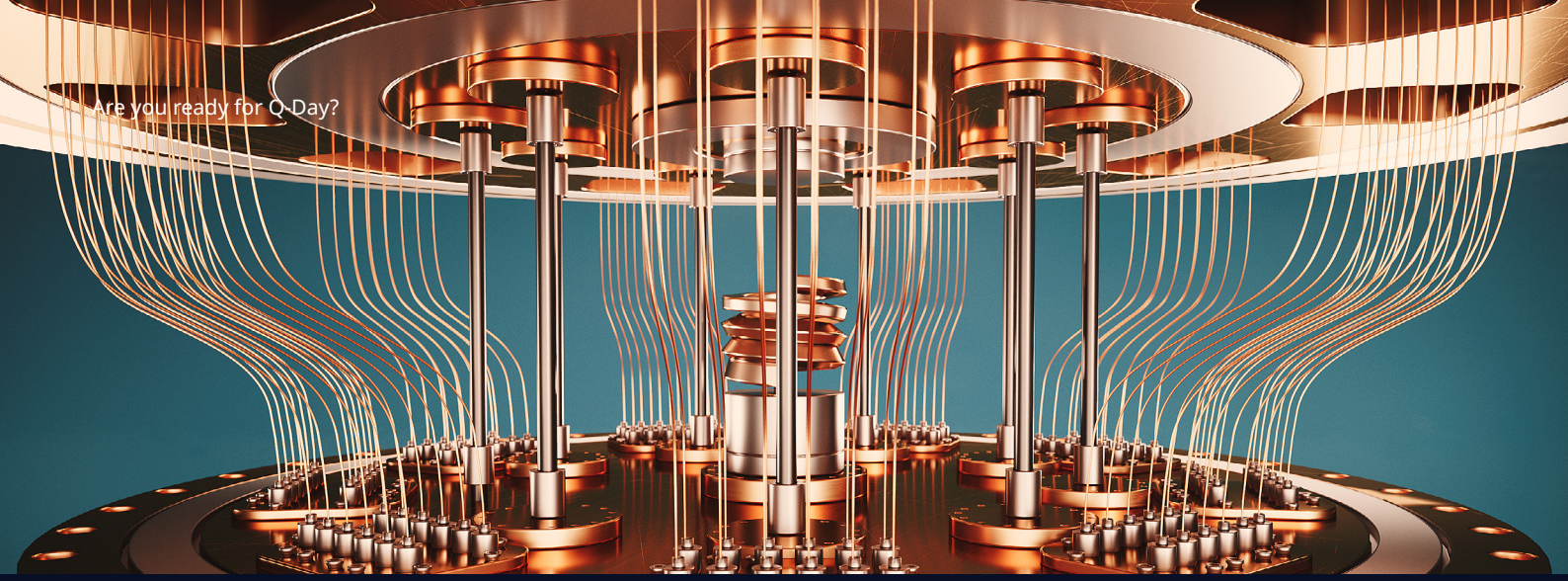
What is post-quantum cryptography? Is it Y2K all over again? Will our passwords, files, text, emails, photos and other data be safe? How much will it cost, and how long will it take to upgrade our security?

The aim of this guide is to help policymakers, public-sector managers and other stakeholders understand and prepare for what has been dubbed "Q-Day" — the day (or era, to be more precise) when a strong enough quantum computer will make today's most sophisticated encryption methods ineffective.

We provide an overview of the state of quantum computing and explain why this technology holds both benefits and threats, especially in cryptography.

To fully understand the potential attack surface of current cryptographic implementations, we take a small step back to the basics of cryptography and show why these implementations are insufficient in the quantum-computing era. Then we discuss how organizations can become quantum-safe.

Finally, before highlighting NTT DATA's expertise, experience and approach, we set out the key considerations and challenges organizations must navigate when preparing for the post-quantum era.



What is quantum computing?

Several countries and private entities are racing to develop quantum-computing capabilities, and the technology promises to be disruptive.

Quantum computers can perform an enormous number of calculations simultaneously, which means they can solve problems much faster than classical computers using the standard mode of computing that's been in place for the past few decades.

Classical computers work with standard bits, which can have only one of two values: 0 or 1. And they work sequentially, processing billions of bits one by one, one possibility at a time.

Quantum computers, on the other hand, rely on quantum-mechanical phenomena known as "qubits," or quantum bits. Unlike standard bits, qubits can be in two states simultaneously ("superposition") and the state of one qubit can depend on that of another, no matter how far apart they are ("entanglement").

Two ways to fill out your tax form

1 The traditional approach

Using a standard computer, you enter each number one at a time and go through each form and calculation step by step. You get there in the end, step by step, but it's a slow process.

→

2 The quantum approach

A quantum computer can look at all your financial documents at once. It considers every possible deduction and scenario simultaneously (superposition), and if one part of your finances changes, it instantly updates related parts (entanglement).

In the business world, quantum computing has applications in data analytics, AI, optimization, simulation and data management.[1] However, its capabilities can also be exploited to compromise the cryptographic systems that are now in use.

1 Kelvin Leong and Anna Sung. What business managers should know about quantum computing? Journal of Interdisciplinary Sciences, Volume 6, Issue 2. November 2022.

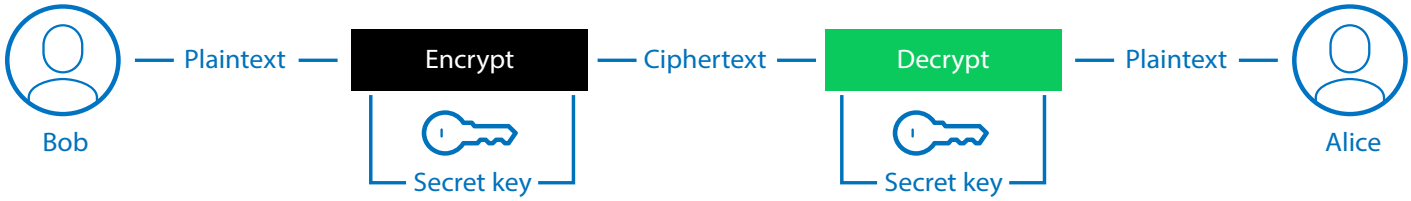
Classical encryption systems

Let's take a step back to understand why current algorithm standards are vulnerable to quantum computing.

Pre-1970s: The symmetric key

Before the 1970s, when two parties — let's call them Alice and Bob — wanted to exchange encrypted or signed messages, they had to use a symmetric (preshared) key.

Exchanging this key was a challenge, though. Besides the fact that it wasn't always practical to meet in person to exchange keys, there was also the risk of the exchange being intercepted. And what if John wanted to share information with Carlos, Dave and Erin, too?



Picture 1

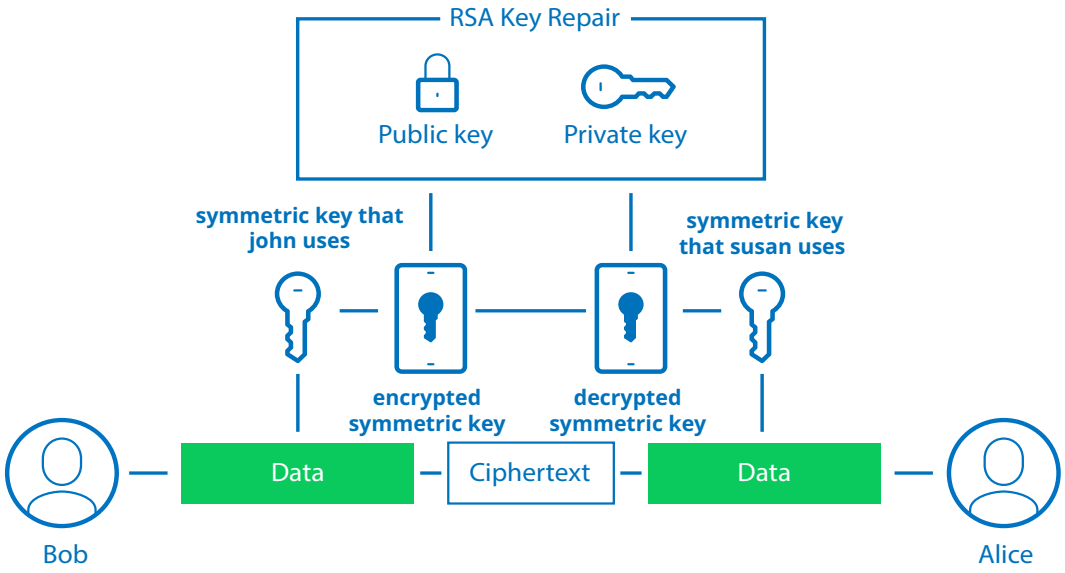
1970s: Asymmetric (public-key) cryptography

In the 1970s, researchers introduced the concept of asymmetric or public-key cryptography. This concept was based on the principle of a public key, which can be shared publicly, and a mathematically linked private key, which must always remain secret.

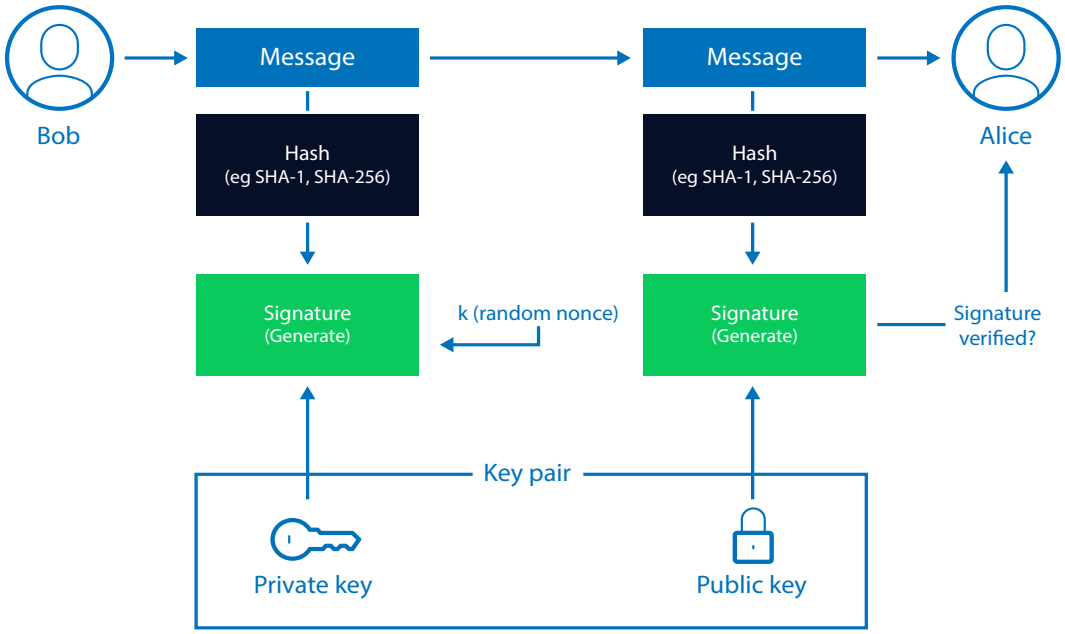
Public–private key pairs are not used to encrypt, decrypt or sign large messages directly due to performance limitations. Instead, they are used to encrypt and decrypt symmetric keys (in hybrid encryption schemes – picture 2) and to sign and verify message digests or hashes (in digital signature schemes – picture 3). As such, they help to solve the key-sharing problem Susan and John faced earlier.

Securing messages with the hash function

An algorithm called a hash function can be used to convert a message of any size into a fixed-length string of apparently random characters. It is not feasible to retrieve the original message from the hashed output.



Picture 2



Picture 3

Since the 1970s, various asymmetric algorithms have been introduced, refined and standardized. These include:

- Rivest Shamir Adleman (RSA)
- Elliptic curve cryptography (ECC)
- Diffie–Hellman key exchange
- Digital Signature Standard (DSS)

These algorithms are built on tough mathematical problems like the integer factorization problem (IFP) and the discrete logarithm problem (DLP). They are considered secure because solving either problem would take regular computers an extremely long time — often years, or even centuries — making it practically impossible with today's technology.

For quantum computers, however, solving factoring or discrete logarithm challenges is easy, at least, in theory

1994: Quantum computing challenges the status quo

In 1994, mathematician Peter Shor developed the first of various theoretical quantum algorithms that would allow quantum computers to solve the IFP or the DLP.

It is not yet possible to deploy these algorithms on quantum computers, as they need more qubits than are currently available as well as many hours of stable operations.

However, advances are being made. In 2024, researchers cracked an RSA key of 50 bits.[2] (To put things in perspective, the National Institute of Standards and Technology (NIST) in the US currently still recommends using key sizes of at least 2,048 bits.) [3]

[2] Chao Wang, Qi-Di Wang, Chun-Lei Hong, Qiao-Yun Hu and Zhi Pei. Quantum annealing public key cryptographic attack algorithm based on D-wave advantage. Chinese Journal of Computers, Volume 47, Number 5. May 2024.

[3] NIST Information Technology Laboratory. NIST SP 800-57 Part 1 Rev 5: Recommendation for key management: Part 1 – General. May 2020.

Standards for Q-Day

When will Q-Day come? Will a specific day or event mark the onset of post-quantum cryptography, or will it happen quietly without public knowledge? When will it become possible to crack 2,048-bit RSA keys easily, and how long will it take?

It could become a reality tomorrow, within five, 10 or 20 years, even longer — or never. The consensus of 32 experts in the 2024 Quantum Threat Timeline report is that the realization of a cryptographically relevant quantum computer is not a case of "if" but "when." They estimate there is a 19% to 34% likelihood of Q-Day happening in the next decade, and a 50% to 98% likelihood of it happening in the next 30 years.[4]

National Institute of Standards and Technology (NIST)[5]

Standard	Security strength	Transition
Key establishment based on Diffie–Hellman and MQV over finite field and elliptic curves (SP 800-56A)	112-bit security strength (~2,048 bit keys)	Deprecated after 2030, disallowed after 2035
	128-bit and higher security strength (~3,096 bit keys)	Disallowed after 2035
Key establishment based on RSA (SP 800-56B)	112-bit security strength (~2,048 bit keys)	Deprecated after 2030, disallowed after 2035
	128-bit and higher security strength (~3,096 bit keys)	Disallowed after 2035
Digital signatures include RSA, ECDSA, EdDSA (FIPS 186-4).	112-bit security strength (~2,048 bit keys)	Deprecated after 2030, disallowed after 2035
	128-bit and higher security strength (~3,096 bit keys)	Disallowed after 2035

As an alternative, they have selected and published new post-quantum cryptography standards.[6]

[4] Global Risk Institute. Quantum Threat Timeline Report 2024. December 6, 2024.

[5] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson and David Cooper, NIST. NIST IR 8547: Transition to Post-Quantum Cryptography Standards. November 12, 2024.

[6] Federal Register, US Government. Notices, Volume 89, Number 157. August 14, 2024.

The standardized algorithms are:

- Federal Information Processing Standard (FIPS) 203 (based on ML-KEM, the module-lattice-based key-encapsulation mechanism)
- FIPS 204 (based on ML-DSA, the module-lattice-based digital-signature algorithm)
- FIPS 205 (based on SLH-DSA, the stateless hash-based digital-signature algorithm)

FIPS 206 standardization — built around FALCON, a cryptographic digital-signature algorithm based on the NTRU lattice problem and the fast Fourier transform algorithm, or FN-DSA for short. Its final release is expected soon, following the draft publication in March 2025.

Hamming Quasi-Cyclic (HQC), which has been announced on March 11th, 2025, will serve as a backup for ML-KEM, the main algorithm for general encryption.[7]

While the NIST standardization process is continuing in the US, with calls for other algorithm candidates based both on the key-exchange mechanism and on the digital signature, standardization efforts in other countries will also eventually result in new cryptographic standards.

European Commission (EU) recommendations

In the European Union, the European Commission has issued a comprehensive set of recommendations to member states, with post-quantum cryptography additions for KEM. The Commission makes explicit reference to the Network and Information Systems Directive 2 (NIS2), which updates and expands the original NIS Directive aimed at strengthening the cybersecurity posture of EU member states.

This underscores the crucial role of post-quantum cryptography in achieving a high level of cybersecurity across the EU. The recommendation encourages member states to coordinate their efforts in migrating to post-quantum cryptography and work together to develop a detailed, unified roadmap.

The recommendation encourages member states to coordinate their efforts in migrating to post-quantum cryptography and work together to develop a detailed, unified roadmap.

EU Agency for Cybersecurity cryptography guidelines

The EU Agency for Cybersecurity recently published its list of new agreed cryptographic mechanisms, with four post-quantum algorithms added:

- ML-DSA (NIST FIPS 204)
- SLH-DSA (NIST FIPS 205)
- ML-KEM (NIST FIPS 203)
- FrodoKEM (under Internet Engineering Task Force standardization)

These determine what cryptography should be used in products to obtain security certifications under EU Common Criteria.[8]

Other noteworthy standardization initiatives have been undertaken by, among others, the:

- International Organization for Standardization
- International Electrotechnical Commission
- Internet Engineering Task Force
- European Telecommunications Standards Institute
- Korean Post-Quantum Cryptography initiative
- Chinese Association for Cryptologic Research

[7] NIST. NIST PQC standardization process | HQC announced as a 4th round selection. March 11, 2025.

[8] ENISA. EUCC Guidelines on Cryptography. July 17, 2024.

Preparing for Q-Day: 10 essential takeaways

Drawing on NTT DATA's extensive experience in supporting government data initiatives, we have identified the following considerations with regard to preparing for Q-Day.

01. "Harvest now, decrypt later" is a real threat

Organizations dealing with sensitive or classified data could already be under attack.

When attackers steal substantial amounts of encrypted data using standard techniques (such as phishing, brute-force attacks or malware exploits), they can store this data until they have the post-quantum resources to decrypt it.

This is especially problematic for data that must remain confidential over extended periods of time, such as national identity numbers, intellectual property, medical records, sensitive financial transactions and government or military secrets.

> By retaining our well-understood cryptography while gradually integrating post-quantum cryptography, we guard against new vulnerabilities being introduced because of unexpected flaws in a post-quantum algorithm or implementation.

02. Migrations are complex and take time

Why not wait until Q-Day, then quickly migrate? If we look at previous migration movements, this is probably not the best idea.

The secure hash algorithm SHA-1 was under attack as early as 2005 and was only banned by NIST in 2011. In 2016, more than 10 years after the first successful known attack, more than one-third of websites still used this function, lacking any security assurance. Even today, we occasionally see the use of MD5, the predecessor of the SHA family, despite MD5 having been successfully attacked for the first time in 1996.

Furthermore, migrations are complex, and it's not that easy to simply replace RSA and ECC with their successors. For a start, there has never been absolute proof of security for RSA and ECC, and these algorithms have undergone decades of scrutiny and real-world testing. When we deploy the brand-new post-quantum algorithms, there will still be doubts.

By retaining our well-understood cryptography while gradually integrating post-quantum cryptography, we guard against new vulnerabilities being introduced because of unexpected flaws in a post-quantum algorithm or implementation.

Furthermore, unlike RSA or ECC, the selected quantum-resistant algorithms cannot be used for both key exchanges and digital signatures. This means we will need a dedicated algorithm and a determination of its security level (1 to 5) for each use case.

03.
Long-lived systems present challenges

Products, especially industrial products, are often operational for a long period of time — sometimes even decades. Even if software updates for these products are feasible, post-quantum cryptography may require more advanced hardware to function.

This applies to industries such as aerospace, healthcare, defense and critical infrastructure, which should all focus on early adoption.

04.
A cryptographic bill of materials is a good starting point

We recommend starting with an inventory of the cryptographic primitives and protocols already deployed within an organization. Ideally, this entails a full cryptographic bill of materials (CBOM).

Using a standard CBOM format as an inventory provides a more streamlined way for the organization — as well as its suppliers and clients — to create, manage and analyze an inventory. In this context, it is best to identify the systems involved, data types, and dependencies on other organizations.

Crypto discovery tools can be implemented to support the discovery of crypto libraries and crypto objects (certificates, keys, application programming interfaces and secrets).

Furthermore, if obsolete implementations are found, these can be updated in the meantime to comply with current best practices — for example, by migrating from Transport Layer Security (TLS) 1.1 to TLS 1.3.

05.
Risk assessment lays a solid foundation

Based on the CBOM, a comprehensive quantum risk assessment can then be conducted.

This assessment should focus on:

- The quantum weakness of the currently implemented cryptography
- The expected impact of attacks
- The deadline for data to be secure (taking into account the suspected advent of Q-Day)
- The estimated time and effort required to migrate to an environment that's ready for post-quantum cryptography

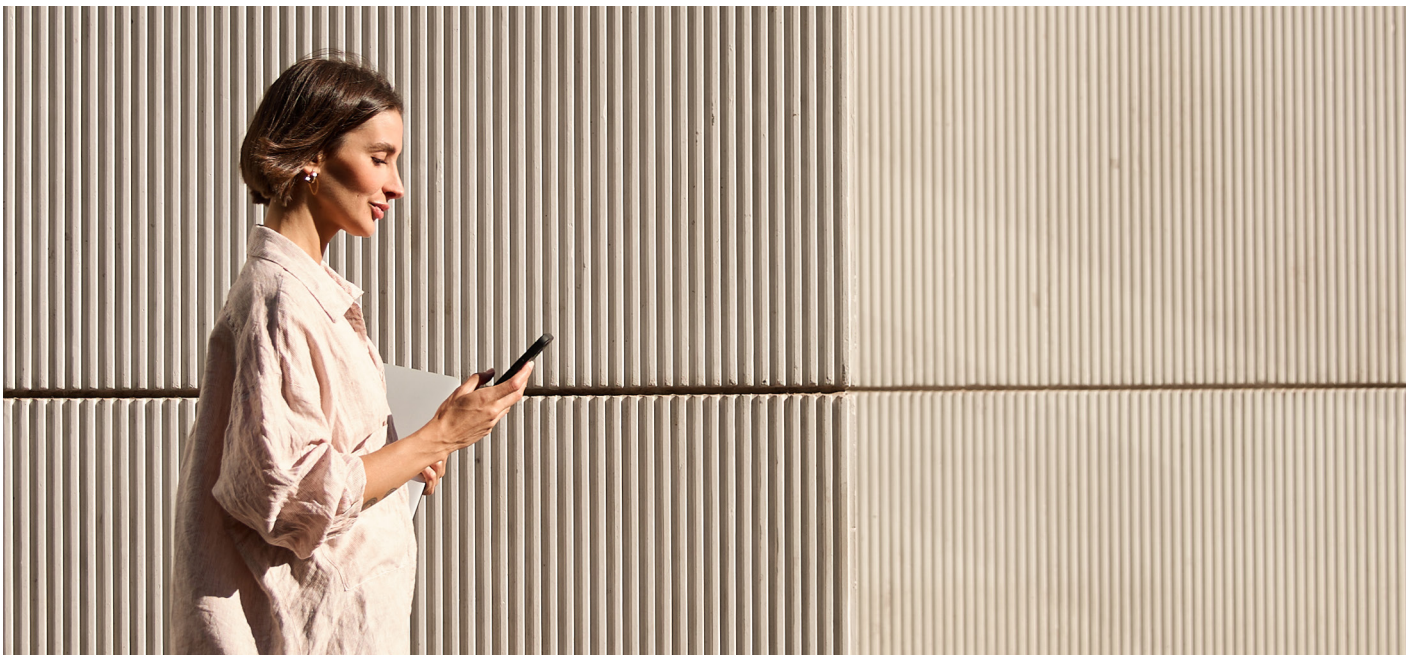
Such an assessment can form the basis for planning, prioritizing and budgeting for a proof of concept, a full migration or other mitigating actions.

06.
Policies need to be reviewed

Given technical and regulatory developments, an organization's cryptographic policies may require revision.

Policies should be made compliant with legislation, anticipate regulatory changes and reflect the findings of the quantum risk assessment.

To facilitate the management and enforcement of such policies, organizations should aim to centralize the lifecycle management of cryptographic objects (especially keys and certificates) and adopt dedicated tools and technologies, such as key-management systems.



07.
Cryptographic agility deserves attention

We recommend establishing as much cryptographic agility as possible when revising existing cryptographic infrastructures.

Cryptographic agility refers to the practice of structuring technologies, processes and policies so that cryptography can be configured in an efficient and highly flexible manner. The greater your agility, the easier it is to update, change or replace the cryptography with minimal effort and consequences such as downtime.

08.
A backup plan is essential

A robust migration strategy is crucial, but it's equally important to be prepared for the unexpected.

You may need to deviate from the original plan in the case of unforeseen developments such as a breakthrough in quantum computing, alternative methods or an attack on an established cryptographic standard.

Draw up a pragmatic backup plan that sets out how best to establish business continuity and minimize downtime in these circumstances.

09.
Don’t procrastinate

The longer you delay, the greater the risk becomes.

Post-quantum cryptography is increasingly considered as being state of the art in cryptography, and many organizations, both governmental and industrial, have already begun adopting it.

Those that delay the adoption of quantum-safe solutions risk vulnerabilities as quantum-computing capabilities progress. Businesses risk being left behind by their customers, who will require them to be quantum-proof to continue doing business with them.

Most modern browsers support post-quantum key negotiation using the standardized ML-KEM algorithm. Technology giants like Google and Cloudflare have integrated quantum-safe key-exchange protocols into their servers, enabling post-quantum cryptography during TLS handshakes. As a result, we see a steady increase in human traffic to Cloudflare, protected by post-quantum cryptography, as shown on the Cloudflare Radar.

10.
Keep an eye on quantum key distribution

Quantum key distribution (QKD) is sometimes referred to as an alternative to post-quantum cryptography, but it has its limitations.

This communication protocol uses quantum-mechanical principles to securely exchange cryptographic keys and detect any interception attempts.

However, QKD is still in the early stages of maturity due to practical scalability limitations, such as the need for specialized hardware, distance limitations, vulnerability to physical channel attacks and integration challenges with conventional networks. A major cybersecurity limitation of QKD is that it tackles only confidentiality and does not cover authentication, integrity or nonrepudiation.

As a result, cybersecurity agencies like the French Cybersecurity Agency, the German Federal Office for Information Security, the Dutch National Communications Security Agency, the Swedish National Communications Security Authority, the US National Security Agency and the EU Agency for Cybersecurity (ENISA) recommend migrating to post-quantum cryptography, which is seen as a more reliable and scalable solution for addressing the quantum threat.

Cryptographic agility refers to the practice of structuring technologies, processes and policies so that cryptography can be configured in an efficient and highly flexible manner. The greater your agility, the easier it is to update, change or replace the cryptography with minimal effort and consequences such as downtime.

Building your post-quantum cryptography program

Currently, there are no off-the-shelf solutions for post-quantum cryptography — only some building blocks. We therefore recommend a proof of concept (POC) approach to evaluate whether the available technologies will meet your organization's functional and security standards.

Our approach to post-quantum cryptography migration

The NTT DATA approach for the rollout of post-quantum cryptography projects, both in our own organization and for our clients, follows a five-step roadmap. Each step is designed to ensure the smooth and secure adoption of next-generation cryptographic technologies.

1. Inventory:

Before we implement any post-quantum cryptography, we help you understand the current environment in your organization.

2. Strategy:

Depending on our findings in the previous phase, we define priorities, involve the right stakeholders and develop a project plan for a POC.

3. POC:

During the POC, we evaluate the feasibility of the program and the impact on business processes and performance, all while developing technical expertise.

4. Migrate:

After a successful Proof of Concept, we help you migrate to post-quantum cryptography in a production environment.

5. Improve:

As with any project, your organizational requirements will change and technologies will evolve. We offer ongoing assistance in adopting next-generation technologies, building expertise and improving ways of working.

NTT DATA and post-quantum cryptography

Research, development and innovation

NTT DATA is part of NTT Group, which invests over $3.6 billion each year in R&D and employs about 2,300 researchers and developers (680 of whom hold PhDs) at specialized laboratories in (14 in Japan and three in Silicon Valley in the US.)

In addition, NTT is a world leader in research and development in optical communications, information security, voice recognition and quantum computing. The company holds about 21,000 patents and conducts roughly 2,400 research presentations and lectures annually.

In the field of information security, about 15% of papers presented at top-level international conferences on cryptography involve members of NTT laboratories. These cover topics including attribute-based encryption, homomorphic encryption and functional encryption.

Post-quantum cryptography is a focus area in this context. We develop and propose new algorithms to NIST and other industry players, and we invest in breaking existing algorithms.

According to our lead scientists, the quantum threat cannot be underestimated.

"It could take years to integrate post-quantum capabilities into existing infrastructure while maintaining compatibility with current workflows. As such, this would be the time to start, so that we can quickly migrate to new post-quantum cryptographic algorithms if and when scalable quantum computing becomes imminent."

Hoeteck Wee, PhD, Senior Scientist, NTT Research (MIT / UC Berkeley)

"Indeed, for extremely sensitive data, the immediate adoption of post-quantum cryptography is even more relevant due to 'harvest now, decrypt later' attacks."

Brent Waters, PhD, Distinguished Scientist, Head of CIS Labs at NTT Research (Princeton/Stanford)

Our partner ecosystem

Apart from fundamental research, we also invest in an EU-based partner ecosystem comprising the best players in the market. We are a premium partner of Thales, the French multinational working in cybersecurity, aerospace, defense and more.

We also partner with CryptoNext Security, the post-quantum cryptography pioneer and leader, founded in 2019 by the award-winning mathematician Jean-Charles Faugère after more than 20 years of research. Since 2016, CryptoNext Security has been an active contributor to post-quantum cryptography standardization initiatives at NIST, the National Cybersecurity Center of Excellence and the Internet Engineering Task Force. They have developed a core quantum-safe library and are the first and only company in the EU to receive NIST Cryptographic Algorithm Validation Program (CAVP) certification for all three standardized quantum-safe algorithms. Now, they offer a full software suite to help organizations assess their cryptographic exposure to the quantum threat and manage the transition to quantum-safe, crypto-agile operations.

Proof of concept: European Commission

NTT DATA, with more than 40 years of research experience in cryptography and nearly 10 specifically in post-quantum cryptography, provides comprehensive services ranging from crypto risk assessments to solution implementations and support.

We position ourselves as a strategic partner in this field, proposing innovative solutions based on best practices to address the emerging challenges and maximize security of critical systems. In this capacity, we were asked by the European Commission to conduct a PoC in April 2024.

For this POC, we worked with CryptoNext Security and Thales to:

- Prepare the integration of the post-quantum cryptography layer in existing information systems or their future versions and replacements
- Evaluate the impact on business processes and performance
- Develop expertise in internal technical teams
- Provide insights for future policies and purchases
- Build trust and gain compliance approval

With this in mind, we worked with the European Commission to:

1. Define four end-to end hybrid post-quantum cryptography secured communication scenarios that are as close as possible to the existing production environment:

- Public-key infrastructure (PKI) to generate classical, post-quantum and hybrid digital certificates using various post-quantum cryptography algorithms
- A virtual private network (VPN) tunnel in a classified context, consisting of two nested IPsec tunnels (one legacy and one post-quantum cryptography only, or hybrid where both are supported)
- An email system with post-quantum-cryptography-enabled encryption and digitally signed emails
- Hybrid, post-quantum-cryptography-enabled user-to-user, user-to-app and app-to-app generic web-app secured communication

2. Identify and deliver the required software and hardware:

- VPN server and client (CryptoNext Security strongSwan GW plugin/TheGreenBow VPN client)
- Email clients (CryptoNext Security Outlook plugin)
- Web servers (Apache)
- Servers (Linux)
- TLS proxies (CryptoNext Security — TLS Forward/Reverse Proxy)
- PKI (CryptoNext Security PQC EJBCA-CE version)
- Hardware security modules (Thales Luna 7 with PQC Functionality Module — post-quantum-cryptography-compatible firmware embedding CryptoNext Security Quantum-Safe Library).

In terms of cryptography testing, hybrid post-quantum cryptography implementations have been tested. As discussed earlier in this guide, we selected specific hybrid post-quantum algorithm combinations — RSA, ECC (classic) and Kyber and FrodoKEM (KEM), ML-DSA and Falcon (DS) [PQ].

Outcome of the POC: Testimonials

"Through our expertise and products, we are honored to partner with Thales and NTT DATA to contribute to solving one of the most disruptive cybersecurity challenges today, help the European Commission design its systems and provide guidelines for our cyber sovereignty. The Commission proves that this can be tackled and implemented to combat 'harvest now, decrypt later' as of today."

Jean-Charles Faugère, Founder of CryptoNext Security

"This POC showcases the power of collaboration. Together with NTT DATA and CryptoNext, Thales Luna hardware security modules provided the cryptographic foundation for our post-quantum POC. The strength of Thales's cybersecurity products lies in our ability to bridge cutting-edge cryptography with real-world deployment needs. Our platforms help ensure crypto agility, compliance and operational resilience throughout the post-quantum transition."

Romain Deslorieux, Vice President, Strategic Partnerships for Cybersecurity Products, at Thales

---

"Thanks to the POC, the European Commission could raise its level of competence in post-quantum cryptography and start preparing a transition plan for its most sensitive IT assets."

EU official, European Commission

Next steps

Being informed and prepared is critical to staying ahead of the threat. We hope this guide has given you insight into this complex field and will help to guide discussions in your organization as you prepare for Q-Day.

To learn more about our approach, expertise and services in this area, please contact our post-quantum cryptographic specialists via olivier.deleuze@nttdata.com.