CYBERNETICA

Quantum safety with Cybernetica

All-in-one overview of Post-Quantum Cryptography and how Cybernetica can aid you in building a future-proof digital society

Whitepaper
2025

Public

Table of contents

Our vision for quantum-safe cryptography — 2

What is the quantum threat and who is affected? — 3

Why is post-quantum cryptography a solution? — 5

State of PQC in Q2-2025 — 7

Preparing governments and businesses for a quantum future — 8

Upgrading apps and services to be quantum-safe — 9

Post-quantum transition for interoperability platforms — 10

Post-quantum transition for High-Assurance digital identity platforms — 10

Cybernetica's post-quantum pledge — 11

Get in touch with our experts — 12

Our vision for quantum-safe cryptography

Cryptography is essential for maintaining data confidentiality, integrity, and authenticity across various online services, but these concepts are increasingly threatened by advancements in quantum computing. As quantum computers reach a certain technological threshold, they could theoretically break majority of today's cryptographic mechanisms. While it's uncertain when or if a "cryptographically relevant" quantum computer will be built, experts are already developing and standardising Post-Quantum Cryptography (PQC) to mitigate these risks.

Looking at the monitoring data from Cloudflare – a worldwide network infrastructure provider – in 2025, we see that about 35% of all clients connecting through their network use post-quantum key agreement in secure connections. But secure transport isn't everything and there are many other use cases for cryptography in different layers, shapes and forms. All of which will require certain amount of attention to migrate to PQC.

What not everyone might realise straight away is that, in certain confidentiality scenarios, this quantum threat was already here yesterday. A potential attacker might store encrypted data today, then decrypt it later as a sufficiently powerful quantum computer becomes available. Thus, if we have encrypted data that need to stay secret for another, say, 20 years, they are already at risk of being decrypted by a threat actor in the future.

Apart from simply migrating to much stronger cryptography, we also have an opportunity to review our current IT systems: to assess their stability, uncover security flaws, and maybe even introduce the important concept of cryptographic agility – the ability to replace cryptographic algorithms with little effort. Some current cryptography implementations did not expect the future need to switch to algorithms and mechanisms with a different structure, thus making the migration significantly more complicated.

At Cybernetica, we strongly believe it is important to disseminate the importance of this IT migration – all its decisions, processes, obstacles, and caveats. That is why we compiled this document, introducing all relevant theoretical and practical topics. Our vision is to help the digital society keep its data private and secret throughout all time and we recognise post-quantum cryptography as one of the tools for such goal.

Sincerely,

Oliver Väärtnõu
CEO of Cybernetica

What is the quantum threat and who is affected?

Cryptographically Relevant Quantum Computer (CRQC)

In principle, quantum computing means utilising physics of the world of atoms and small particles to perform certain computations. Its applications are very broad, with drug discovery, climate modeling, energy sector, and artificial intelligence advancements being most widely promoted. However, there is another potential use of a quantum computer: to solve the hard mathematical problems on which our internet security relies on.

In 1994, Peter Shor showed that a sufficiently powerful (call that “Cryptographically Relevant”, CR) quantum computer (QC) will be able to break the cryptographic algorithms we use today for creating digital signatures or establishing secure communication channels. Shor's algorithms target special type of cryptography called “asymmetric”. Unfortunately, this type is utilised almost everywhere – when browsing the internet, communicating with peers and the state, safeguarding sensitive information remotely, cloud storage and services, internet banking, etc.

Who will have the first quantum computers?

Currently, only large tech leaders are openly developing a quantum computer, with possibly others growing it in secret. Due to a very high operational costs of a quantum computer, nations and states are expected to be the first customers. Over time, the availability and cost of performing quantum computations will probably increase and decrease respectively, introducing this service to broader community.

Who is at risk?

Eventually, everybody using current cryptography to secure their services, networks, and applications. But some are at risk sooner than others. It all depends on how long your data need to stay hidden due of the "store-now-decrypt-later" attack. Imagine a state or commercial secrets (which don't usually change in time) being stored in encrypted form today. An attacker could keep this for-now unreadable secret until a CRQC becomes available, then retrospectively decrypt and uncover the secrets in the future.

In general, if data (available on open channels) needs to stay confidential for longer than the time it gets to construct CRQC, you should start planning mitigations as soon as possible. Otherwise, you have a bit more time to establish a robust migration plan.

Which cryptography remains usable?

Although the main target of quantum threat seems to be asymmetric algorithms, there are also consequences for symmetric cryptography. In 1996, Lov Grover proposed a quantum algorithm that reduces the bit security of symmetric algorithms by half. Thus, in theory, for symmetric encryption algorithms (such as AES) and hash functions (such as the SHA family), doubling key size or hash output would be sufficient to protect against quantum computers. For example, systems utilizing AES with 128-bit keys should upgrade to AES with 256-bit keys.

When will a CRQC become operational and how much will it cost?

Technological and scientific advancements in quantum computing have been happening steadily over the last two decades, but no one can precisely determine when will a cryptographically relevant quantum computer be constructed. See Figure 1 for rough estimation from experts. They say there is on average above 50 % chance for CRQC to be constructed by 2040.
At the first occurrence of CRQC, estimates of breaking a single RSA-2048 instance go up to millions of US dollars (although doing such estimations is incredibly hard at this point). In anticipation of this, large countries have set deadlines for moving away from cryptography that could be vulnerable to a quantum computer.

2024 opinion-based estimates of the likelihood of a digital quantum computer able to break RSA-2048 in 24 hours, as function of time

Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents

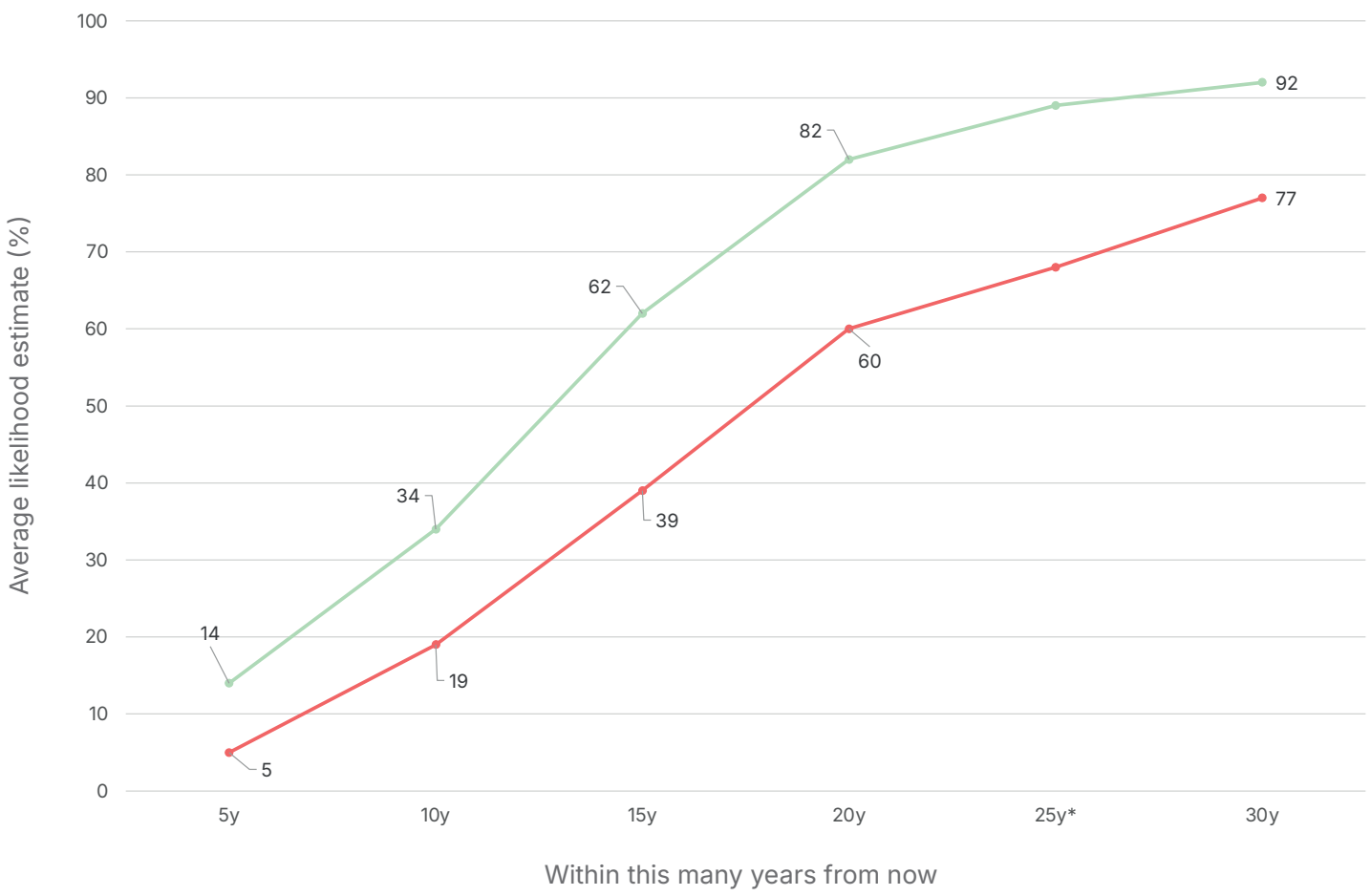

Figure 1: Estimate of CRQC being operational
*25-year timeframe was not explicitly considered in the questionnair
Source: Global Risk Institute (2023). *2023 Quantum Threat Timeline Report*

Why is post-quantum cryptography a solution?

What is post-quantum cryptography (PQC)?

Post-Quantum Cryptography (PQC) is a new set of algorithms for which no attacks are yet known on quantum or standard computers. Note that these algorithms do not require a quantum computer to run. They can be implemented and run on commodity devices quite effortlessly even today.

How is PQC able to protect against a quantum computer and current cryptography cannot?

The difference lies within the hard mathematical problems these algorithms are based on. PQC does not rely on the hardness of finding prime factors of very large integers or finding discrete logarithms (which we use today and CRQC could solve easily). Instead, researchers found new hard problems that even CRQC shouldn't be able to solve.

How will PQC be deployed? Will it require special new hardware?

Primarily, PQC will come as a software update in applications and libraries that utilize the vulnerable classical cryptography. In case of systems with hardware roots of trust (like hardware secure modules, hardware accelerators, IoT devices or smartcards), vendors are already developing and certifying new versions capable of running post-quantum cryptography.

Does PQC demand more resources?

In general, post-quantum cryptography is more demanding in terms of computational time, memory, and storage resources. However, in most cases, modern computing hardware can run PQC without users noticing the change. Some PQ schemes are even computationally more efficient than their classical counterparts. The edge cases might include high-load servers and constrained devices, where optimizations and further engineering efforts must be performed.

Are there international standards for PQC?

To ensure global interoperability and support adoption, PQC will need to be standardized. Since 2016, the US National Institute for Standards and Technology (NIST) has been leading the international PQC standardization process with global participants. In August 2024, NIST published the first three PQC standards – two digital signature algorithms and one key encapsulation mechanism (an interactive scheme for establishing shared secrets). Although standardisation continues to search for more algorithms, this has been an important milestone as next phases of the migration may begin.

In Europe, ISO is believed to run a rather private standardisation process. Other bodies like ETSI, BSI, and ANSSI run their own evaluation processes with the aim to yield only recommendations on algorithms, not creating new standards.

Are there already post-quantum products and software?

There are only a handful of certified post-quantum products. Software implementations (including open-source ones) are available for engineers to experiment and prototype. However, keep in mind that the field of PQC is not about creating new products, but to upgrade the existing ones, i.e., everyone will eventually need to look at their own application/system and figure out how to perform the PQ migration.

What will happen with classical cryptography?

Regardless of CRQC ever being built, standardization bodies are already putting up timelines for classical cryptography deprecation. For example, US NIST deprecates ECDSA and RSA algorithms after 2030 and disallows them after 2035.

Will a quantum computer break post-quantum cryptography?

It is very unlikely, yet not completely ruled out. Many mathematicians and scientists around the world are actively looking for weaknesses in known post-quantum cryptography and new ways of protection against a quantum computer.

What is the difference between post-quantum cryptography and quantum cryptography?

Post-quantum cryptography can run on classical computer we know and love today. Quantum cryptography, on the other hand, utilises the principles of quantum physics. Its main product is quantum key distribution (QKD) which requires custom hardware to protect communication between two nodes. No other quantum cryptography solutions are available for digital identity, document encryption or advanced cryptographic protocols.

As of Q1 2025, prioritizing PQC instead of QKD is recommended by many international security authorities. This is mostly due to the flexibility, credibility, and ease of migration to PQC, compared to migrating to QKD (which also bears a significant setup cost).

What is the current state of post-quantum cryptography?

Post-quantum cryptography is a new technology where the state-of-the-art changes rapidly. Standardisation bodies are establishing new cryptography standards, engineers are exploring ways how to utilise PQC, application and service vendors are slowly establishing a migration plans, and customers are starting to ask whether they are quantum safe.

For latest updates, contact Cybernetica to learn the most recent developments and how they affect your approach towards quantum-safety.

State of PQC in Q2-2025

What applications already use post-quantum cryptography?

There are several early adopters of PQC who have developed the infrastructure and software to offer quantum safe communications. In September 2023, the popular secure messaging system Signal announced that the app has developed post-quantum key establishment to protect against "store-now-decrypt-later" attacks. Similarly, Apple announced in February 2024 that the iMessage system is adopting post-quantum cryptography. Other companies such as Google, Meta, and Amazon implemented quantum-safe TLS key establishment in their internal networks and are looking into further distribution to the public services as well.

Who uses post-quantum cryptography on the public internet?

The most impactful use of PQC on the public internet is the hybrid (combination of post-quantum and classical cryptography) key exchange in the secure communication protocol TLS running between web browsers and servers. Google Chrome, Microsoft Edge and Mozilla Firefox enabled PQC by default around April-May 2024. However, for communication to be post-quantum, it also be enabled on the server side. Since October 2022, all Cloudflare servers support this feature by default and, as of March 2025, Cloudflare measures around 35 % of its traffic to be secured against a cryptographically relevant quantum computer.

Progress on international standards for post-quantum cryptography

There are two standardisation directions. First, a standardisation of post-quantum algorithms themselves. The United States NIST standardized 3 algorithms in summer 2024 under the names ML-KEM, ML-DSA, and SLH-DSA (with two more confirmed to be standardised in the future). There are also other standardisation tracks running in different parts of the world. ISO is also looking into algorithms that were already denied by NIST. South Korea also launched a competition resulting in standardisation of another 4 algorithms.

The second standardisation direction tries to determine how to apply new algorithms in existing protocols and applications. All standardisation bodies in the world must review their own published standards, and figure out how to apply PQC. For example, the Internet Engineering Task Force (IETF) is focusing on applied cryptography on the internet, ETSI is handling digital signatures and their legal usage, ISO/IEC handles information security and its certification. New application standards from these organisations are dependent on the standardisation of the algorithms and are thus, still somewhat behind.

Post-quantum engineering

Post-quantum engineering is a field of understanding new algorithms, their requirements, differences, computational overhead, and being able to implement them in existing applications and infrastructures. There are several open-source libraries, applications and projects to help with this task. As the engineering standardisation track lacks behind standardising algorithms, current engineering efforts are mostly in the form of experiments, prototypes, and proofs of concepts.

In general, there are a lot of interoperability and implementation issues that require solving on a global scale. There are also many engineering obstacles and nuances that might prolong and complicate the migration on an individual scale.

Preparing governments and businesses for a quantum future

How are apps and services affected?

It is rare to encounter a digital service not utilising some form of cryptography to achieve security. All usage of public-key cryptography or asymmetric cryptography is heavily impacted and will have to get upgraded to post-quantum cryptography in the near future.

Which apps and services need to be upgraded first?

Thankfully, the more crucial or time-sensitive part – the data confidentiality – is also much easier to migrate. We already have a post-quantum algorithm for establishing shared secret standardised, and we can start implementing it in protocols, which translates to encrypting our products and data in a quantum safe way.

On the contrary, security functions like client authentication and binding digital signatures require figuring out post-quantum certification of products, services (including Public Key Infrastructure), and certification of those services. These steps (often involving third-party actors) prolong and complicate the process.

In summary, we should start upgrading cryptography that handles data encryption first. At the same time, we should focus on solving issues with other use cases and making a post-quantum migration plan.

How will apps and services be transitioned to post-quantum cryptography?

Most of the transitions require a software update, however this process is preceded by others such as migration planning, cryptographic inventory, design and development. More niche or critical use cases that require also hardware cryptography will require recollection and redistribution of new devices.

Characteristics of post-quantum migration

Overall, post-quantum migration poses a significant challenge for an IT world. It is unfortunately not only about a simple switch of cryptographic algorithms. There are many engineering challenges to solve, which on the other hand present an opportunity for businesses to perform an in-house IT modernisation, re-evaluate current security practices and introduce new ones. Perhaps establish a proper cryptography management system with crypto-agile (easily swappable utilised cryptography) components, thus preparing for any future migrations.

Cryptography discovery and inventory

Often presented as the first step of post-quantum migration, cryptography discovery, and inventory is a process of (either manually or with automatic tools) identifying and collecting used cryptography concepts within a system. It can contain details on utilized algorithms, protocols, libraries, applications, certificates, keypairs, and metadata. Cryptography inventory helps with identifying algorithms vulnerable to CRQC that need to be replaced.

Migration strategy resources

Post-quantum migration is an inevitable, global process that will influence almost every single IT system. Although there are global standardization efforts, it is only natural that there will be an enormous number of resources, often incompatible and maybe even contradicting each other. It is important to establish a clear, educated and up-to-date source of knowledge base for post-quantum cryptography and its migration. Given the importance and indispensability of cryptography in general, it might even make sense to hire an outside consultancy for PQC.

Upgrading apps and services to be quantum-safe

How are apps and services affected?

It is rare to encounter a digital service not utilising some form of cryptography to achieve security. All usage of public-key cryptography or asymmetric cryptography is heavily impacted and will have to get upgraded to post-quantum cryptography in the near future.

Which apps and services need to be upgraded first?

Thankfully, the more crucial or time-sensitive part – the data confidentiality – is also much easier to migrate. We already have a post-quantum algorithm for establishing shared secret standardised, and we can start implementing it in protocols, which translates to encrypting our products and data in a quantum safe way.

On the contrary, security functions like client authentication and binding digital signatures require figuring out post-quantum certification of products, services (including Public Key Infrastructure), and certification of those services. These steps (often involving third-party actors) prolong and complicate the process.

In summary, we should start upgrading cryptography that handles data encryption first. At the same time, we should focus on solving issues with other use cases and making a post-quantum migration plan.

How will apps and services be transitioned to post-quantum cryptography?

Most of the transitions require a software update, however this process is preceded by others such as migration planning, cryptographic inventory, design and development. More niche or critical use cases that require also hardware cryptography will require recollection and redistribution of new devices.

Post-quantum transition for interoperability platforms

How are interoperability platforms affected?

Modern interoperability platforms like UXP and X-Road provide secure and authenticated transport of data between organisations public and private sector organisations. They use public key infrastructures, digital signatures for authentication and TLS protocol for secure transfer of data. Both instances will need to get replaced by post-quantum alternatives within their framework (programming language, technological stack, etc).

How will these platforms be transitioned to post-quantum cryptography?

Interoperability platforms will be transitioned via a software update which implements the logic for post-quantum key establishment and TLS. Call to action is to contact your interoperability platform vendor for their roadmap to PQ transition.
Cybernetica’s UXP platform has post-quantum cryptography on its roadmap.

Post-quantum transition for High-Assurance digital identity platforms

How are high-assurance digital identity platforms affected?

Not only high-assurance digital identity platforms, but all systems that rely on public key infrastructure are affected and must be migrated to post-quantum version. Qualified Signature Creation Devices (QSCD) are systems that provide authentication of users or enabling them create legally binding digital signatures. They utilise asymmetric keypairs that are held by users and organised, distributed, and asserted by public key infrastructure. A CRQC would be able to forge digital signature or authenticate into the system as another user.

How will these platforms be transitioned to post-quantum cryptography?

Some of these systems rely on hardware modules (such as smart cards), which will probably require completely new hardware, capable of running PQC. Other systems might use some kind of distribution to protect private keys (e.g., Cybernetica's SplitKey), where only a software update is required. Call to action is again to contact your solution vendor for their roadmap to PQ transition.
Cybernetica’s SplitKey platform has post-quantum cryptography on its roadmap.

Cybernetica's post-quantum pledge

Cybernetica’s post-quantum capabilities

Cybernetica has been working on post-quantum cryptography since 2017. Our Information Security Research Institute has published peer-reviewed designs for post-quantum digital identity, interoperability and advanced applications like internet voting. We have published guidance for transitioning legacy systems to post-quantum cryptography and have compiled regular overviews on post-quantum developments.
Cybernetica has also developed a post-quantum engineering platform for our products. We have used it to implement post-quantum VPN, interoperability, digital identity and internet voting systems.

We help you put together a post-quantum strategy

We believe our experience and resources are extensive enough to provide support from the start of your post-quantum transition journey. We can provide aid with infrastructure categorisation and identification of quantum-unsafe spots. We can help choose the correct post-quantum technologies for your infrastructure and establish a clear strategy with effective timeline and resource allocation.

Our systems are ready for post-quantum cryptography

With in-house personnel dedicated for PQC research and engineering, we feel capable of reliably ensure future safety of our in-house developed systems by using most up-to-date technologies, standards, and data formats. We are also embracing the concept of crypto agility in new and optionally existing applications.

We have a post-quantum strategy for our products

Cybernetica has post-quantum transition plans in place for all major products that will be impacted by a quantum computer first – UXP and SplitKey. We provide support in transitioning. Contact us for timelines, updates and further information.

Get in touch with us

Dan Bogdanov, PhD
Chief Scientific Officer

dan.bogdanov@cyber.ee

cyber.ee

Cybernetica

CYBERNETICA

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency.
Neither the European Union nor the granting authority can be held responsible for them.

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Funded by the European Union