Data Security Impacts of Quantum Computing – Preparedness Recommended

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

www.huoltovarmuuskeskus.fi

Security of supply refers to society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in the event of serious disruptions and emergencies.

The National Emergency Supply Agency (NESA) is an organisation operating under the Ministry of Economic Affairs and Employment of Finland. It is tasked with planning and measures related to maintaining Finland's security of supply.

The National Emergency Supply Organisation (NESO) is a network that works together for the good of Finland's operating capability and the security of supply necessitated by it. It includes the National Emergency Supply Agency and its Board of Directors, the National Emergency Supply Council and the sectors and pools of different industries. The NESO also engages in cooperation with regional actors, such as Regional State Administrative Agencies, municipalities, cities and regional committees.

Publisher: National Emergency Supply Agency
Prepared by: The National Emergency Supply Organisation's Digipool and VTT Technical Research Centre of Finland Ltd
Cover image: Getty Images
Layout: LM Someco Oy
Year of publication: 2024
ISBN: 978-952-7470-33-6

Table of contents

Introduction

The aim of these guidelines is to clarify for the reader what the benefits of quantum computing are as well as what threat it poses to cyber security. Another aim is to propose measures that organisations can take to protect their information from the quantum threat. In order to reach this goal, we first provide the reader with a brief introduction to the impacts of quantum computing from the perspective of cyber security. Next, we present a review of the existing literary material, focusing on the plans ('roadmap') that various parties have prepared in preparation for the quantum threat. In the second part of the literary review, we focus on the national guidelines issued by different countries on preparing for the quantum threat.

After the literature review, we present a situation analysis of the readiness of Finnish enterprises critical to security of supply for the quantum threat. The information analysed was gathered through a survey targeted at enterprises and supplemented by interviewing an expert. The analysis indicates that the Finnish private sector has not understood the impacts of the cyber threat posed by quantum computing and is therefore also ill-prepared for it. This jeopardises the enterprises' critical information and undisrupted continuation of operations and, through them, the security of supply of Finnish society.

Finally, based on the literature review and situation analysis, we present a plan (roadmap) for preparing for the quantum threat. We conclude these guidelines with the key conclusions and recommended actions.

Quantum computing brings tremendous computing power but also new threats to cyber security

Quantum computing plays a key role in the ongoing technological transformation. Quantum computing will not replace traditional data processing. In certain areas of application, however, quantum computing is absolutely superior to traditional data processing. Quantum computers can be used to solve problems that are practically impossible or very difficult for classical supercomputers.

Examples of future areas of application could include:

- Broad optimisation problems in logistics and economy.
- Design of new medications and materials. Quantum computers can be used to simulate the behaviour of molecules and chemical reactions very accurately and quickly.
- Machine learning: Quantum computers can tremendously improve the performance of machine learning algorithms, thereby facilitating increasingly complex models and larger data sets.
- Predicting the weather: Quantum computing facilitates accurate and quick simulation of weather phenomena, thereby allowing for accurate weather forecasts in terms of time and location.
- Simulation of physics phenomena: Quantum computing facilitates accurate simulation of particle and quantum physics phenomena, for instance.

Quantum computers make it possible to solve major challenges, but their great computing power may also be misused. The development of quantum computing poses a significant threat to the existing cryptographic solutions for information and telecommunications. For economic reasons alone, the most significant threats are related to state actors: In the hands of a hostile country, a quantum computer threatens the national security and security of supply of other countries. This also applies to Finland. For example, China has invested tens of billions of euros in the development of quantum technology. Russia has also said that its goal is to develop a quantum computer for military defence. However, the country's economic situation and economic sanctions reduce the country's capability to develop quantum technology, which is why their current quantum computing capacity is at the same level as in Finland.

Today, information is encrypted with both symmetric, i.e. secret, key methods and public key methods. The quantum threat particularly applies to public key methods, which are used in electronic signatures, among other applications. Many of the encryption methods widely used on the internet, such as TLS (Transport Layer Security) and PGP (Pretty Good Privacy), are also based on public key cryptography.

Organisations can protect themselves against attacks aided by quantum computers by strengthening their existing symmetric cryptography by increasing the length of the encryption key, whereas public key methods require entirely new algorithms. New methods already exist, and their standardisation will be completed in 2024. Organisations must prepare for the deployment of these methods now to also ensure the security of critical information and systems in the future.

Finland is at the forefront in the development of quantum computers, and we can also do the same in post-quantum security. We have the expertise, but we need to take action now. However, even post-quantum cryptography is insufficient if the management and implementation of the existing cryptographic solutions is inadequate or the solutions are not even known – the overall situation is what matters.

Authors
Senior Scientist Visa Vallivaara,
Applied Cryptography, VTT
Research Scientist Mari Muurman,
Applied Cryptography, VTT
Research Scientist Outi-Marja Latvala,
Applied Cryptography, VTT
Lead, Cyber Security, Petri Puhakainen, VTT

Impacts of quantum computing on cyber security

Quantum computing is based on quantum mechanics phenomena. Instead of bits, quantum computers use quantum bits, also known as qubits, which allows certain problems to be solved more quickly than by using classical supercomputers.

A quantum computer is more efficient than a classical computer in simulating real-world events affected by quantum phenomena, such as predicting the weather. Quantum computing is also quicker than classical computing in solving problems involving an enormous number of combinations. A quantum computer's more efficient computing capacity could be used for things such as optimisation problems too complex for a classical computer to solve. Such a problem could be related to logistics or resource allocation, for instance. When used correctly, quantum computing can improve society's security of supply. Although quantum computing is still being developed, it not only offers benefits but also poses a threat to cyber security and security of supply.

A practical quantum computer can be used to break existing public key cryptographic methods. They are based on mathematical problems that are highly difficult to solve with traditional data processing ('classical computing') but easy for a quantum computer. Examples of such problems include factoring large numbers, discrete logarithm problems in finite fields and discrete logarithm problems in elliptic curves. Not even existing supercomputers are able to solve these problems in a reasonable amount of time – unlike quantum computers. Shor's algorithm, which uses quantum computing, can be used to efficiently solve the mathematical problems on which existing public key cryptographic methods are based.

Post-quantum cryptography (PQC) requires new types of mathematical problems without a known quantum algorithm for solving them, which means that they are difficult to solve for both a classical and quantum computer. The best PQC algorithms are currently lattice-based (further information on algorithms is available in the chapter 'PQC support material' in these guidelines).

Although the qubits of existing quantum computers are prone to error, error correction is developing very rapidly. In general, both quantum computers and algorithms are evolving. As development is taking place in so many areas, it is difficult to accurately estimate when it will become possible for public key methods in particular to be broken by a quantum computer. The estimates given by different experts vary from less than 10 years to approximately 20 years[1].

For a health care and medical research company, for instance, this could lead to the exposure of information such as the following:

(1) client information (incl. names, addresses, any medical records and diagnoses),

(2) research data (incl. clinical trial outcomes, new medications and treatments under development) and

(3) business information (incl. finances, strategic plans, contracts). This would have significant legal and business ramifications, not to mention long-term loss of reputation.

[1] 2023 GRI Quantum Threat Timeline Report: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

When should post-quantum cryptography be adopted and what does it entail?

Although the realisation of a cryptographically relevant quantum computer is still in the future, the preparations for its impacts must be started now. There are at least three good reasons to do so:

(1)

Encrypted network traffic may be recorded now and decrypted later with the help of a quantum computer. This type of attack may target information requiring long-term preservation, such as banking and health data. A clear plan must also be drawn up for a situation in which this type of previously stolen information is decrypted and possibly released by the party that stole it. The plan also prepares for the possibility that the information thief will disclose the information to a third party.

(2)

Updating the systems to be quantum-resistant is an extensive and time-consuming project, as, in any event, it concerns several systems and cryptographic solutions.

(3)

PQC solutions are already available. Moreover, the standardisation of PQC algorithms will be completed in 2024.

Organisations should first review the encryption methods they are currently using and identify the most critical information to be kept secret and the duration for which it must be kept secret. Preparing a cryptographic inventory will help with this process. Based on this review, organisations can analyse which systems need to be updated and also identify the most critical ones. Updating everything all at once is not sensible; instead, the migration should be carried out in phases. Based on the review, organisations can prepare a concrete plan (roadmap) that includes a schedule spanning from the testing of post-quantum methods to their deployment in production. The general recommendation is to migrate to post-quantum methods by 2030 (see, for instance, the next chapter: DHS).

One illustrative tool for assessing the quantum threat is Mosca's inequality (Figure 1). It compares the amount of time required by a migration to PQC + the time for which information must be secret to the duration of the development of a relevant quantum computer. This theorem can be used to calculate the year in which the process of changing the algorithms must be initiated.

Mosca's inequality: 2024 + Q – X –Y, where
Q is the number of years until the arrival of a cryptographically relevant quantum computer,
Y is the number of years that it will take to change the algorithms in your industry,
X is the number of years for which the information must remain confidential.

For instance, Q = 20, Y = 5 and X = 15 means that the preparations must be started this year.

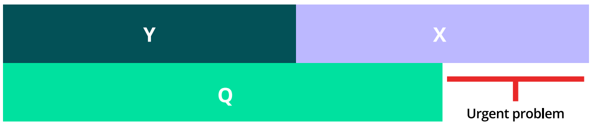


Figure 1. Mosca's inequality

Key tool of the migration: cryptographic inventory

In simple terms, a cryptographic inventory is a list of all of the cryptography used by the organisation. The inventory describes what cryptography is used by which applications for what purpose. It may include information about algorithms, their usage modes, keys and key management, certificates, protocol versions and library versions, as well as non-technical details such as data security classification, supply chains, and the names of the responsible persons.

A cryptographic inventory allows the organisation to monitor secure cryptographic practices and respond quickly to security challenges. It is helpful in rapidly carrying out strategic changes, such as migrating cryptographic services to a cloud service or deploying PQC. Some organisations have been maintaining cryptographic inventories for years, but this concept has only recently started to become mainstream thanks to standards[2] as well as recommendations issued by experts[3].

In practice, each organisation's inventory is slightly different, depending on how and where cryptography is used in relation to the organisation's critical operations. If the goal is to monitor the cryptographic scheme, the inventory must be at least as detailed as the scheme itself. For instance, if the cryptographic strategy only allows a particular cryptographic algorithm in connection with a particular protocol, the inventory must comment on the protocols. If the scheme mandates that only particular cryptographic libraries are to be used, the inventory must list the cryptographic libraries and library versions used.

[2] NIST Special Publication SP 800-57 – Key management recommendations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf

[3] Gartner, Better Safe Than Sorry: Preparing for Crypto-Agility: https://www.gartner.com/en/documents/3645384

Approaches proposed by literature for preparing for the quantum threat

Various ways to prepare for the quantum threat have been published by organisations such as NIST (National Institute of Standards and Technology), DHS (The U.S. Department of Homeland Security)[4], IBM[5] and Google[6] as well as the NSA[7]. All of these documents present similar phases that are intended to ensure a secure and controlled migration to post-quantum solutions.

In 2021, **DHS** in collaboration with NIST published a roadmap for mitigating cyber security risks related to the development of quantum computers. This roadmap includes seven phases:

1. Cooperation with standards organisations should be increased in relation to the development of new post-quantum algorithms.
2. Inventory of the most critical data and the duration for which it must remain confidential.
3. Inventory of cryptographic solutions.
4. Identification of the organisation's internal acquisition, data security and cyber security standards. They must be updated to be quantum-resistant.
5. Identification of systems that use public key cryptography and 'marking' them as quantum-vulnerable.
6. Prioritisation of systems for the migration to PQC. This is particularly dependent on the criticality of the organisation's functions and systems as well as the actual threat posed to them and, through this, the risks.
7. Plan for migration to PQC based on the inventories and prioritisation.

Schedule for the actions:
2021–2023: Inventory and prioritisation of systems.
2024: Publication of the new PQC standards.
2024–2030: Migration of systems to PQC.
2030: Cryptographically relevant quantum computer potentially available.

IBM's roadmap presents a plan for a migration to PQC. The roadmap also presents IBM's tools and services that can help organisations to flexibly discover, observe and edit the cryptography that they need. Some of these tools are already available, while others are still under development. For instance, the purpose of the IBM Quantum Safe Explorer tool is to help discover cryptographic assets by scanning the source code and identifying widely used libraries.

IBM has also implemented some of the PQC algorithms (such as CRYSTALS-Kyber and CRYSTALS-Dilithium) chosen for standardisation by NIST. IBM is involved in consortiums that promote the development and deployment of PQC, such as OQS (Open Quantum Safe). OQS maintains open-source libraries containing post-quantum algorithms. Another example is the PQC Coalition, which focuses on promoting understanding and deployment of PQC in commercial and open-source technologies, among other things. Further information about algorithms is available in the chapter 'PQC support material' in these guidelines.

[4] https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf
[5] https://www.ibm.com/quantum/assets/quantum-safe/IBM_Quantum_Safe_Roadmap.pdf
[6] https://www.nature.com/articles/s41586-022-04623-2
[7] https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF

In 2021, **Google and SandboxAQ** published a document about the migration of organisations to PQC. The document puts forward recommendations regarding (1) how and when organisations should start the migration, (2) which standards they should follow and (3) which resources they should utilise. The document highlights the urgency of the migration due to save-now-decrypt-later attacks, as they jeopardise sensitive information with a long secrecy lifetime.

The document puts forward recommendations for the flexibility of cryptography, prioritisation and the use of hybrid algorithms as follows:

(1)
Flexibility of cryptography: Organisations should design their systems so that changing cryptographic algorithms and key lengths is easy. The importance of flexibility is highlighted particularly because the standardisation process is still ongoing. The term crypto-agility is also used.

(2)
Prioritisation: There is no need to update all systems to be quantum-resistant in one go. Organisations must prioritise critical systems and information requiring long-term protection.

(3)
Hybrid algorithms: Classical and post-quantum algorithms may be used side-by-side, so that organisations do not have to give up the level of security they have already achieved.

In autumn 2023, **the NSA (National Security Agency), CISA (Cybersecurity and Infrastructure Security Agency) and NIST (National Institute of Standards and Technology)** published a factsheet intended for organisations that support critical infrastructure. The purpose of the factsheet is to promote the migration to PQC. The document highlights the importance of careful planning and preparing in advance. This will reduce the threat posed by a cryptographically relevant quantum computer while also ensuring a PQC migration that is as smooth as possible.

The document highlights that reaching this goal requires careful planning ('roadmaps') and risk assessment throughout the production chain. Organisations must identify the cryptographic systems and methods they use. Based on this inventory, organisations can determine the actual risks posed by the quantum threat and the need to migrate to PQC. During the migration process, organisations must particularly identify the phases in which cryptography is used as the primary method for protecting information critical for operations and any sensitive information. They must also estimate for how long the information needs to be protected.

National guidelines for preparing for the quantum threat

Many countries already have national guidelines in place for preparing for the quantum threat. Countries where such guidelines exist include the Netherlands, Australia, South Korea, the United Kingdom, France, Germany and Finland.

In 2023, the **Dutch** national communication security operators TNO (Applied Cryptography and Quantum Algorithms), CWI (Cryptology Group) and AIVD (Netherlands National Communications Security Agency) published 'The PQC Migration Handbook – Guidelines for Migrating to Post-Quantum Cryptography'. The purpose of the handbook is to help organisations (1) conduct a risk analysis of their systems in relation to quantum computers, (2) plan the necessary measures for migrating to post-quantum algorithms and (3) carry out the migration. The guidelines are available in both Flemish and English. The handbook instructs organisations to identify as one of three personas in relation to the quantum threat: (1) urgent adopters, (2) regular adopters and (3) cryptography experts. Urgent adopters, as well as the management and security architects of these organisations in particular, are the main target group of the document. Less urgent cases may be left to wait for the algorithms to mature for the time being. Cryptography experts are enterprises and other parties that supply solutions for user organisations.

ASD (Australian Signals Directorate), which operates under the **Australian** government, succinctly instructs all companies and public administration to follow their national data security manual. It will be updated as the standardisation of PQC progresses. ASD also encourages broad research and development work to be undertaken in the field of quantum computing. As practical advice, organisations are urged to prepare an inventory of the public key technologies they use and the information that these technologies protect. Next, organisations must draw up a plan on the migration to the new algorithms.

Due to a language barrier, we have relied on news reports and machine translations with regard to **South Korea**. The South Korean government has published a six-part plan (roadmap) for a migration to post-quantum solutions. Based on news reports, the plans include technological development, updating the regulation, standardisation, training, and support for the transition period, among other things. South Korea is also in the middle of its own PQC standardisation competition, and the winners will be included in the national standards. Based on news reports, eight algorithms have moved on to the second round.

The **British** National Cyber Security Centre (NCSC) published a whitepaper on preparation for the quantum threat in 2020. The NCSC also considers PQC to be the most effective solution to the cyber threat posed by quantum computers. Large organisations should prepare for attacks carried out with quantum computers in their long-term plans. The users of cryptographic systems are instructed to keep up with current data security guidelines and migrate to PQC once the standards are ready and products that use them are available. The guidelines do not actually use the word 'hybrid solution', but they point out that classical methods and new post-quantum methods will most likely need to be used side-by-side. The NCSC warns that organisations should not rush to deploy non-standardised solutions due to potential compatibility issues.

In 2023, the NCSC published another whitepaper that is intended for critical infrastructure organisations, among others. This publication instructs owners of large IT systems to take the costs of the deployment of new algorithms into account in their budgets. The deployment should be planned to take place within ordinary technology upgrades to the systems. The document mentions that CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ and FALCON, as well as the stateful hash-based LMS and XMSS, have been chosen to be standardised, but it recommends that organisations wait for the final standards for both algorithms and protocols. Regarding the use of hybrid solutions, the document specifically mentions their complexity, inefficiency and troublesome maintenance. However, the NCSC mentions that organisations should transition to the PQC era in phases at some point. Careful planning and implementation of hybrid solutions play a key role in this process.

The **French** Cybersecurity Agency (ANSSI) published a situation analysis in January 2022 and an update to it in December 2023. ANSSI also recommends hybrid solutions and crypto-agility due to the immaturity of post-quantum algorithms. However, the agency also points out that organisations should not delay the deployment of new algorithms for critical assets. All industrial sectors should start using new algorithms alongside existing algorithms in phases so that trust towards the new algorithms and their implementations can be established in the first place. ANSSI particularly recommends hybrid solutions for information and systems for which the expected lifetime extends to 2030 or beyond.

To support the gradual migration, the situation analysis presents a three-phase roadmap that is also followed by the security visas granted by ANSSI: In the first (1) phase, i.e. the present situation, classical cryptography is a mandatory requirement while PQC solutions may be used for added protection. In the second (2) phase, the situation otherwise remains the same, but quantum resilience can be justified and may be an important feature of the system or product. In this phase, ANSSI has identified the criteria for acceptable post-quantum algorithms, which may deviate from those selected by NIST. The second phase is expected to continue until 2030, and the updated document has brought its start forward to 2024–2025. ANSSI lists usable algorithms (CRYSTALS-Kyber, FrodoKEM, CRYSTALS-Dilithium, Falcon, XMSS/LMS and SPHINCS+) to support users, although it also highlights that this list is not complete and that it does not wish to restrict development and innovation by only recommending particular solutions. In the third (3) phase, post-quantum algorithms are expected to be reliably usable without a need for hybrid solutions.

In 2021, the **German** Federal Office for Information Security (BSI) published an English version of its guidelines on PQC migration: 'Migration to Post Quantum Cryptography – Recommendations for Action by the BSI'. The BSI recommends seven actions in relation to post-quantum security:

1. Both new and existing systems should be developed to be crypto-agile to ensure their ability to adapt to future changes.
2. Stateful hash-based signatures must be used in firmware updates.
3. In long-term applications in particular, the key length of symmetric cryptographic algorithms should be 256 bits in the future.
4. A separate pre-distributed shared key can be used as a short-term protective measure to protect the actual key exchange protocol. However, there is no universal solution to the distribution of this key.
5. A hybrid solution combining both classical and post-quantum algorithms must be used whenever technically possible. This is considered to be a more secure option than only using new algorithms. Hybrid solutions are required for high-security applications.
6. It must be noted that there will be changes to cryptographic protocols due to the migration to new cryptographic algorithms and hybrid solutions in particular.
7. The FrodoKEM and Classic McEliece algorithms are the BSI's conservative choice for situations in which long-term secrets must be protected from quantum computers.

FrodoKEM did not make it to the finals in the standardisation competition for the same reason for which the BSI recommends it: its structure is simple. The more complex structure of more efficient algorithms reduces the BSI's trust in their security.

In **Finland**, the utilisation of post-quantum algorithms was studied in the PQC Finland project, which concluded in 2022. The project also sought to develop Finnish cryptographic expertise in view of the upcoming era of quantum computers. A policy brief called 'Kvanttiturvalliset salausmenetelmät Suomessa' (Post-quantum cryptography in Finland) was published about the project's results. It stated that Finland is currently at the forefront in the development of both PQC and quantum computers, but retaining this position requires well-educated workers as well as investment in research, product development and the implementation of methods. It is also important to increase national awareness of the threat posed by quantum computers, as it will take a great deal of time and resources to update the systems.

The greatest difference between the national guidelines is found in the use of hybrid algorithms. English-speaking countries do not recommend hybrid solutions, instead urging organisations to migrate directly to PQC solutions. In contrast, major EU Member States recommend the use of hybrid solutions during the transition phase.

Key recommendations made by literature

From existing literature, we can derive measures that every organisation must take in preparation for the cyber threat posed by quantum computers:

(1) **Classification of systems** Organisations must prepare an inventory of their existing systems that use cryptography and document them clearly for further action. If the system documentation is not up to date, this must be taken care of in any case in this context. An up-to-date cryptographic inventory improves data security and agility. Organisations can prepare the inventory themselves or seek the help of an external expert.

There are different types of systems – therefore, the migration to post-quantum methods requires organisations to carry out different measures. **One way to classify systems is to group them by service provider:**

a. System software and off-the-shelf software provided by software developers. In their case, planning the migration to PQC is the responsibility of the software developer, and organisations can ask for more information from the software developer's representatives (e.g. software of major and local software developers: Microsoft, Oracle, SAP, Salesforce, Visma).

b. Cloud services. The migration to PQC is the service provider's responsibility, and organisations can ask for more information from their service provider (e.g. Google, Amazon, Microsoft, Oracle, IBM).

c. Company-specific systems created by software developers. Organisations can ask their software supplier about the migration to PQC, and the supplier is also responsible for planning the migration. If the software does not include PQC migration, organisations must plan the acquisition of new software.

d. Systems created by the organisation itself. For this type of software, the organisation must prepare its own plan for the migration to PQC.

e. There are also network protocol implementations, solutions and tools used solely for encrypting telecommunications, such as SSL/TSL, HTTPS, SSH, VPN, IPSec, PGPGPG, Wi-Fi Protected Access (WPA/WPA2/WPA3), DTLS and X.509-based certificate solutions. In their case, the supplier of the cryptographic solution in question is responsible for both crypto-agility and the migration to PQC. At its simplest, this involves updating the browser's cryptographic features in conjunction with an operating system update, for instance. SSH, for example, has also implemented PQC solutions for side-by-side use with classical cryptographic solutions.

(2) **Systems prioritisation** Information and systems must be prioritised from the perspective of the migration to PQC. Organisations must first focus on the most critical systems for their operations. They must know what information their different systems process. They can determine this on their own or hire an external expert. Moreover, organisations must understand the secrecy needs and secrecy lifetimes of the information in question. These are determined in accordance with statutory or client requirements. In addition to requirements, the actual risks posed by the quantum threat to information and, through it, to the enterprise's operations must be analysed. The magnitude of the risk is the key determinant of the need to migrate to PQC and the urgency of the migration. If the information is not subject to any actual threat, there is also no risk – consequently, there is no need to update to PQC. Besides cryptography, the magnitude of the risk posed to information is also affected by other actions taken to protect the information (i.e. data security controls). The need for an update is not urgent if the information is sufficiently protected by other means.

(3) Deciding on the need for an update Based on the previous points, the organisation identifies (a) the systems in need of an update and (b) how critical it is to update each system. Organisations should not – and are unable to – update everything all at once, and the migration must in any case be carried out in phases.

(4) Preparing a plan Based on phases 1–3, a concrete plan is drawn up for the organisation for updating each system, including the systems to be updated, the schedule, the budget and the implementers. The organisation can seek help from an external expert for this. It should be noted that organisations will not carry out most of the updates by themselves; instead, they will be carried out by the service provider or system supplier according to their general schedule (see phase 1 above).

Survey for operators in Security of Supply Organisation

During the project, an online survey was carried out for operators in Finnish Security of Supply Organisation. The survey focused on the use of cryptography and readiness for the quantum threat. They survey was supplemented by interviewing an expert. There were 20 questions, and 100 responses were received from a broad range of industries (Figure 2). Of the responses in the category 'Other' (Figure 2), significant industries included media and communications, water services, central government and environmental management. Of the enterprises that responded, 44% were large (>250 employees), 38% were medium-sized (50–249 employees) and 17% were small enterprises.

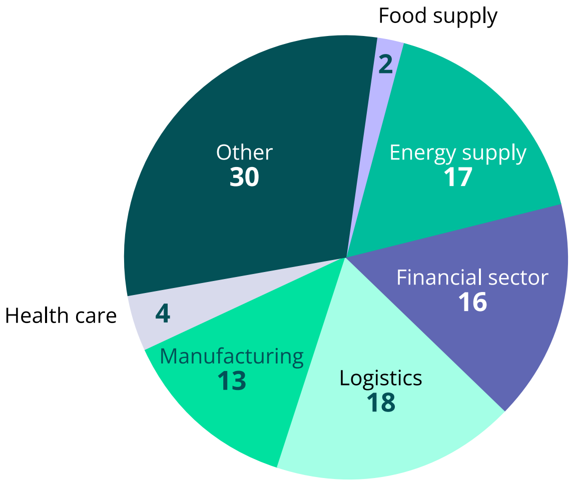


Figure 2. Responses gathered, grouped by sector.

Cryptographic service suppliers used. Based on the survey, most operators in Security of Supply Organisation use either commercial cryptographic services or public digital certificates only. Therefore, only a small proportion of the respondents manage their cryptography completely on their own (Figure 3). Those that use another solution primarily use a combination of these, depending on the situation. Among the respondents, 72% are able to switch freely between different commercial products, while 21% have limited options. The rest of the respondents either have one option available to them (3%) or use their own implementation (4%).

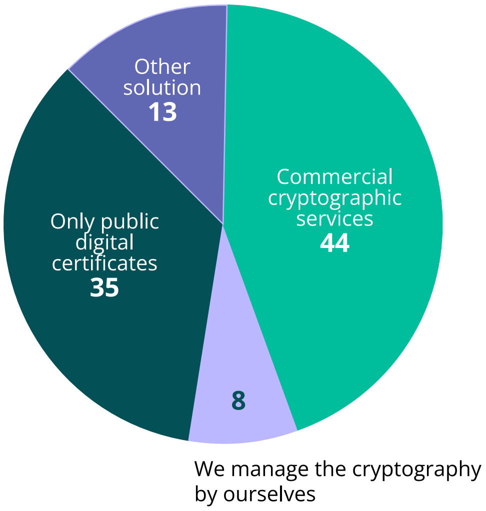


Figure 3. Cryptographic services used by operators in Security of Supply Organisation.

Cryptography used. Based on literature, the first phase is to identify the cryptography used. Most of the respondents (73%) do not have an inventory of the cryptography they use. The reason may be that the market for cryptographic inventory tools is still underdeveloped. Based on the responses, it also appears that the respondents largely consider the management of cryptography to be outsourced, as 67% of them did not define it. Of the respondents, 37% do not have a cryptographic scheme or strategy (Table 1).

No	37
Case-specific guidelines and processes	48
Limited scheme	10
General scheme	5

Table 1. Cryptographic schemes and strategies among operators in Security of Supply Organisation.

Approximately half of the respondents (48%) have case-specific guidelines and practices (processes), while 10% have a limited scheme and 5% have a general scheme. These figures are low by global standards. In a study conducted by Ponemon Institute in 2022,[8] 62% of the respondents have a general scheme, 22% have a limited scheme and only 16% have no scheme at all. Finland was not included in the study. There is country-specific variation (50–80%) in the general scheme percentages, and in Sweden, for instance, 50% of the respondents have a general cryptographic scheme. There is clearly room for development in the establishment of a general cryptographic scheme among operators in Finnish Security of Supply Organisation.

The survey also looked into the replaceability of cryptographic algorithms with new methods. Among the respondents, 57% said that they are able to change their algorithms with external help, while 18% can have their own employees change their algorithms and 8% responded that the methods are very difficult to change. The rest of the respondents were unable to assess replaceability. If such a large proportion of operators require external assistance for changing the algorithms, it raises the question of whether existing resources are sufficient to provide everyone with the necessary expertise.

[8] https://www.entrust.com/resources/reports/global-encryption-trends-study

Assets protected with cryptography. The survey asked about assets protected with cryptography by presenting three options, of which respondents could select all that applied. The encryption of communications and data transmission, as well as the encryption of databases and hard drives, were the most popular (97% and 86%, respectively). Of the respondents, 41% use cryptography on the certificates of their own products.

Client/personal data	14
Classified and confidential documents and other information, product information	12
Databases	10
Authentication/certificates	8
Hardware and software	6
VPN	3
Information systems	2
Hard drives and mass storage	2
User interface connections	1

Table 2. Assets protected with cryptography that were identified as the most critical.

When the respondents were asked to identify the most critical assets with regard to cryptography through an open answer field, the most critical assets identified were client/personal data, telecommunications and various confidential documents. Communications and data transmission were also popular assets. Of the respondents, 41 left this question unanswered.

The retention period of critical information varied a great deal. Most of the respondents have information with a short retention period of 0–10 years, but approximately one in three have confidential information with a retention period longer than 20 years.

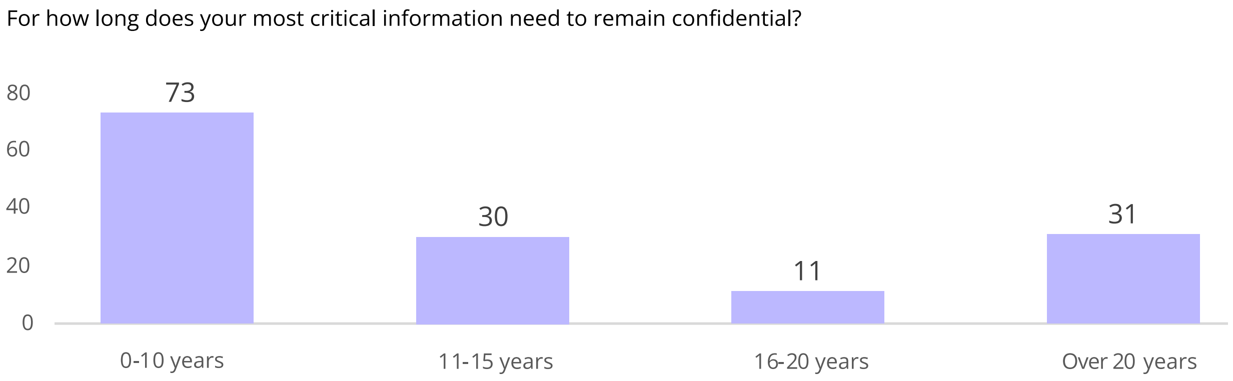


Figure 4. Retention period of critical information. The respondent may have selected more than one option.

A total of 55 respondents have information that must be kept secret for longer than ten years. All of the responses are compiled in Figure 4. It should be noted that one respondent may have selected more than one option.

Awareness of the quantum threat. The survey sought to determine security of supply operators' awareness of the quantum threat and its impacts on cryptography. Among the respondents, 74% were aware of the threat posed by quantum computing to public key cryptography. However, only 10% of all respondents had acquainted themselves with post-quantum methods and NIST's PQC standards, while 34% had acquainted themselves with them to some degree. The majority (56%) had not acquainted themselves with them at all. Several organisations have at least heard about the quantum threat, but this has not by any means always led to action.

Unreadiness for the quantum threat also became apparent in other questions. Only 21% of the respondents assessed the cryptography they use and identified the methods that are at risk. Management teams had not addressed the quantum threat: 90% of the respondents had not addressed the matter at all, 9% had addressed it, 3% had taken action and 2% had reserved resources. The question allowed respondents to select multiple options. Only 3% had a plan in place for changing the cryptographic algorithms.

Skilled personnel are required for carrying out the migration to PQC. Among the respondents, 64% do not have an employee well-versed in PQC challenges, 19% have the relevant expertise among their personnel and 28% have a subcontractor that has the expertise. As the respondents were able to select more than one option for this question, some of them have access to the relevant expertise both among their personnel and through a subcontractor.

Operators in Security of Supply Organisation clearly consider it to be more likely that they will acquire new post-quantum technology (81%) than that they will carry out migration measures by themselves (19%). So far, 11% have taken the quantum threat into account in their new procurements. This indicates that organisations wish for ready-made solutions that they can incorporate into their systems in order to protect themselves from the quantum threat.

Of the responses to the survey, we also studied the health care sector, financial sector and water services more closely.

Health care. Four responses were received from the health care sector, with two being from medium-sized and two from large enterprises. The most important assets protected with cryptography that were identified included patient information, applications, terminal devices, telecommunications, and telecommunications between a patient information system and a client. As expected, all of the operators have data with a secrecy lifetime of over 20 years. All of the respondents were aware of the threat posed by the development of quantum computing, and one of the respondents had addressed the quantum threat with their management team and taken the threat into account in their procurements. No other actions had been taken. Three out of four organisations had employees well-versed in the PQC migration among either their own or a subcontractor's personnel.

Financial sector. A total of 16 responses were received from the financial sector, of which 13 came from large and three from medium-sized enterprises. The most critical assets protected with cryptography included client information, databases, the identification of users and equipment with certificates, telecommunications and other business-critical data. Most of the operators are able to switch freely between commercial products, but a significant proportion (approx. 31%) have either limited options or only one option for a service provider. The financial sector had a great amount of information with a secrecy lifetime of over 20 years. Of the respondents, 37.5% had identified cryptography that they considered to be at risk. One of the respondents had taken action to reduce the threat.

Water services. Four responses were received from water services operators, of which three were from medium-sized and one from a large enterprise. The most critical assets protected with cryptography were password management, client data, confidential documents as well as services and remote connection solutions implemented via a public interface. All of the respondents had heard about the quantum threat, but none of them had yet identified precisely what cryptography is at risk or taken any other concrete action. However, all but one of the respondents have employees well-versed in PQC among either their own or a subcontractor's personnel.

Interview with an information security expert. In addition to the survey, we also interviewed a member of the management team of the Finnish Information Security Cluster (FISC). This highlighted some of the challenges involved in the migration to PQC. The issue is not necessarily operators being unwilling to adopt the technology. But if the underlying infrastructure does not support the adoption of PQC without massive changes, the adoption inevitably slows down with the steep increase in costs. Although awareness of the quantum threat has spread, the mental image of it may be unclear, and the threat may be unspecified. The focus is often more on the benefits of quantum computing rather than on protecting yourself from the quantum threat. Challenges are posed by the availability of PQC solutions and certified products in particular. There are industries that have very specific requirements for the cryptography used. In order to speed up the adoption of post-quantum systems, we need active oversight by the government and possibly legislation, which is what the United States has done.

Operators in Security of Supply Organisation clearly have a need for PQC. Of those who responded to the survey, 94% used cryptography for data transmission, and 55% were responsible for sensitive information with a secrecy lifetime longer than 10 years. Additionally, 31% were responsible for information with a secrecy lifetime longer than 20 years. The survey revealed that the migration to PQC is challenging because operators in Security of Supply Organisation have a poor understanding of cryptography and its use. Many lacked cryptographic schemes and strategies as well as an inventory of the cryptography they use. This situation is considerably better in Finland's neighbouring countries. It is a cause for concern that cryptographic strategies are not required and the use of cryptography is not regulated even for organisations critical to security of supply.

Readiness roadmap for operators in Security of Supply Organisation

Figure 5 presents a roadmap for preparing for the quantum threat. It is based on existing PQC roadmaps, national recommendations and the survey results, and every organisation can use it as a basis for preparing their own plan, or roadmap, towards PQC solutions.

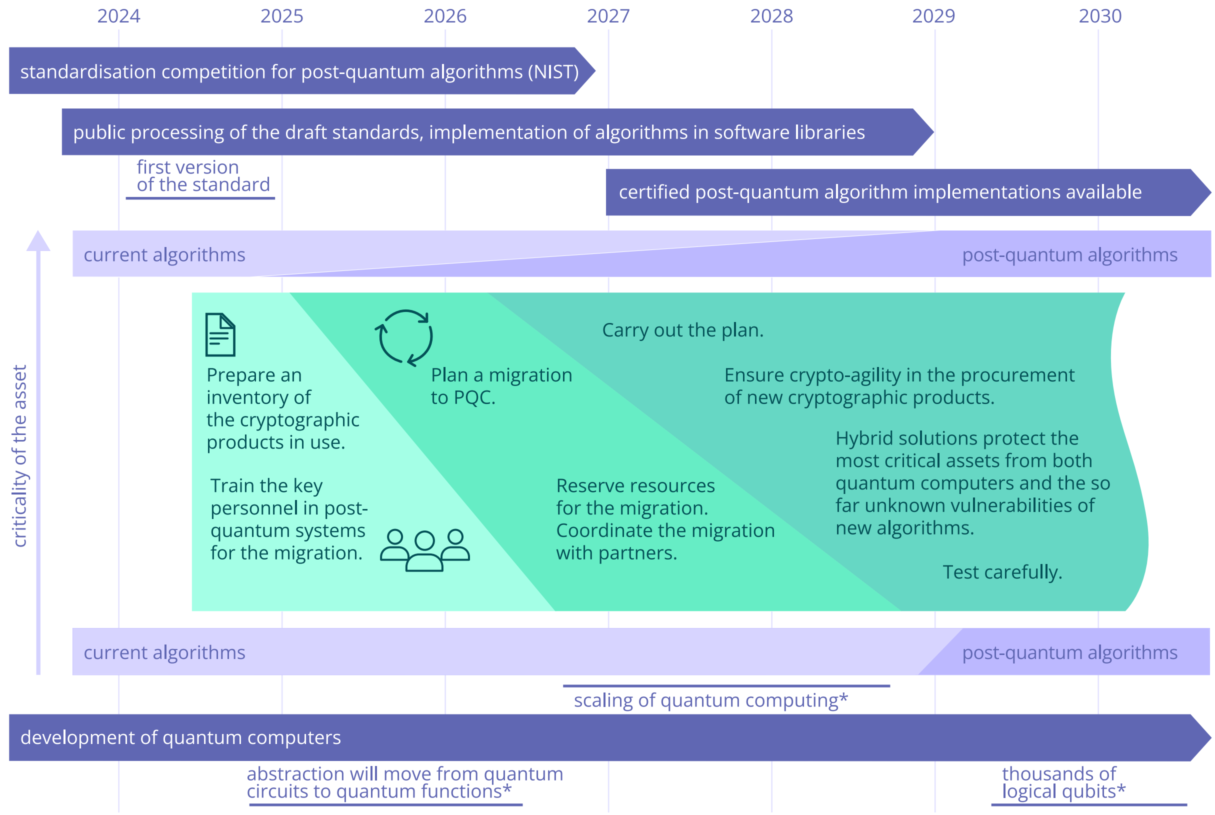
Cryptographic products implemented using public key cryptography are particularly vulnerable to the quantum threat. Although sufficiently efficient quantum computers do not yet exist, their development is rapid. Moreover, organisations have a great deal of information that they must keep secure for decades. The migration to PQC products must therefore be started in good time. The migration roughly includes the following phases (Figure 5):

1. Prepare an inventory. Identify the cryptographic solutions used by your organisation, covering both software and hardware. Identify at least the essential encrypted information stored, classify it according to the need for secrecy and prioritise the information according to the need for re-encryption.

2. Plan the migration to post-quantum solutions. Carefully prepare a plan for updating the cryptographic systems based on the criticality of the systems and the actual risks.

3. Carry out the migration according to the plan, starting from the most critical systems based on risks.

Readiness roadmap for the data security impacts of quantum computing


2024
2025
2026
2027
2028
2029
2030
standardisation competition for post-quantum algorithms (NIST)
public processing of the draft standards, implementation of algorithms in software libraries
first version of the standard
certified post-quantum algorithm implementations available
current algorithms
post-quantum algorithms
criticality of the asset
Prepare an inventory of the cryptographic products in use.
Train the key personnel in post-quantum systems for the migration.
Plan a migration to PQC.
Reserve resources for the migration. Coordinate the migration with partners.
Carry out the plan.
Ensure crypto-agility in the procurement of new cryptographic products.
Hybrid solutions protect the most critical assets from both quantum computers and the so far unknown vulnerabilities of new algorithms.
Test carefully.
current algorithms
post-quantum algorithms
scaling of quantum computing*
development of quantum computers
abstraction will move from quantum circuits to quantum functions*
thousands of logical qubits*

Highlights from the IBM roadmap, see https://www.ibm.com/roadmaps/quantum/

Figure 5. Roadmap for preparing for the quantum threat.

1. Prepare an inventory (2024–2026)

- Most of the operators in Security of Supply Organisation did not have certain information about the cryptographic solutions they employ. The first step towards PQC is to prepare a cryptographic inventory: identify the cryptographic solutions used by your organisation, covering both software and hardware. Preparing the inventory is a laborious task. It must cover the algorithms used in cryptographic products, key lengths, the usage modes and life cycle of the products as well as their suppliers. This phase includes identifying the algorithms vulnerable to the quantum threat for further action. This information must be documented clearly for further action (e.g. using manual bookkeeping as shown in Table 3 or documenting the information in a system such as the Configuration Management Database (CMDB)). The dependencies on suppliers of cryptographic solutions must also be determined: how flexibly the organisation is able to change the solutions it uses, as well as their suppliers, and whether any critical services rely on a single supplier. Suppliers of cryptographic services must take particular care when carrying out this assessment. Next, take inventory and document your organisation's data sets that are stored encrypted: what type of information is stored encrypted and where it is located. You should also document what information is in active use and what information is passively stored. Information must also be classified according to the secrecy requirements, e.g. less than five years, 5–15 years, or over 15 years. The secrecy lifetime affects the urgency of the migration to PQC solutions. Table 3 presents an excerpt from an organisation's cryptographic inventory. Because the goal is to form a comprehensive understanding of the cryptography used by the organisation and any needs for improvement, the work should be carried out as group work, involving experts from different parts of the organisation, such as data security experts, systems architects, IT administrators and system owners (business).

- Assess the risks posed to the cryptographic systems and encrypted information. The criticality of the system and information for the organisation's operations ultimately decides the criticality of the PQC migration. The more critical the function that the system and information support, the greater the risk and the more urgent the need for an update. On the other hand, it is good to assess how attractive the system and information are to an attacker. The more attractive the asset is from an attacker's perspective, the greater the threat and also the risk.

- The prioritisation of the need to update systems is affected by the criticality of the system and the information it contains for the business; the attractiveness of the information processed by the system from an attacker's perspective (e.g. financial value); other protective measures taken to protect the system, i.e. data security controls; the system's operating environment and, through it, the ease of carrying out an attack (cloud service, internal network, public network); and the consequences to the enterprise should the information be revealed. If the system and the information it contains are not critical and the risks and their consequences are negligible, the need to update the system is not urgent. If the secrecy lifetime of the stored information is long and/or the information is subject to heavy legal requirements or requirements from the client or other stakeholders, the re-encryption should be carried out soon. Doubling the length of the symmetric encryption key alone provides good protection against the quantum threat.

- You should start planning the migration to PQC solutions. Start training the key personnel and/or acquiring external assistance. Also appoint responsible persons within your organisation to prepare the migration plan, which should take into account the schedule, budgeting and implementers.

System	Cryptographic method	Algorithm/ protocol	Key	Key management	Encrypted data	Vulnerabilities
CRM	Data transmission	TLS 1.3	2,048 bits	Centralised	Client information	Vulnerable to the quantum threat
Email	Data transmission	TLS 1.3	2,048 bits	Centralised	Emails	Vulnerable to the quantum threat
Backup system active	Storage	AES 256	256 bits	Local	Backup copies	Compatibility with existing equipment. Not critical from the perspective of the quantum threat. Doubling the key length is not urgent.

Table 3. Example extract from a cryptographic inventory

2. Plan the migration to post-quantum solutions (2025–2028)

- Plan the update to the cryptographic systems based on the systems' criticality and the actual risks posed to them. Take into account the updating responsibilities also mentioned in the literature review. The organisation itself is only responsible for some of the updates. The service provider or system creator will take care of a large proportion of the updates.

- Plan the re-encryption needs of your organisation's own encrypted information resources based on risks. The longer the information must be kept secret and the more attractive it is to an attacker, the more quickly it must be protected from the quantum threat by increasing the length of the encryption key through re-encryption. In addition to the order in which the migration will be carried out, decide what algorithms you want to use for each asset. This phase requires understanding of the risks posed to information and systems, as well as of the cryptographic algorithms themselves, which is why most organisations require help from an external expert on top of their own expertise.

- The most critical assets require hybrid solutions, i.e. combinations of classical cryptography and PQC. PQC algorithms are used to protect information from save-now-decrypt-later attacks, while classical algorithms are used in case the new algorithms still have undiscovered vulnerabilities.

- With regard to less critical assets, organisations should wait for PQC algorithms to mature and migrate directly to them later, without urgency. However, most migrations will be taken care of by service providers and software developers.

- Ensure crypto-agility when procuring new cryptographic products: try to choose and ask service providers for products with cryptography that is easy to update and change. This is particularly important when procuring equipment with a service lifetime longer than ten years.

- Reserve the planned resources for carrying out the migration. Most organisations will most likely carry out the change with external assistance towards 2030. In this event, a lack of experts may pose a challenge, so organisations should take action in good time.

- Organisations that depend on each other should migrate to post-quantum systems in a coordinated manner. In a linear dependency, the organisations at the forefront should migrate to post-quantum systems first before the organisations dependent on them carry out their own migration. Organisations closely networked with each other should migrate to post-quantum systems at the same time.

3. Carry out the migration according to the plan (2026–2030)

- Start the migration from the most critical assets based on risks. Not all systems need to be updated – the risks are the deciding factor. You may have to migrate the most critical assets to PQC before the plan for the entire organisation's migration is ready and even before implementations meeting the standards are widely available. The crypto-agility of systems helps organisations respond to changes.

- Reserve sufficient time and resources for testing new cryptographic products. They must provide the promised level of security and be compatible with the other hardware and software in use.

Summary

Operators in Security of Supply Organisation clearly have a need for PQC. Of those whoresponded to the survey, 94% used cryptography for data transmission, 55% were responsible for sensitive information with a secrecy lifetime longer than 10 years and 31% were responsible for information with a secrecy lifetime of over 20 years. Quantum computers are a real threat on this time scale. Table 4 summarises the key actions presented by the readiness roadmap, which were determined based on the literature review and survey intended for enterprises critical to security of supply.

Action	Responsible party	Considerations
Inventory of cryptographic solutions (cryptographic inventory)	The organisation itself; an external expert may provide assistance. E.g. IBM offers consulting and also tools in part.	There are different types of systems. The organisation is responsible for identifying and documenting the systems it uses.
Inventory and classification of encrypted information	The organisation itself; an external expert may provide assistance.	Some information is in active use and some is passive; the secrecy lifetime varies.
Putting the management of encryption keys in order	The organisation itself; an external expert may provide assistance.	If the management of encryption keys is not put in order, a PQC migration is almost pointless. The management of encryption keys is partly outsourced/hidden from the organisation (e.g. encryption of browser traffic).
Prioritisation of system updates and the need to re-encrypt information based on risks	The organisation itself; an external expert may provide assistance.	The criticality of updates and re-encryption is affected by things such as the criticality of the information and systems for the organisation's business operations, the consequences of the information being revealed, the attractiveness of the information and systems from an attacker's perspective, i.e. the actual threats and risks.
Cryptography update plan. Cryptography based on public key methods in particular must be updated if required by the risks. Systems at low risk do not necessarily need to be updated.	The organisation should be aware of the parties responsible for the updates. The organisation is responsible for any systems and services it provides itself.	The responsibility for updating to PQC often falls to the service provider or system supplier / software developer.
Update plan for the re-encryption of information	The organisation itself; an external expert may provide assistance.	This is another instance in which the organisation is dependent on the cryptography supplier. Stored information is typically encrypted with symmetric methods. The cryptographic solution must support the doubling of the key length from the current secure key lengths.
PQC solutions, as well as crypto-agility, as requirements in procurements	The organisation itself	New procurements must support PQC algorithms and agile replacement of cryptography.
Implementation of updates and re-encryption by 2030	The organisation itself; an external expert may provide assistance. However, service providers and system suppliers / software developers will carry out a large proportion of the updates according to their own plans.	The migration is an extensive and therefore laborious and time-consuming task.

Conclusions

There is a need for systematic communication about the impacts of quantum computing as well as the necessary preparedness measures and solutions. The study indicated that the understanding of the cyber threat posed by quantum computing is lacking. This is apparent from the fact that few enterprises have taken concrete action to take the quantum threat into account, for example. The survey found that although 74% are aware of the quantum threat and 75% believed that they are able to change their algorithms, only 27% had a list of the methods they use and only 21% had identified the cryptography at risk.

In practice, this is a concerning situation because only 11% have taken the quantum threat into account in their procurements, only 9% of the respondents said that their management teams had addressed the matter, and only 3% had taken action. It is important to increase awareness so that organisations are able to prepare for the actions required by the quantum threat with sufficiently careful planning

The survey indicated that many enterprises lacked cryptographic schemes and strategies, as well as an inventory of the cryptography they use, which means that there is much work left to be done.

One in five of the respondents are interested in participating in a research project for planning, carrying out and testing PQC. We propose that a follow-up project be carried out in collaboration with Finnish enterprises that provide post-quantum solutions (such as SSH). The project could include practical workshops, training and validation of post-quantum methods. The follow-up project could also develop and test tools and methods for preparing a cryptographic inventory.

PQC support material

In addition to the NIST standard, the Internet Engineering Task Force (IETF) has also produced good PQC support material. The IETF issues voluntary standards and guidelines that are often utilised by internet users, network operators and equipment manufacturers.

- NIST PQC standard:
  https://csrc.nist.gov/Projects/post-quantum-cryptography

- IETF PQC guide for engineers:
  https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/

- IETF PQC hybrid algorithm terminology:
  https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/

- PQC programming libraries:
  - PQClean (C) – Clean versions of the NIST algorithms
  - libOQS (C) – Wrappers for the C++, Python, Java, Go, .NET and Rust programming languages
  - BouncyCastle (Java), rustpq/pqcrypto (Rust), pqm4 (C, Cortex-M4)

Contact information

Project Manager
Visa Vallivaara
Tel. +358401398326
visa.vallivaara@vtt.fi
www.vttresearch.com

Chairperson of the steering group
Antti Nyqvist
Tel. +358408619446
antti.nyqvist@teknologiateollisuus.fi
www.digipooli.fi

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency