The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

December, 2023

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

This handbook has been created with the highest standard of care and expertise of the parties involved. The aim of this publication is to create awareness around the urgency to start with migrations and to enhance knowledge of cryptography as an integral part of cybersecurity. Given the fact that its implementation is highly dependent on the type of organisation you are working in and risks involved, this handbook is not intended as a standard approach for each organisation and you might require additional guidance and advice.

Therefore, no rights can be derived from this publication and included advice may prove to be outdated after publication of this handbook. TNO and CWI are under no circumstances liable for any follow-up of the advice given in this publication.

Management Summary

This handbook assists organisations with concrete steps and advice to mitigate the threat of quantum computers on today's cryptography. Even though it is impossible to predict when quantum computers will be able to compromise the cryptography currently in use, the impact of such an event demonstrates that certain organisations should already start working on mitigating measures now. For instance, organisations handling data that will still be confidential 20 years from now, or organisations developing long-lived systems that will still be in use decades from now. The most promising solution is so-called *post-quantum cryptography* (PQC). PQC can be used by currently used systems and computers, but it is secure against quantum computers. However, migrating from conventional cryptography towards PQC will be a very time- and resource consuming task. Judging from previous migrations this process might take well over five years.

Therefore, we advise all organisations to start preparing for the quantum threat now. As an initial *no regret* move, every organisation should start with the first step; performing a *PQC Diagnosis*. The goal of this diagnosis is to identify the stance an organisation should have based on the type of data they handle and their risk surface. Furthermore, we advise to start making an inventory of all the cryptography that is in use, what data it protects and who manages these assets. Only then can a proper judgment of the level of urgency be made. Having this inventory in place will also reduce the risk of having to do a hasty, error prone migration later on, which will introduce unnecessary costs and risks in the future. As eventually every organisation will have to perform this migration, it is beneficial for every organisation to make and maintain such an inventory.

After this first step, the handbook then focusses on the so-called *urgent adopters*. These are organisations that need to start the PQC migration as soon as possible, because the impact of a breach in cryptography, within the coming decades, would be unacceptable. The next two steps in the migration are the *planning* and the *execution* of the migration. In the planning phase, it is important to form a dedicated team to perform the migration and to make sure all business processes are in place to smoothen the migration. On the technical side, different choices can be made in how PQC is implemented. Further, not all PQC solutions might be suitable for all application scenarios. This handbook gives concrete handles to define a strategy for deploying PQC, taking different application scenarios into consideration. The PQC deployment might require new hardware or switching to new vendors that support the right PQC solutions.

Finally, the PQC migration plan has to be executed. In this execution, organisations have to be very careful not to introduce new risks; for instance, by unintentionally introducing new vulnerabilities. This handbook gives guidance on how to perform the migration for different types of cryptography and the various strategies picked in the planning phase. Furthermore, it is not unlikely that new weaknesses of the PQC solutions are discovered in the coming years. Therefore, it is important to realize or maintain a form of *cryptographic agility*. Cryptographic agility allows organisations to quickly modify or replace deployed cryptographic primitives without significantly disrupting the processes in an organisation. This is especially important for when cryptographic protocol improvements or new vulnerabilities are discovered.

Acknowledgements

Contents

1) Introduction

The goal of this handbook is to help organisations identify the risks of their current cryptographic land-scape toward so-called *quantum computers*. Numerous white papers and position papers have already been published to warn for these risks and address the urgency to start planning the inevitable migration. This handbook builds on these advices and additionally gives concrete, actionable steps to start working on a migration strategy. The main audience of the manual are organisations that have no time to wait much longer, so-called *urgent adopters*. However, note that almost every organisation is using cryptography nowadays and is therefore vulnerable to some extent.

Cryptography is of utmost importance in today's digital society as cryptography forms an integral part in the cybersecurity of all organisations. For organisations good cryptography is crucial to prevent the theft of sensitive data, to ensure the received data is correct and to prevent unauthorised access to systems. Weak cryptography can pose huge risks as it can lead to data breaches, unauthorised access, stolen company or state secrets and worse.

However, a substantial part of the cryptography that is currently in use is weakened or even rendered completely insecure by the uprise of quantum computers. At the moment, quantum computers are not yet powerful enough to break cryptographic schemes currently in use, but the development of quantum computers is happening at an increasingly rapid rate. It is likely that in ten to twenty years, quantum computers will be able to break important cryptographic standards used today. Cryptographic schemes that are secure against classical computers, but not against quantum computers, are referred to as *classical cryptography*. Schemes that are additionally secure against quantum attackers are referred to as *post-quantum cryptography* (PQC). There are already three key reasons why organisations should identify and start working on the migration to PQC now already:

1. Sensitive information is at risk of being intercepted and stored now and decrypted in the future with a quantum computer. Such an attack is called a store-now-decrypt-later attack. There are serious suspicions that this harvesting of encrypted data is already taking place. Thus, data which needs to remain protected for a long time is already at risk of being decrypted before the end of this confidentiality period.

2. Long-lived systems and critical infrastructures developed and deployed now are very hard or even impossible to update to PQC later on. Even if it is possible to upgrade the software running on these systems, PQC requires heavier machinery to function, which might be impossible to replace once the system is deployed.

3. Updating or replacing cryptographic infrastructure to post-quantum alternatives is a very cumbersome and resource-consuming task. Judging from previous migrations, it is expected that updating legacy systems will require a lot of planning and preparation. As an example, it took many organisations over five years to migrate from SHA-1 to SHA-256, even after the specifications and implementations were available.

Regardless of when quantum computers are strong enough to break current cryptography, PQC has to become the new standard of cryptography to ensure security of cryptographic schemes in the future. Therefore, all organisations will have to migrate to PQC eventually. While the exact costs of the migration to PQC are unknown, it is certain that every organisation will need to free up resources in terms of people, time and money to perform this migration. Furthermore, appliances might need to be replaced in case they cannot support PQC or if the vendor is not planning to include PQC. Finally, PQC requires stronger hardware compared to current algorithms to function properly, because of which some hardware will need to be replaced.

It is advised that all organisations start working on a diagnosis to make an inventory of the cryptographic landscape of the organisation in order to properly judge the level of urgency of the migration. The earlier this inventory is available, the earlier an (initial) plan for the migration can be made. With this plan in place, some of those assets can already be made ready for migration to smoothen the process and reduce costs later on. Waiting too long and having to do a hasty migration under pressure is prone to mistakes that can be very expensive. For assets that are currently managed by vendors or are going to be bought from vendors, this agility can already be demanded.

1.1 ） Goal of this Manual

The aim of this document is to assist security architects and management within organisations on the migration to post-quantum cryptography. Specifically, this manual focuses on organisations which sense (or should sense) some urgency in migrating to PQC. The migration to post-quantum cryptography should be urgent for organisations to which key reasons 1 and/or 2 highlighted above directly apply. Furthermore, preparing for the migration early reduces the probability of setbacks leading to risk exposure later on.

For this audience, this document provides information about the risk, action steps, pros and cons of migrating and practical advice to draw up a plan for migrating their organisation to post-quantum cryptography. Note that ultimately, each organisation is responsible for drawing up their own plan in line with their own risk appetite. For CISOs and CIOs who instead wish to get a more high-level overview of the threat of quantum computers on classical cryptography, we refer to earlier white papers by TNO [MvH20] and the NBV [NBV21]. In comparison to these papers, this document provides more concrete steps to identify whether quantum computing currently poses a threat to an organisation and which steps need to be taken in order to mitigate these risks.

In this work, we take into account that there is a vast variety of organisations in the Netherlands, each requiring very different advice when migrating to PQC. For this reason, our advice will be different for the various organisational groups, so that each organisation can get advice tailored to its own needs. Note that even within one organisation different departments or teams might have a different level of urgency based on the data or systems they handle.

1.2 ） Associated Risks

All assets currently protected using classical cryptography are at risk of being broken by quantum computers to some extent. However, quantifying this risk is challenging and precise estimations are difficult to make. In this section, the considerations concerning the risks of quantum computers are explained.

Firstly, it is unclear whether or when quantum computers will be capable of breaking cryptography. Current estimations are that this will be in ten to twenty years, but it is entirely possible that an unexpected breakthrough shortens this time [MP21]. In general, the risk grows the longer an organisation delays the migration. Secondly, the faced risk depends on the type of assets protected. If the asset is a system or a piece of data with a lifespan longer than the arrival of strong enough quantum computers, the risk is already high due to store-now-decrypt-later attacks and migration needs to be done as soon as possible. By contrast, functionalities such as authentication and system availability cannot be attacked retrospectively. They are however susceptible to acute attacks by a quantum device when it is fully available. Hence, in these cases a different risk analysis applies. Thirdly, a lot of analysis and scrutiny is being performed on the various PQC algorithms during the standardisation process and new vulnerabilities are discovered frequently. Therefore, performing the entire migration too early introduces the risk of having to migrate again later on if a new attack is discovered. On the other hand, doing it too late may result in severe damage in terms of stolen information and

public reputation if an organisation's systems are broken. The migration of a certain asset can be delayed based on the risk an organisation is willing to take. Because of this, costs can either be reduced or increased by waiting and hence a good balance needs to be found between moving assets early or late.

Finally, it is unknown how long the process of migrating every asset will take. Judging from previous (smaller) migrations, this might take well over five years. Therefore, depending on their risk appetite, organisations can already start preparing for the migration to some extent. Without having to perform the actual migration, organisations can already start identifying vulnerable assets, prioritising them and drawing up a plan without executing the migration. This minimises additional risks introduced by delays and costs of unexpected setbacks during the eventual migration.

1.3) Document Structure & Reading Guide

On a high level, this manual follows a three-step approach as also described in [ETS20]:

```
( 1 )                      ( 2 )                      ( 3 )

┌─────────────┐    ┌──────────────┐    ┌──────────────┐
│    PQC      │───▶│   Planning   │───▶│   Executing  │
│  diagnosis  │    │ the migration│    │ the migration│
└─────────────┘    └──────────────┘    └──────────────┘
```

(1) In Chapter 2, the PQC diagnosis is described. This chapter is mainly interesting for strategy and policymakers and might require involvement of people with knowledge of the type of data/assets that are in place in an organisation. First, the urgency to migrate for an organisation is identified. To this end, the concept of *PQC Personas* is introduced. The purpose of these personas is to assist organisations with finding out what their stance towards PQC migration should be. In order to identify an organisation with one or more personas, (visual) decision trees and schemas are presented. Afterwards, an inventory should be made of all cryptographic protocols as well as of the systems using this cryptography.

(2) Chapter 3 describes the planning of the migration process on both a technical and organisational level. Based on the urgency identified in the previous chapter, it is recommended for urgent adopters to read this thoroughly. After the diagnosis, the level of urgency as well as the cryptography that needs to be migrated has been identified. Using this knowledge, the next step is to decide what mitigation strategies are going to be implemented for the vulnerable assets. Furthermore, the timing of the migration process for the various assets needs to be decided in this step. The target audience of this chapter are again strategy and policymakers. They are required for planning and prioritising the migration process and getting the right team together to perform the migration. Furthermore, this chapter is interesting for (security) architects who are going to be leading the migration process from a technical perspective.

(3) Chapter 4 is primarily intended for a technical audience. In this chapter, handles are presented from a technical perspective to decide *how* the cryptography needs to be migrated. First, generic strategies and considerations for migrating cryptography are given. Afterwards, strategies for specific cryptographic algorithms and protocols are presented.

Finally, in Chapter 5, in-depth technical information for various popular cryptographic constructions is given. This chapter mainly serves as a reference to look up details of cryptography that is being used by an organisation. It is not necessary to read this chapter as a whole. The intended audience of this chapter are technical leads of the migration process as well as (security/cryptographic) developers who will be working on the migration.

1.4) Cryptography Background

Before going into the PQC migration itself, we explain some fundamentals from cryptography.

	Symmetric-key	Asymmetric-key
Encryption	Block Cipher + Mode, Stream Cipher	Public-key Encryption
Authentication/ Integrity	Message Authentication Code	Digital Signature
Key Generation/ Distribution	(Pseudo) Random Number Generator	Key Exchange, Key Encapsulation

Table 1.1: Overview of some building blocks used to achieve certain cryptographic goals, using either symmetric or asymmetric keys.

Cryptography is the study of ensuring safe communication and storage of data in the presence of adversaries. Cryptography aims to protect (a combination of) four basic goals: confidentiality, authenticity, integrity and non-repudiation. *Confidentiality* refers to preventing sensitive data from being disclosed to unauthorized parties. Secondly, *authenticity* focusses on verifying the source of data. Thirdly, *integrity* aims to ensure that data has not been altered by untrusted entities. Finally, non-repudiation prohibits senders and recipients from denying their involvement in sending or receiving certain messages.

The building blocks of cryptography are called cryptographic *primitives*, which are low-level algorithms which can in turn be used to form more complicated and involved cryptographic *protocols*. Examples of primitives are RSA and AES, while examples of protocols are TLS and SSH. An overview of important functionalities and which cryptographic primitives they can be built from, can be found in Table 1.1.

Arguably the most well-known cryptographic functionality is provided by *encryption schemes*. These cryptographic schemes protect the confidentiality of data and prevent the data from being eavesdropped by unauthorised parties. For this, encryption schemes use an encryption key to encrypt the data to obtain a ciphertext that can only be decrypted with the correct decryption key.[1]

Another widely used cryptographic functionality is provided by *signature schemes*. The main goal achieved by these schemes is proving authenticity and integrity of data. For this, a signing key is used to sign the data after which the signature can be verified using a verification key.

The third application that we consider in this document is *key generation*. Cryptographic schemes are used to generate and agree on keys that can later be used by other cryptographic protocols in a manner that ensures that only the correct parties get access to the keys.

For all of these functionalities the keys can either by *symmetric* or *asymmetric*, leading to either symmetric-key or asymmetric-key cryptography. With symmetric-key cryptography, the encryption and decryption keys (or signing and verification keys) are the same and have to be agreed upon beforehand by the involved parties. An example of such a symmetric-key encryption algorithm is AES, which falls in the more generic class of block ciphers. A special class of symmetric-key cryptography is formed by so-called *hash functions*. Hash functions turn a message into a digest in such a way that it is easy to verify that some digest corresponds to a certain message while it is hard to extract the message from the digest, or to find two messages with the same digest. Message Authentication Codes (MACs) achieve authenticity and integrity by creating a tag of a message such that the receiver can verify that the received message has been sent by the desired party and has not been altered by someone else in transit. These are typically constructed from

---

[1]   Note that encryption schemes can also achieve authenticity and non-repudiation, as in some cases only a certain party may know the encryption key and thus only that party can create a valid encryption.

hash functions or block ciphers. Finally, symmetric-key cryptography and hash functions can be used when building Pseudo Random Number Generators (PRNGs) that can be used as to generate key material for other cryptographic primitives.

With asymmetric-key cryptography, the two keys are different and are often referred to as the *public* key and the *private* key. This is because one party can generate the keypair and can publicly announce its public key such that anyone can encrypt messages or verify signatures. However, only that one party can decrypt messages or generate signatures with its private key. Typically, symmetric-key cryptography is faster than asymmetric-key cryptography but is harder to set up. Therefore, it is common practice to make an encryption scheme by using asymmetric-key cryptography to securely exchange a symmetric key, which is used to encrypt the rest of the conversation, for example with AES. This process is also known as a key exchange protocol. An example of this is the Diffie-Hellman key exchange protocol.

Threat of Quantum Computers

The extent to which quantum computers pose a threat to the above protocols and use cases differ. Theoretically, Grover's quantum algorithm [Gro96] presents up to a quadratic speed-up in attacking symmetric-key cryptography. Essentially, this means that the security level of a hash function or symmetric-key encryption scheme is lowered. However, the algorithms themselves are still usable as long as the key or output size is sufficiently increased. For hash functions, the risk of a Grover attack is already mitigated if its output is enlarged by a factor 1.5. For symmetric-key encryption, doubling the key size is sufficient. By analysing the costs of a Grover attack in detail, one might even conclude that these measures are conservative. However, these recommended measures are simple and relatively low cost. All in all, mitigating the risk of quantum computers can be achieved relatively easily for symmetric cryptography.

On the other hand, most asymmetric-key cryptography that is standardised nowadays is completely broken by Shor's algorithm [Sho94]. This means that algorithms currently in use are no longer safe when large enough quantum computers become available and thus need to be replaced by suitable alternatives. This makes the mitigation of quantum risks for asymmetric cryptography a much larger task.

About Quantum Key Distribution

In practice, asymmetric-key cryptography is typically used to establish a shared key to be used for a symmetric scheme for every communication link. This process is known as key distribution. For example on the internet, lots of connections need to be set up with unknown people and each connection needs a new key. Another quantum-safe solution researched for key distribution is Quantum Key Distribution (QKD). QKD refers to a way of achieving key agreement using quantum communication between two parties. This mechanism is promoted as being resistant to both classical and quantum attacks. While this may seem a promising alternative, it is generally considered not practical for replacing classical cryptography for several reasons. Firstly, it only replaces key distribution and itself requires cryptographic authentication. Secondly, to communicate securely using QKD, two parties should be linked by a quantum communication channel. Concretely, this means being directly connected by an optical fibre, or an optical (free-space) communication channel. Further, a low noise level on the quantum communication channel is required. This limits the distance over which (quantum) information can be transferred. A solution to overcome this distance limitation is the use of repeaters. However, this involves trusting a third party with the unencrypted sensitive information, which is not realistic in terms of security. Therefore, using QKD requires large infrastructure investments and is only possible in some specific cases. As QKD by definition relies on this hardware infrastructure, it cannot provide security between virtualised environments. Hence, it is unfit to replace classical cryptographic algorithms. Finally, the specific equipment used for QKD provides new attack vectors. There is a long history of examples showing that commercial QKD devices are vulnerable to side channel attacks or Denial-of-Service attacks.

All in all, post-quantum cryptography is less expensive, more flexible and more mature than QKD. PQC can replace classical cryptography in all contexts as it is able to be executed on machines similar to the ones in use now.

For these reasons, major security agencies do not support the use of QKD to secure communications and agree that post-quantum cryptography should be regarded as the best way to mitigate the quantum threat. For more information on this topic, see the white paper from the Dutch NBV [NBV21] as well as position papers from ANSSI (France) [ANS20b], the NCSC (UK) [NCS20b] or the NSA (USA) [NSA21].

1.5 ⟩ Related PQC Migration Work

Dutch Organisations

In 2020 and 2021 respectively, the Dutch research organisation TNO [MvH20] and the Dutch Communication Security Agency NL-NCSA [NBV21] warned for the risks introduced by quantum computers. Next to that, they present some considerations for cases in which the migration needs to take place immediately. Both works agree to use symmetric-key cryptography with sufficient key-sizes or hybrid solutions for asymmetric-key cryptography. This guide holds on to this advice and additionally provides concrete action steps to implement these solutions, also for other (less urgent) cases.

In 2022, the Dutch National Cyber Security Centre released their guidelines for quantum-safe transport-layer encryption [NCS22]. This is specifically targeted towards urgent adopters who already need to make a choice for a post-quantum alternative. Our recommendations are aligned with their guidelines.

Standardisation Bodies

Historically, the standardisation and the adaptation of new cryptographic protocols have been initiated and led by the National Institute of Technology and Standards (NIST, US) and the European Telecommunications and Standardisation Institute (ETSI). The currently most visible work of NIST is the process started in 2016 to solicit, evaluate and standardise cryptographic protocols that are secure against quantum computers. In July 2022, the first candidates to be standardised were announced [NIS22a]. The actual standards are expected to arrive in 2024. The recommendations for post-quantum algorithms presented in this document are aligned with these draft standards.

Furthermore, both NIST and ETSI are active giving advice on the actual migration. In 2020, ETSI released their "Migration Strategies and Recommendations for Quantum-safe Schemes" [ETS20] defining three key steps organisations should take to enable the migration:

1. making an asset inventory;
2. preparing a migration plan;
3. performing the migration.

Finally, they give some pointers on what to pay attention to. This document has been approved by ETSI's technical committee on cybersecurity, which regroups experts from industry and government organisations. Our guide follows this same three-step approach. NIST is currently in the process of setting up a project consortium [NN21] to perform research on the same three-step approach where the initial scope is to develop tooling that aids with the discovery in the first step. It is currently unknown when this project will start and whether the developed tools and knowledge will be made available to the public.

Other Organisations

In 2021, the European Union Agency for Cybersecurity (ENISA) published a technical overview of the (generic) mathematical properties of the various post-quantum algorithms as well as their specifics and available implementations [BDH+21]. This document gives an overview of the state of play in terms of available algorithms and hybrid solutions but lacks a presentation of concrete action steps.

The German Federal Office for Cybersecurity (BSI) also published a guide explaining the inner workings of the algorithms as well as recent developments in politics, research and industry related to PQC [BSI22]. Finally, they give some basic recommendations for steps to take. The advice and steps in our guide largely align with their recommendations but focus less on the details of the algorithms and more on the strategy to migrate to these algorithms.

Finally, the UK's National Cyber Security Centre (NCSC) also published a generic white paper on the need to prepare for post quantum cryptography in 2020 [NCS20a].

2 ⟩ Diagnosis

Summary

This chapter gives concrete guidance for organisations to determine the risk and urgency for migrating to PQC standards and what they need to start this migration. The first part of this chapter gives handles for whether an organisation should already start taking first steps towards PQC migration. This is achieved by dividing the landscape of organisations into different personas, so that each (sub)organisation identifies as at least one of these personas. The second part advises on the infrastructure diagnosis that organisations should make before embarking in the PQC migration.

The persona(s) of an organisation depend on a couple of factors, such as the sort of data and systems handled by it, the threat level and its dependency on other organisations. With these factors, three main personas can be drafted, namely: *Urgent Adopters*, *Regular Adopters* and *Cryptography Experts*. Firstly, Urgent Adopters are organisations which should already start taking steps towards PQC migration now, or should already have done so. Secondly, Regular Adopters are organisations which can take a more reactive stance towards PQC migration for now, as their assets allow awaiting further development of PQC standards before starting with migration. Lastly, Cryptography Experts are organisations which supply, service or deliver cryptographic knowledge or infrastructure to other organisations. This chapter contains sufficient information for organisations to decide which persona(s) they identify as.
If an organisation identifies itself as an Urgent Adopter, we advice to start its *PQC diagnosis* as soon as possible. This involves gathering the necessary data concerning the current security architecture to decide which assets should be migrated first. This step requires the establishment of four documents: a risk assessment; an inventory of cryptographic assets used in the organisation; an inventory of the data handled by the organisation; and an inventory of the suppliers of cryptographic assets. Organisations which do not identify as Urgent Adopters can wait before performing this PQC diagnosis, although in some cases it might be beneficial to start this diagnosis now as well.

The subsequent chapters focus on giving advice in the form of concrete action steps to Urgent Adopters. It is hence vital that PQC personas get determined accurately, to ensure that all organisations which need to take steps towards PQC migration now, indeed do so.

2.1 ⟩ PQC Personas

Before embarking on the journey towards PQC migration, organisations need to find out whether they should even start on this journey now and if not now, when. To help organisations with this choice and to best address the different needs of organisations when making the PQC migration, we have divided the landscape of organisations into a small number of categories, called PQC personas. Firstly, this allows us to identify which organisations need to take steps towards migration as soon as possible and which organisations can wait a bit more. Secondly, this allows us to tailor advice to different organisations with similar structure.

The PQC Migration Handbook | GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

We have drafted different concrete action steps for each of the personas, varying in terms of urgency, timeline, risk analysis, attention to be taken and more. We used the following characteristics to make this division:

- **Attack surface:** What infrastructure does the organisation provide/have which is prone to attacks aided by a quantum computer?
- **System types:** Which kind of systems are handled and what is the impact of a malfunction of these systems?
- **Data types:** Which kind of data and information is handled in terms of criticality, disclosure sensitivity and the consequences of unauthorised and undetected modification?
- **Time pressure:** How quickly does PQC migration need to take place to ensure safety of data and sytems?
- **Dependency on other organisations:** How do different organisations depend on one another?
- **Threat level:** How realistic is it that a malicious actor with a quantum computer will choose to attack this organisation?

The PQC persona can be divided into three main categories:

| URGENT ADOPTERS | REGULAR ADOPTERS | CRYPTOGRAPHY EXPERTS |

Urgent Adopters | Organisations which handle sensitive data or provide critical or long-lived infrastructures. These organisations should start taking first steps on PQC migration as soon as possible. Within this category, we have made a distinction between the different kind of organisations that have to move quickly, depending on why they are at risk of being attacked by a quantum computer.

Regular Adopters | Organisations which do not handle sensitive data and do not provide critical or long-lived infrastructures with a high risk of being attacked. These organisations may, for example, still handle sensitive data, but it is unlikely that data is currently being stored for decryption by a future quantum computer.

Cryptography Experts | Organisations that supply cryptographic standards or infrastructure. The main differences between cryptography experts and urgent adopters are that cryptography experts should have most of the necessary cryptography knowledge for PQC migration in house already, and that they are responsible for cryptographic assets of other organisations as well.

This manual mainly focuses on giving advice and concrete steps to urgent adopters, and hence the main goal of this section is for organisations to determine whether they are an urgent or regular adopter. The following chapters contains extensive advice for urgent adopters, however there will also be advice for the other two categories.

2.1.1 Urgent Adopters

Within the urgent adopters persona, various subpersonas can be drafted out. These subpersonas are not meant as a division of the urgent adopters persona, but can be thought of as examples of urgent adopters. These examples are based on the different risks quantum computers bring to urgent adopters. In general, advice for these subpersonas will be the same, but some action points will be stressed more for certain subpersonas than others. More information on this will follow in the next chapter.

Personal Data Handlers

Organisations that handle **personal data with a long confidentiality span.** These organisations are required by law to protect such personal data. The biggest risk these organisations face are store-now-decrypt-later attacks. Personal data is any information related to an identified or identifiable individual. This includes but is not limited to social security number, telephone number, credit card number, health data, appearance or address.

Such data are prone to store-now-decrypt-later attacks if there are other parties for which this data is interesting even in 20 years or more. Thus, even though most organisations handle personal data, this persona focuses on personal data for which a quantum computer already poses a significant threat today. This means for example that sport clubs, webshops and universities do not fall under this persona. Examples of organisations which do fall under this persona are governments, organisations in healthcare such as hospitals, financial organisations and insurance providers.

It should be noted that there are currently no laws for protecting personal data against quantum computers or the use of PQC to mitigate it. However, if a future quantum computer is used to decrypt data which is currently being stored, it is likely that the owners of this data will still be held responsible.

Organisationally Sensitive Data Handlers

Organisations that handle **organisationally sensitive data with a long confidentiality span.** This entails state secrets, transactions, minutes, trade secrets, and any information which is classified for entities outside of the organisation. The biggest risk these organisations face are store-now-decrypt-later attacks. Such data is prone to store-now-decrypt-later attacks if there are other parties for which this data is interesting even in 20 years or more. Examples of such organisations are the military, national intelligence organisations, governments, financial organisations, knowledge institutes and universities.

The main difference between personal and organisationally sensitive data is that personal data needs to be kept secret to protect the privacy of individuals, while organisationally sensitive data needs to be kept secret from an organisational perspective. A data breach of the first would result in a company breaking laws regarding personal information, while a data breach of the second would likely result in a company losing (some of) its competitive advantage in the market, a loss of knowledge or state security, or a general negative impact on the entire economy.
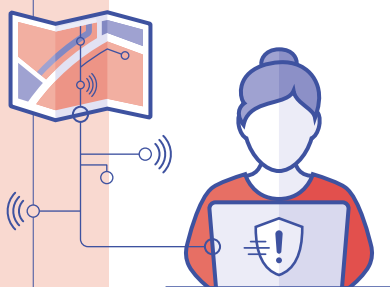
Critical Infrastructure Providers

Organisations that provide **systems that are crucial for the functioning of large groups of people**, such as towns, cities, provinces or even countries. There are a variety of such systems, but most of these are concerned with providing large groups of people with basic needs, such as water, electricity, transport, communication and healthcare. A malfunction of these systems can have different results with different degrees of impact. Usually, malfunctioning results in many people having their daily lives seriously disrupted, but in some cases it might even result in serious damage, injury or even death.

There are many examples of cyber attacks on critical infrastructure, one of the most noteable being the Triton malware attack on Saudi petrochemical plant, designed to cause loss of life. To read more about this and other examples, please look at [Wei21].

The difference with the first two personas is twofold. On the one hand is availability of much greater importance than integrity and reliability for these organisations. On the other hand is the risk appetite much lower, as malfunctioning u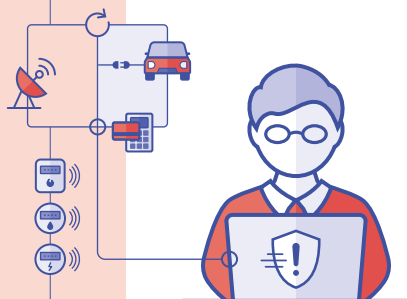sually has a major impact. The migration process might look different. Examples of critical infrastructure providers are energy or water providers, transport organisations such as train companies or airports, communication companies such as telecom providers, web browsers and healthcare providers such as hospitals.

Long-lived Infrastructure Providers

Organisations that provide **systems which are built to have a long life-span**, because they are otherwise not profitable. The main risk these organisations face is that the systems which are produced over the next decade will probably still be in use once quantum computers become available. Hence these systems should have the ability to be swiftly updated to quantum-safe standards. Post-quantum cryptography usually has different (usually heavier) hardware requirements than current cryptography, because of which the production of systems with a life-span of more than 20 years should already take these hardware requirements into account. Examples are satellites, payment terminals, cars, telecommunication networks, energy providers, smart meters, smart industry (4.0) and sensor networks.

2.1.2 Regular Adopters
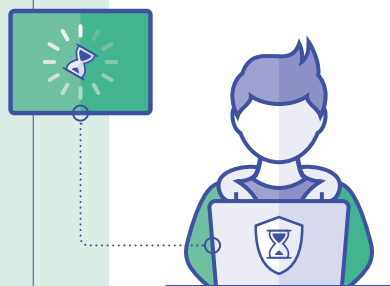
Any organisation that does not identify as any of the urgent adopter personas. These organisations possibly handle data or provide systems, but the kind of data is not currently prone to store-now-decrypt-later and the kind of systems are not critical or long-lived. Note that in later stages these organisations may be prone to attacks using a quantum computer, but for these organisations it is more beneficial to await further standardisation of PQC, as early migration also comes with extra risk, as mentioned before. There are, however, steps these organisations can already take now and they should also remain mindful about possible changes in advice or their own persona(s). More information on this can be found in the next chapter. Most organisations will be regular adopters, with some examples being retailers, schools and sport clubs.

2.1.3 Cryptography Experts

Although the aim of this work is not to give concrete advice to these sorts of organisations, as they should have all the necessary knowledge themselves, we do mention them for a couple of reasons.

First of all, it is important for our main audience of urgent adopters to know that this group exists and what to expect from them. Most urgent adopters have cryptography experts as vendors of their cryptography. Urgent adopters who want to start migrating to PQC should be able to ask these vendors whether their products are quantum-safe or if not, when they expect their products to be quantum-safe. In some cases these urgent adopters may have to choose to switch to a different vendor for their cryptographic assets.

Secondly, the above brings concrete advice to the cryptography experts. They should be ready to expect questions from their customers related to PQC, such as timelines to achieve PQC in their products and which algorithms they are planning to implement. Because of this, they should start migrating their products to PQC standards as soon as possible as well.
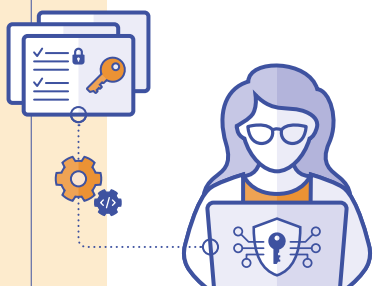
Standard Developing Organisations
Organisations that define **cryptographic standards and/or protocols**. These are standards and protocols which are standardised for a wide variety of applications, using cryptography in some way. Most of these standards are used for either communication or security, such as secure communication, secure data storage, protection of systems or TLS. These organisations almost always operate at a national or international level because of the importance of interoperability between regions and nations. Examples are NIST, ETSI, IETF, TLS, IEEE, ISO/IEC, TCG, ANSI, W3C and ENISA.
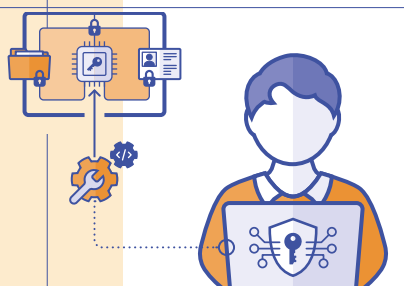
Cryptographic Infrastructure Providers
Organisations that develop, implement or service **cryptographic infrastructure for other companies to use**. These organisations usually operate at a national or international level. Examples are FOX- Crypto, Logius, Compumatica, NXP, Brightsight, Technolution, Apache and MSSPs (Managed Security Service Providers) such as Cipher and SecurityHQ.
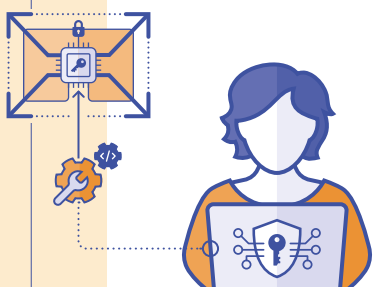
Providers of Cryptography Beyond Secure Communication
Organisations that develop, implement or service **infrastructure based on cryptographic protocols which are used for purposes beyond secure communication**. Note that this sort of cryptography does not necessarily give higher security guarantees. The difference lies in the fact that the cryptographic protocols developed by these organisations are used for different purposes and may be based on different principles. Examples of such protocols are blockchain, Zero-Knowledge Proofs, Multi-Party Computation and Idemix. This persona is mentioned seperately as the sort of cryptography developed can be so significantly different, that different measures have to be taken by these organisations than by organisations which develop more standard cryptographic functionalities. As these forms of cryptography are relatively young in practice, most organisations of this persona are currently start-ups which use one of the mentioned techniques for specific use cases. Examples are Roseman Labs, Linksight, Cosmian (all MPC) and IRMA.

2.1.4 Determining Your Persona

Levels of Cryptography

Generally speaking, there are three levels of cryptography which an organisation is responsible for, namely:

1. its own cryptographic infrastructure;
2. its cryptographic knowledge;
3. cryptographic infrastructure related to the supplying of services or products to other organisations.

Each of these three have to be taken into account when migrating to PQC and hence influence what kind of persona you are. Level 3 is treated separately as by supplying to other organisations, attacks on this supplying organisation can work through to these supplied organisations via so-called supply-chain attacks. A sup-

Figure 2.1: Visual example of organisations with their PQC Personas

Scope of the manual

ply-chain is a chain of organisations where each organisation supplies to the next organisation in the chain. An example of certain organisations forming a supply-chain can be found in Figure 2.1. In this diagram, the arrows indicate that organisations supply to one another (e.g, Microsoft supplies to the recruitment agency and the tel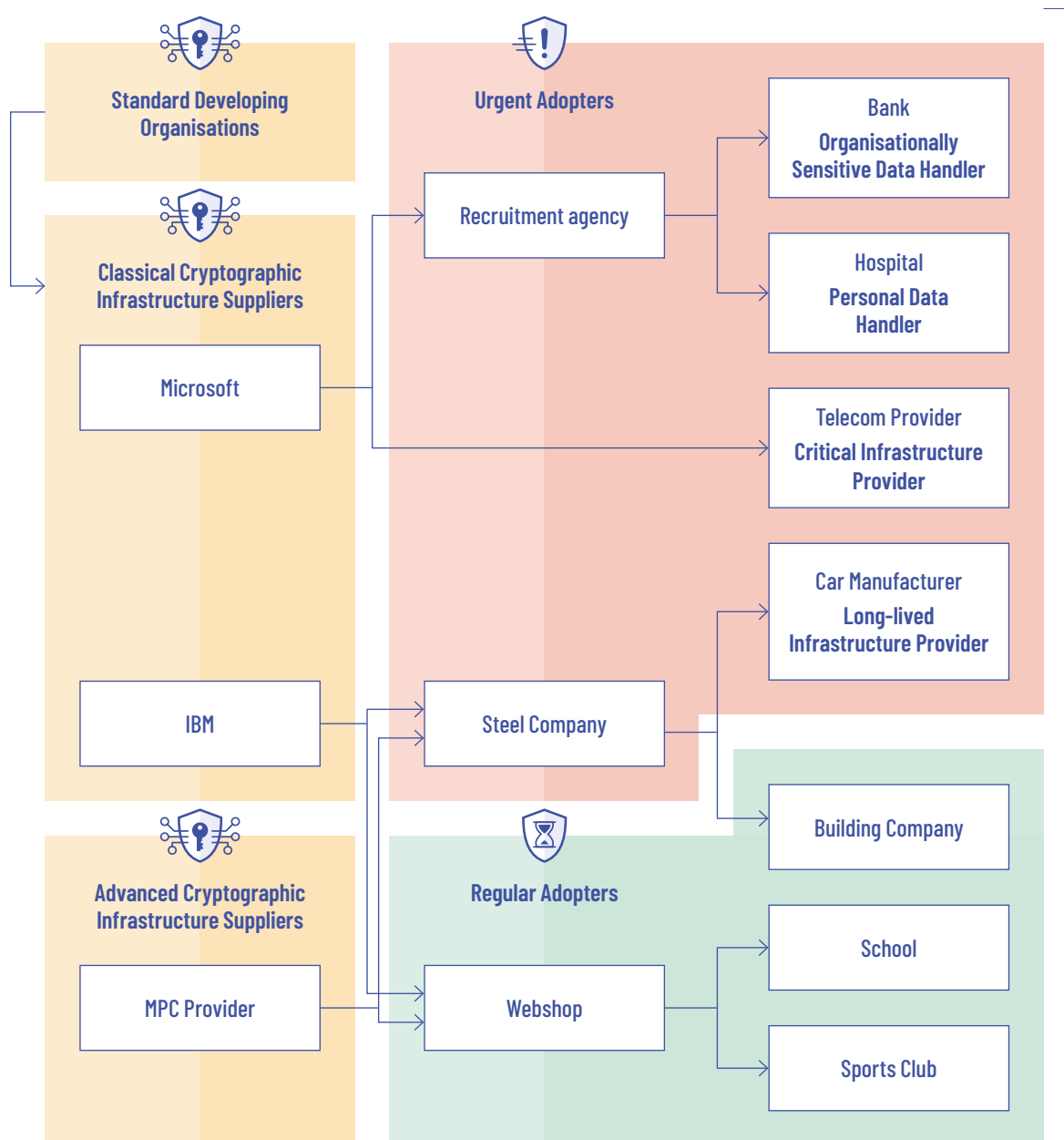ecom provider). Attacks on organisations higher on the supply-chain can also pose a risk to organisations further down the supply-chain.

An example of a supply chain attack is the SolarWinds hack in 2020. In this attack, hackers inserted a malicious piece of code into one of the products offered by software company SolarWinds. After this insertion, SolarWinds (unknowingly) shipped this as an update to thousands of organisations including major multinationals and the US government, whose data, networks and systems could then be accessed by the hackers. Examples of the supplier persona are IT/software vendors such as Microsoft and IBM, Cloud providers and anti-virus/IDS vendors.

Determining Your Persona

When determining one's persona, an organisation has to take into account all three of the levels mentioned above. Firstly, it should consider its own infrastructure to come up with one (or more) suitable persona(s). Secondly, an organisation may identify as certain personas because of the cryptographic knowledge it possesses. This results in a cryptography experts persona. Lastly, an organisation inherits the same persona as all the organisations it supplies to, because it has to follow the same advice as the organisations it is supplying to. Otherwise, it poses too high a risk to the organisations it supplies to. This inheriting of personas continues even further down the supply-chain, meaning that an organisation inherits all the personas of organisations which are below it in the supply-chain. As an example, this means that in Figure 2.1, the recruitment agency is both an organisationally sensitive as personal data handler, the steel company is also a long-lived infrastructure provider, and Microsoft is both a organisationally Sensitive data Handler, personal data handler as well as critical infrastructure provider.

Taking all these personas together, each organisation should be able to identify itself as an urgent or regular adopter and potentially also a cryptography expert. If an organisation is an urgent adopter, it might identify as more than one of the subpersonas.

Additionally, it should be noted that the persona(s) of an organisation may change over time, because the risks it faces over time may change. We advise to carefully reassess which persona you identify as each time your organisation starts taking new steps in PQC migration. We also emphasise that some organisations may think they are regular adopters, while they are an urgent adopter in practice because of either their own cryptographic infrastructure or the infrastructure of one of the organisations it supplies to. Because of this, we advise organisations to be conservative in determining ones PQC persona. If you are on the boundary of being an urgent or regular adopter, it is advised to follow the advice in Section 3.2, as this section will give further guidelines on when you should start migrating certain assets.

The best way to find out which persona(s) suit(s) your organisation or the organisations you supply to is to read the descriptions of all the personas above and see which description(s) apply to the relevant organisations. In addition, the flowchart in Figure 2.2 aims to give a visual aid for determining one's PQC persona(s).

Advice for Organisations Which Have Multiple Personas

As mentioned above, some urgent adopters persona may identify itself as multiple of the urgent adopters personas. For instance, financial institutions are both personal data handlers and organisationally sensitive data handlers. Although this does not change the advice mentioned in the next section, the different subpersonas do give an indication which action steps should receive more focus. The first action steps (the one in Running the PQC Diagnosis, see next section) are the same for the different subpersonas. For the later steps, the diagnosis should make it clear which cryptographic asset falls most under which persona and hence which action steps should receive most focus for this asset.

START

Do you develop or provide cryptographic standards or protocols?

YES → You are a **Standard Developing Organisation**

NO

Do you develop, service or provide cryptographic infrastructure?

YES

How much of this cryptography is based on advanced cryptographic theory such as blockchain, MPC or ZKP?

NONE → You are a **Cryptographic Infrastructure Provider**

SOME

ALL → You are a **Provider of Cryptography Beyond Secure Communication**

NO

Do you handle confidential data with a long confidentiality span?

YES → You are a **Organisationally Sensitive Data Handler**

NO

Do you handle personal data with a long confidentiality span?

YES → You are a **Personal Data Handler**

NO

Do you produce systems crucial to functioning of large bodies of people?

YES → You are a **Critical Infrastructure Provider**

NO

Do you produce systems with a long life-span (more than 10 years)?

YES → You are a **Long-lived Infrastructure Provider**

NO

Do you supply to at least one organisation which would answer yes to at least one of the above questions?

YES → Rerun this flowcharts for all such organisations you supply for. You also identify as the personas that these organisations identify as.

NO

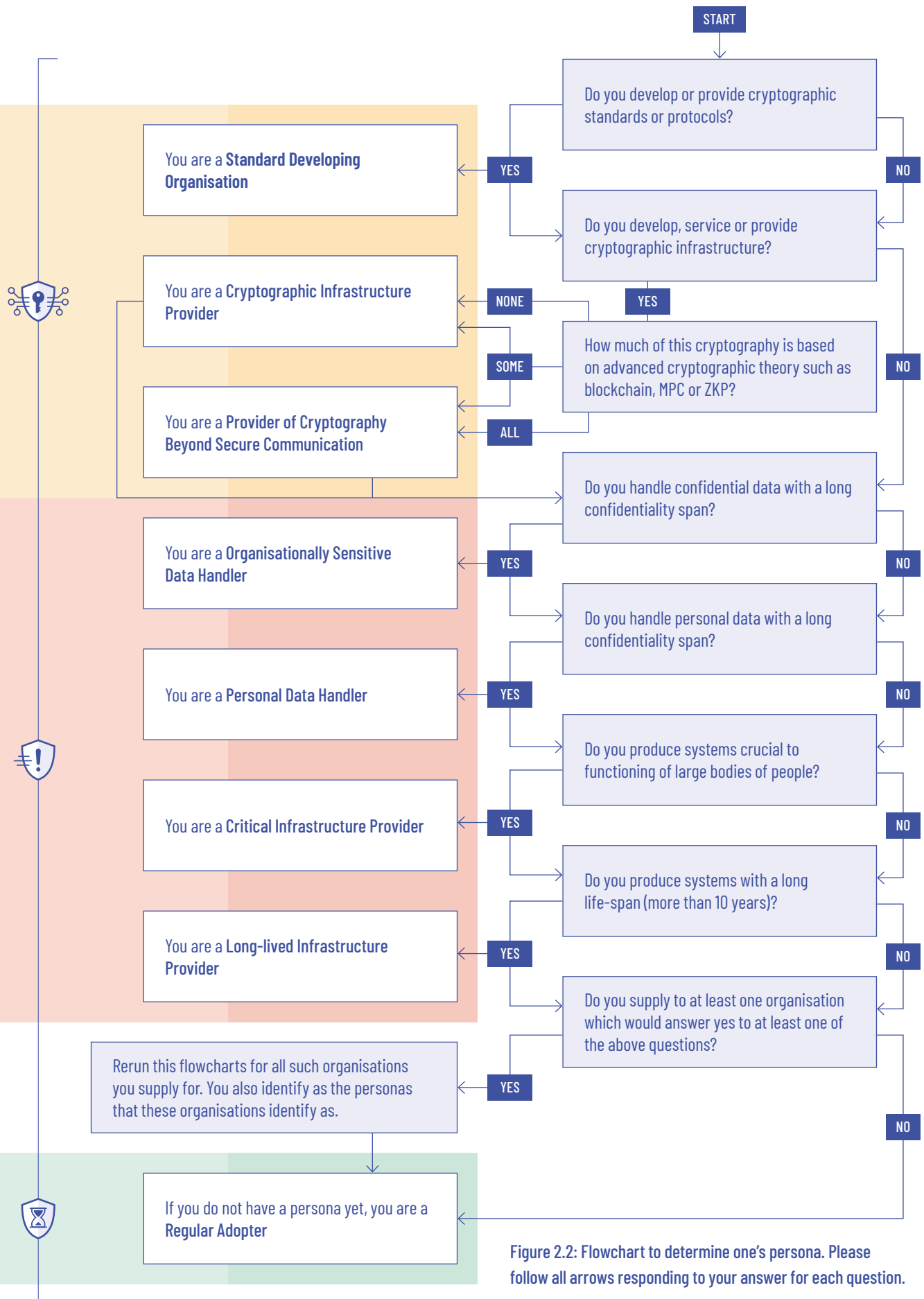If you do not have a persona yet, you are a **Regular Adopter**

Figure 2.2: Flowchart to determine one's persona. Please follow all arrows responding to your answer for each question.

Interoperability During PQC Migration

PQC migration is often not a process that can be executed by individual organisations because of dependencies between different organisations. This dependency can happen both at an organisational as well as a technical level. In order to maintain interoperability between different organisations, coordination between these organisations during PQC migration is required.

This can happen in a variety of ways. If an organisation A depends linearly on an organisation B, organisation B needs to migrate to PQC standards before organisation A can do so. Often times such dependencies between organisation are not so linear but happens in the form of a certain network structure. If this is the case, all the organisations involved in this network structure should coordinate their PQC migration to ensure both interoperability as well as security of their data and systems. If this is the case, organisations should take into account all the PQC personas of the respective organisations when performing PQC migration.

2.2 〉 PQC Diagnosis

Now that you identify as a persona, you can determine if you should proceed with the migration, starting with performing the PQC diagnosis.

Urgent Adopters

Organisations identified as urgent adopters should start their PQC diagnosis as soon as possible to ensure migration happens as soon as possible. The rest of this document is mainly intended to guide such organisations through the migration process.

Regular Adopters

Organisations identified as regular adopters do not need to react to the quantum threat yet. However, these organisations should make sure that they are in the best condition to migrate later. The following recommendations apply.

First, these organisations should make sure they are up-to-date with the latest security guidelines (for instance migrate from TLS 1.2 to TLS 1.3) and favour crypto-agile solutions. For more information about crypto-agility, please see the 'Cryptographic Agility' paragraph in Section 4.1. They can also anticipate the fact that future updates will have an impact on the performance of cryptographic algorithms. These organisations can also start doing the risk-assessment and diagnosis steps of the migration plan described in Section 2.2.1.

Second, these organisations should stay well-informed and follow the standardisation efforts. Within 5 to 10 years after the publication of the post-quantum standards, new recommendations specifically dedicated to these organisations will be announced, taking into account the developments and lessons learned from early adopters.

Finally, some organisations identified as regular adopters may want to act proactively and go further in applying the migration plan described in this manual, in particular starting with the PQC diagnosis. There are various reasons for doing this, some of which are: your organisation is about to make large infrastructure investments; your organisation changes its activity or your organisation has new clients, which changes the risk assessment. Either way, these steps will have to be taken at some point, so it is never completely useless to initiate the first migration steps now.

Cryptography Experts

Organisations identified as cryptography experts should also start applying the migration recommendations to their own infrastructure. Moreover, as suppliers of cryptographic assets, all other actors of the supply-chain rely on them. Therefore, they should be ready to start implementing quantum-safe algorithms as soon as the standards are available.

In order to facilitate planning the migration for organisations they are supplying to, cryptography experts should communicate clearly to their clients. For each of their products, they should state whether it resists quantum attacks. If it is not the case, they should propose quantum-safe alternative solutions. They should provide clear timelines for when they intend to offer such solutions.

Concerning Providers of Cryptography Beyond Secure Communication, we highlight that some widely used advanced cryptographic protocols are not quantum-safe.

2.2.1 Running the PQC Diagnosis

Having decided to start PQC migration, the first step consists of making a diagnosis of the current situation of your organisation with respect to cybersecurity. This step aims at gathering the necessary data to decide which assets should be migrated first, identify the dependencies and anticipate the consequences of the migration.

In general, the knowledge of the following information is a prerequisite to the establishment of a suitable migration plan in the next chapter:

- Risk assessment;
- Inventory of all cryptographic assets used in the organisation;
- Inventory of all the data handled by the organisation;
- Inventory of the suppliers of cryptographic assets.

Risk Assessment

Each organisation regularly assesses the risk of its IT infrastructure being subject to attacks and the potential consequences (financial, reputational, legal, etc.). The risk is assessed depending on several parameters: the value of the information, the vulnerability and the threat.

The first phase of the risk assessment consists of reassessing the risk of the current IT infrastructure in a new scenario where an adversary has access to a large scale quantum computer. The quantum threat does not affect the value of the information: the valuable assets remain the same. But it creates new vulnerabilities: some information that was protected by cryptographic algorithms considered secure in a classical model is not protected any more. Moreover, one should anticipate new threats: attackers targeting the new vulnerabilities created by this situation. Hence, the risk should be reassessed accordingly. A proper risk assessment will be vital to decide which systems should be migrated first.

Inventory of Cryptographic Assets

In order to conduct the migration, you need to identify all the cryptographic assets within your organisation , including assets that will soon enter the organisations. This is an important step to make sure that all assets are correctly migrated. If one algorithm remains that is vulnerable to a quantum attack, this could serve as en entry point for a larger attack on the entire system.

Therefore, you should aim to obtain an exhaustive list of all uses of cryptography by your organisation, both software and hardware. The information collected should be as detailed as possible, including the nature of the algorithm, key length, usage, etc. It will be used to determine whether a cryptographic asset is vulnerable to quantum attacks and which quantum-safe solution could be used instead. For assets that are not con-

trolled by your organisation, you should identify the supplier. This inventory could take the form of a Configuration Management Database (CMDB). Past cryptographic migrations have shown that creating an inventory of cryptographic assets is the most important and most difficult part of the diagnosis. Organisations should take into account that this step will take a significant amount of time.

There exist automated tools to help identify where and how cryptographic algorithms are used in your infrastructure. NIST is currently working on the development of such a tool [NN21]. Other asset discovery tools can be used, such as testssl.sh [Wet].

In addition, one should consider that such an inventory is useful outside the scope of this migration project. Indeed, having a full picture of the exact cryptographic algorithms deployed can help identify vulnerabilities in the current system. Such vulnerabilities are far from uncommon and need to be fixed. Hence, a good inventory of all cryptography at use will ease the mitigation of both quantum and non-quantum threats. This inventory can also be used to simplify compliance issues. Note that due to the continuously changing nature of cryptographic landscapes, this inventory should be continuously updated as well.

It should be noted that due to the continuously changing nature of cryptographic landscapes, this inventory should be continuously updated as well. In addition, it should be noted that such an overview is very sensitive as it contains all the vulnerabilities of an organisation. It is hence of utmost importance that it is properly secured and cannot be accessed by outsiders.

Inventory of Data Assets

In order to plan your migration, a list of the data assets handled by your organisation will help you make good decisions. More precisely, you do not need an exhaustive list of the data, but rather a list of types of data, depending on several factors:

- Kind of data (data at rest, data in transit or data in use);
- Location of the data;
- Value of the data (confidentiality, availability);
- Classification of data;
- Risk assessment for each data asset.

Inventory of Cryptographic Dependencies

For most organisations, a significant part of the cryptographic assets (hardware and software) are provided by external suppliers. Therefore, a large part of the migration consists of making sure that your suppliers are migrating and offering new quantum-safe solutions, or finding new suppliers otherwise. The goal of this inventory is to identify your cryptography supply-chain. For each supplier, you should try to list all the products that you use from them, whether you have an ongoing contract with them, and how to contact them. This list should also include certificate authorities. Besides the official suppliers of cryptographic assets, an organisation should also consider internal communication tools (instant messaging, collaborative platforms) as well as shadow IT.

Note that this also holds the other way around, if you supply solutions using cryptography. The organisations you supply to will be making a similar assessment of their dependencies and might require you to properly communicate your intentions with respect to PQC. It is not necessary to make an exhaustive list of all of your clients but keep this in mind when deciding on an appropiate strategy.

3) Migration Planning

Summary

This chapter provides a description of the action steps to help organisations with planning their post-quantum migration. It is mainly intended for organisations that identify as urgent adopters, or regular adopters who would like to act proactively.

This chapter assumes that your organisation already went through the diagnosis step described in Chapter 2. Specifically, in order to decide which assets should be migrated first, you will need the information described in Section 2.2.1 concerning the current security architecture of your organisation. Using this information, this chapter will guide you in determining two things.

The first part of this chapter is here to help you determine exactly when to migrate. In a few years, certified post-quantum cryptographic standards and libraries will be released. Some organisations can afford to wait for them to be available, while others have to start migrating today. This will influence your migration policy. The first section of this chapter provides all necessary information for you to decide which migration scenario corresponds to your organisation.

The second part of this chapter gathers advice on how to plan your migration. This is where you decide which cryptographic assets need replacement, what to replace them with and in which order you should replace them. This involves prioritising, identifying dependencies and anticipating some consequences of the migration, such as the necessity to temporarily isolate some data assets.

After carefully planning your migration, the subsequent chapter will guide you through the execution of the migration. Note that although this document describes the migration steps (diagnosing-planning-executing) sequentially, in practice an organisation should not wait to entirely complete one step before starting the next one. Organisations should start by identifying their most critical assets, planning a first migration phase for these critical parts and proceeding to this migration, while in parallel actively working on extending the diagnosis to a larger part of their infrastructure that will be migrated in a second phase.

3.1) When to Start Migrating?

3.1.1 Different Migration Scenarios

Considering that systems may need to be migrated in the short term, it is now time to decide exactly *when* to migrate. This is determined by three variables, namely the time X the asset must remain secure, the migration time Y, and the time Z left until a quantum computer will be able to break public-key cryptography. We must ensure that we migrate in time such that $X + Y < Z$, called Mosca's inequality [MP21]. The closer $X + Y$ is to Z, the more urgent the migration is. It is important to note that all of these variables are merely estimates and may not fully represent reality. They are meant as a test to understand whether it is time to migrate.

While X is something which an organisation should be able to estimate from its own business processes, the quantity Y is harder to guess. Below we give advice on how to estimate this quantity. For this, one needs to consider the journey to industry-certified implementations of NIST post-quantum cryptography standards

and its milestones. There are three suspected milestones in this journey, from which there are four different moments at which a cryptographic asset can be migrated, which can be seen in the figure below. This section aims to aid with the decision which moment should be chosen for which cryptographic asset.
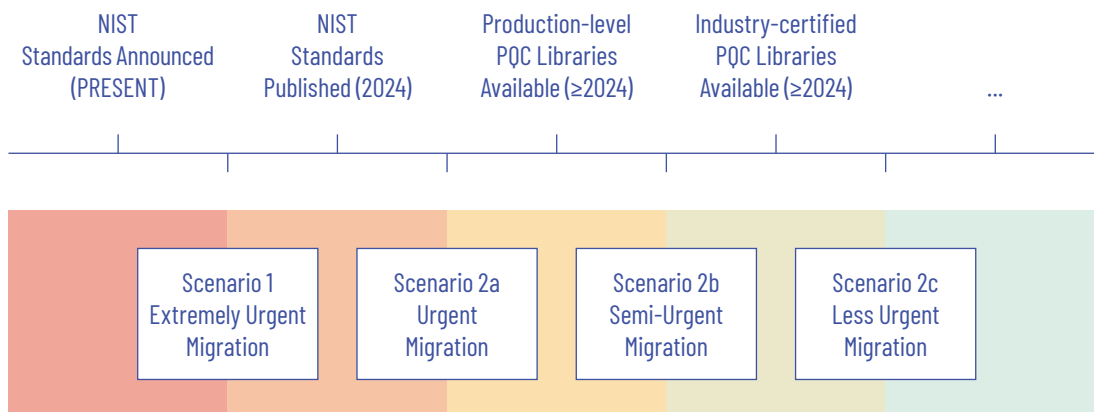

Figure 3.1: Timeline of different migration scenarios.

Hence, the total migration time $X + Y$ when migrating from Scenario i can be rephrased as $X + W_i + Y_i$, whereby

- X is the estimated time the data must remain secret;
- W_i is the estimated waiting time until the milestone associated with Scenario i;
- Y_i is the estimated time it takes to perform the migration in Scenario i.

Each asset should be migrated in Scenario i so that the migration time $X + W_i + Y_i$ is less than Z. The scenarios in Figure 3.1 also give an indication of the corresponding urgency. Note that if $X > Z$, then W_i and Y_i are irrelevant and migration needs to happen with extreme urgency.

Note that for each option, the time to actually perform the migration may vary per organisation or even per asset because, for example, library documentation, commercial support and overall knowledge of PQC will most likely be more complete the later the migration starts. Hence, it is imperative that any system, if the situation allows it, migrates to either production-level or certified implementations of NIST PQC standards. Once again, the exact timing of migration will heavily depend on the risk appetite of the organisation. We will discuss this further in the following sections.

These differentiations between options may seem like small details. However, by focusing on these details, one may ensure that important data that is core to the organisation is adequately protected. Overlooking the security of important core data can be the difference between the success and the downfall of an organisation.

Note on Certified Libraries

For some organisations it will be vital to migrate from Scenario 1, 2a or 2b, which will mean migrating to PQC standards without certified libraries being available. It should be mentioned that this brings an extra disadvantage because using uncertified libraries can lead to certification issues and using non-production-level code can lead to a slew of security problems. This disadvantage should be taken into account when choosing which Scenario to migrate from. It is important to note, however, that the current most-used standard for cryptography, FIPS 140-2, already allows for hybrid schemes. This means that it is possible to obtain at least that certification using the hybrid approach. For more information on the hybrid approach, please see the 'Hybrid solutions' paragraph in Section 4.1.

3.1.2 Step-by-Step Process

Step 1: Estimating W_i and Y_i and Z

Estimating W_i and Y_i. Naturally, it is difficult to determine when production-level and/or industry-certified PQC libraries are available for general use. This is especially true due to the fact that different PQC libraries will be aimed at optimising the algorithms for different use cases, such as smartcards or IoT devices. Hence, using experience of similar situations is a useful way of determining this timeframe.

Furthermore, end-users can have an influence on these timelines. This is the period when vendors should start developing production-level libraries. Contacting these vendors or making the desire for these librar-ies clear on the community feedback or online forums can influence how quick or slowly the libraries are published.

Estimating Z. Estimating when a quantum computer has the capabilities to break public-key cryptography is difficult and still being debated between experts. To simplify this process, Figure 3.2 shows the expert opinions on the probability that a quantum computer will break RSA-2048 in 5, 10, 15, 20 and 30 years [MP21]. From this figure, a conservative estimate is that quantum computers will break public-key cryptography in 2040, while a less conservative one fears that it already happens in 2030. Note however that at the time of publication, this research study is almost two years old. New research studies with new estimates on Z are likely to be released in the coming years.
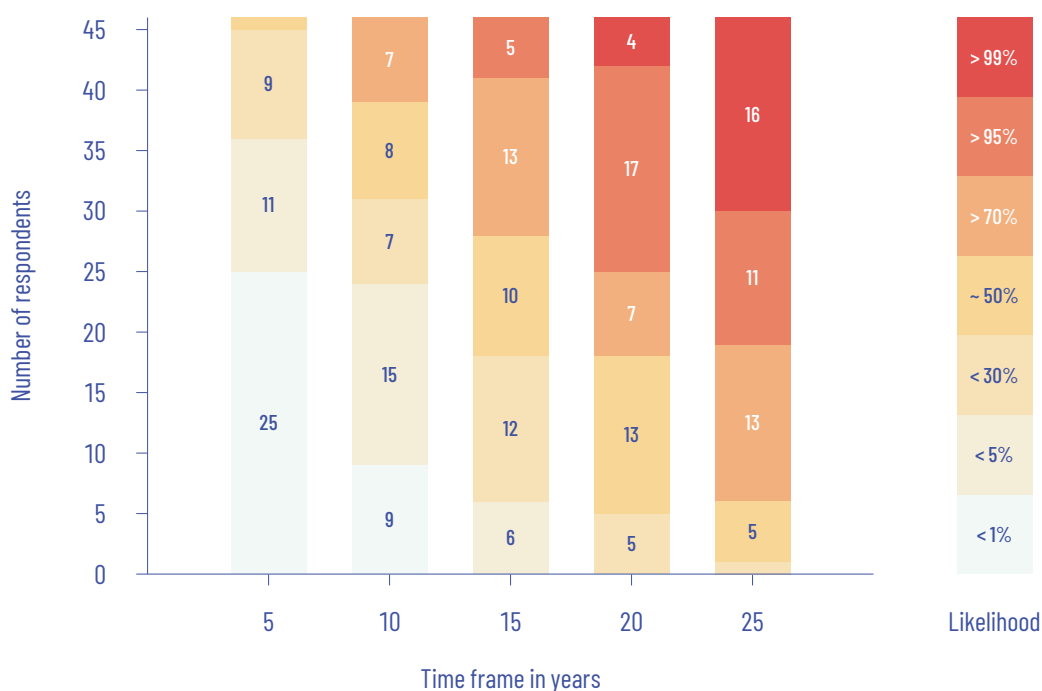
Figure 3.2: Expert opinions on breaking RSA-2048 with a quantum computer from [MP21].

Step 2: Determining Your Migration Scenario

Once a rough sketch of the timeline for each milestone has been drafted, it can be decided for each asset in which Scenario it should migrate using the following decision tree:
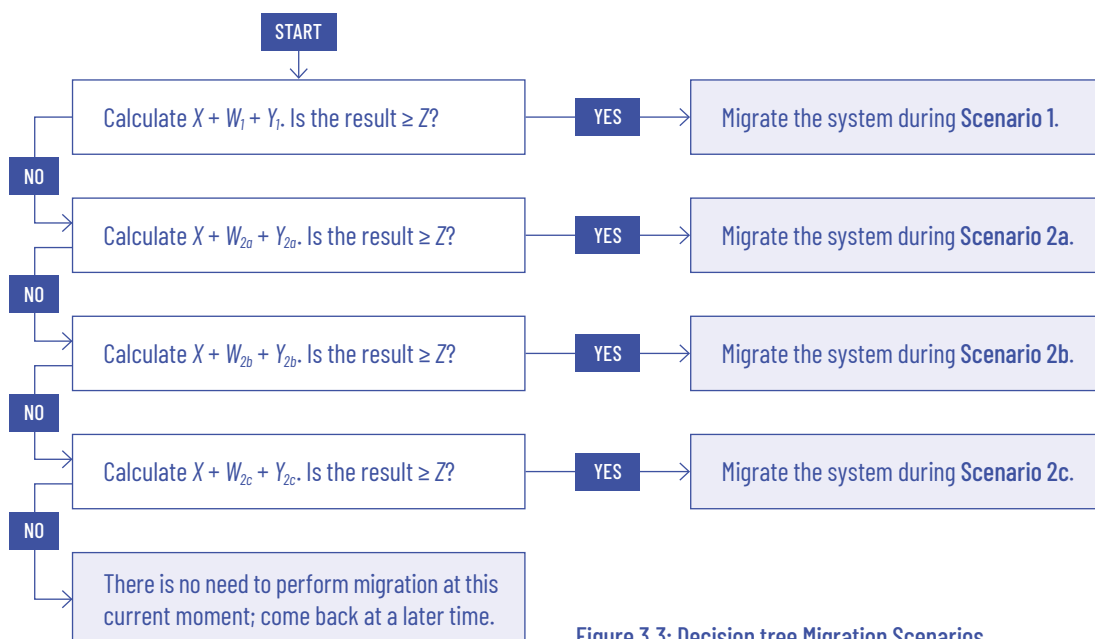
Figure 3.3: Decision tree Migration Scenarios.

In Chapter 4, advice on how to migrate asymmetric primitives will be provided depending on your scenario. Note that in the rest of the document scenarios 2a, 2b and 2c are clumped together under the name Scenario 2. This is because, at a high-level, the advice for all three are the same. Note however that this advice may change once the milestones above are achieved.

Step 3: General Strategy

As it is impossible to migrate everything at once, a general strategy is required. It is recommended to migrate outdated protocols to protocols that are currently recommended by the NCSC first. This will test the asset management and the overall agility of both the cryptography and the organisation at a whole. Only once this is done is it recommended to begin the migration to PQC. This way, an organisation can already start modernising its migration process to smoothen the eventual transition.

3.2) Advice on Migration Planning

The second part of this chapter gathers advice on how to plan your migration. The main goal of this step is twofold.

1. For each cryptographic asset, decide if it needs to be replaced, and if so, identify what it should be replaced with.
2. Decide the order in which the different cryptographic assets should be migrated.

This section provides useful resources to help you decide which cryptographic elements should be replaced and suggest solutions to replace them with (see Chapter 4). The prioritisation depends on your risk assessment established in the previous chapter, but should also take into account the dependencies and the consequences of the migration for your business.

3.2.1 Business Process Planning

As a considerate part of migration considers business processes, it is important that the planning phase focuses on this. First, a migration manager should be appointed, who will be responsible for the execution of the migration. This should be someone with knowledge of the overall organisation and access to all parts of the organisation so that they can instruct all the necessary employees within the company on the steps they have to take for migration and when. Second, sufficient budget should be allocated to the necessary migration steps, such as time, finance and facilities. Lastly, during the process of migration, there will be moments when certain services and parts of the organisation will have to be isolated and shut down. The management of this "down time" should be carefully considered and planned beforehand to minimise the effect on the continuity of the organisation.

An appropriate planning takes into account the migration paths of other organisation to maintain interoperability as well. For this reason, it is wise to **consider planning the migration together with a community of similar organisations**. In some cases this might even be necessary because of cryptographic systems and assets between organisations being interrelated. Even if this is not the case, performing a migration planning together can still be beneficial because the workload of planning the migration can be divided.

We refer the reader to the technical report [ETS20] written by ETSI for more advice on the business process planning.

Costs

While the exact costs of a migration to PQC are hard to estimate, it is certain that this will be a very costly process that requires proper planning and budgeting.

In terms of human resources, a team will need to be set up, which should include a migration manager, and 5-10 other people depending on the size of the organisation. This team needs to begin with creating an overview of the cryptography that is in place in an organisation, prioritise the assets that need to be replaced first and draw up a plan for the migration of those assets. Depending on what is already in place and the size of the organisation, this process might take up to two years [ETS20].

Furthermore, appliances might need to be replaced in case they can not support PQC or if the vendor is not planning to include PQC. Additionally, PQC algorithms often require more computational steps, for which the currently used cryptographic hardware might not be sufficient. If it turns out that the current hardware is not sufficient anymore, this also needs to be replaced.

Lastly, potential costs can be incurred due to the risks related to the migration. As mentioned in the introduction, migrating too soon as well as too late brings risks, which could result in additional costs. In addition, there is a risk that current vendors do not migrate to PQC standards soon enough. In this case, additional costs will be incurred as well. Both of these potential costs should be taken into account as well.

3.2.2 Technical Planning

The technical part of the planning should focus on aspects such as which cryptography should be migrated, when it should be migrated and which methods should be used.

Dependency of Assets

An important goal of this planning is to identify the dependencies between the different cryptographic assets and decide the order of the migration. If an asset A depends on an asset B, decide whether A or B should be migrated first. Such dependencies should be clear from the inventory. To maintain interoperability between the assets during the migration, the post-quantum protocol can be made optional at first, until all the related assets have been migrated.

Cryptography Replacement

With the cryptographic inventory established and the dependency of cryptographic assets sorted out, the actual planning of replacing cryptographic assets can start. For each cryptographic asset it should first be decided whether it should be replaced, redesigned, retired or something else. This decision depends on different factors, such as importance of the asset to the organisation, consequences of misfunctioning of the asset, risk of the asset being attacked, but also available resources. Once it is decided that an asset needs to be replaced or redesigned, the next step is to decide which quantum-safe solution needs to be used. Chapter 4 suggests replacement solutions depending on the cryptographic asset and its use case. We advise to use a cryptographic solution which is crypto-agile, so that the implementation can quickly be updated once later standards or rules comes out. For more information on crypto-agility, see the 'Cryptographic Agility' paragraph in Section 4.1.

It is important that cryptographic assets are protected during migration as well. This can be done in several ways. The easiest way is by keeping the classic cryptographic protection on the asset until after the asset is protected with the new quantum-safe solution. If this is not an option, asset isolation is the alternative.

Asset Isolation

In some cases, data/system isolation is the only way to completely protect an asset. This is particularly true for personal data and organisationally sensitive data handlers. There are different cases for when asset isolation is advised or even necessary. Firstly, data isolation brings protection against the so-called store-now-decrypt-later attacks. By physically separating this data from the network, the risk of such an attack can be taken away. This mainly holds for data in transit as these attacks are performed by listening in on a communication channel. Data at rest is less vulnerable to store-now-decrypt-later attacks.

Another situation when asset isolation is useful, is when it is not an option to keep asset protected during migration as mentioned in the previous paragraph. As migration is an involved process, it might not be possible to update all systems at the same time. Because of this, it may be necessary for some systems or data to remove their current cryptographic protection before the quantum-safe protection can be applied. Alternatively, it might be that it is currently too expensive to migrate certain assets, but you still wish to keep them protected. In either case, isolating the asset for the time that the asset is vulnerable makes sure that it keeps the required protection. After the required migration steps have taken place, the asset can then again be taken out of isolation.

However, it should be mentioned that asset isolation has a huge impact on functionality and availability of the data. As long as the asset is isolated, the asset cannot be used at all. This is an important aspect which should be taken into account when choosing to isolate an asset. In some scenarios asset isolation is not even an option because of this restriction.

Hardware Replacement

The migration may necessitate to replace hardware devices. In case of large-scale hardware replacement, the availability of the new product and the deployment time should be taken into account in the planning of the migration.

Testing

New solutions on both the hardware and software level will necessitate a phase of testing. The testing part is very important and should be anticipated. The tests should make sure that the new algorithms are compatible with the rest of the infrastructure and indeed provide the promised security.

4 〉 Execution

Summary

This chapter aims to give more information and guidelines on how to execute the migration. It will provide guidelines on migrating insecure cryptography and protocols. These guidelines provide both high-level and lower-level steps to successfully migrate to a quantum-safe environment. Many steps are conditional on when the organisation will actually perform the migration, which means it is recommended to first determine your migration scenario in the previous chapter. Furthermore, it is important to start working on the cryptographic agility of the assets already. The main recommendation for almost all protocols is to utilise a hybrid approach.

4.1 〉 General Strategies

The description of the last stage of the migration is high-level for now. The reader should keep in mind that the migration is a long process. Several institutions are currently working on detailed guidelines for this stage. More detailed information will be available in a few years. This should not prevent you from starting the first stages of the migration.

The final stage of the migration is the execution of the plan devised in the previous chapter. Ideally, at this point a complete overview of cryptographic assets is available, and a plan has been made outlining which PQC alternatives the vulnerable assets need to be migrated to. Alternatively, an organisation might opt to already start migrating high priority assets before the complete plan is finished and perform the final stage in parallel to the other stages. Be aware that IT environments are constantly changing. An asset inventory made two years ago will most likely not represent the current cryptographic landscape of an organisation. Therefore, it is important to continuously keep this asset inventory up to date.

The first section in this chapter gives some general strategies which can be applied in the PQC migration. The following two sections discuss in detail how to migrate cryptographic primitives and protocols.

Warning | The application of the migration plan should be performed with great care. Indeed, the replacement of certain cryptographic assets by others could introduce new vulnerabilities. An incorrect choice of replacement algorithm or an error in the new configuration could decrease the security level. In addition, the migration phase in itself increases the attack surface. Even if an organisation outsources this task, it is required to maintain a certain level of understanding of post-quantum cryptography internally, so as to understand the different trade-offs offered by each replacement solution. It is also important to acknowledge that post-quantum asymmetric cryptography is less mature than classical asymmetric cryptography and still requires years of thorough cryptanalytical work to achieve the same level of confidence. Still, this should not be an argument to postpone the migration. Hybrid schemes allow for a security at least as good as the security level of the classical algorithm used , which strictly reduces the threat of quantum computers.

Cryptographic Agility

For all assets that an organisation is managing itself, it is important to start working on making the assets *crypto-agile*.

The term *crypto-agile* refers to the practice of implementing cryptographic protocols, products and systems in such a way that the cryptographic algorithms involved can be changed with minimal effort and without requiring to make significant changes to the rest of the architecture. Note that this is not simply something an organisation can buy, but something that requires structuring people, processes and technology. Properly adopting crypto-agility makes swapping out cryptographic systems much easier once new best practices or standards arise.

As post-quantum cryptography is still relatively young, the associated parameters might vary and new vulnerabilities will be unveiled over time. These new insight will require protocol parameters to be changed while different protocols will be standardised and adopted by different organisations. It is important to already start preparing an organisation for this by ensuring that parameters and protocols can quickly be swapped with minimal effort of the organisation. Especially when choosing to partially migrate certain assets *before* actual standards and validated implementations are available, an organisation needs to be prepared to easily switch the cryptographic algorithms once the relevant standards are available or a new implementation is recommended. This is different from current classical cryptography where standards and good parameter choices are well established. As PQC will demand more capacity from hardware, it is important to assess whether the current hardware is suitable to run PQC. If this is not the case, it is important to start thinking about alternatives already. More information on the requirements for various PQC alternatives can be found in Chapter 5. Some concrete tasks that need to be done in order to improve cryptographic agility is to enforce the use of cryptographic agility for new or updated systems and incorporate crypto-agility scans in continuous integration/continuous delivery (CI/CD) solutions. To make new systems or systems that are updated inherently crypto-agile, it is advised to abstract the cryptography from the actual code as much as possible. This might for example entail using abstract calls to (high-level) libraries or cloud services to perform cryptographic operations and/or external key management [Saf21]. By enforcing these principles, eventual migration of these systems becomes much easier. For more information about these tasks towards cryptographic agility, it is advised to read the white paper of Cryptosense [Cry21]. They are also working on tools to help automate parts of these tasks.

Migration of Primitives vs. Protocols

Before discussing the migration of either primitives or protocols, there are important differences to be made clear. Cryptographic primitives generally do not live in isolation, but are used as a single piece in a larger protocol. This means that most organisations do not actually ever directly interact with purely the intimate details of cryptographic algorithms. Rather, they interact and use libraries that implement commonly used protocols that use cryptography, such as TLS. Various cryptographic choices can be made through these libraries, such as which primitives or key-sizes to use, but it is normally not the organisation's responsibility to implement their own cryptographic algorithms in libraries.

Generally, directly migrating primitives rather than protocols is reserved for the rare cases that an organisation is directly interacting with purely cryptographic libraries and potentially implementing their own protocols. The first part of Chapter 5 provides a list of the main classical primitives, their main characteristics and whether or not they provide quantum security. This chapter also presents the main post-quantum primitives.

Migration of symmetric cryptography & hash functions

A quantum computer will be able to reduce the level of security of classical symmetric-key cryptography or hash functions. For symmetric-key encryption, this means that a message might be decrypted by someone who is not supposed to not know the secret key, compromising the confidentiality of the message. Hash functions are typically used as a building block in systems that protect integrity. Migrating symmetric cryp-

tography to post-quantum standards typically involves increasing the key length of the used algorithm to guarantee a sufficient level of security. This needs to be done now for documents that are encrypted using symmetric-key encryption and need to remain confidential for a longer period, to avoid store-now-decrypt-later attacks. Hash functions are not prone to these store-now-decrypt later attacks.

Another category that needs to be investigated are long-lived systems that rely on symmetric cryptography or hash functions such as SIM cards, satellites or operational technology. Long-lived systems can be hard or impossible to update in the future and should be updated with algorithms using longer symmetric-keys or larger hash outputs. An organisation should be prepared for the fact that longer key sizes will lead to larger storage requirements and slower algorithms.

Migration of Asymmetric Cryptography Using Hybrid Solutions

A quantum computer will be able to break classical asymmetric-key cryptography and therefore all the guarantees given by protocols that depend on these algorithms. Similar to symmetric-key cryptography, the main concerns that need to be addressed now are the confidentiality of data that need to remain confidential for a long period and the security of long-lived systems.

Hybrid Solutions

Hybrid solutions denotes the use of both classical and post-quantum cryptography together in parallel within one single protocol. To break the scheme, an adversary would need to break both the classical and the post-quantum algorithm. Hence, the security of the complete scheme is at least as good as the security of each algorithm separately.

This aims at mitigating the security risks induced by the relative lack of maturity of the new post-quantum algorithms, as well as having the added security of the post-quantum algorithm.

Hybrid is particularly recommended for organisations that need to deploy quantum-safe cryptography before reference implementations of the new standardised algorithms become available, for instance if your data is prone to store-now-decrypt-later attacks today already. The main drawback of this technique is that it can induce an overhead (in time and/or memory) as now two cryptographic algorithms need to be executed for a single encryption or signature. But as most post-quantum schemes already induce relatively more costs compared to classical cryptography, this additional cost should be reasonable.

Warning | When you encounter products claiming to use hybrid encryption or signature, make sure that this corresponds to the above description, that is, using classical AND post-quantum algorithms at the same time for the encryption or signature. This is not to be mistaken with having a choice between using classical OR post-quantum algorithm for encryption (see below).

Downgrade Attacks

Some hybrid approaches face the risk of downgrade attacks. This happens when a system implements *hybrid OR* instead of hybrid AND explained above. Hybrid OR, or equivalently optional *post-quantum* describes a situations where both the classical and the post-quantum algorithm are implemented on the server. However, to communicate with the server, a client can choose to use the classical or the quantum-safe protocol and is not forced to use both. Such a configuration is benefical for backwards compatibility. This backwards compatibility is very convenient during the testing and early development phase to provide interoperability. Such solutions present an important risk: an adversary can pretend not to support post-quantum protocols and hence force the server to communicate using the classical algorithm. This is known as a *downgrade attack*. Even if the malicious actor cannot break the classical primitive used, it can still perform store-now-decrypt-later attacks.

Therefore, it is generally recommended that internal systems use hybrid in the hybrid AND form described above. However, for externally facing systems this can be more cumbersome and hybrid OR might be the only option. Policies and strategies need to be formed for when and how such systems can use hybrid schemes correctly.

Migration of Assymetric Cryptography Using Pre-shared Keys

Another way to make asymmetric cryptography quantum-safe is by using classical symmetric cryptography with pre-shared keys. This method aims to establish communication without any form of public-key cryptography. To use this method, pre-shared keys need to be established in a physical way, such as via USB. Because of this, establishing such keys is usually quite a cumbersome process and it in particular makes this solution scale poorly in many-to-many infrastructures. Moreover, since public-key cryptography is avoided, validating certificates is not possible. However, once such pre-shared keys are established, this is a very high-security and efficient approach.

It is therefore recommended to use the hybrid approach, unless the system satisfies *all* of the following requirements:

1. The system needs to be migrated from Scenario 1.
2. The system is within the full control of the organisation and is completely trusted.
3. The system will only communicate with equally trusted and fully controlled systems.
4. There is a practical way of sharing the secret keys between the communication systems.
5. The networks in which these communicating systems exist are very confidential and its layout does not frequently change.
6. Adding nodes to or removing nodes from these networks is not done frequently and is not practical.

Examples of protocols for which using pre-shared keys is an option are TLS and IPSec.

4.2 〉 Migrating Primitives

This section is aimed at library developers and security architects and gives an overview of common classical and post-quantum cryptography. For each functionality for which cryptography is used, we list primitives which are recommended or acceptable, and which primitives should not be used. Because of the intended public and the information to be discussed, a certain basic knowledge of cryptography is assumed in this section.

Whilst there is a recommended choice for each functionality, we list acceptable alternatives as well to allow flexibility. This is mainly done because there is a wide variety of use cases for which a certain functionality can be used. It will also aid in understanding which primitives should not be used.

An overview of all recommended, acceptable and not-to-use cryptography can be found in Table 4.1. A detailed description of each primitive can be found in Chapter 5. The rest of this section gives further information on each of the above functionalities. In addition, it gives information on which primitive is recommended depending on which scenario is being migrated from.

Post-quantum primtives can be configured to have security levels between 1 (lowest security) and 5 (highest security). The trade-off is that the higher the security level, the worse the performance. It is **strongly recommended that all post-quantum primitives have at least security level 3 and above**. Security level 1 and 2 are acceptable.

Type	Functionality	Recommended	Acceptable	Do not use
Symmetric	*Block Cipher*	AES-256	Camellia-256	AES-128, AES-192 (T)DES, IDEA, and Blowfish
Symmetric	*Stream Cipher*	ChaCha20 with 256-bit key	-	RC4
Asymmetric (All scenarios)	*Public-Key Encryption/KEMs*	CRYSTALS-KYBER	Classic McEliece, FrodoKEM	Any classical PKC
Asymmetric (Scenario 1 with Stateful Hash-based Signatures)	*Digital Signatures*	XMSS, XMSS^{MT} LMS, HSS	Any NIST (Draft) Standards	Any classical PKC
Asymmetric (Scenario 1 without Stateful Hash-based Signatures)	*Digital Signatures*	Any NIST (Draft) Standards	-	Any classical PKC
Asymmetric (Scenario 2)	*Digital Signatures*	Any NIST (Draft) Standards	XMSS, XMSS^{MT} LMS, HSS	Any classical PKC
Hash Functions	*Hashing*	At least SHA-3-256 or SHA-256	BLAKE2, SHAKE256	SHA1, MD5, SHAKE128, SHA-3-224, SHA-224
MACs	*Block Cipher Construction*	CMAC-AES-256	CMAC-Camellia	CBC-MAC
MACs	*Hash Constructions*	HMAC with at least SHA-256 or SHA-3-256	BLAKE2-MAC	HMAC-MD5
MACs	*Universal Hashing*	Poly1305-AES, ChaCha20-Poly	-	-

Table 4.1: Recommended, Acceptable and Do not use Cryptographic Primitives per functionality.

4.2.1 Symmetric Cryptography

Symmetric Cryptography Migration

Scenario 1 and 2 | For symmetric cryptography, the recommended, acceptable and do not use options are the same for all migration scenarios. These can be found in Table 4.1.

It is important to note that AES is the recommended choice due to it being standardised by NIST and well-established. Camillia is standardised in various protocols such as TLS 1.2 [KK10], IPSec [AMK05] and S/MIME [Mor04], which is why it is also considered an acceptable choice. Furthermore, note that key lengths less than 256 bits should not be used.

It is important to note that organisations that deal with many legacy systems, such as banks, will probably find that TDES is frequently used in their systems. Due to its small block and key sizes, TDES will be completely deprecated by the time a quantum computer is large enough to break public-key cryptography.

4.2.2 Assymetric Cryptography: Public-key Encryption and Key Encapsulation Mechanisms

PKE and KEM Migration

Scenario 1 and 2 │ For public-key Encryption and Key Encapsulation Mechanisms, the recommended, acceptable and do not use options are the same for all migration scenarios. These can be found in Table 4.1.

There are no classical primitives for these two functionalities which are quantum-safe. That is why the only recommended and acceptable primitives are the ones offering quantum security. Again, it should be noted that none of these schemes are standardised or tested as well as their classical counterparts. For more information on these PQC primitives, please see Section 5.3.

4.2.3 Asymmetric Cryptography: Digital Signatures

Digital Signature Migration

Stateful hash-based signatures (HBS) schemes are signature schemes that can only produce a fixed amount of signatures, and whose hardness depends on a certain hash function. Because of the fixed amount of signatures, careful state management of the used keys is essential. Since stateful hash-based signatures are not intended for general use, it is important to make a clear distinction between the systems that should and those that should not implement these signatures. Hence, choose **Scenario 1** with stateful hash-based signatures if and only if the system that is currently being migrated conforms to all of the following require-ments [SP 20]:

1. You have identified your migration scenario as 1;
2. The implementation of stateful hash-based signatures would have a long lifetime;
3. Further transitioning to a different signature scheme in the near future would not be practical;
4. You are able to effectively and correctly keep track of one time public/private key pairs that have been used (and hence, manage the state);
5. The system will only need to sign an limited number of messages.

This is because stateful hash based-signatures require very careful state management which limits general applicability.
If the system does not conform to the aforementioned requirements, choose **Scenario 1** without stateful hash-based signatures.

Asymmetric Cryptography: Scenario 1

Scenario 1: HBS │ For asymmetric cryptography, Table 4.1 shows the recommendation for systems with Scenario 1 with HBSs. The reason for these choices is that Classic McEliece is a conservative and thoroughly studied algorithm, despite its downside of large key sizes. It is also a finalist in the NIST Round 4 standardi-sation process. Furthermore, FrodoKEM is also an acceptable alternative as a more conservative choice with regards to security. Note that FrodoKEM will not be standardised by NIST.

Scenario 1: non-HBS | For asymmetric cryptography, Table 4.1 shows the recommendation for systems with Scenario 1. Naturally, when NIST announces their standards and appropriate production-level or certified implementations are available, it is important to switch to the new standards.

Asymmetric Cryptography: Scenario 2

For Scenario 2, it is strongly recommended to wait for the NIST PQC Standards. Note that HBSs are also an acceptable choice here. It is, once again, important to note that it is important to fully understand the implications of utilising HBSs before deciding on them. The list of primitives can be found in Table 4.1.

Due to the number of choices when selecting which asymmetric primitive to use, it is also important to consider use cases along with each primitive's pros and cons. These can be found in Chapter 5.

4.2.4 Hash Functions

Hash Functions Migration

Scenario 1 and 2 | For hash functions, the recommended, acceptable and do not use options are the same for all migration scenarios. These can be found in Table 4.1.

The reason why the SHA family is chosen ahead of BLAKE2 is due to its NIST standardisation.

4.2.5 MACs

MAC Migration

Scenario 1 and 2 | For MACs, the recommended, acceptable and do not use options are the same for all migration scenarios. These can be found in Table 4.1.

The reason why CMAC-AES-256 was chosen instead of CMAC-Camellia is due to AES being standardised by NIST. Furthermore, HMAC is standardised by NIST and can be paired with other standardised hashes, unlike BLAKE2-MAC. We therefore recommend HMAC. These can be found in Table 4.1.

4.3) Migrating Protocols

This section discusses how to migrate protocols to a quantum-safe version. Different commonly-used protocols are discussed, and for each protocol at least one solution to migrate to PQC is listed. For each of these solutions, action steps are listed for both system administrators, library developers and personnel responsible for security policies in the organisation. Note that this is still quite high-level, but already gives advice to some of the relevant parties.

It should be noted that only very common protocols are presented in this section, namely TLS, SSH, S/MIME, PGP, IPSec and X.509.

Many of these aforementioned protocols are defined in a type of document called an RFC (Request for Comments). These are standardisation documents that are produced by the Internet Engineering Task Force (IETF). Draft standards are called Internet-Drafts.

TLS

Descripton | Ensures the confidentiality, authenticity and integrity of communication over the Internet [Res18].

Current Version | TLS 1.3 [Res18]

Standardisation Documents | RFC 8446 [Res18].

Common Usage | TLS is used in a variety of domains such as HTTPS and secure email.

To migrate TLS to PQC, there are two options: using pre-shared keys (Option 1) and the hybrid approach (Option 2).

Note to System Administrators | For any scenario or option, it is recommended to use TLS 1.3. Furthermore, ensure that either **AES-256-GCM** or **ChaCha20-Poly1305** are included in the chosen cipher suites for the Authenticated Encryption with Associated Data ciphers.

TLS Option 1: Pre-shared Keys

Necessary Policies | Whilst the policies may vary from use case to use case, a strict policy for sharing these symmetric keys must be established to prevent malicious actors from obtaining them and to prevent them from being accidentally shared to the wrong system. Furthermore, a policy that clearly defines which systems use TLS with pre-shared keys must also be established. Lastly, key management policies must be updated to reflect the introduction of these pre-shared keys.
Pre-shared keys should be at least 256-bit to prevent store-now-decrypt-later attacks. However, a lower bit key can also be acceptable taking into consideration how long the information needs to remain confidential, as previously discussed.
Lastly, a clear policy stating when and how to perform the shift from pre-shared keys to either a hybrid or fully post-quantum is required.

System Administrators | Naturally, the system administrator must configure TLS to utilise pre-shared keys. This information can be found in the TLS vendor's documentation and if the TLS implementation does not support pre shared keys, contact the TLS vendor.

Library Developers | A detailed technical overview of implementing hybrid capabilities into TLS is defined in RFC 4279 [ET05] and RFC 5487 [Bad09]. Library developers should ensure that their TLS implementation conforms to these standards.

TLS Option 2: Hybrid Approach

An Internet-Draft indicating on how to perform hybrid key-exchange is a helpful tool to understand how the hybrid solution can be implemented in TLS [SFG22].

Necessary Policies | A discussion with the system administrator and if necessary, cryptographic experts, about the allowed cipher suites that can be used to ensure quantum-safety. It may not be required to ensure that all systems are quantum-safe as per the previous explanations on store-now-decrypt-later attacks, so defining which systems would use this altered TLS is imperative.
This is especially important as the RFC is currently in draft and is bound to be updated, which means that the policies need to reflect these changes. Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | The system administrator must configure the TLS to utilise this hybrid approach. This information can be found in the TLS vendor's documentation and if the TLS implementation does not support this RFC, consider changing TLS vendor or contact the TLS vendor.

Library Developers | Library developers can implement this experimental feature based on the RFC. Naturally, more revisions of this draft will be published, so it is expected that implementations will change over time.

SSH

Descripton | Allows parties to perform secure remote network services.

Current Version | SSH-2 [LY06c].

Standardisation Documents | RFC 8446 [LY06c].

Common Usage | One of the most common usages is using SSH to remotely login and remote command execution.

Since the SSH protocol does not accept pre-shared keys, all scenarios should consider the hybrid approach. An Internet-Draft on hybrid key-exchange shows how hybrid SSH can be implemented [KSF+20].

Necessary Policies | A discussion with system administrator and if necessary, cryptographic experts, about the allowed ciphers that can be used to ensure quantum-safety. It may not be required to ensure that all systems are quantum-safe so defining which systems would use this altered SSH is imperative. This is especially important as the RFC is currently in draft and is bound to be updated, which means that the policies need to reflect these changes.
Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | The system administrator must configure SSH to utilise this hybrid approach. This information can be found in the SSH vendor's documentation and if the TLS implementation does not support this RFC, consider changing SSH vendor or contact the SSH vendor.

Library Developers | Library developers can implement this feature based on the RFC. Naturally, more revisions of this draft will be published, so it is expected that implementations will change over time.

S/MIME

Descripton | S/MIME provides confidentiality and authentication to MIME data (audio, pictures...).

Current Version | S/MIMEv4 [Hou02].

Standardisation Documents | RFC 8551 [SRT19] and RFC 3369 [Hou02].

Common Usage | S/MIME is frequently used in secure email communication.

At this moment in time, there is little research on post-quantum S/MIME. OpenQuantumSafe offers a fork of OpenSSL that includes a quantum-safe S/MIME that either uses a hybrid approach or only uses post-quantum primitives. However, they state that their library is not meant for production environments which limits real-world usage.
Since this protocol does not accept pre-shared keys, all scenarios should consider the hybrid approach.

Necessary Policies | Probably the ideal policy to implement is to not use email to exchange information which needs to be kept confidential longer than the start of the decryption phase of store-now-then-decrypt-later attacks. Any exchange of such information should be flagged as a security incident. If the vendor implements a production-ready quantum-safe version of S/MIME, then a policy should be implemented that indicates the correct usage and transitioning to this new version.
Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | If the vendor implements a production-ready quantum-safe version of S/MIME, then the system administrator should configure this new version of S/MIME as per the established policy. Contacting the current S/MIME vendor to inquire about quantum-safety is also an option.

Library Developers | The aforementioned OpenQuantumSafe library can be used as a basis for altering the S/MIME library to be quantum-safe. This should be explicitly labelled as an experimental feature and the developer should continue to monitor for new developments in this area.

PGP

Descripton | PGP provides confidentiality and authentication to data and services for key and certificate management.

Current Version | OpenPGP [FDC+07] and GnuPGP [MJ21].

Standardisation Documents | RFC 4880 [FDC+07].

Common Usage | PGP is frequently used in secure email communication.

System Admins | Any exchange of such information should be flagged as a security incident.
Contacting the current PGP vendor to inquire about quantum-safety is also an option and the organisation should continue to look for new developments in this area.

Library Developers | Monitoring any RFC drafts and scientific literature in this area is imperative so that PGP can begin to be migrated to a quantum-safe version.

IPSec

Descripton | IPSec encrypts and authenticates IP packets between communicating parties.

Current Version | IPSec-v3 [FK11].

Standardisation Documents | RFC 6071 [FK11].

Common Usage | IPSec is frequently used in VPNs.

To migrate IPSec to quantum-safe, there are two options: using pre-shared keys (Option 1) and the hybrid approach (Option 2).

IPSec Option 1: Pre-shared Keys

Necessary Policies | Whilst the policies may vary from use case to use case, a strict policy for sharing these symmetric keys must be established. Furthermore, a policy that clearly defines which systems that use IP-Sec with pre-shared keys must also be established. Lastly, key management policies must be updated to reflect the introduction of these pre-shared keys.
It is important that the parties holding the symmetric pre-shared keys conform to the requirements that the keys must be at least 256 bits long to avoid store-now-decrypt-later attacks. However, a lower bit key can also be acceptable taking into consideration how long the information needs to remain confidential, as previously discussed. Lastly, it is important that there is a clear policy that states when and how to perform the shift from pre-shared keys to either a hybrid or fully post-quantum.

System Administrators | Naturally, the system administrator must configure IPSec to utilise pre-shared keys. This information can be found in the IPSec vendor's documentation and if the IPSec implementation does not support pre shared keys, consider changing IPSec vendor (at least for the systems' that require pre-shared keys) or contact the IPSec vendor.

Library Developers | A detailed technical overview of this process is defined in RFC 7296 [KHN+14]. Library developers should ensure that their IPSec implementation conforms to these standards. There is also an Internet-Draft that can be useful for developers to utilise pre-shared keys to achieve quantum-safety [FKMS20].

IPSec Option 2: Hybrid Approach

A helpful technical resource to achieve quantum-security in IPSec is ETSI TR 103 617 [EST18].

Necessary Policies | A discussion with the system administrator and if necessary, cryptographic experts, about the allowed cipher suites that can be used to ensure quantum-safety. It may not be required to ensure that all systems are quantum-safe as per the previous explanations on store-now-decrypt-later attacks, so defining which systems would use this altered IPSec is imperative. This is especially important as the RFC is currently in draft and is bound to be updated, which means that the policies need to reflect these changes. Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | The system administrator must configure IPSec to utilise this hybrid approach. This information can be found in the IPSec vendor's documentation and if the IPSec implementation does not support this hybrid approach, consider changing IPSec vendor (at least for the systems' that require a hybrid system) or contact the IPSec vendor.

Library Developers | Library developers can implement this feature based on the ETSI technical report [EST18]. Naturally, more revisions of this draft will be published, so it is expected that implementations will change overtime.

X.509

Descripton | X.509 proves ownership of a public-key.

Current Version | X.509v3 [X5019].

Standardisation Documents | RFC 5280 and ITU-T X.509 [X5019].

Common Usage | X.509 is frequently used to authenticate websites in HTTPS.

Since the X.509 protocol does not accept pre-shared keys, all scenarios should consider the hybrid approach. The ITU-T has already standardised hybrid (multiple-algorithms) certificates in Section 9.8 of [X5019]. It is based on the expired Internet-Draft by Truskovsky et al. [TGF+18]. There is also the issue of root CAs and CAs not accepting or issuing these kinds of certificates yet, so all of these may need to be self-signed for the time being. Naturally, more root CAs and CAs will begin to offer post-quantum certificates, so it is important to keep up to date with the market.

Necessary Policies | It may not be required to ensure that all certificates are compatible with the hybrid solution as per the previous explanations on store-now-decrypt-later attacks, so defining which systems would use this altered X.509 certificate is imperative. Furthermore, it must be noted that cryptographic and protocol libraries must then be compatible with the new certificates.
Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum. To achieve all this, communication and planning with the CA or root CA is essential.

System Administrators | The system administrator must configure X.509 certificates to be compatible with the hybrid approach.

Library Developers | Library developers can implement this experimental feature based on the RFC and the paper by Bindel et al. Naturally, more revisions of this draft will be published, so it is expected that implementations will change over time.

5 〉 Background on Primitives

Summary

The goal of this chapter it to aid library developers to select various primitives to include in their libraries and to help organisations understand which to choose and how to configure them when migrating to a quantum-safe version of a protocol. It is also intended to aid asset discovery and risk assessments. Because of the intended public and the information to be discussed, a reasonable overview of the cryptographic landscape is assumed.

For this, we provides a list of the main cryptographic primitives in use. Note that we make use of the word "primitive" in a broader sense than usual. For each primitive, we present their main characteristics and whether or not they provide quantum security.

Table 5.1 shows the list of classical primitives that are commonly used. This is not an exhaustive list, and it is imperative that any other cipher and cryptographic algorithm in use in the organisation is appropriately noted.

Symmetric	Asymmetric	Hash Functions	MAC	HBS
AES	RSA	SHA Family	HMAC Constructions	XMSS
(T)DES	ElGamal	MD5	BLAKE2-MAC	XMSS^{MT}
ChaCha20	ECDSA	BLAKE2	CMAC Constructions	LMS
Blowfish	EdDSA		CBC-MAC Constructions	HSS
RC4	ECDH		Poly1305	
Camellia				
IDEA				

Table 5.1: Commonly Used Primitives

5.1) **Classical Primitives**

5.1.1 Symmetric Ciphers

AES

Description | AES is a block cipher that is standardised by NIST [FIP01] and is the de facto standard for block ciphers.

Supported Key Lengths (bits) | 128, 192, 256.

Applications | AES is used in a wide range of both software and hardware implementations.

Further Comments | AES is the de facto standard for symmetric ciphers.

Standardisation Documents | FIPS 197 [FIP01], ISO/IEC 180330-3:2010 [ISO10b].

Quantum-secure? | Yes, if a 256-bit key is used.

(T)DES

Description | DES is a block cipher that was previously standardised by NIST as de facto standard for symmetric encryption [FIP99]. Nowadays, the Triple DES (TDES) variant is mostly used, which combines either two or three DES keys to increase the overall key length.

Supported Key Lengths (bits) | 56 (DES), 112 (TDES), 168 (TDES).

Applications | (T)DES is used in a wide range of both legacy software and hardware implementations.

Further Comments | (T)DES is common in the banking and payments industry. It is already deprecated for new systems and in 2024 for all systems.

Standardisation Documents | NIST SP 80067 Rev. 2 [SP 17], ISO/IEC 18033-3:2010 [ISO10b].

Quantum-secure? | No, the security of (T)DES is reduced to either 56 or 84-bit.

ChaCha20

Description | ChaCha20 is a stream cipher that is normally combined with Poly1305 [NL18] when used in TLS.

Supported Key Lengths (bits) | 128, 256.

Applications | ChaCha20 is used in a variety of protocols such as TLS and S/MIME (generally, in the software domain).

Further Comments | ChaCha20 is known for its speed and simplicity of implementation.

Standardisation Documents | RFC 8439 [NL18].

Quantum-secure? | Yes, if a 256-bit key is used.

Blowfish

Description | Blowfish is an older general purpose symmetric block cipher with which was released as an alternative to DES [Sch94].

Supported Key Lengths (bits) | 32-448.

Applications | Blowfish is mostly used in legacy systems.

Further Comments | Blowfish is susceptible to *birthday attacks* due to its 64-bit block size.

Standardisation Documents | Original publication [Sch94].

Quantum-secure? | Blowfish is not recommended for modern usage due to its small block sizes.

RC4

Description | RC4 is a popular stream cipher that is known for its simplicity and speed [Pop15].

Supported Key Lengths (bits) | 40-2048.

Applications | RC4 is considered insecure and hence legacy.

Further Comments | -

Standardisation Documents | Deprecated.

Quantum-secure? | RC4 is already considered insecure in a classical setting.

Camellia

Description | Camellia is a block cipher that provides similar security as AES [NTT05].

Supported Key Lengths (bits) | 128, 192, 256.

Applications | Camellia is intended to be used in a variety of settings, from low-powered systems to high throughput systems.

Further Comments | Camellia is part of the TLS 1.2 ciphersuites.

Standardisation Documents | ISO/IEC 18033-3:2010 [ISO10b], PKCS #11 [OAS20], RFC 3713 [MMN04].

Quantum-secure? | Yes, if a 256-bit key is used.

5.1.2 Asymmetric Ciphers

RSA

Description | RSA is a very popular general-use asymmetric cipher based on the difficulty of factoring a number into two primes [MKJR16].

Public-Key Sizes (bits) | ≥ 1024.

Private-Key Sizes (bits) | Approximately the size of the public key.

Ciphertext Size (bits) | At most the size of the public key.

Hardness | Integer Factorisation.

Crypto Functionality | RSA is used for key-encapsulation algorithms and digital signatures.

Applications | RSA is used in a wide range of both software and hardware domains.

Further Comments | -

Standardisation Documents | FIPS 186-4 [FIP13], NIST SP 800-56B [SP 19] rev 2, RFC 8017 [MKJR16], ANSI X9.44 [ANS17a], PKCS #1 [MKJR16], ISO/IEC 14888-2:2008 [ISO08], ISO/IEC 11770-3:2021 [ISO10a], ISO/IEC 9796-2:2010 [ISO10c], ISO/IEC 18033-2 [ISO10c].

Quantum-secure? | No, RSA is quantum-unsafe.

ElGamal

Description | ElGamal is a popular asymmetric cipher based on the the decisional Diffie Hellman problem [ISO10a].

Public-Key Sizes (bits) | At most ≈ $3p$, whereby p is the order of the chosen cyclic group G. Typically, p is at least 2048.

Private-Key Sizes (bits) | At most p.

Ciphertext Size (bits) | ≈ $2p$, hence ≥ 4098.

Hardness | Decisional Diffie Hellman.

Crypto Functionality | ElGamal is used for key-encapsulation algorithms and digital signature.

Applications | ElGamal is used in the software domain.

Further Comments | ElGamal is one of the cryptosystems available to use in GnuPGP.

Standardisation Documents | ISO/IEC 11770-3:2021 [ISO10a].

Quantum-secure? | No, ElGamal is quantum-unsafe.

ECDSA

Description | ECDSA is an elliptic curve variant of the Digital Signature Algorithm standardised by NIST [FIP13].

Public-Key Sizes (bits) | This depends on the curve used. For example, using NIST P-256P results in a 512-bit uncompressed public-key.

Private-Key Sizes (bits) | This depends on the curve used. For example, using NIST P-256P results in a 256-bit private-key.

Ciphertext Size (bits) | Double the length of the private-key.

Hardness | Discrete Logarithm.

Crypto Functionality | ECDSA is used for digital signatures.

Applications | ECDSA is used in a wide range of both software and hardware domains.

Further Comments | ECDSA is one of the de facto standards for digital signatures.

Standardisation Documents | FIPS 186-4 [FIP13], ANSI X9.63 [ANS17b], ANSI X9.142 [ANS20a], ISO/IEC 14888-3:2018 [ISO18b], SECG SEC-1 [Bro09].

Quantum-secure? | No, ECDSA is quantum-unsafe.

EdDSA

Description | EdDSA is an elliptic curve variant of the Digital Signature Algorithm standardised by NIST. In EdDSA, twisted Edwards curves are used, such as Curve25519 [JL17].

Public-Key Sizes (bits) | 512 (uncompressed).

Private-Key Sizes (bits) | 256.

Ciphertext Size (bits) | 512.

Hardness | Discrete Logarithm.

Crypto Functionality | EdDSA is used for digital signatures.

Applications | EdDSA is suitable for general use.

Further Comments | EdDSA is based on the Schnorr signatures.

Standardisation Documents | FIPS 186-4 [FIP13], RFC 8032 [JL17].

Quantum-secure? | No, EdDSA is quantum-unsafe.

ECDH

Description | ECDH is an elliptic curve variant of the Diffie-Hellman key exchange [SP 19].

Public-Key Sizes (bits) | This depends on the curve used. For example, using NIST P-256P results in a 512-bit uncompressed public-key.

Private-Key Sizes (bits) | This depends on the curve used. For example, using NIST P-256P results in a 256-bit private-key.

Ciphertext Size (bits) | Double the length of the private-key.

Hardness | Discrete Logarithm.

Crypto Functionality | ECDH is used for key exchange.

Applications | ECDH is incorporated into protocols that require key exchange.

Further Comments | ECDH is used in the Signal Protocol.

Standardisation Documents | NIST SP 800-56A Rev. 3 [SP 19], ANSI X9.63 [ANS17b], SECG SEC-1 [Bro09]

Quantum-secure? | No, ECDH is quantum-unsafe.

5.1.3 Hash Functions

SHA

Description | SHA is a set of hashes originally designed by the NSA [FIP02], resulting in the primitives SHA-1 and SHA-2. Later, Keccak extended this to SHA-3 through an open competition [FIP15b]. SHA-3 is considered the de facto standard for hash algorithms. Note that SHA-1 is deprecated and will not be discussed.

Hash Output Sizes (bits) | 224, 256, 384, 512.

Applications | SHA is used in a wide range of both software and hardware domains.

Further Comments | SHA is the de facto standard.

Standardisation Documents | FIPS 180-4 [FIP15a], NIST SP 800 107 Rev. 1 [SP 12], RFC 6234 [Hr11], ISO/IEC 10118-3:2018 [ISO11b] (SHA-2), FIPS 180-4 [FIP15a], FIPS 202 [FIP15b], NIST SP 800 107 Rev. 1 [SP 12], ISO/IEC 10118-3:2018 [ISO11b] (SHA-3).

Quantum-secure? | Yes, if a 256-bit or higher message digest is used.

MD5

Description | MD5 is an insecure hash function [Tur11] that is still widely used.

Hash Output Sizes (bits) | 128.

Applications | MD5 is used as a non-cryptographic hash function in various domains.

Further Comments | MD5 is considered insecure as a cryptographic hash function.

Standardisation Documents | RFC 1321 [Riv92].

Quantum-secure? | MD5 is already considered insecure in a classical setting.

BLAKE2

Description | BLAKE2 is a hash function that has better software performance than SHA-3 [BLA17]. It comes in two "flavours", BLAKE2b and BLAKE2s.

Hash Output Sizes (bits) | ≤ 256 (BLAKE2b), ≤ 128 (BLAKE2s).

Applications | BLAKE2 is used both in cryptographic and non-cryptographic settings.

Further Comments | -

Standardisation Documents | RFC 7693 [SA15].

Quantum-secure? | Yes, if BLAKE2b is used.

5.1.4 MACs

HMAC

Description | HMAC is a way to construct a MAC from cryptographic hashes [KBC97].

MAC Key Sizes (bits) | Arbitrary.

MAC Output Sizes (bits) | This dependent on the chosen hash.

Applications | HMAC is used in IPSec, SSH and TLS protocols.

Further Comments | HMAC may suffer from performance issues.

Standardisation Documents | FIPS 198-1 [FIP08], RFC 2104 [KBC97].

Quantum-secure? | Yes, if the underlying hash function is 128-bit quantum-safe.

BLAKE2-MAC

Description | BLAKE2 does not need to use the HMAC transformation to be used as a MAC as it already includes a keying mechanism [SA15].

MAC Key Sizes (bits) | Arbitrary.

MAC Output Sizes (bits) | ≤ 256 (BLAKE2b), ≤ 128 (BLAKE2s).

Applications | BLAKE2-MAC is used in the software domain.

Further Comments | BLAKE2-MAC is faster than HMAC due to its built-in keying mechanism.

Standardisation Documents | RFC 7693 [SA15].

Quantum-secure? | Yes, if BLAKE2b is used.

CBC-MAC

Description | CBC-MAC is a way to construct a MAC from a block cipher [ISO11b].

MAC Key Sizes (bits) | This depends on the chosen block cipher.

MAC Output Sizes (bits) | This depends on the chosen block cipher.

Applications | CBC-MAC is normally used for fixed-length messages.

Further Comments | CBC-MAC is superseded by CMAC.

Standardisation Documents | ISO/IEC 9797-1 [ISO11b].

Quantum-secure? | Yes, if the underlying block cipher is 128-bit quantum-safe, but consider using HMAC or CMAC instead.

CMAC

Description | CMAC is another way to construct a MAC from a block cipher [ISLP06].

MAC Key Sizes (bits) | This depends on the chosen block cipher.

MAC Output Sizes (bits) | This depends on the chosen block cipher.

Applications | CMAC is not as widely used as CBC-MAC.

Further Comments | CMAC is recommended by NIST instead of CBC-MAC.

Standardisation Documents | NIST SP 800-38B [SP 16], RFC 4493 [ISLP06], ISO/IEC 9797-1:2011 [ISO18a].

Quantum-secure? | Yes, if the underlying hash function is 128-bit quantum-safe.

Poly1305

Description | Poly1305 is a high-speed MAC that is decoupled from any other block ciphers or hashes.

MAC Key Sizes (bits) | 256.

MAC Output Sizes (bits) | 128.

Applications | Poly1305 can be used in domains that require high-speed traffic or that do not have any AES acceleration hardware.

Further Comments | Poly1305 combines with ChaCha20 for authenticated encryption.

Standardisation Documents | RFC 8439 [NL18], ISO/IEC 9797-3:2011 [ISO11a].

Quantum-secure? | Yes.

5.2 〉 Stateful Hash-based Signatures

XMSS and XMSSMT

Description | The eXtended Merkle Signature Scheme (XMSS) is a stateful hash-based signature scheme that uses WOTS+ for one-time signatures and is based on Merkle hash trees. XMSSMT is a variant that has multiple hash trees [SP 20].

Public-Key Sizes (bits) | 416-544.

Private-Key Sizes (bits) | Multiple one-time private keys that are dependent on many variables and assumptions.

Ciphertext Size (bits) | 11936-221504.

Hardness | Collision Resistance.

Further Comments | Careful state management is essential and the main issue with the algorithm.

Standardisation Documents | [SP 20].

Quantum-secure? | Yes.

LMS and HSS

Description | Leighton-Micali Signatures is a stateful hash-based signature scheme that uses LM-OTS for one-time signatures and is based on Merkle hash trees. HSS is a variant that has multiple hash trees [SP 20].

Public-Key Sizes (bits) | 384-448 (only for LMS, no standardised parameter for number of hash trees in HSS).

Private-Key Sizes (bits) | Multiple one-time private keys that are dependent on many variables and assumptions, difficult to estimate.

Ciphertext Size (bits) | 6240-74592 (only for LMS, no standardised parameter for number of hash trees in HSS).

Hardness | Collision Resistance.

Further Comments | Careful state management is essential and the main issue with the algorithm.

Standardisation Documents | [SP 20].

Quantum-secure? | Yes.

5.3 ⟩ Post-Quantum Primitives

Table 5.2 shows the strengths and weaknesses of each post-quantum primitive. A distinction is made between Key Exchange (KE) and Digital Signatures Schemes (DSS). Dark green indicates a strength, light green indicates a mild strength, orange indicates a mild weakness and red indicates a strong weakness.

	Features			Speed			Memory		
	QUANTUM-SAFE?	STANDARD-ISED	CONFIDENCE[1]	KEY GEN	ENCRYP-TION/ SIGNING	DECRYP-TION/ VERI-FICATION	PUB KEY	PRIV KEY	CIPHERTEXT/ SIGNATURE
RSA (KE)	red	green	green	red	green	red	green	light-green	green
Elliptic-curve (KE)	red	green	green	green	green	light-green	green	green	green
CR.-KYBER (KE)	green	green	light-green	green	green	green	light-green	orange	light-green
FrodoKEM (KE)	green	light-green	green	orange	orange	orange	red	red	red
McEliece (KE)	green	green	green	red	green	green	red	red	green
CR.-DILITHIUM (DSS)	green	green	light-green	light-green	light-green	green	light-green	orange	orange
FALCON (DSS)	green	green	green	red	orange	light-green	light-green	red	light-green
BIKE (DSS)	green	orange	orange	green	green	light-green	green	light-green	orange
HQC (DSS)	green	orange	orange	light-green	green	light-green	orange	green	orange
SPHINCS+ (DSS)	green	green	green	orange	red	green	green	green	red

Table 5.2: Strengths and weaknesses of various traditional as well as post-quantum primitives.

For the table the benchmarking suite by openquantumsafe is used for the speed benchmarks [OPE23], while the status report on the third round by NIST is used for the memory benchmarks [NIS22b]. For the speed benchmarks, the level 3 security is chosen, with the x86_64-noport implementation. If there are multiple level 3 parameter sets, an arbitrary one is chosen. The implementation on 2023-09-06 -26 is used. For all columns, the colour thresholds are chosen to highlight the strengths and weaknesses of each of the algorithms.

---

[1] This column depicts the confidence that the scientific community has in the cryptographic scheme. Generally speaking, older schemes have more confidence, as their security has been studied longer.

5.3.1 Digital Signature

CRYSTALS-DILITHIUM

Description | CRYSTALS-DILITHIUM is a lattice-based signature scheme that is one of the NIST finalists for standardisation [BLK+21a].

Public-Key Sizes (bits) | 10496-20736.

Private-Key Sizes (bits) | 20224-38912.

Ciphertext Size (bits) | 19360-36760.

Hardness | Module Small Integer Problem (MSIS) and Module Learning with Errors (MSIS).

Further Comments | CRYSTALS-DILITHIUM is a digital signature counterpart to the public-key KEM CRYSTALS-KYBER, which is also a NIST selected algorithm.

Supported Security Levels | 1, 3, 5 [ABB+21b].

Standardisation Documents | Official website [ABB+21b].

Quantum-secure? | Yes.

FALCON

Description | FALCON is a lattice-based signature scheme that is one of the NIST finalists for standardisation [FHK+21].

Public-Key Sizes (bits) | 7176-14264.

Private-Key Sizes (bits) | 10248-18440.

Ciphertext Size (bits) | 5328-10240.

Hardness | Short integer solution problem over NTRU lattices.

Further Comments | FALCON uses floating point arithmetic, which is not very common in cryptography.

Supported Security Levels | 1, 3, 5 [FHK+21].

Standardisation Documents | Official website [FHK+21].

Quantum-secure? Yes.

SPHINCS+

Description | SPHINCS+ is a stateless hash-based signature scheme that is based on a previous signature scheme called SPHINCS. According to literature, the improvements in relation to SPHINCS are in reduced signature sizes [HBD+21].

Public-Key Sizes (bits) | 32-64.

Private-Key Sizes (bits) | 64-128.

Ciphertext Size (bits) | 7856-49856.

Hardness | Collision Resistance.

Further Comments | SPHINCS+ is selected as a NIST draft standard.

Supported Security Levels | 1, 3, 5 [HBD+21].

Standardisation Documents | Official website [HBD+21].

Quantum-secure? | Yes.

5.3.2 Public-key Encryption and Key-establishment

BIKE

Description | BIKE is a code-based KEM whose hardness is based on Quasi-Cyclic Moderate Density Parity-Check codes. It was submitted to NIST and is currently a candidate in Round 4 [ABB+21a].

Public-Key Sizes (bits) | 12320-40792.

Private-Key Sizes (bits) | 2244-4640.

Ciphertext Size (bits) | 12579-41229.

Hardness | Quasi-Cyclic Moderate Density Parity-Check codes.

Further Comments | Bike is a NIST Round 4 candidate.

Supported Security Levels | 1, 3, 5 [ABB+21a].

Standardisation Documents | Official website [ABB+21a].

Quantum-secure? | Yes.

Classic McEliece

Description | Classic McEliece is a conservative code-based KEM that is based on the 1978 original McEliece cryptosystem [ABC+20]. It is a NIST round 4 candidate.

Public-Key Sizes (bits) | 2088960-10862592.

Private-Key Sizes (bits) | 51936-112960.

Ciphertext Size (bits) | 1024-1920.

Hardness | Syndrome Decoding Problem (SDP).

Further Comments | Classic McEliece requires very large key sizes but small ciphertexts, so probably not usable for low storage systems such as smartcards or IoT.

Supported Security Levels | 1, 3, 5 [ABC+20].

Standardisation Documents | Official website [ABC+20].

Quantum-secure? | Yes.

CRYSTALS-KYBER

Description | CRYSTALS-KYBER is a lattice-based KEM that is one of the NIST finalists for standardisation [BLK+21b].

Public-Key Sizes (bits) | 13056-25344.

Private-Key Sizes (bits) | 6400-12544.

Ciphertext Size (bits) | 6144-12544.

Hardness | Modular Learning with Errors (MLWE).

Further Comments | CRYSTALS-KYBER is a public-key KEM counterpart to the digital signature CRYSTALS-DILITHIUM, which is also a NIST selected algorithm.

Supported Security Levels | 1, 3, 5 [ABB+21b].

Standardisation Documents | Official website [ABB+21b].

Quantum-secure? | Yes.

FrodoKEM

Description | FrodoKEM is a lattice-based KEM that supports conservative, yet practical constructions. It will not be standardised by NIST. [ABD+21].

Public-Key Sizes (bits) | 76928-172160.

Private-Key Sizes (bits) | 159104-344704.

Ciphertext Size (bits) | 77760-173056.

Hardness | Learning with Errors (LWE).

Further Comments | Currently, FrodoKEM will not be standardised by NIST.

Supported Security Levels | 1, 3, 5 [ABD+21].

Standardisation Documents | Official Website [ABD+21].

Quantum-secure? | Yes.

HQC

Description | HQC is a code-based KEM submitted to NIST and is currently a candidate in Round 4 [MAB+21].

Public-Key Sizes (bits) | 17992-57960.

Private-Key Sizes (bits) | 320.

Ciphertext Size (bits) | 35848-115752.

Hardness | Decisional Syndrome Decoding Problem.

Further Comments | HQC is a NIST Round 4 candidate.

Supported Security Levels | 1, 3, 5 [MAB+21].

Standardisation Documents | Official website [MAB+21].

Quantum-secure? | Yes.

Bibliography

[ABB+21a]   Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean- Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor, Vasseur. Valentin, Santosh Ghosh, and Jan Richter-Brokmann. BIKE Website. https://bikesuite.org/, 2021. [Accessed: 22/08/2022].

[ABB+21b]   Roberto Avanzi, Shi Bai, Ducas Lé Bos, Joppe, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Stehlé. CRYSTALS Website. https://classic.mceliece.org/index.html, 2021. [Accessed: 23/05/2022].

[ABC+20]   Martin Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece Website. https://classic.mceliece.org/index.html, 2020. [Accessed: 23/05/2022].

[ABD+21]   Erdem Alkim, Joppe Bos, Léo Ducas, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, Douglas Stebila, Karen Easterbrook, and Brian LaMacchia. FrodoKEM Website. https://frodokem.org/, 2021. [Accessed: 23/05/2022].

[AMK05]   Kato Akihiro, Shiho Moriai, and Masayuki Kanda. The Camellia Cipher Algorithm and Its Use With IPsec. RFC 4312, December 2005.

[ANS17a]   Key Establishment Using Integer Factorization Cryptography. Standard, ANSI, November 2017.

[ANS17b]   Key Agreement and Key Transport Using Elliptic Curve Cryptography. Standard, ANSI, February 2017.

[ANS20a]   Financial services - Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm - ECDSA. Standard, ANSI, September 2020.

[ANS20b]   ANSSI. Technical Position Paper: QKD v2.1 - Should Quantum Key Distribution be Used for Secure Communications? https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/, 2020.

[Bad09]   Mohamad Badra. Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode. RFC 5487, March 2009.

[BDH+21]   Ward Beullens, Jan-Pieter D'Anvers, Andreas T Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, and Nigel P Smart. Post-quantum cryptography: Current state and quantum mitigation. 2021.

[BLA17]   BLAKE2 - fast secure hashing. https://www.blake2.net/, 2017. [Accessed on 24-03-2022].

—) Bibliography

[BLK+21a]   Shi Bai, Ducas Lé, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (Version 3.1). https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf, 2021. [Accessed: 23/05/2022].

[BLK+21b]   Shi Bai, Ducas Lé, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation (Version 3.02). https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf, 2021. [Accessed: 22/08/2022].

[Bro09]   Daniel Brown. Elliptic Curve Cryptography. Standard, Standards for Efficient Cryptography Group, May 2009.

[BSI22]   BSI. Quantum-safe cryptography – fundamentals, current developments and recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html, 2022.

[Cry21]   Building a Crypto-agile Organization? https://cryptosense.com/whitepapers/crypto-agility-whitepaper, 2021.

[EST18]   ESTI. Quantum-Safe Virtual Private Networks. Standard, ETSI, Valbonne, FR, September 2018.

[ET05]   Pasi Eronen and Hannes Tschofenig. Pre-shared key ciphersuites for transport layer security (TLS). RFC 4279, 2005.

[ETS20]   ETSI. Migration strategies and recommendations to Quantum Safe schemes. https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes, 2020.

[FDC+07]   Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney L. Thayer, and David Shaw. OpenPGP Message Format. RFC 4880, November 2007.

[FHK+21]   Pierre-Alain Fouque, Jeffrey Hoffstein, Vadim Kirchner, Paul Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON Website. https://falcon-sign.info/, 2021. [Accessed: 23/05/2022].

[FIP99]   Data encryption standard (DES). Standard, NIST, Gaithersburg, MD, October 1999.

[FIP01]   Advanced encryption standard (AES). Standard, NIST, Gaithersburg, MD, November 2001.

[FIP02]   Announcing Approval of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard; a Revision of FIPS 180-1. Notice, NIST, August 2002.

[FIP08]   The Keyed-Hash Message Authentication Code (HMAC). Standard, NIST, Gaithersburg, MD, July 2008.

[FIP13]   Digital Signature Standard (DSS). Standard, NIST, Gaithersburg, MD, June 2013.

[FIP15a]   Secure Hash Standard (SHS). Standard, NIST, Gaithersburg, MD, August 2015.

Bibliography

[FIP15b]   SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Standard, NIST, Gaithersburg, MD, August 2015.

[FK11]   Sheila Frankel and Suresh Krishnan. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071, February 2011.

[FKMS20]   Scott Fluhrer, Panos Kampanakis, David McGrew, and Valery Smyslov. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security. RFC 8784, June 2020.

[Gro96]   Lov K. Grover. A fast quantum mechanical algorithm for database search. In STOC, pages 212–219. ACM, 1996.

[HBD+21]   Andreas Hüsling, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS+ Website. http://sphincs.org/index.html, 2021. [Accessed: 22/08/2022]

[Hou02]   Russ Housley. Cryptographic Message Syntax (CMS). RFC 3369, September 2002.

[Hr11]   Tony Hansen and Donald E. Eastlake 3rd. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234, May 2011.

[ISLP06]   Tetsu Iwata, Junhyuk Song, Jicheol Lee, and Radha Poovendran. The AES-CMAC Algorithm. RFC 4493, June 2006.

[ISO08]   Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms. Standard, International Organization for Standardization, Geneva, CH, April 2008.

[ISO10a]   Information technology – Security techniques – Key management – Part 1: Framework. Standard, International Organization for Standardization, Geneva, CH, April 2010.

[ISO10b]   Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. Standard, International Organization for Standardization, Geneva, CH, December 2010.

[ISO10c]   Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms. Standard, International Organization for Standardization, Geneva, CH, December 2010.

[ISO11a]   Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function. Standard, International Organization for Standardization, Geneva, CH, November 2011.

[ISO11b]   IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions. Standard, International Organization for Standardization, Geneva, CH, March 2011.

Bibliography

[ISO18a]   Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher. Standard, International Organization for Standardization, Geneva, CH, October 2018.

[ISO18b]   T Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. Standard, International Organization for Standardization, Geneva, CH, November 2018.

[JL17]   Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, January 2017.

[KBC97]   Dr. Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.

[KHN+14]   Charlie Kaufman, Paul E. Hoffman, Yoav Nir, Pasi Eronen, and Tero Kivinen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296, October 2014.

[KK10]   Masayuki Kanda and Satoru Kanno. Camellia Cipher Suites for TLS. RFC 5932, June 2010.

[KSF+20]   Panos Kampanakis, Douglas Stebila, Markus Friedl, Torben Hansen, and Dimitrios Sikeridis. Post-quantum public key algorithms for the Secure Shell (SSH) protocol. Internet-Draft draft-kampanakis-curdle-pq-ssh-00, Internet Engineering Task Force, October 2020. Work in Progress.

[LY06c]   Chris M. Lonvick and Tatu Ylonen. The Secure Shell (SSH) Protocol Architecture. RFC 4251, January 2006.

[MAB+21]   Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Bidoux. Löıc, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Lacan. Jerome, Robert. Jean-Marc, and Pascal Veron. HQC Website. http://pqc-hqc.org/, 2021. [Accessed: 22/08/2022].

[MJ21]   Nikos Mavrogiannopoulos and Simon Josefsson, 2021. [Accessed: 22/02/2022].

[MKJR16]   Kathleen Moriarty, Burt Kaliski, Jakob Jonsson, and Andreas Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017, November 2016.

[MMN04]   Mitsuru Matsui, Shiho Moriai, and Junko Nakajima. A Description of the Camellia Encryption Algorithm. RFC 3713, April 2004.

[Mor04]   Shiho Moriai. Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS). RFC 3657, January 2004.

[MP21]   Michele Mosca and Marco Piani. 2021 quantum threat timeline report. https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/, 2021.

[MvH20]   Frank Muller and Maran van Heesch. Migration to Quantum-safe Cryptography. https://www.tno.nl/en/digital/digital-innovations/trusted-ict/cyber-security-through-quantum-safe/, 2020.

Bibliography

[NBV21]   NBV. Bereid je voor op de dreiging van quantumcomputers. https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers, 2021.

[NCS20a]   NCSC. Whitepaper: Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography, 2020.

[NCS20b]   NCSC. Whitepaper: Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, 2020.

[NCS22]   NCSC. Guidelines for quantum-safe transport-layer encryption. https://www.ncsc.nl/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption, 2022.

[NIS22a]   NIST. Post-Quantum Cryptography - Selected Algorithms 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022, 2022.

[NIS22b]   NIST. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/pubs/ir/8413/upd1/final, 2022.

[NL18]   Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439, June 2018.

[NN21]   NIST and NCCoE. Migration to Post-Quantum Cryptography. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms, 2021.

[NSA21]   NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/, 2021.

[NTT05]   NTT. Japan's First 128-bit Block Cipher "Camellia" Approved as a New Standard Encryption Algorithm in the Internet. 2005. [Accessed on 23-05-2022].

[OAS20]   OASIS. OASIS PKCS 11 TC. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11, 2020. [Accessed on 23-05-2022].

[OPE23]   OPEN QUANTUM SAFE. OQS algorithm performance visualizations. https://openquantumsafe.org/benchmarking/, 2023.

[Pop15]   Andrei Popov. Prohibiting RC4 Cipher Suites. RFC 7465, February 2015.

[Res18]   Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.

[Riv92]   Ronald L. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, April 1992.

[SA15]   Markku-Juhani O. Saarinen and Jean-Philippe Aumasson. The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). RFC 7693, November 2015.

[Saf21]   How Agile Is Your Cryptographic Strategy? https://safecode.org/blog/how-agile-is-your-cryptographic-strategy/, 2021.

⏤)   Bibliography

[Sch94]   Bruce Schneier. Academic: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) – Schneier on Security. https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html, 1994. [Accessed on 24-03-2022].

[SFG22]   Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-04, Internet Engineering Task Force, January 2022. Work in Progress.

[Sho94]   Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In FOCS, pages 124–134. IEEE Computer Society, 1994.

[SP 12]   Recommendation for Applications Using Approved Hash Algorithms. Special publication, NIST, Gaithersburg, MD, August 2012.

[SP 16]   Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication. Special publication, NIST, Gaithersburg, MD, June 2016.

[SP 17]   Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. Special publication, NIST, Gaithersburg, MD, November 2017.

[SP 19]   Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. Special publication, NIST, Gaithersburg, MD, March 2019.

[SP 20]   Recommendation for Stateful Hash-Based Signature Schemes. Special publication, NIST, Gaithersburg, MD, October 2020.

[TGF+18]   Alexander Truskovsky, Daniel Van Geest, Scott Fluhrer, Panos Kampanakis, Mike Ounsworth, and Serge Mister. Multiple Public-Key Algorithm X.509 Certificates. Internet-Draft draft-truskovsky-lamps-pq-hybrid-x509-01, Internet Engineering Task Force, August 2018. Work in Progress.

[Tur11]   Sean Turner. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. RFC 6151, March 2011.

[Wei21]   Adam Weinberg. Analysis of top 11 cyber attacks on critical infrastructure. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/, 2021. [Accessed: 05/04/2022].

[Wet]   Dirk Wetter. testssl.sh. https://testssl.sh/.

[X5019]   Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. Standard, ITU-T, Geneva, Switzerland, October 2019.

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY