HAPKIDO

Work Package 3 - Deliverable 3.1

Governing the transition to quantum-safe PKIs in the Netherlands:

Paving the way for our quantum-safe future

Lærke Vinther Christiansen, Ini Kong, & Nitesh Bharosa

November 2023

Table of Contents

Summary ____ ***2***

1. Introduction ____ ***3***

1.1 Need for transition ____ **4**

1.2 Goal & Aim ____ **5**

1.3 Research Question(s) ____ **6**

1.4 Research Approach ____ **6**

2. Challenges in the transition ____ ***8***

3. Actors and Levels in the QS Transition ____ ***13***

3.2 Transition Actors ____ **14**

3.2.1 Identifying actor types ____ 14

3.2.2 Subset of actors in relation to the Dutch government ____ 16

4. Recommendations for policy guidelines to address the challenges ____ ***19***

5. Conclusion ____ ***21***

Reference list ____ ***23***

Summary

Quantum computers are being developed at unprecedented rates, each day bringing humanity closer to some of the most significant advancements made in fields like medicine and health sciences in recent history. However, no technological marvel comes without inherent risk. One of the most ubiquitous tools of cyber security is *public key infrastructure systems* (PKI). In the most simplistic of definitions, PKI authenticate users though digital certificates, which are verified by a registration authority and validated by a third-party user. This system is presently one of the most common tools for ensuring digital safety and ensure safe data communication. However, quantum computers pose a significant threat to PKI systems, threatening to render one of the most ubiquitous cybersecurity tools useless. Some of these threats from quantum computers are already present now and will only continue to develop further in the future. This report looks at what governance means in relation to the transition to quantum-safe (QS) PKI, what the challenges are in this transition, and what recommendations we can make based on this.

Ultimately, this report identifies nine challenges in the transition to QS PKI. These challenges showcase the diverse variety of challenges that socio-technical systems bring with them, as they span across complex technical issues, to social and organizational issues like knowledge gaps, lack of in-house management, unclear governance, and lack of awareness. All of these challenges interconnect and contribute to each other, but also distinguish themselves through their own unique complication. Secondly, this report looked at what 'actor' means in the context of transitioning to QS PKI and drew three main conclusions. First, each actor will present a unique set of needs and interdependencies. Secondly, each actor can be categorized within a role as an adopter. These adopter types are *regular, urgent,* and *developers.* Lastly, the Netherlands has three different layers of actors in the transition to QS PKIs, namely a *macro,* a *meso,* and a *micro* level. Lastly, this report recommends four policy guidelines to address these challenges. These guidelines center on creating collective awareness through social networks, emphasizing interdependencies, increasing comprehension of technical standards, and employing real-life use cases.

1. Introduction

The development of quantum computers is currently scaling at unprecedented speeds. At the time of writing, IBM is the latest actor to claim quantum supremacy amongst a long line of previous contested claims by industry rivals like Google. IBM's claim to quantum supremacy are based on the imminent release of their "Condor" quantum computer with 1121 qubits by the end of 2023 (Choi, 2022). They estimate they will increase this number of qubits fourfold by 2025 (Choi, 2022). These developments are remarkable, but they also bring with them certain risks for our collective cybersecurity infrastructures. Cybersecurity infrastructures ensures the safety of our shared online platforms by relying on cryptography to encrypt our data communication safely. The security of current-day cryptography is based on the difficulty to solve certain mathematical operations (e.g. factorization into prime integers). Due to the complex nature of quantum computers, they can solve these mathematical problems in a very efficient way, thus making the current cryptosystems insecure.

This is especially true for *public key infrastructure systems* (PKI), which is one of the most important information-security mechanisms used nowadays. PKI is used to distribute and authenticate cryptographic keys and the type of encryption utilized in PKI systems is especially vulnerable to attacks from quantum computers (Kong et al., 2022). Paired with the fact that PKI systems are presently so ubiquitous that they are used by all major societal sectors, such as healthcare, government, banking, and telecommunications it is incredibly pertinent that we create quantum-safe alternatives to present day PKI systems and prepare users to transition to these new systems already now.

Currently, cryptography and cybersecurity experts are working on developing quantum-safe (QS) versions of PKI systems, which means the main challenge for now is creating awareness of the issue and elucidating to the actors how they can prepare to migrate from their current platforms onto the quantum-resistant alternatives while the QS PKI systems are being developed. However, transitioning to quantum safety is a highly complex task that requires advanced recommendations for multiple levels of governance. It is essential to establish clear structures and guidelines for the organizations looking to migrate to QS PKI. The process will be highly complex with a significant level of interdependencies (Kong et al., 2022). This is why the relevant actors need to make the move collectively to successfully navigate the changes in this socio-technical system. By socio-technical system we mean applications, such as PKI, which are characterized by an interaction and codependence between users and

technology. With a lack of clear procedures to guide the collaborative effort in the migration towards QS PKI, this report aims to provide the first steps in achieving this. Thus the report will consider governance aspects, challenges in the transition, and recommendations for future policymakers.

1.1 Need for transition

As established in the section above, there are grounds for concern in relation to the security risks associated with quantum, computers, especially for PKI systems. Diving more into the PKI aspect, this section will explore the need for transition for PKI users. Firstly, one of the main risks for PKI systems are that an attacker with access to a large enough quantum computer can forge unauthorized cryptographic material: the attacker can obtain the cryptographic keys associated to a digital entity (like an official institution) and steal its digital identity. A successful attacker can therefore operate in a malicious manner undetected, since it would pass all security checks belonging to the alleged identity. While the threats associated with a quantum computer strong enough to achieve prime factorization are mainly considered to be a future issue, there are also threats occurring presently. This includes concepts like "store-now-decrypt-later" (SNDL). SNDL is when high-quality data (i.e., data that does not degrade over time) gets stolen in encrypted form and stored away to be decrypted later once large enough quantum computers become available (Attema et al., 2023; Kong et al., 2022).

Hence, the sooner the transition to QS PKI can be initiated the better, as there will be more time to reach important milestones before the threat fully materializes (cf. Figure 1). However, the collective awareness around the topic is low (Kong et al., 2022). With low awareness of the topic there is a general lack of urgency surrounding the threat. This issue is not unique to the topic of QS PKI, rather lack of awareness and decentralized decision making is common among cybersecurity issues (Gillard et al., 2022; Housen-Couriel, 2022; Pitt et al., 2017). While cybersecurity is a central pillar to the functionality of modern society as it becomes increasingly dependent on technology, the decision-making actors on cyber security topics are usually decentralized and limited in numbers (Bauer & van Eeten, 2009). This means that large-scale transitions for common-place systems such as PKIs are very difficult to facilitate as they require collective action from actors, but only very few are aware of the issues and decisions being made. Moreover, the exact amount of time available to accomplish the transition is unknown. There are multiple suggestions from different researchers and developers guessing at the timeline, but it is not possible to definitively prover one true or false. One of the more commonly estimated lengths of time for migrating is 10-15 years' (Grimes, 2019; Lindsay, 2020b) and is believed to allow for a stable and low-risk transition. Looking to the timeline presented in Figure

1, we can see that the more time that passes between the present moment and operationalization of quantum computers, the safer the transition will be (Attema et al., 2023). As can be seen, the longer the transition timeline, the more key milestones can be reached, and the safer the transition actors will be. If the threat should materialize within the next few years the risk would be substantial. Many major sectors in society rely on PKIs for safe data communication. Hereunder, the government sector, the banking sector, the telecommunications sector, and the healthcare sector to name a few. This would mean citizens would be unable to communicate with their governments and access their banks online, make transfers, or in severe cases, withdraw money from ATM's. Likewise, sensitive healthcare data would no longer be able to be kept private and the same goes for call records and text messages. Needless to say, the implications would be enormous.

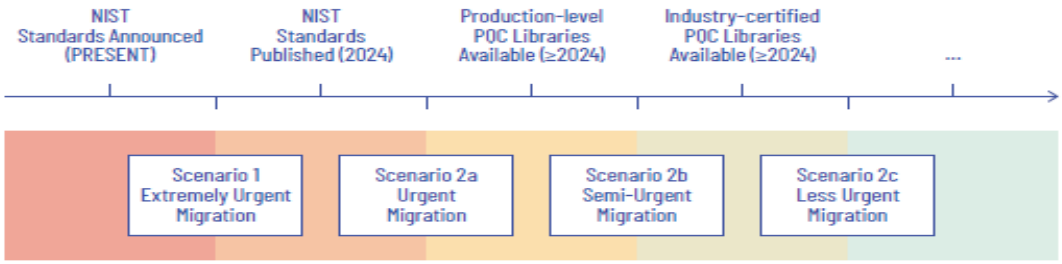

Figure 1: Migration urgency timeline (Attema et al., 2023)

1.2 Goal & Aim

The goal of this report is to discuss the initial necessary and relevant elements in the transition to QS PKI from a governance perspective. This report is structured as follows. Firstly this report focuses on the relevant background information for the topic of governing QS PKI. The second section covers the fundamentals of PKI systems and presents a table of the different PKI terminologies and components. The third section focuses on the research approach. The fourth section presents the results. Firstly, the section looks at technology governance and its relation to transitioning to QS PKI. Secondly, the section looks at the challenges that can be identified in the process of QS PKI. Lastly, the section presents a set of suggested policy guidelines to help mitigate these challenges. In the fifth section, the report presents its conclusions.

1.3 Research Question(s)

Based on what is outlined above, as well as the intended goals and aims of this report, we present three questions to answer:

1. What are the challenges for the transition mentioned in the literature?
2. What are the actors types we can identify in the transition towards quantum-safety for Dutch PKI users?
3. What are the recommendations for next steps in the transition?

1.4 Research Approach

This report relies on a literature-based approach. A systematic approach has been utilized to retrieve and include literature in the report, similar to the PRISMA approach. (Moher et al., 2009) This means the literature included has gone through multiple rounds of screening to ensure relevancy and legitimacy.

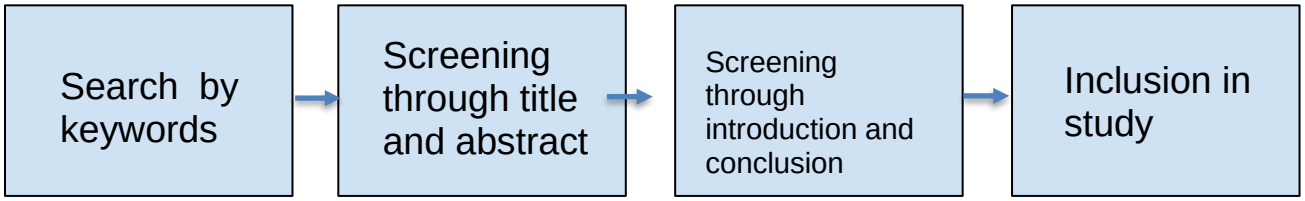

Figure 2. Overview of systematic literature review process

As can be seen in Figure 2, multiple levels of screening were employed. Thus only literature that guaranteed relevance and sufficient quality was included in the report. The different topics of the report underwent their own literature search, while the different topics also informed each other, thus creating a body of knowledge highly relevant to the topic. The topics included in this process were PKI systems, PKI governance, transition challenges, and policy guidelines. Thus bringing these topics together, the report seeks to address the challenge of governing QS PKI. The results from the literature review presented in this report are further explored in the article *Challenges in the Transition Towards a Quantum-Safe Government* by Kong et. al. (2022).

Likewise, this report relied on a set of expert focus groups hosted in December 2022. In these workshops experts who belonged to one or more of four categories were invited. The categories were:

1. Knowledge of PKIs
2. Awareness of the Quantum Threat
3. Works sectors that rely on PKI systems
4. Experience in implementing and integrating new technologies and facilitating change in organizations and institutions.

After the workshop their answers where compiled and analyzed into four set of policy recommendations for the Dutch quantum transition. These are the results that are being presented in this report.

2. Challenges in the transition

This section presents the results of our systematic literature review and highlights the list of challenges found in the selected literature.

The systematic literature review was conducted to give an overview of challenges found in the literature from transitioning the current PKI systems. Search engines such as Scopus, SpringerLink, ScienceDirect, Google Scholar, and Mendeley were used to identify the literature from the year 2010 to 2021. This was done using keywords such as "quantum-safe PKI", "challenges", "post-quantum cryptography", and a combination of these keywords like "post-quantum cryptography challenge", "quantum-safe cryptography challenge" and "quantum-safe transition challenge" (Kong et al., 2022).

Along with the academic literature, white papers, expert reports, and conference proceedings found on Mendeley were added to provide more in-depth knowledge on this topic of research. In total, 2266 articles were found, and 154 articles were chosen after screening the title and abstract of each paper. Then 19 duplicate articles were excluded (Kong et al., 2022). From the remaining 135 articles, 93 irrelevant articles were excluded with several additional criteria: (a) 23 articles were not related to quantum computing, (b) 44 articles were not about QS PKI, and (c) 26 articles were not about QS PKI challenges. As a result, 42 relevant articles (including 11 academic literature and 31 grey literature) were selected for the review (Kong et al., 2022).

The challenges that were identified in this review are presented in Table 1. In this table are listed nine overall challenges relevant for the transition to QS PKI in the Netherlands. Below the table, there are a more in-depth explanation for each of them.

Table 1. Nine identified challenges in the transition

Challenges	References
Complex PKI system & interoperability	(NIST, 2021), (ISARA, 2018), (AccentureLabs, 2018), (CSIRO, 2021), (CCC, 2019), (Vermeer & Peet, 2020), (ENISA, 2021), (Macaulay & Henderson, 2019), (Grote, Ahrens, & Benavente-Peces, 2019)
Perceived Lack of Urgency	(Lovic, 2020), (TNO, 2020), (Lindsay, 2020b), (Vermeer & Peet, 2020), (ETSI, 2015)
Knowledge Gaps in quantum computing	(Mulholland et al., 2017), (TNO, 2020), (CCC, 2019), (Niederhagen & Waidner, 2017), (Macaulay & Henderson, 2019), (Ma et al., 2021), (Vermaas, 2017)
Lack of In-house management support	(Mosca, 2015), (TheHagueSecurityDelta, 2019), (CCC, 2019), (NIST, 2018), (Buchholz, Mariani, Routh, Keyal, & Kishnani, 2020)
Unclear QS governance	(Mulholland et al., 2017), (NIST, 2021), (TheHagueSecurityDelta, 2019), (Machatan & Heintzman, 2021), (Wiesmaier et al., 2021), (CSIRO, 2021), (Niederhagen & Waidner, 2017)
Perceived lack of awareness	(Mulholland et al., 2017), (Lovic, 2020), (TNO, 2020), (Vermeer & Peet, 2020), (Macaulay & Henderson, 2019), (ETSI, 2015)

No clear ownership & operating institution	(Mulholland et al., 2017), (NIST, 2021), (Lindsay, 2020b), (Ma et al., 2021), (Lindsay, 2020a)
Lack of policy guidance	(TheHagueSecurityDelta, 2019), (Lovic, 2020), (Tibbetts, 2019), (Lewis & Travagnin, 2018), (Lewis et al., 2018), (Lindsay, 2020a), (Lewis, 2017)
Need for various stakeholders	(Mulholland et al., 2017), (TheHagueSecurityDelta, 2019), (CCC, 2019), (Vermeer & Peet, 2020), (Chen & Moody, 2020), (Räsänen et al., 2021)

Complex PKI system

PKI systems have a chain of dependencies that extend to various actors such as standardizing bodies, governing bodies, hardware providers, and third-party software, which may also include third-party component libraries (Accenture Labs, 2018; CCC, 2019; ISARA, 2018; Vermeer & Peet, 2020). Thus, changes in PKI systems cannot occur in isolation and QS cryptographic algorithm cannot be replaced with a simple 'drop-in' method (ENISA, 2021; NIST, 2021). Also, changes in cryptographic algorithms need to be recognized in devices (e.g. encryption levels in the X.509 scheme) and must be the same or compatible to enable secure and correct communication (CSIRO, 2021; Grote et al., 2019; Macaulay & Henderson, 2019).

Lack of Urgency

Advocates for the transition to QS PKI argue there is a perceived lack of urgency amongst the future afflicted parties, although the transition is estimated to be a decade(s)-long process (Lindsay, 2020b, p. 20; Lovic, 2020; TNO, 2020). A large-scale quantum computer is not yet available, and many organizations do not recognize quantum threats, such as the "store now and decrypt later" method (ETSI, 2015).

While NIST is developing the QS cryptographic algorithm standards, there is not yet a collective sense of urgency, and organizations find it difficult to select QS solutions and achieve inter-agency collaboration for the QS transition (Vermeer & Peet, 2020).

Knowledge Gaps in quantum computing

It is difficult even for experts to fully grasp the concept of quantum theory, so it not so strange to see knowledge gaps regards quantum related threat among organizations. These organizations may overlook the threats imminent to them from quantum computing technology due to their lack of insight on the topic (Macaulay & Henderson, 2019; Mulholland et al., 2017; Vermaas, 2017). For those who do not have relevant expertise and knowledge, it is much more challenging to explain the threats of quantum computing and the need for QS transition. Knowledge gaps may delay organizations from transitioning the current PKI systems (CCC, 2019; Niederhagen & Waidner, 2017). Without prior knowledge, organizations risk not taking timely action, which results in unforeseen vulnerabilities (Ma et al., 2021; TNO, 2020).

Lack of In-house management support

The lack of upper management support in organizations can slow the process of QS transition since organizations still need to identify the needs and requirements of the QS transition in the current infrastructure (Buchholz et al., 2020; Vermeer & Peet, 2020). It is crucial to have a support base that can prioritize the QS transition as a high priority. Without the support of upper management, it is difficult for organizations to proceed with the QS transition and develop a tactical roadmap that may involve different teams in the organization (Mosca, 2015; NIST, 2018; The Hague Security Delta, 2019).

Unclear QS governance

Organizations often do not know their cryptographic assets and how to facilitate updates in their current infrastructure (CSIRO, 2021; NIST, 2021). It is difficult to assess vulnerabilities and where and with what priority the QS alternatives should be implemented (Mashatan & Heintzman, 2021; The Hague Security Delta, 2019). Although much research is done on the fundamentals of QS cryptographic algorithms, it has not yet been applied in practice (Mulholland et al., 2017).

The uncertainties on how to transition current infrastructure call for a high degree of decision-making, coordination, and leadership efforts (Lindsay, 2020b; The Hague Security Delta, 2019).

Lack of awareness

There is a lack of awareness of the threats associated with quantum computing technology. The risks surrounding quantum computing are often largely ignored, and more emphasis is put on its opportunities for scaling quantum industry (ETSI, 2015; Lovic, 2020; Macaulay & Henderson, 2019). Organizations need to draw transition plans and recognize the amount of lead-time needed to make changes in their security products and infrastructure (Vermeer & Peet, 2020). However, It is difficult to change current infrastructure, and security requirements needed for quantum protection without recognizing the issue of quantum threats (TNO, 2020).

No clear ownership & operating institution

With complex technical dependencies, organizations need to negotiate and coordinate problems to modify the infrastructures relevant to the transition (Lindsay, 2020a). The PKI system is known to be a technology that is used by all but owned by none. Organizations cannot operate and deploy changes in PKI systems in isolation (Mulholland et al., 2017). Multiple stakeholders are needed since organizations do not have complete control over PKI systems. For QS transition, the ownership of current PKI systems cannot be clearly defined and its boundaries blur the extent to which organizations should initiate and take responsibilities (Lindsay, 2020b; NIST, 2021).

Lack of policy guidance

The topic of quantum computing is not yet the popular topic of discussion in the European Parliament (ETSI, 2015). There is a lack of awareness and risks associated with quantum computing technology, which may translate into a lack of policy guidance (Lindsay, 2020a; Lovic, 2020). There is currently no European government regulation that enforces organizations to modify current infrastructure and security protocols to become quantum-resistant (A. M. Lewis & Travagnin, 2018; Mosca, 2015; Tibbetts, 2019). Having right incentives and early adoption programs may encourage organizations to participate in the QS transition and further stimulate business cases (A. Lewis, 2017; A. M. Lewis & Travagnin, 2018; The Hague Security Delta, 2019).

Lack of coordination among stakeholders

Developing cryptographic algorithms is very complex and requires knowledge in multiple sciences and engineering fields in applied cryptography and system security (CCC, 2019; Chen & Moody, 2020). Likewise, transitioning current infrastructure with QS cryptographic algorithms also requires collaboration on many levels (The Hague Security Delta, 2019). In order to establish well-coordinated contingency planning in the QS transition, collaboration among various stakeholders is needed (Chen & Moody, 2020; Rasanen et al., 2021; Vermeer & Peet, 2020). There are varying interests and needs in government standards bodies, software solution providers, hardware vendors, service providers, international consortiums, and PKI users (CCC, 2019).

3. Actors and Levels in the QS Transition

The transition to QS PKI systems will invariably be long and complex, but the more we can parse about the situation beforehand, the easier the transition will be to handle. As it is now, the research for facilitating this transition is just getting started, meaning there is still a lot of ground to cover. This is true for the technical side of the transition, but it is especially true for the organizational, governance aspect of the transition. Some initial work has been done in discussing the quantum related threats and their timelines (Joseph et al., 2022; Lindsay, 2020a; Mosca, 2015), and likewise efforts have been made in mapping the current state of quantum preparedness and what needs to be done next (Christiansen et al., 2023; Kong, 2022; Rodriguez, 2023).

For this section of the report, we will explore two topics. Namely, the transition actors; the lens through which we can view them and the how they can be categorized in the transition. Secondly, the report will consider the different levels of actors in the transition, what these levels might be, which actors can be included where, and how these levels function off the page.

3.2 Transition Actors

This section of the report aim to explore and identify a subset of the actors in the transition and what their roles are. Firstly, it is relevant to clarify a define this reports' use of the word 'actor', for the sake of legibility going forward. Within the framework of this project, we are not considering individual users and consumers, but rather the institutions and organizations employing it. By the word 'actor' we are referring to the groups that will be impacted by the transition to quantum safety. This is of course a very large pool of actors, so here are two additional disclaimers. 1) Below we explore the types of transition actors there can be in the transition to QS PKI. Here the word 'actor' refer to all potentially afflicted parties. 2) Further below, we explore a subset of current actor in the transition to QS PKI in relation to the Dutch government. In this part we are referring to the actors in or affiliated with the Dutch Government. Please also note, the subset of actor listed below is not a complete list, but rather a small compilation for the purpose of providing a tangible example.

3.2.1 Identifying actor types

There are multiple ways in which we can choose to perceive the actors in the transition to QS PKIs. Some look through the lens of followers and leaders in the transition. Other distinguish actors according to who will be affected directly and who will be affected indirectly. Another distinguishing lens used is the socio-technical perspective, where actors are categorized according to the relevant labels, such as vendors, developers, regulating bodies, users, etc. However, none of these lenses give a very actionable understanding for actors who will need to transition. While it might provide some understanding at a higher level of abstraction, it does not give them a clear perspective of what their risks are or how urgent it is for them to transition.

When looking to the recent publication of *The PQC Migration Handbook* published by TNO, CWI, and AIVD in March 2023, we can see they argue for the distinction of three types of actor personas in the impending transition. Each category of actors have different needs and therefore a different timeline ahead of them. The three personas are 1) the urgent adopters, 2) regular adopters, and 3) cryptography experts (Attema et al., 2023).

The report proposes the following questions for actors to determine their persona type:

- What infrastructures the organization has which might be prone to the type of attacks a quantum computer can facilitate?
- Which systems does the organization handle and what would the impact of those systems malfunctioning look like?
- What types of data and information at the organization can be considered critical, disclosure sensitive, and have severe consequence if modified unauthorized and undetected?
- How fast does the organization need to transition for the safety of its data and system, considering the store-now-decrypt-later (SNDL) method?
- What is the organizations' dependencies vis-à-vis other organizations in the transition?
- To what extent is it realistic that a malicious actor with access to a quantum computer would target this organization?

Weighing the answers to these questions, actors should be able to infer whether they are an urgent adopter, regular adopter, or cryptography expert as can be seen outlined in Figure 3. The distinguishing elements are that urgent adopters handle sensitive data, provide critical, and/or long-term infrastructures. Regular adopters on the other hand do not manage sensitive data or long-term infrastructures, which are likely to be targeted by someone wielding a quantum computer. They can handle sensitive data, but it is likely that the sensitivity of the data will degrade over time, making it a poor choice for SNDL. Cryptography experts differ entirely on the basis that they are rather the suppliers of cryptographic standards and/or infrastructure. This means, that as experts they most likely already hold the knowledge for their transition within the organization . What distinguishes them is that they are the only one of the three actors also responsible for providing security (cryptography) assets to other organizations.

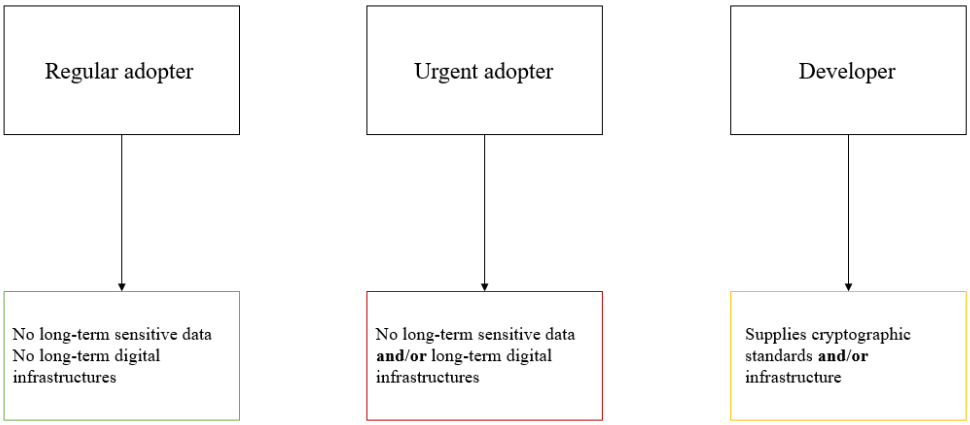

Figure 3: Types of adopters (Attemma et al., 2023)

Being able to identify their adopter type will be a very helpful tool for actors in the transition, as it will give them a clear overview of their own urgency and when it is relevant for them to start moving. Likewise, the identifying questions also give them the opportunity to identify their most critical data assets and infrastructures, which is a very valuable oversight to have irrespective of the transition. Inasmuch, the questions provided above are quite difficult to answer and no one person will be able to answer every question for their organization themselves. Rather it will have to be a collective effort of an organization to find answers for the topics addressed in the questions. While it will then be an effort for an organization to answer all the questions, it will in the end be a worthwhile one.

3.2.2 Subset of actors in relation to the Dutch government

The section above offered some insight on how to distinguish between actors and their respective urgency. This section will explore what these adopters can look like in practice. When looking to the actors represented in Figure 4, we can see a subset of the actors in the transition has been filled in as an example case. These actors outlined in Figure 4 were chosen on the basis of their direct connection to the QS PKI transition in the Netherlands. Thus, looking to Figure 4, this is only an example outline of the QS transition actors. In reality there are many more actors both passively and actively involved in the transition, but it would not have been possible to include them all. The actors presented can all also be placed within the framework of the three adopter types outlined above, with primarily urgent adopters and developers present.

The map proposes three different levels of actors in the transition to QS PKI in the Netherlands. These levels are the macro, meso, and micro levels. At each level, examples of actors in the transitions have been added, however these do not represent the full extent of transition actors in the Netherlands within this topic. At the macro level there are both national and international governing bodies, such as the Ministry of the Interior and of Kingdom Relations (BZK) and the European Commission. At the meso level are the organizations that exist at a link-to-link level. These are the organizations that are providing necessary elements for a successful transition to QS PKI, such as software, hardware, research and developments. As such they are all interlinked and interdependent on each other in the process. The micro level is largely concerned with the organizational implementation and governance of QS PKI. These can be organizations that have a significant interest in initiating their transition as soon as possible in an effort to mitigate risk and disrupt their organization as little as possible.

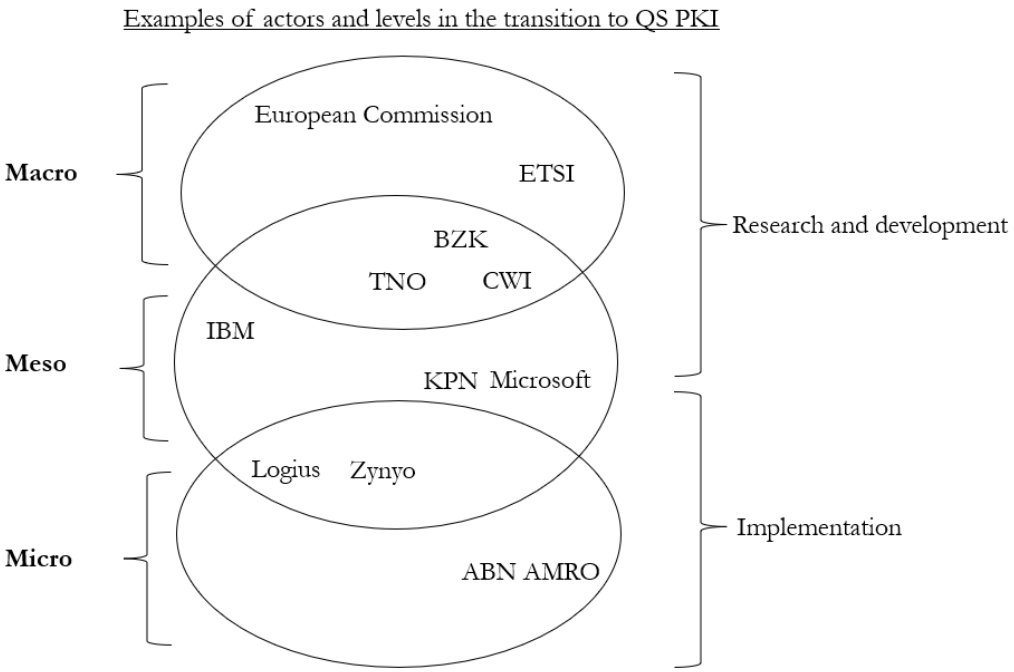

Figure 4: Actor map

Naturally, it can be argued this applies for all future adopters, but for the micro level it is especially relevant to highlight urgent adopters who are at risk, but not in a position to develop solutions themselves. An example of this could be organizations in the banking sector which has large quantities of sensitive user data, as well as a very interactive customer base. The actors in the banking sector can largely considered to be in the high-risk user category. While many of the actors in this sector would technically be able to develop their own solutions within their organization, they are highly dependent on interoperability with other organizations. Not just within the banking sector, but also other sectors, like the government sector. This is why the transition has to be a coordinated effort wherein the approaches offered has been developed with interoperability and agility in mind.

While each sector will have its own sets of needs and requirements, just like each actor will, the impact of the transition will span far beyond a single actor or sector. Present day society is highly reliant on technology and the functionality of our social structures are tied up in digital systems. Without these our core needs as a society would no longer be able to be met. Each major sector connects and impacts each other, both with their actions and inactions. The full extend of the transition to QS PKIs cannot be viewed exclusively through the lens of a singular sector or at a singular level, they all connect and impact one another, which is shown by the overlapping circles in Figure 4. So while the banking sector quite possibly could create and employ their own quantum safe solutions, it would potentially lock them out from their closest collaborative sectors on the national level, as well as impact their business internationally. As such, the banking sector is in a precarious situation as they wait for the necessary solutions to be developed, as are many other urgent adaptors. Therefore it is very important that we begin to prepare for governing the transition at the higher meso and macro levels. At these levels, it now falls to the actors there to ensure that the socio-technical transition mechanisms are in place to support the adopters when the time comes. To initiate this work, we recommend a set of policy guidelines for policy makers to consider in moving forward with preparing for the transition in the next section.

4. Recommendations for policy guidelines to address the challenges

In this section, we will present four suggested policy guidelines that policymakers and legislators can take in addressing these challenges. These guidelines are based on data derived from an expert focus group held in December 2022, wherein experts where asked to rank and comment on different elements of and tools to aid the QS PKI transition. As mentioned in 1.4 Research Approach, the experts were selected based on cross section of four requirements that made them uniquely relevant to discuss this topic.

Upon reviewing the data derived from this expert focus group, it was possible to condense the knowledge into four overarching policy guidelines recommendations, that will be explained further below:

1) Increase collective awareness of QS PKI through social networks.
2) Acknowledge and emphasize the interdependencies in the transition
3) Facilitate the basis for a broader understanding of the technical standards amongst PKI users
4) Increase real-world impact by utilizing use cases to emphasize the consequences of both action and inaction by actors in the transition to QS PKIs (Christiansen et al., 2023).

Collective awareness through social networks:

The transition to QS PKI needs to be actively reliant on collective awareness and utilizing social networks in the process. There are several challenges that would benefit from this approach. It would assist in addressing the transition's need for various stakeholders, perceived lack of awareness, as well as mitigating knowledge gaps amongst transition actors. In cybersecurity systems, knowledge has a tendency to become stratified (Bauer & van Eeten, 2009), but by relying on user networks and creating collective awareness these systems can come to function as knowledge-sharing mechanisms (Pitt et al., 2017). Such mechanisms could play a big role in addressing the above mentioned challenges.

Acknowledging and emphasizing interdependencies:

It is crucial to emphasize the interdependencies in the transition to aid the participants in understanding not just the extent of the transition and its importance, but also to create complete transparency about costs, needs, and potential benefits of the transition. By being transparent about these elements we allow for users to gain a full comprehension of what is needed by them in the transition, which in turn can help address challenges such as a lack of in-house management as users then will be more accurately able to anticipate their own needs for the transition. To that extent, such a policy could also assist in creating further awareness and better users' understanding of the urgencies surrounding the transition.

Better understanding of technical standards for PKI:

The level of technical complexity when it comes to the QS PKIs are high. This contributes to both challenges related to knowledge gaps and complex PKI systems. Thus implementing policies that facilitate a broader and more common understanding of the relevancy of technical standards for PKIs and its providers could potentially aid users in a more successful transition.

Improving impact through use cases:

Lastly, many practical aspects of the transition remain opaque and unclear to users. If policymakers prioritize relying on real-life use cases, many of these uncertainties can be addressed. Furthermore, the impact hereof could be further improved through the combination of use cases that emphasizes both positive and negative scenarios. Through such a tool policymakers can effectively address challenges such as unclear governance, lack of policy guidance, and the ambiguity surrounding ownership and operating institutions.

By taking these recommended policy guidelines into consideration, policymakers can begin to address some of the key challenges in the transition toward QS PKIs. It is pertinent that policymakers step up and take a leading role in the transition, as users look to policymakers for initiating the transition, and by providing users with tangible policy guidance with a strong empirical grounding, users can start to realize the steps of their transition.

5. Conclusion

This report has explored three main questions. Firstly, what are the challenges for the transition mentioned in the literature, secondly, what are the actors types we can identify in the transition towards quantum-safety for Dutch PKI users, and, lastly, what are the recommendations for next steps in the transition.

Firstly, the report explored challenges in the transition in Section 2. Here the report outlined a total of nine challenges in the transition to QS PKIs. These challenges show the diverse range represented in a socio-technical challenge such as this. All the challenges are interconnected in various ways, but also distinguish themselves by highlighting their own unique complication. These are all part of a larger eco-system perspective and are relevant across all levels of the transition.

Secondly, when looking at actor types in the context of transitioning to QS PKI, we can draw three main conclusions. Firstly, governing the transition to QS PKI will be a highly complex task with many different actors involved who all have a unique set of needs and interdependencies. Secondly, we can distinguish between actor types in the transition and their roles as adopters. These adopter types are listed as *regular adopter, urgent adopters*, and *developers.* These types helps clarify the relevant transition for actors, as it lets us identify the most urgent adaptors who should be prioritized first in the transition. Moreover, it also lets us identify regular adaptors who will have more time and leniency in their transition as they are less at risk. Lastly, this report finds that in the Netherlands there are different layers of actors in the transition to QS PKIs. Likewise this section explored the interconnected of the actors across all the levels, by highlighting the chain of interdependencies across actors and levels. Here we emphasized that urgent actors are in an precarious situation as they are unable to make independent moves for quantum safety do to the risk that they will lose compatibility with other actors and sectors, both nationally and internationally. Lastly, we argued that it is up to the policy makers ensure that the necessary transition governance mechanism are in place by the time the actors are ready to migrate.

Lastly, this report recommended four policy guidelines for policymakers moving forward. These emphasized collective awareness and social networks, interdependencies, improving technical understanding, and relying on use cases. Each of these recommendations target multiple challenges identified in the transition and can be used as approaches to address them.

Ultimately, scientist and policymakers must rely on each other to successfully pave the road for this transition. This report has therefore aimed to provide background, practical insight, and recommended further actions, with a special focus on policymakers and legislators. However, this report it suitable for any interested party who wishes to be on the forefront of paving the way toward our quantum-safe future.

Reference list

Accenture Labs. (2018). *Cryptography in a Post-quantum World: Preparing intelligent enterprises now for a secure future*.

Attema, T., Duarte, J. D., Dunning, V., Lequesne, M., Schoot, W. van der, Stevens, M., & AIVD Cryptologists & Security Advisors (Eds.). (2023). *PQC Migration Handbook*. TNO, CWI, AIVD. https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10–11), 706–719. https://doi.org/10.1016/j.telpol.2009.09.001

Buchholz, S., Mariani, J., Routh, A., Keyal, A., & Kishnani, P. (2020). *The realist's guide to quantum technology and national security: What nontechnical government leaders can do today to be ready for tomorrow's quantum world*.

CCC. (2019). *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility*. Computing Community Consortium.

Chen, L., & Moody, D. (2020). New mission and opportunity for mathematics researchers: Cryptography in the quantum era. *Advances in Mathematics of Communications*, *14*(1), 161–169. https://doi.org/10.3934/amc.2020013

Choi, C. (2022). *An IBM Quantum Computer Will Soon Pass the 1,000-Qubit Mark*. IEEE Spectrum. https://spectrum.ieee.org/ibm-condor

Christiansen, L., Bharosa, N., & Janssen, M. (2023). *Policy guidelines to facilitate collective action towards quantum-safety*. 7. https://doi.org/10.1145/3598469.3598480

CSIRO. (2021). *The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography*.

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*.

ETSI. (2015). *Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges*.

Gillard, S., David, D. P., Mermoud, A., & Maillart, T. (2022). *Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats* (arXiv:2206.15055). arXiv. https://doi.org/10.48550/arXiv.2206.15055

Grimes, R. A. (2019). *Cryptography apocalypse: Preparing for the day when quantum computing breaks today's crypto*. John Wiley & Sons Inc.

Grote, O., Ahrens, A., & Benavente-Peces, C. (2019). *Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques*.

Housen-Couriel, D. (2022). Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace. In S. J. Shackelford, F. Douzet, & C. Ankersen (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781108954341

ISARA. (2018). *Enabling Quantum-Safe Migration with Crypto-Agile Certificates*.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), Article 7909. https://doi.org/10.1038/s41586-022-04623-2

Kong, I. (2022). Transitioning Towards Quantum-Safe Government: Examining Stages of Growth Models for Quantum-Safe Public Key Infrastructure Systems. *15th International Conference on Theory and Practice of Electronic Governance*, 499–503. https://doi.org/10.1145/3560107.3560182

Kong, I., Janssen, M., & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government. *DG.O 2022: The 23rd Annual International Conference on Digital Government Research*, 282–292. https://doi.org/10.1145/3543434.3543644

Lewis, A. (2017). *The impact of quantum technologies on the EU's policies: Part 1 Quantum Time*. https://doi.org/10.2760/832942

Lewis, A. M., & Travagnin, M. (2018). *The Impact of Quantum Technology on the EU's Policies Part 2: Quantum Communications from Science to Policies*. European Commission.

Lindsay, J. R. (2020a). Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. *Security Studies*, *29*(2), 335–361. https://doi.org/10.1080/09636412.2020.1722853

Lindsay, J. R. (2020b). Surviving the Quantum Cryptocalypse. *Strategic Studies Quarterly*, *14*(2), 49–73.

Lovic, V. (2020). *Quantum Key Distribution: Advantages, Challenges and Policy*. https://www.repository.cam.ac.uk/handle/1810/311529

Ma, C., Colon, L., Dera, J., Rashidi, B., & Garg, V. (2021). CARAF: Crypto Agility Risk Assessment Framework. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab013

Macaulay, T., & Henderson, R. (2019). *Cryptographic Agility in Practice: Emerging User-Cases*. InfoSec Global.

Mashatan, A., & Heintzman, D. (2021). The Complex Path to Quantum Resistance: Is your organization prepared? *Queue*, *19*(2), 65–92. https://doi.org/10.1145/3466132.3466779

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & for the PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ*, *339*(jul21 1), b2535–b2535. https://doi.org/10.1136/bmj.b2535

Mosca, M. (2015). *Cybersecurity in an era with quantum computers: Will we be ready?*

Mulholland, J., Mosca, M., & Braun, J. (2017). The Day the Cryptography Dies. *IEEE Security & Privacy*, *15*, 14–21. https://doi.org/10.1109/MSP.2017.3151325

Niederhagen, D. R., & Waidner, M. (2017). *Practical Post-Quantum Cryptography*.

NIST. (2018). *The Economic Impacts of the Advanced Encryption Standard, 1996 - 2017*.

NIST. (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*.

Pitt, J., Ober, J., & Diaconescu, A. (2017). Knowledge Management Processes and Design Principles for Self-Governing Socio-Technical Systems. *2017 IEEE 2nd International Workshops*

on Foundations and Applications of Self Systems (FAS*W)*, 97–102. https://doi.org/10.1109/FAS-W.2017.127
Rasanen, M., Makynen, H., Mottonen, M., & Goetz, J. (2021). Path to European quantum unicorns. *EPJ Quantum Technol*, *8*(1), 5. https://doi.org/10.1140/epjqt/s40507-021-00095-x
Rodriguez, A. (2023). *A quantum cybersecurity agenda for Europe: Governing the transition to post-quantum cryptography* (EUROPE'S POLITICAL ECONOMY PROGRAMME). European Policy Centre.
The Hague Security Delta. (2019). *Understanding the Strategic and Technical Significance of Technology for Security: Implications of Quantum Computing within the Cybersecurity Domain*.
Tibbetts, J. (2019). *Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decision Makers*. UC Berkeley.
TNO. (2020). *Migration to Quantum-safe Cryptography: About Making Decisions on When, What and How to Migrate to a Quantum-safe situation*.
Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*, *19*(4), 241–246. https://doi.org/10.1007/s10676-017-9429-1
Vermeer, M. J. D., & Peet, E. D. (2020). *Securing Communications in the Quantum Communications in the Quantum Computing Age: Managing the Risks to Encryption*. RAND Corporation.