Timelines for migration to post-quantum cryptography

Activities which organisations must carry out to migrate safely to post-quantum cryptography in the coming years.

Executive summary

The national migration to post-quantum cryptography (PQC), mitigating the threat from future quantum computers, is a mass technology change that will take a number of years.

The NCSC recognises the need both to offer guidance on some of the early-stage migration activities, and to set some indicative timelines that UK industry, government and regulators can follow. In this guidance, the NCSC sets out some key target dates for migration activities.

Although the core timelines are relevant to all organisations, this guidance is *primarily* aimed at technical decision-makers and risk owners of large organisations, operators of critical national infrastructure systems including industrial control systems, and companies that have bespoke IT. Different sectors will have different current states of cryptographic maturity, and so the weight of activities might vary across the three periods, but a focus on those headline dates is important for investment decisions and broader cyber security planning.

The key milestones are:

- **By 2028**
  - Define your migration goals
  - Carry out a full discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)
  - Build an initial plan for migration
- **By 2031**
  - Carry out your early, highest-priority PQC migration activities
  - Refine your plan so that you have a thorough roadmap for completing migration

By 2035

- Complete migration to PQC of all your systems, services and products

There will be a small set of more rarely used technologies for which migration by 2035 may be more difficult. This may impact some sectors more than others, but all organisations should work towards these key dates.

Note: Most of the work needed to prepare for and deliver a successful migration involves activities that are central to good cyber security practice. Organisations should use migration as an opportunity to build broader cyber resilience into their systems.

Background

The threat to cryptography from future large-scale, fault-tolerant quantum computers is now well understood.

Quantum computers will be able to efficiently solve the hard mathematical problems that asymmetric public key cryptography (PKC) relies on to protect our networks today.

The primary mitigation to the risk this poses is to migrate to post-quantum cryptography (PQC); cryptography based on mathematical problems that quantum computers cannot solve efficiently.

In November 2023, the NCSC published a white paper 'Next steps in preparing for post-quantum cryptography', with small updates in August 2024 to reflect NIST's publication of 3 algorithm standards. A core signal in that paper was that organisations should be beginning or continuing their preparation for migration to PQC now. That will happen most effectively as part of a broader uplift in cyber security as systems are replaced.

In a supporting post, 'Post-Quantum Cryptography, What Comes Next?', we outlined our priorities:

- supporting regulated sectors
- supporting central government
- ensuring that the UK has access to the right skills to enable their future migration

Migration to PQC is a global-scale change to IT and operational technology (OT) systems, and will typically involve activity that spans multiple leadership cycles in most large organisations. Like any major IT or OT upgrade, the total financial cost of PQC migration could be significant, so it's essential that organisations budget accordingly, including for preparatory activities as well as the actual migration.

About this guidance

This guidance:

- sets out the necessary steps towards PQC migration
- describes how the preparatory work might vary across different sectors
- advises on timescales for key activities on the long journey to PQC

It is primarily aimed at technical decision-makers and risk owners of large organisations, operators of critical national infrastructure (CNI) systems including industrial control systems (ICS), and companies that have bespoke IT (such as proprietary communications systems).

Small and medium-sized enterprises (SMEs) often use mainly commodity IT, such as standard browsers, operating systems and mobile devices. For such SMEs, PQC migration will be more straightforward and should happen seamlessly, as services are updated by their vendors. Where custom or specialised software is used, PQC-compatible updates or replacements will need to be identified and deployed; this should follow the same timetable as for larger organisations.

Planning your PQC migration

In many ways, migration to PQC will follow the same patterns as any significant technology programme. The primary goal is to integrate PQC into your systems without raising other cyber security risks, and so early and thorough planning is essential.

There are many models for carrying out a successful technology migration; all organisations will have their own preferred approach or framework. Core to all of them are a number of key phases of work. They are outlined here in a way that is intended to be agnostic to your delivery methodology; although they are set out sequentially, in practice they are interrelated.

Defining migration goals

Primarily, migration to PQC is a mitigation to a cyber security threat. This currently comes from the cryptographic risk that quantum computing poses. However, as PQC adoption becomes more widespread in the future, those who do not migrate in a timely way will end up running significant legacy estates, with the risks that this will entail. So, primary functional goals will include those that relate to a robust cryptographic infrastructure for your organisation, but as part of a set of wider cyber resilience objectives. You will have sector- and business-specific risks and drivers that will influence these, and in many cases you will need to meet regulatory requirements.

You should also consider the agility of your systems in future. We know that one of the challenges for this migration will be that, particularly in older systems, cryptographic services have evolved over many years in sometimes haphazard ways. This complexity will make both *discovering* the cryptographic components in use, and *identifying* and *executing* appropriate mitigation strategies more difficult. PQC migration is an opportunity to simplify your estate, which will also help to reduce other cyber security risks.

Discovery and assessment

Any technical system migration needs to start with building a clear understanding of your current estate. This includes:

- identifying your key services and applications

- forming a record of the data you hold (including its expected lifetime and its value to an adversary)
- identifying how data is protected in transit and at rest

You will need to map the systems that operate these services, and through which your data is processed, and ensure you have processes for identifying and managing your assets – software and hardware – effectively.

You will also need to understand how your systems and services are managed. For example, are they on-premises or in the cloud? Do you manage them yourself or rely on managed service providers? For many organisations, managed service providers are likely to deliver most of your IT capability, in which case it is important to ensure that they are also carrying out these assessment activities for all the services that they provide.

Building this understanding of your entire estate should include:

- systems and services operated by your organisation (both for internal use and those that external users interact with)
- products made or used by your organisation that have a cryptography, cyber security, communications or data processing function
- software applications used by your organisation
- networking and communications hardware (for example routers, switches, hubs, modems, gateways, VPNs, repeaters and base stations)
- mobile devices managed by your organisation
- servers and workstations
- internet of things (IoT) and industrial control system (ICS) devices with a communications function
- devices and tokens issued to end users
- devices and sensors installed in-the-field

This is **not** intended to be a formal asset register. At this stage, it is more important to understand the nature of each system under consideration (rather than build a detailed inventory of each individual item) so that a migration plan can be drawn up. However, you should seek to quantify the scale of each system

and, where available, you should capture version information and patch levels. You should also identify dependencies between components of your systems and services. This should enable you to identify where the migration challenge will be reasonably simple to solve, either through your service provider, or through routine updates from major commodity IT suppliers.

For some of your services, particularly those running on IT or OT which you manage directly, you may need to gain a more thorough understanding of their cryptographic components, so that you can map exactly the cryptography, protocols and hardware on which they depend.

There is a role for both a top-down and a bottom-up approach to carrying out the more detailed parts of the assessment. A top-down analysis ensures that you can focus on your core services and architectural interdependencies. But sometimes you will also need to perform a more low-level exploration of the use of cryptography on your networks to identify components that will need updating. Consultancies with deep cryptographic expertise can help you understand where you are carrying risk.

Migration strategy selection

You will need to decide on an approach for the migration of each system, service or product that you are responsible for. Where you rely entirely on commodity platforms, it is likely that upgrades to PQC will be delivered by your service provider. In such cases you will not need to make wholesale changes beyond routine improvements that will come through normal, timely refresh of your commodity hardware (such as laptops, phones, servers and routers). Further information on this is available in the NCSC's guidance on keeping devices and software up to date.

Where you do **not** rely on commodity technology, you have a number of different options:

- **In-place migration:** replacing the vulnerable PKC components with PQC equivalents, making minimal changes to the rest of the system.
- **Re-platform:** switching the service to a new or upgraded platform that does offer PQC compatibility, perhaps taking the opportunity this exercise

provides to review your broader architectural choices. For example, you might choose to move from on-premises to cloud-based infrastructure.

- **Retire the service:** setting a future date for withdrawing it to avoid the necessity for migration.
- **Run until end-of-life**, where a system is likely to be decommissioned or deprecated anyway within a defined timeframe.
- **Tolerate the risk:** continuing to operate without a mitigation to the quantum computing threat.

You may also have some systems that are not vulnerable to quantum computing attack (for example, because there is no PKC in use), in which case no action is required.

Conversely, you may already have some legacy systems (long-lived physical infrastructure, old IT platforms and systems relying on outdated protocols) that are not capable of being transitioned to support PQC. Your strategy will need to account for this.

Developing your migration plan

This is the point at which you need to develop a set of migration activities. You will have identified:

- your priority services (that is, those processing your most valuable or long-lived data)
- where you have a dependency on long-lived hardware
- your supply chains, and your service providers
- where you currently have risks to manage from legacy systems

There will be several steps in the migration of each system, and your migration plan should include timelines for each of these. The steps could include researching available technology options, procurement, commissioning, testing, data backup and migration, leading up to the actual rollout.

Your plan should also account for business continuity; that is, you should identify to what extent you can tolerate outages during migration, and have a roll-back

plan in case of difficulty. Where you have OT, or an extensive physical infrastructure, you will need to pay particular attention to the constraints that infrequent replacement cycles impose.

Except for the very simplest systems (which can be replaced in a single effort with a 'big bang' uplift to PQC), you will likely find that you need traditional PKC and PQC to co-exist for a while within your environment. Because the introduction of PQC involves making compatibility-breaking changes to encryption, you may need new PQC systems also to support traditional PKC algorithms as an option during the migration period. You should therefore seek solutions that offer *cryptographic agility*; that is, the ability to readily support alternative suites of cryptographic algorithms, and you should identify the criteria you will use to determine when to end support for the traditional algorithms. You will be fully secure against the quantum computing threat once you no longer have any sole dependence on traditional PKC.

PQC migration for enterprise PKI

Large enterprise IT systems typically include a privately hosted Public Key Infrastructure (PKI). This issues certificates to machines (and sometimes users) which are used to confirm identity as part of a network protocol. Migrating an enterprise PKI will require both the creation of a new PQC root-of-trust, and issuing new PQC certificates to all entities on the network. While this will usually be possible remotely via the network management system, some devices may require physical interaction.

There are several different possible migration models. The simplest is a new parallel enterprise PKI with the PQC algorithms, to run alongside traditional PKI. In some very controlled environments, you may be able to move in one jump from the legacy to the new PKI, without ever operating them both at the same time. More likely, you will have to operate them both simultaneously for a period, allowing a staged migration. This requires the use of protocols (such as TLS and IKE) that allow the negotiation of specific certificates to be used in a cryptographic exchange, so that PQC certificates can be used as soon as both communicating parties have been upgraded to PQC. Alternatively, you may wish to consider the introduction of a new PQC root-of-trust that cross-signs the old one, allowing non-upgraded certificates to still be verified.

You will need to assess the security implications of your chosen approach on a case-by-case basis. In general, your system will not provide quantum-secure authentication until migration of your PKI is complete, and traditional certificates have expired or been revoked.

All your planning and sequencing should be informed by an understanding of the readiness of robust, standards-compliant implementations of PQC algorithms and protocols. It will take a number of years for all protocols and global

cryptographic infrastructure to be fully PQC-ready, and for there to be trusted implementations of everything you will need. Migration will be an iterative activity, with multiple deployment and testing cycles, so your plans should take this into account. In particular, the services to protect confidentiality of your key assets will be available soonest; certificate-based PKI, and IoT and ICS protocols will follow more slowly.

Note: Other than a very small number of companies who hire cryptography specialists, your plan should **not** involve you (nor most of your suppliers) producing your own implementations of post-quantum cryptography. There will be certified implementations of PQC algorithms and trusted libraries (both open source and proprietary) incorporating PQC into protocols.

Executing your migration plan

We are now looking further into the future. You will carry out higher priority activities first, as outlined in your migration plan. As you do this, you are likely to refine your plan, and as your suppliers evolve their plans, yours will move with them. Similarly, as the wider PQC ecosystem matures and there is greater availability of commercial PQC infrastructure, you will be able to add more precision to the later stages of your migration.

As with any major IT migration, testing and validation should be a core part of your plan, and embedded in its execution. You should ensure that your testing is extensive enough not just to cover *integration* of PQC-supporting libraries and software and hardware modules into individual systems, but also the *interoperability* with other services, in line with the dependencies you have identified.

Incorrectly configured cryptography does not necessarily lead to loss of service, but it can weaken security. You should therefore carry out additional tests to check that the cryptography is actually performing as expected. For example, once standardised PQC cipher suites are available for TLS, you will need to check that your systems are actually using them, and not falling back to traditional cryptography. There are tools available to help with this analysis.

You will also need to have a rigorous assurance process that ensures that the *implementation* of your PQC migration (and wider related cyber security uplift) is meeting your core goals. This might include metrics for measuring the success of

the migration. For example, you should be able to quantify how many of your software clients are using PQC, and be able to identify those that are not. The metrics will help you gauge how far through migration you are, whether any remedial action is required, and when you will be able to turn off support for the traditional algorithms.

PQC migration across different sectors

Some of the UK's regulated sectors include companies that operate in truly global markets, with a need for some level of technology convergence across those markets. This includes many (but not all) banking and financial services organisations, and companies in the telecoms sector. In these sectors (and others whose services are mostly internet-facing and using common protocols), we would expect:

- an earlier focus on migration (in line with the availability of well-implemented PQC)
- alignment with global partners in the same sector

For other sectors, particularly those with complex physical infrastructure that rely on OT, the path for PQC migration may initially be less clear, with fewer PQC products becoming available in the near future. However, any necessary changes to physical infrastructure will need significant planning and should be done, as far as possible, to coincide with other infrastructure maintenance and improvements. Furthermore, continued OT / IT convergence means that, increasingly in these sectors, planning for conventional IT upgrades to support PQC will need to be a core part of business.

PQC migration for an industrial control system

ICS networks typically involve OT and IT zones separated by a DMZ firewall. All the usual considerations for PQC migration of an enterprise IT network apply equally in an ICS context. With remote logins over the internet now commonplace, it is important to securely authenticate access to the ICS IT zones. So these channels will need to become quantum-secure.

However, there is an increasing prevalence of wirelessly-connected fielded OT devices and sensors which also need to be secure. While the confidentiality of their data might not require strong cryptographic protection, the integrity of the data is likely to be critical, since faulty sensor readings or commands can lead to ICS failures.

Industrial IoT devices present additional challenges for PQC migration, and therefore require special attention in migration planning. For example, these devices:

- might be resource-constrained
- might not be upgradeable
- might be installed in locations that are difficult to service
- might be embedded into larger products
- might not be designed to be replaced
- might use proprietary communications protocols, or protocols that are not yet PQC-compatible

Where these devices are internet-connected (for example to use a cloud service), they offer an entry point to attackers into the control networks, and from there to the ICS enterprise IT zone through the DMZ.

Maturity of PQC technology

The existence of algorithm standards is vitally important, as they are a building block on which cryptographic protocols, products and services will be constructed. As technical standards evolve, the NCSC will issue specific guidance on patterns and configurations for common cryptographic technologies when they become ready for use, and continue to provide organisations and regulators with up-to-date advice.

The PQC algorithms that will be the most widely used were standardised by NIST in 2024:

- ML-KEM (FIPS 203)
- ML-DSA (FIPS 204)
- SLH-DSA (FIPS 205)

These supplement two earlier algorithms with a more limited set of uses:

- LMS, XMSS (NIST SP 800-208)

Since 2024, a steady, and growing, stream of vendors have achieved validated testing of implementations of PQC algorithms through NIST's Cryptographic Algorithm Validation Program.

During 2025, we expect to see the first cryptographic modules validated to FIPS 140-3 under the NIST's Cryptographic Module Validation Program. These will then form a basis for building implementations of PQC into future security systems.

Some vendors have already developed secure boot solutions based on LMS and XMSS digital signature algorithms. Later in 2025, we expect to see cryptographic hardware roots of trust become available, such as hardware security modules (HSMs) and secure boot solutions using the new NIST standards. The efficiency of these implementations will improve during 2026-27 as hardware acceleration for PQC calculations is developed.

The vendors of several of the most popular internet browsers have now incorporated support for PQC into their communications stacks. These browsers can agree a post-quantum secure key with compatible websites and services using a mechanism that is a hybrid of both traditional key exchange and post-quantum key exchange using ML-KEM. However, an exact mechanism for doing this has not yet been standardised across the industry, so is still subject to change and further updates can be expected.

The standardisation of PQC within TLS (the dominant protocol for secure internet access) and other important internet protocols is underway within the Internet Engineering Taskforce (IETF), with final standards likely around 2027. All major

cloud service and hyperscale providers have roadmaps for deploying PQC into their services.

Other standards defining organisations (SDOs) responsible for security protocols have been waiting for final NIST algorithm standards to become available. Now that they are, work is underway in these bodies to incorporate the new algorithms into the security protocol specifications. The FIDO Alliance has committed to providing a seamless transition to PQC for PKC-based secure authentication solutions. New PQC standards will also be required for Trusted Platform Modules, X.509 PKI certificates, UEFI Secure Boot, and 6G cellular communications. Developing and agreeing new standards can take several years and most SDOs have not yet committed to timescales, but it is reasonable to expect the emergence of some standards by 2028.

The NCSC has identified two areas where it believes the development of post-quantum secure protocols will be more challenging than a simple replacement of traditional cryptographic mechanisms with their PQC equivalents. One is the WebPKI , which relies on an ecosystem of trusted roots, Certificate Authorities, Certificate Transparency (CT) log providers and Certificate Revocation List (CRL) providers. There is not yet agreement on how to incorporate post-quantum signatures into WebPKI certificates while maintaining compatibility with traditional WebPKI components. Since the WebPKI is by its nature decentralised, coordination of migration of all its components is likely to be hard to sequence.

The second area of risk for the development of PQC standards is ICS protocols. There are legacy protocols in use in ICS that have never been brought up to modern cryptographic standards. As these are replaced, not only will the new algorithms need to be used, but architectures will need to evolve around them to enable the use of modern key management solutions.

For both these reasons, your initial migration plans should include enough flexibility to adapt to future ecosystem developments.

Timelines for PQC migration

The NCSC believes that 10 years is a sufficient period for a rich set of PQC standards to appear, for an ecosystem of products that uses them to be developed, and for uptake to become widespread, which will enable the deprecation of most quantum-vulnerable traditional PKC. This leads to a target date of 2035 for completing migration to post-quantum cryptography.

While there is likely to be a tail of technologies for which migration will take longer, it is reasonable to expect all organisations to focus on this 2035 target, prioritising those systems which process business and personally sensitive data, or which manage critical communications and systems.

The activities described in planning your migration are substantial, and is critical to reducing cyber risks. Migration **will** happen, globally. It will not be possible to avoid PQC migration, so preparing and planning now will mean you can migrate securely and in an orderly fashion.

The NCSC's recommended timeline of activities

We expect it will take large organisations (and those who run their own IT infrastructure) **2-3 years** to:

- carry out discovery and assessment exercises
- define a migration strategy
- build an initial migration plan.

We expect it will also take **2-3 years** to:

- carry out early migration activities
- refine the plan

Once the ecosystem matures, the remaining, more complex migration activities can be completed. This means that the NCSC can recommend the following activities are completed by the specified dates.

Date	Activities
2028	Complete the discovery and assessment phase. Create an initial migration plan identifying: • highest-priority, earliest migration activities • dependencies on your suppliers and physical infrastructure • any investment needed to implement them • requirement to migrate any long-lived hardware roots of trust Communicate your needs to your suppliers.
2031	Complete your highest priority migration activities to protect your most critical assets. Ready your infrastructure to support a PQC future. Refine your plan so that you have a clear route to full migration by 2035.
2035	Complete your migration to PQC, taking the opportunity to build more robust general cyber resilience into your systems.

Download the infographic of the timeline. Also available from the Downloads section on this page.

Next steps

In this guidance, we have set detailed expectations for the early parts of PQC migration, as well as target completion dates for migration. Carrying out preparatory activities ensures that, once robust implementations of PQC in products become available, you will be able to carry out a principled, staged

migration, in a way that limits any disruption to your organisation's business, reduces the risk of insecurity and ultimately reduces total cost.

PQC migration is an ecosystem-wide activity. To signal the demand to your suppliers and demonstrate to your customers and other stakeholders that you are actively addressing the threat, you could consider sharing a statement of intent for your PQC migration. This statement of intent could include recognition of the quantum threat, your proposed responses, level of ambition and timelines, and the desired end-state. This will help suppliers understand the demand for PQC migration and bring post-quantum secure products to market.

The NCSC will soon launch a pilot scheme to assure those consultancy companies that offer support to the discovery, assessment and planning activities. This will ensure that skills are accessible within the UK to help organisations with their migration to PQC. We would also be keen to see organisations share their own experiences, and examples of good practice – perhaps through their relevant industry bodies, or in regulator forums.

A successful migration will be underpinned by good asset management, clear views into your systems, services and infrastructure, and actively managed supply chains. All these are aspects of good cyber security governance for your organisation, so provide a natural framework for a large cryptographic migration alongside broader improvements to cyber resilience.

PUBLISHED

20 March 2025

REVIEWED

20 March 2025

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector