Challenges in the Transition towards a Quantum-safe Government

Kong, Ini; Janssen, Marijn; Bharosa, Nitesh

DOI
10.1145/3543434.3543644

Publication date
2022

Document Version
Final published version

Published in
Proceedings of the 23rd Annual International Conference on Digital Government Research

Citation (APA)
Kong, I., Janssen, M., & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government. In L. Hagen, M. Solvak, & S. Hwang (Eds.), *Proceedings of the 23rd Annual International Conference on Digital Government Research: Intelligent Technologies, Governments and Citizens, DGO 2022* (pp. 282-292). Article 82 (ACM International Conference Proceeding Series). ACM. https://doi.org/10.1145/3543434.3543644

Challenges in the Transition towards a Quantum-safe Government

Ini, I, Kong
Faculty of Technology, Policy, and Management, Delft University of Technology
i.kong@tudelft.nl

Marijn, M, Janssen
Faculty of Technology, Policy, and Management, Delft University of Technology
m.f.w.h.a.janssen@tudelft.nl

Nitesh, N, Bharosa
Faculty of Technology, Policy, and Management, Delft University of Technology
n.bharosa@tudelft.nl

ABSTRACT

The computation power of quantum computers introduces new security threats in Public Key Infrastructure (PKI), a system used by many governments to secure their digital public services and communication. This calls for an inevitable need for governments to be quantum-safe (QS) by modifying their PKI systems to be resistant to the attacks of quantum computers. However, there is limited academic literature on a QS PKI system, and in this limited literature, the transition challenges are perceived as exclusively technological. This paper aims to create a structured overview of challenges when transitioning to a QS PKI system. We do this by reviewing literature and classifying the challenges using Technology-Organization-Environment (TOE) framework and using an expert workshop to explore the challenges in the context of the PKI system in the Dutch government. The main challenges in the technological context include no universal QS solution, legacy system, complex PKI interoperability, and vulnerable Root CA. The main challenges in the organizational context include knowledge gap, unclear governance, lack of urgency, and in-house management support. Furthermore, the main challenges in the environmental context include institutional void, stakeholder collaboration, lack of awareness, and policy guidance. The results indicate that the QS transition from the current PKI system is complex, and the challenges are socio-technical. For policy-makers, this implies that they should start early to prepare, whereas organizations are hardly aware of the process of QS transition and the topic of quantum computing is yet to develop the urgency in organizations.

CCS CONCEPTS

• **General and reference** → Document types; General conference proceedings.

KEYWORDS

Quantum-Safe Government, Post Quantum Cryptography, Public organization, Public Key Infrastructure transition challenges, Systematic

dg.o 2022, June 15–17, 2022, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-9749-0/22/06.
https://doi.org/10.1145/3543434.3543644

ACM Reference Format:
Ini, I, Kong, Marijn, M, Janssen, and Nitesh, N, Bharosa. 2022. Challenges in the Transition towards a Quantum-safe Government. In *DG.O 2022: The 23rd Annual International Conference on Digital Government Research (dg.o 2022), June 15–17, 2022, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3543434.3543644

1 INTRODUCTION

In the light of a rapidly developing digital society, governments increasingly provide electronic public services using a Public Key Infrastructure (PKI). Although it is not always obvious to users and policy-makers, the facilitation of electronic identification schemes and secure communication and information exchange in PKI depends on asymmetric cryptography [16, 52]. The asymmetric cryptography, also known as Public Key Cryptography (PKC), verifies digital identities for electronic government services using digital certificates and ensures confidentiality and integrity of communication by preventing unauthorized parties from accessing or manipulating the data [1]. The use of PKC schemes not only protects citizens' communication and personal data against cybercrime but also strengthens the process of managing, validating, and authenticating digital identities without requiring the physical presence of individuals [2-4].

The studies have indicated that the introduction of quantum computers will potentially break widely-used key encryption schemes (eg. using Shor's algorithm and Grover's algorithm), including previously mentioned PKI schemes [5, 6]. This means that PKI system will become obsolete and no longer provide secure electronic government services [7]. Although a large-scale quantum computer is not yet available, recent research breakthroughs published in Nature (eg. [8-10]) show that the development of quantum computers has been steadily advancing over the last decade. Notably, IBM has announced that a series of larger quantum computers will be delivered by 2023, paving the way for the real-world manufacturing and application of quantum computers [11]. In order to secure electronic services and communication against quantum computers, studies are calling attention to the risk of quantum computing and the need to become quantum-safe (QS) by modifying current PKC schemes in the PKI system [7, 12-14].

A deeper understanding of the challenges in transitioning towards a quantum-safe (QS) PKI system may provide us with important insights into QS transition. However, there is no structured overview of the challenges when transitioning from the current PKI system to the one that is quantum-safe. Prior literature on a QS PKI system largely focuses on technological challenges by addressing the limitation of a legacy system and the development of QS cryptographic algorithms [15-20]. By identifying different challenges

using Technology-Organization-Environment (TOE) framework, the paper provides an overview of complex challenges involved in the QS transition from the current PKI system. In doing so, the paper contributes in, namely, i) identifying relevant challenges that organizations may encounter and prioritize, ii) providing research and practical implication for the QS transition, and iii) suggesting areas for further research.

The structure of the paper is as follows: section two lays the foundational basis of current PKI systems and the need to move to a QS PKI system. In section three, the research methodology used in this paper is presented. This is followed by section four, which provides the list of challenges found in the literature review and examination of the results gathered from the workshop discussion. The paper is then concluded in section five with an overview of the results, limitations, and directions for future research.

2 BACKGROUND

This section highlights the foundational basis of current PKI systems and addresses the need to move to a QS PKI system to safeguard against quantum-computing-based threats.

2.1 Public Key Infrastructure (PKI)

PKI systems are widely used for securing digital services and information exchange. With a combination of hardware, software, security policies, and encryption mechanisms, the security framework of PKI generates, stores, distributes and manages digital certificate practices [2-4]. The digital certificates act as digital passports and guarantee the identity among the parties involved in the transactions over public networks, such as the Internet [14, 17].

To manage these digital certificates, there are several important components in the PKI system. The registration authority (RA) first needs to verify the identity of a certificate requester before Certificate Authority (CA) can issue and revoke the digital certificates [4, 21]. Thus, when RA successfully identifies the requesters, RA assures CA that the identity is checked and digital certificates can be issued. After the certificate is digitally signed by CA, it is issued and placed into a repository where certificate registers can access it [4, 22]. The digitally signed certificate from CA ensures authentication, integrity, and non-repudiation in the PKI system [23, 24].

The CAs in the PKI system are tied to Root Certification Authority (Root CA) which has the highest authority. In technical terms, PKI ensures the trustworthiness of all certificates that are issued from the CAs through a chain of trust [4]. In non-technical terms, CAs are chained together to form a certification path from Root CA. Several intermediate CAs can be created under the Root CA, and the following certificates that were issued by these intermediate CAs are trusted in the lower-level CA [3]. Thus, if Root CA is compromised, the entire certification path can no longer guarantee secure communication, confidentiality, authentication, and integrity of information [23].

Moreover, the digital certificates in the PKI system are created with digital signatures and Public Key Cryptography (PKC). The PKC uses a key pair, including one public key that must be verifiably authentic and one private key that must remain private [2, 24]. The large enough key sizes in encryption can differentiate the decryption time for those who have the key versus those who do not. The foundational basis of digital certificates lies in PKC, and the strength of PKC determines the secure environment of PKI. The most widely known PKC schemes are Rivest-Sharmir-Adleman (RSA), Diffie-Hellmann key exchange (DHKE), and Elliptic Curve Cryptography (ECC) [25].

2.2 Quantum Threat to PKI

With the existing traditional computers, it is under the assumption that modern PKC schemes seem to be secure [26]. As the pace of quantum research continues to accelerate, unfortunately, these are no longer safeguarded for two reasons. On the one hand, quantum computing works in a different physical mechanism that has the potential to perform computations much more quickly than classical computers. On the other hand, the threat of quantum computing can occur even today without having a large-scale quantum computer ready due to the store now-decrypt later attack [27].

To elaborate on the first point, the RSA encryption scheme uses the difficulty in factoring a key pair of a large prime number to ensure security against third parties who are unauthorized to find the secret key [3]. Although this is true for classical computers, quantum computing can bypass this time-consuming process and enable a key extraction algorithm for the decryption key using a method called Shor's Algorithm [5]. For other encryption schemes that are not prone to Shor's Algorithm, the need for an extensive brute-force search applies. However, these can still break with a different method called Grover's Algorithm. It offers a shortcut by allowing quantum computers to speed up this search process. Thus, Grover's Algorithm allows the search of a given size amounts to the time proportional to the square root of that size [6, 28].

With new advancements in quantum research, it is only a matter of time before the quantum computer becomes superior to a classical computer in one stage or another [29]. In 2019, Google and the KTH Royal Institute of Technology in Sweden further highlighted a breakthrough that it may be possible to break a 2048-bit RSA integer using a 20 million qubit computer in only 8 hours [30]. Thus, it comes with no surprise that further development will rapidly shorten the amount of time it takes to break modern PKC.

To continue on the second point, the threat of quantum computing can occur even before having a large-scale quantum computer. This is possible because any data that is under the vulnerable PKC schemes in the current PKI system can be under the attack Store Now, Decrypt Later [27]. Thus, the longer the data that needs to remain secure, the more susceptible it is to the attack because it will be exposed to the threat of getting harvested, stored, and decrypted later once the quantum computers become available. Even if the advanced quantum future may be years away, organizations need to begin the QS transition planning in current PKI systems as soon as possible [31].

2.3 Post Quantum Cryptography & Quantum Key Distribution: Two Solution Directions

There are various motivations across academia, industries, and governments to develop secure alternatives for current PKCs that are resistant to quantum attacks (for instance, from unfriendly

states and hacking groups). Two main areas for quantum-safe cryptography include (a) Post Quantum Cryptography (PQC) and (b) Quantum Key Distribution (QKD).

After its first workshop in 2015, the US National Institute of Standards and Technology (NIST) is currently working to find new cryptographic solutions and standards for QS PKI. The promising candidates of PQC are code-based cryptosystems, lattice-based encryption, and hash-based digital signatures [31, 32]. Although this paper does not specifically go in-depth in addressing the differences in each cryptography, it is worth noting that PQC already holds an advanced level of the theoretical ground, and it is known to fit well into existing IT infrastructures without making immense changes [33]. However, limitations still exist in the long key sizes, which may become a problem for providing an efficient system because it would take much processing time and high price for commercial usage [13].

On the other hand, QKD uses the rules of quantum mechanics of quantum bits, also known as qubits [34]. These have properties of superposition can that represent 0 and 1 simultaneously, and entanglement, where the state of one entangled particle can alter the state of all entangled particles [27, 35]. Thus, using the quantum properties in cryptography, it would be possible to detect whether the information has been corrupted and intercepted. However, additional research is needed to overcome research constraints in its distance, key generation rate, and practical application of QKD [26, 33]. To implement QKD, a quantum infrastructure is necessary, but it would result in high costs of delicate equipment [36, 37].

Although both solution directions hold appealing properties that are promising, different limitations exist in terms of optimization and performance [31]. Further research is taking place in order to identify many distributed computing scenarios, usage contexts, and hardware-based security schemes to better substitute existing algorithms [27, 29, 48].

2.4 Quantum-safe PKI Transition

The EU's Cybersecurity Strategy presented in 2020 aims to promote secure, trustworthy digital technologies and provide an impetus for cyber defense capabilities [38]. In addition to the development and application of new technologies, the strategy addresses a secure digitalization with solutions and standards of cybersecurity [39]. The topic of quantum computing was discussed next to AI and EU 5G, and the European Council expressed that there is a need for strong encryption to protect digital security and fundamental rights. However, the discussion at the EU level on quantum computing is only beginning to emerge and the organizations both in the public and private sectors still heavily rely on the previously constructed PKI system, which may still take several years to adopt and implement.

Moreover, for long-term information that needs to remain secure, it is crucial to assess the vulnerability by calculating the amount of time it would take to achieve quantum-resistance. According to Mosca [14], there are three factors to consider when assessing the quantum risk: X, Y, and Z. The X refer to the security of shelf-life, which is the time the information must remain confidential. The Y is the transition time, and the Z is the collapse time when the quantum computer is realized [14, 40]. If the time X and Y take longer than the time Z, the system will no longer be safeguarded and is susceptible to quantum-computing based threats (e.g., store now and decrypt later). Thus, the transition of the current PKI system to the one that is quantum-safe should be planned as soon as possible to prevent the potential damages.

In addition, determining the transition time for organizations would need to consider multiple factors, including the organization's cryptographic assets, vulnerability, crypto agility, and the transition budget [40]. However, the complexity of PKI transition is not often discussed, and it is described to be exclusively technical. The transition of a QS PKI system needs to take place in the entire organization so that organizations can implement QS cryptography as a solution. From the technical perspective, the latter may largely depend on the IT team's expertise and training, but the former is beyond what the organization's IT team can achieve.

3 RESEARCH METHOD

The following research questions have been formulated to identify and understand challenges in transiting to a QS PKI system.

Research Question 1: What challenges are mentioned in the literature in transitioning to a QS PKI system?

Research Question 2: What challenges are considered important and urgent for the Dutch government to transit to a QS PKI system?

Due to limited understanding of the challenges faced in the transition process toward a QS PKI system, the first research question is formulated to give an overview of challenges found in the literature when transitioning from the current PKI system to the one that is quantum-safe. The second research question builds up on the list of challenges found in the literature from the first research question to give a more in-depth understanding of the challenges faced by the Dutch government. We selected an example of the PKI system in the context of the Dutch government (eg. PKIoverheid) because 1. It provides an example of a public organization as a frontrunner in the PKI system 2. It facilitates the infrastructure with diverse stakeholders, including individuals, businesses, and other government agencies. 3. It is currently looking to transit towards a QS PKI system. We employed two research instruments to answer the above questions: (a) systematic literature review and (b) workshop discussion.

3.1 Systematic Literature Review

The systematic literature review (SLR) is a process-oriented research method that reviews the previous work on the relevant research topic and provides new research directions. The more literature acquired, the more imperative it is to interpret and understand the diverse findings from the literature [41].

Following the guidelines by Kitchenham and Charters [42], the systematic literature review was conducted by 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". The literature was identified using search engines: Scopus, SpringerLink, ScienceDirect, Google Scholar, and Mendeley. Then, it was sorted from the year 2010 to 2021 to gather up-to-date literature on the topic of challenges associated with the transition to a QS PKI system. Since the academic

Table 1: List of Participants in the Workshop

Participant	Role	Organization
1	Manager of PKIgovernment	Government Agency
2	Consultant	Research Institution
3	PKI Expert	Tech Industry
4	Entrepreneur/ PKI Expert	Tech Industry
5	Researcher	Academic Institution
6	Researcher	Academic Institution

Table 2: Workshop Overview

Session	Duration	Theme
Introduction	3 min	-Quantum-safe PKI challenges & Workshop objectives
List of Challenges & SLR process	5 min	-24 challenges found in the literature
Part 1: Challenges & their importance	5 min	-Identifying four most important challenges in each context
Break	5 min	
Discussion	10 min	-Open discussion: list of 12 important challenges
Part 2: Challenges & their urgency	5 min	-Identifying three most urgent challenges from the list
Discussion	15 min	-Open discussion: Three challenges that are important & urgent
Closing	2 min	-Follow up

literature was not sufficiently rich, white papers, expert reports, and conference proceedings found on Mendeley were added to provide more details on this topic of research.

Overall, the literature search resulted in 2266 articles. After screening the title and abstract of each paper, 154 articles were chosen. Then 19 duplicate articles were excluded, and the remaining 135 articles were all read. Furthermore, 93 irrelevant articles were excluded with several additional criteria: (a) 23 articles were not about quantum computing, (b) 44 articles were not about QS PKI, and (c) 26 articles were not about QS PKI challenge. Thus, 42 relevant articles (including 11 academic literature and 31 grey literature) were selected for the review.

3.2 Workshop Discussion

To further refine the list of challenges found in the literature on the current PKI system, an interactive workshop was included in this paper. The workshop provides an interactive session with participants to discuss an issue or question [43]. This process allows the workshop to be optimized as a research method to collect data and create an environment for collaboration by extending the discussions outside the literature and sharing insights from the organization level. Due to the early-stage nature of the problem, the number of persons with expertise solely on QS-PKI was limited. The six participants in the workshop discussion included PKI experts, consultants, and researchers. The 50-minute workshop took place on 2-November, 2021, and the list of the six participants is shown in Table 1.

The overview of the workshop is shown in Table 2. The discussion in the workshop was supported by using an interactive tool called 'Mentimeter' (http://www.mentimeter.com).

For part 1 of the workshop, the participants used Mentimeter to rate each challenge from 1 (not important) to 5 (most important). Then, the four challenges in each context with the highest rate of importance were selected. For part 2 of the workshop, the participants used Mentimeter to choose three urgent challenges from the list of challenges developed in part 1 of the workshop and identified the challenges that are both important and urgent.

4 RESULTS

Section 4 is divided into 4.1 and 4.2. In section 4.1, we present the results of our systematic literature review. We do this by first explaining the framework used and providing a descriptive overview of the challenges found in the selected literature. In section 4.2, we present the discussion from the workshop about challenges that are considered important and urgent in the context of the PKI system in the Dutch government.

4.1 Long List of Challenges Found in Literature

To cluster the challenges found in the literature, the TOE framework was adopted. This is because TOE framework provides a multi-perspective view that focuses on technology implementation at an organizational level rather than an individual level [44]. Moreover, the inclusion of factors in technological, organizational, and environmental context bring an advantage when understanding a diverse set of challenges (technical or non-technical) that can emerge within and outside organizations.

The TOE framework shows that the implementation process of technology is influenced by three different contexts: Technological, Organizational, and Environmental [45]:

Technological Context: refers to the relevant technologies in the enterprise, including existing, company-related tools and emerging technologies.

Table 3: Overview of the challenges in Technological Context

Challenges in Technological Context	References
Incompatible Legacy System	[33], [46], [47], [48], [49], [50], [51], [52], [53]
Not-yet achieved standards from NIST	[31], [50], [52], [54], [55], [56]
No universal QS algorithm	[13], [31], [52], [53], [56], [57]
Implementation flaws and side-channel attacks	[48], [55], [54], [58]
Lack of reliability in QS cryptography	[46], [52], [53], [58], [59], [60]
Vulnerable Root CA	[46], [55], [61], [62], [58], [63]
Complex PKI system & interoperability	[31], [46], [50], [51], [52], [53], [56], [58], [64]
Cost of Transition	[40], [46], [53], [60], [61], [65], [66], [67]

Organizational Context: refers to the organizational characteristics including size, management structure complexity, quality of its human resources, and domestic slack resources.

Environmental Context: refers to the space where an organization carries out its activities, including participants and the administration. It is outside of an organization, which has restrictions and prospects for a high-tech revolution.

Technological Context: The list of challenges towards a QS PKI system from the literature is shown in Table 3.

- Incompatible Legacy system

Two main approaches to achieving QS cryptography are available: Post-quantum cryptography (PQC) and Quantum Key Distribution (QKD) [33]. In order to ensure the same level of protection in the legacy systems, however, more research is needed [48, 49]. Also, it is unclear how hardware and/ or software can be upgraded in the existing system and when these would be available for devices that have been operating with pre-quantum cryptographic algorithms [50-53]. While PQC may not need new infrastructure, QKD requires quantum infrastructure. With the latter approach, practical compatibility with legacy systems remains a bigger concern [46, 47].

- Not-yet achieved NIST standards

The standardization can bolster the use of cryptography and maximize interoperability [55]. The international standard can facilitate the widespread implementation of cryptography that is resistant to quantum-computing threats. In 2016, the National Institute for Standards and Technology (NIST) began a process to select practical standards and parameter guidelines for QS cryptography (eg. PQC) [31, 50, 54]. However, the process is not yet completed. The suitable alternatives to today's widely deployed algorithms still require further analysis, and algorithm characteristics are open to debate [52, 56].

- No Universal QS algorithm

There is relatively little chance that a single QS cryptographic algorithm will be selected as a replacement [13]. This is because different algorithms offer different trade-offs in key sizes and computing requirements which may affect compatibility in application devices and usage contexts [31, 52, 56]. Thus, NIST is looking to provide several alternatives (eg. PQC) within the new QS cryptographic standards. However, if too many protocols are accepted in QS standard, the complexity will result in slow transition, and additional interoperability challenges across organizations may arise [53, 57].

- Implementation Flaws & Side-Channel Attacks

The changes in the PKI system can lead to implementation flaws and side-channel attacks [58]. These include fault injection attacks, side-channel cryptanalysis, and physical cryptanalysis [54]. It is crucial to analyze how PQC algorithm functions in the interfaces offered by libraries, protocols, and hardware. The introduction to new patterns of memory usage, failure modes, and timing can expose vulnerabilities in addition to cryptographic weakness [48, 55]. Thus, it is crucial to maintain a controlled QS transition process in the PKI system to avoid any possible implementation flaws.

- Lack of reliability in QS cryptography

Not only is the standardization process of QS cryptographic algorithms currently being developed from NIST, it would also take years for new algorithms to be able to substitute existing algorithms [46, 60]. There is currently no widespread real-world use of QS cryptography, and it has yet to stand the test of time to prove its reliability and robustness [52]. Thus, new cryptography may still result in vulnerabilities being overlooked [53, 58]. Even if the standardization is complete, the newly introduced algorithms will need to be fully deployed into security systems and be accepted in organizations [59].

- Vulnerable Root CA

The Root CA creates a certification path for every certificate issued across the organization's environment. The transition to a QS PKI system also requires Root CA to be updated [58, 63]. For end-entities, a root certificate must guarantee the authenticity and validity of the certification. Thus, if your Root CA is compromised, your intermediate CAs and the key management of PKI are also no longer safe [55, 61, 62]. It is crucial that Root CA remains secure when migrating to a new system since it is difficult to detect malicious issuance once CA breaches occur and multiple fraudulent certificates are already issued [46].

- Complex PKI system & Interoperability

QS cryptographic algorithm cannot be replaced with a simple 'drop-in' method [31, 56]. This is because PKI systems have a chain of dependencies that extend to standards bodies, hardware providers, and third-party software, which may also include third-party component libraries [46, 50, 52, 53]. To enable secure and correct communication, changes in cryptographic algorithms must

Table 4: Overview of the challenges in Organizational Context

Challenges in Organizational Context	References
Lack of Urgency	[37], [40], [49], [53], [60]
Knowledge Gaps in quantum computing	[12], [40], [52], [54], [58], [67], [68]
No one-size-fits-all transition process	[13], [31], [40], [51], [52], [56], [63], [67], [69]
Lack of Crypto-Agility	[31], [48], [58], [60], [63], [64], [67], [70]
Lack of In-house management support	[14], [33], [52], [65], [71]
Unclear QS transition benefits & business case	[14], [29], [33], [51], [53]
No technical skills & qualified personnel	[40], [51], [65], [72]
Unclear QS governance: not knowing how to facilitate	[12], [31], [33], [47], [48], [51], [54]

be the same or compatible [51, 58]. The devices need to be upgraded accordingly; otherwise, they cannot guarantee the security of newly adopted cryptography [64].

- Cost of Transition

The new selection of QS cryptography may need changes in software, and hardware in the existing PKI system. Depending on the availability of resources and assets, the cost will also vary among organizations [40, 46, 67]. If the organization requires new software and upgrades in hardware for new standards, then it is inevitable that the transition will result in high costs [53, 65]. Moreover, In the absence of established QS alternatives, the solution may be to deploy hybrid solutions, and using hybrid certificates schemes could double the cost on the server infrastructure as it requires management of two systems and two certificates or more [61, 67].

Organizational Context: The list of challenges towards a QS PKI system from the literature is shown in Table 4.

- Lack of Urgency

Although it is estimated that a full QS transition of the current PKI system is a decade-long process, many organizations currently do not have the urgency to transit [37, 40, 49]. This is because the arrival of a large-scale quantum computer is perceived to be decades away, and many do not recognize the near-term threat of "store now and decrypt later" [60]. In addition, there is uncertainty in organizations to fully commit to the selection of QS cryptographic algorithms when standards are still being developed [53]. Without a collective sense of urgency, it is difficult to achieve inter-agency coordination and collaborations for a QS PKI system.

- Knowledge Gaps in Quantum Computing

Poorly understood quantum computing may delay organizations from transitioning to a QS PKI system [52, 54]. Quantum theory is often framed as something inexplicable and even difficult for physicists to fully grasp the concept. Thus, explaining the threat of the technology to other stakeholders who are not in the field is much more challenging [12, 58, 68]. When organizations do not have prior knowledge, they risk not taking timely action and resulting in fragmented solutions with unforeseen vulnerabilities [40, 67]..

- No One-Size-Fits-All Transition Process

The cryptographic assets and areas that will potentially be vulnerable to quantum computers need to be identified [40, 63]. The time and strategy needed to transit from the current PKI system would vary across organizations [13]. The transition process would depend on a selection of QS cryptographic algorithms, the lifespan of technology in the current PKI system, resources, and the capacity available [52, 69]. Also, different QS cryptographic algorithms will have different trade-offs in the performance outcomes [31, 56]. Thus, there is no direct one-way QS transition process, and the organizations need to review the constraints of their assets and the operational environment [51, 67].

- Lack of Crypto-Agility

Rapid adaptation of new cryptographic primitives and algorithms is difficult without making changes to the current PKI system, including key sizes, signature sizes, error handling properties, and key establishment processes [31, 58, 70]. Unfortunately, many protocols were not designed with cryptographic agility in mind. The established PKI system is rigid and resource-constrained to only support a handful of algorithms [60, 67]. It is essential to build crypto-agility so that a system becomes more flexible and scalable [48, 63, 64]. Lack of crypto-agility hinders organizations from responding and updating its system when vulnerabilities are discovered.

- Lack of In-House Management Support

The lack of drive to mitigate against quantum threats from the upper management can slow the process of QS PKI transition. Without the support of transition initiatives within the industry, it is difficult for organizations to realize the needs and requirements to change their existing infrastructure [52, 71]. It is crucial for organizations to develop a tactical roadmap and have a coherent policy that supports different teams in the organization to guide the process [33, 65]. Thus, without such a support system, it is difficult for organizations to put a high priority on driving the QS transition from the current PKI system [14].

- Unclear QS Transition Benefits & Business Case

Most people in the organization outside of the IT team are generally unaware of issues surrounding quantum computing- based-threats. The organizational leadership and budget controllers need to be first convinced that there are potential risks, and QS transition offers business benefits and opportunities [14, 51, 53]. Due to a limited use case of the QS cryptographic algorithm, organizations find it challenging to develop a business case to enter long-term QS transition commitment [29]. The activities related to QS transition may still remain in the areas of R&D programs, and its practical application will still be delayed [33].

- No Technical Skills & Qualified Personnel

Table 5: Overview of the challenges in Environmental Context

Challenges in Environmental Context	References
Low level of Investment in EU	[29], [52], [73], [74], [75]
Lack of awareness	[12], [37], [40], [53], [58], [60]
No clear ownership & operating institution	[12], [31], [49], [67], [76]
Different interpretation of QS PKI system (scenarios)	[31], [56], [68], [69], [77]
Lack of policy guidance	[33], [37], [59], [74], [75], [76], [78]
Various Stakeholders: Need for collaboration	[12], [33], [52], [53], [57], [73]
Legal Issues (eg. Laws & Legislation)	[54], [67], [69], [78]
Bureaucratic process (eg. ICT standards & regulations)	[58], [74], [76]

QS cryptographic schemes are relatively new and challenging even for cryptographic experts. To carry out a successful QS transition, educating qualified personnel and refining the relevant knowledge are crucial [40, 51]. Reportedly, most cryptographers work for the NSA, other government agencies, or in academia. There are only a few commercial cryptographers, and they are mostly employed by large multi-national corporations [65]. If organizations do not meet have the necessary expertise to fully execute the QS transition, they may only rely on external third parties or not at all.

- Unclear QS Governance: Not knowing how to facilitate

The research on QS cryptographic algorithms will need to be applied in a real-world environment outside the research labs [12]. However, there is no inventory in organizations to facilitate updates in infrastructure and related protocols to QS solutions [31, 51]. Organizations often do not know their entire cryptographic asset and vulnerabilities. Thus, it is difficult to assess where and with what priority the QS alternatives should be implemented [33, 47]. This calls for a high degree of decision-making, coordination and leadership efforts [33, 49].

Environmental Context: The list of challenges towards a QS PKI system from the literature is shown in Table 5.

- Low Level of Investment

There is no clear scope on how secure the quantum computing technology will be and when will quantum computing markets be profitable [29]. The investment returns for the technology will only be visible in the long run, and it is viewed that the development of quantum computing remains premature [74, 75]. The EU-based companies are not patenting enough and are lagging behind the global trend in capital investments in quantum technology [73]. Moreover, for the companies that require short-term security needs, it would be difficult to incentivize the early implementation of QS solutions and ensure that the investments have the desired impact [29, 52].

- Lack of Awareness

There is a lack of awareness of quantum computing and the threats associated with the technology. Without recognizing the issue, it is difficult to execute operational changes and security requirements needed for quantum protection [40]. In public, the risks surrounding quantum computing are largely ignored and mostly focused on its unique opportunities for scaling industry advantages [37, 58, 60]. It is crucial to create awareness so that organizations can draw up transition plans and recognize the amount of lead-time needed to make changes in their security products and infrastructure [53].

- No Clear Ownership & Operating Institution

The PKI system is known to be a technology used by all but owned by none. When organizations deploy PKI systems, they do not operate in isolation [12]. Under a complex system integration, any alterations in technological infrastructure would require actors to negotiate and coordinate problems [76]. Thus, the organizations do not have complete control over their PKI systems and require multiple stakeholders in the operating model. However, it is difficult to define the ownership of PKI systems, and its boundaries blur the extent to which organizations should initiate and take responsibility for facilitating the QS transition from the current PKI system [31, 49].

- Different Interpretations of QS PKI system

The emerging technology comes with great uncertainty and indeterminacy. For quantum computing technology, it makes room for multiple interpretations, measurements, and forecasts of QS solutions [77]. The current framing of quantum theory is yet to be presented with a straightforward meaning and interpretation [68]. With new, promising QS algorithms being presented every year, many competing solutions offer various trade-offs in the current PKI system. Unfortunately, multiple interpretations of what it means to be quantum-safe create too much noise when trying to find fit-for-purpose QS architectures necessary for organizations [31, 56, 77].

- Lack of Policy Guidance

The topic of quantum computing is not yet among the popular topics of discussion in the European Parliament [60]. The low awareness and magnitude of risks require an updated framework to account for quantum-computer-based threats and proactive policy-maker leadership [37, 76]. The right incentives through procurement policy or early adoption programs can help stimulate business cases, encourage QS transition and user engagement [33, 74, 78]. The lack of legislation and government regulations on quantum computing provides no compliance for organizations to enforce operational changes and security implementations to become quantum-resistant [14, 59, 75].

- Need for Collaboration: Various Stakeholders

Designing a cryptographic algorithm is very complex and requires knowledge in multiple sciences and engineering fields in

applied cryptography and system security [52, 57]. Moreover, transitioning to a QS PKI system requires collaboration on many levels [33]. There are varying interests and needs in government standards bodies, software solution providers, hardware vendors, service providers, international consortiums, and PKI users [52]. Thus, collaboration among various stakeholders is needed to establish well-coordinated contingency planning in the QS transition [53, 57, 73].

- Legal Issues

The facilitation of the PKI system requires several legal issues, including privacy legislation, regulations on qualified digital signatures, and NIS directive that ensures the security of network and information systems [75, 78]. The entities that process private data or offer qualified signatures are required by law to protect against state-of-the-art attacks [54]. Although these are not specified in the detailed procedures of the PKI system, the laws provide jurisdiction to ensure regulatory requirements and secure identity management [67]. Thus, legal issues need to be updated and comply with a QS PKI system and its new QS cryptographic algorithms [69].

- Bureaucratic Process

In the EU, governments play a greater role in the elaboration of PKI standards and regulations when compared to the U.S. [74, 76]. This makes it difficult to adapt the New Approach strategy to the development of ICT standards as the process is much slower and formal. While the laws and regulations can also be prescriptive to the technological change, these still require the process of auditing against standards and regulations, identification of risks or threats, and mitigation steps [58]. The bureaucratic process in adopting QS standards and its regulations adds an extra timeline to the transition. Any uncertainty in QS solutions would raise additional regulatory problems and delay the process [58, 76].

4.2 Workshop Discussion: Dutch PKI government

This section further discusses the challenges found in the selected literature in the context of the PKI system in the Dutch government. The public organizations that provide digital services to citizens, businesses, and government agencies are no exception to the quantum-computer-based threats.

The system of PKIoverheid, also known as PKIgovernment, is the PKI system in the Dutch government [79]. The system enables confidential electronic communications through email, websites, and secure information exchange with the use of the electronic signature and remote identification [80]. In order to transit towards a QS PKI system, the current PKIoverheid also needs to be modified, and QS transition needs to be planned. While the responsibility of the policy and strategy for PKIoverheid lies with the Ministry of the Interior and Kingdom Relations (BZK), the tactical management lies with Logius, which acts as Policy Authority (PA) [81].

For part 1 of the workshop, four challenges with the highest importance in each context were selected. For technological context, the important challenges include no universal QS solution, legacy system, complex PKI interoperability, and vulnerable Root CA. For organizational context, knowledge gap, unclear governance, lack of urgency, and in-house management support are identified as important challenges. For environmental context, the important challenges include institutional void, need for stakeholder collaboration, and lack of awareness and policy guidance.

For part 2 of the workshop, a newly selected list of 12 challenges from part 1 was used to further analyze the challenges that are considered both important and urgent in PKIoverheid. The participants each voted for three urgent challenges among 12 challenges. The three important and urgent challenges that were selected are lack of awareness, vulnerable Root CA, and unclear QS governance. The following paragraphs elaborate on these challenges in the context of PKIoverheid, and the discussion extends three policy recommendations that can be addressed in public organizations.

- Policy Recommendation 1: Boost awareness

One of the important and urgent challenges when transitioning to a QS PKI system was a lack of awareness. Although the implementation of eGovernment is a shared responsibility of all government organizations, the policy to develop and manage the information infrastructure is executed by Government ICT unit (ICTU) and Logius [81]. The discussion from the workshop indicated that the topics on quantum computing-based threats are only beginning to emerge in the public domain and the knowledge on how to transition toward a QS PKI system remains premature. Accordingly, most academic research on QS transition is mainly technical, and other non-technical challenges are often discussed by external third-party industries. The participants agreed that organizations would have difficulty realizing the urgency of the problem without being aware of the situation of what quantum computing-based threats are.

The discussion also pointed out that there is no clear set of identified risks or assessments available for Logius to measure the extent to which public organizations could be affected by quantum computing technology. Logius may need to determine its inventory and recognize its cryptographic assets and vulnerability. In addition, the general public is more steered into thinking about quantum advantages rather than focusing on issues created by quantum technology. With the perception of non-urgency regarding quantum computing technology, industries may prioritize scaling business opportunities for quantum advantage over addressing the need to achieve quantum protection. Thus, this may put the public organization in a first-mover position to create awareness for such threats associated with quantum computing technology and raise the urgency for various stakeholders.

- Policy Recommendation 2: Maintain a secure Root CA at all times

A vulnerable root CA was a second important and urgent challenge when transitioning to a QS PKI system. The workshop participants showed that the difference of PKIoverheid exists in the Root CA. Unlike other PKI systems, the Ministry of the Interior and Kingdom Relations (BZK) provides the Root of the PKIoverheid [80]. The discussion also pointed out that Logius, as Policy Authority (PA), needs to manage government-wide ICT solutions and is accountable for providing secure PKIoverheid to users, including individuals, businesses, and other government agencies. Thus, having a vulnerable Root CA is considered fatal for the continuity of many digital government services.

The discussion from the workshop indicated that the transition to a QS PKI system would be meaningless for Logius if Root CA

is compromised and no longer safe to provide root certificates to intermediate CAs and, ultimately, to end-users. The compromised PKI system will be disastrous to the entire digital services offered by public organizations, and all personal data will become vulnerable. The participants shared the view that incidents of data breaches are not only costly to fix but also would violate the promise that government holds to its citizens to regulate data protection under the Personal Data Protection Act (Wet Bescherming Persoonsgegevens, Wbp). Thus, it is crucial for the public organization to maintain secure Root CA in both tt current PKI system and during the process of QS PKI transition.

- Policy Recommendation 3: Establish a clear QS governance

Another important and urgent challnge when transitioning to a QS PKI system was an unclear QS governance. According to workshop participants, the governance in PKIoverheid is complex, and several frameworks (eg ETSI standards framework and eIDAS regulation) ensure that the digital public services operate accordingly and maintain interoperability with various devices, hardware, and software systems. Also, the Programme of Requirements (PoR) that is drawn up by Logius in consultation with the Ministry serves an important purpose for PKIoverheid. The PoR act as a basis for CA admission for external third-parties CAs in order to ensure the statement of compliance. The certificates that are issued from the qualified CAs are registered and checked by Radio Communications Agency (Agentschap Telecom) [79, 80].

The discussion pointed out that although PKIoverheid conforms to multiple standards and regulations, there is no clear governance established that can facilitate QS transition. This was considered to be problematic because the anatomy of PKIoverheid is already complex, and changes in the infrastructure would need to provide system interoperability and backward compatibility in order to function with multiple devices and applications. The participants were uncertain whether additional changes in PKIoverheid would require changes in hardware, software, and other parts of the legacy system. However, they also indicated that since Logius currently has no protocol to follow when modifying the current PKIoverheid, public organizations not only need to look at where and how to modify changes in the PKI system but also need to establish a set of guidelines with relevant stakeholders to coordinate the process of QS PKI transition.

5 CONCLUSION AND FURTHER RESEARCH

Due to the computation power of quantum computing technology and its store now, decrypt later attack, public organizations that rely on PKI systems can no longer provide electronic identification schemes and secure communication and information exchange. There is an inevitable need for public organizations to become quantum-safe by modifying their PKI systems. This paper is the first to systematically explore the challenges in transitioning to a QS PKI system that is resistant to the threats posed by quantum computing. Based on the results from a systematic literature review and workshop discussion, we present a first exploration of the challenges that may be encountered and prioritized when transitioning the current PKI system. The majority of research on the QS PKI transition is mostly taking place in industries, and academic research on the topic has only just begun.

Furthermore, the workshop discussion on PKIoverheid provides the first analysis of challenges faced by public organizations. The discussion showed that challenges in QS transition are diverse and must be tackled in concert. The modification in one part of the PKI system may require changes in other parts of the system. Thus, the challenges may need to be addressed in parallel, and the QS PKI transition requires collaboration among various stakeholders for well-coordinated and contingency planning. The main challenges in the technological context include no universal QS solution, legacy system, complex PKI interoperability, and vulnerable Root CA. In the organizational context, the lack of knowledge, unclear governance, lack of urgency, and in-house management support are identified as the main challenges. In the environmental context, the main challenges include institutional void, need for stakeholder collaboration, and lack of awareness and policy guidance.

In addition, this paper presents a call to action for policy-makers to prepare for these challenges and take part in shaping the QS PKI transition. The three important and urgent challenges for PKIoverheid are lack of awareness, vulnerable Root CA, and unclear QS governance. While public organizations must maintain the security of Root CA at all times, the urgency for quantum computing technology in organizations is yet to develop, and they are hardly aware of the process of QS transition. Thus, the results indicate that the QS transition from the current PKI system is complex, and the challenges are socio-technical. For policy-makers, this implies that they should start early to prepare for the QS transition.

5.1 Limitations and future research directions

We conclude this paper with some limitations and directions for further research. First, six participants in the workshop discussion is a small number. More participants from PKIoverheid and cryptographic experts in public organizations could have extended the knowledge with new ideas and opinions on the QS PKI transition. Second, the workshop discussion was held in the context of the PKI system in the Dutch government, and this presents a geographical limitation. Thus, examining the PKI system in a different context would provide more clarity and in-depth analysis of challenges faced in public organizations.

Moreover, the paper offers a useful starting point for future research in the development of a QS PKI system in public organizations. The topic of QS cryptographic algorithm remains a concept that is relevant to cryptographers and IT teams in the organization. However, it builds an essential foundation for our secure digital communication and information exchange. Since the topic of QS transition is relatively new, perhaps it would also be beneficial to conduct another literature review in the future to track more details on the advancement of a QS PKI system. The topic of QS PKI transition would provide vast opportunities for researchers to contribute their research in the public domain.

Despite the hype around quantum advantage, there needs to be an awareness of quantum protection. Who can raise awareness? How can such awareness be raised? Since the topic of QS transition is not yet a popular topic of discussion, the urgency of the issue has not been raised. Thus, an approach is necessary to create awareness in government, industries, and citizens. Perhaps, this may also link to future research on laws and regulations related to quantum

computing technology and how it can provide incentives to set up an environment that drives the QS PKI transition.

Public organizations need to transit from the current PKI system to one that is quantum-resistant. This brings a lot of uncertainties and issues surrounding the topic and raises questions such as what needs to be changed in the current PKI system to become quantum-resistant? Which QS solution is compatible with which PKI system? Accordingly, we need to assess the impact of quantum-computing-based risks and determine trade-offs of different QS solutions for different organizations. This requires a clear understanding of QS solutions and how the current PKI system is organized in the public domain.

Additionally, it is still unclear how the QS governance should be established. How can various stakeholders collaborate in the process of QS transition? Who needs to be included, and who makes the decision? Since the topic of QS PKI transition in academic research has just begun, there is no clear guidance available that can help facilitate the transition in public organizations. Thus, these governance challenges need to be raised in public organizations to further support the QS transition process from the current PKI system.

ACKNOWLEDGMENTS

This publication is part of the HAPKIDO research project with project number NWA.1215.18.002 of the research programme Cybersecurity, which is (partly) financed by the Dutch Research Council (NWO).

REFERENCES

[1] Baheer, B.A., D. Lamas, and S. Sousa, A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and Prospects. Administrative Sciences, 2020. 10(2).
[2] Hunt, R., Technological Infrastructure for PKI and Digital Certification. Computer Communications, 2001. 24: p. 1460-1471.
[3] Linn, J., Trust Models and Management in Public-Key Infrastructures. 2000.
[4] Bharosa, N., *et al.*, Challegning the Chain: Governing the automated exchange and processing of business information. 2015: Logius & Thauris.
[5] Shor, P.W., Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer. 1994.
[6] Grover, L.K., A fast quantum mechanical algorithm for database search. 1996.
[7] de Wolf, R., The potential impact of quantum computers on society. Ethics and Information Technology, 2017. 19(4): p. 271-276.
[8] Noiri, A., *et al.*, Fast universal quantum gate above the fault-tolerance threshold in silicon. Nature, 2022. 601(7893): p. 338-342.
[9] Amadori, A., J.D. Duarte, and G. Spini, Literature Overview of Public-Key Infrastructures, with Focus on Quantum-Safe Variants Deliverable 4.1, HAPKIDO Project. 2022, TNO.
[10] Mądzik, M.T., *et al.*, Precision tomography of a three-qubit donor quantum processor in silicon. Nature, 2022. 601(7893): p. 348-353.
[11] IBM, The Quantum Decade. 2021, IBM.
[12] Mulholland, J., M. Mosca, and J. Braun, The Day the Cryptography Dies. IEEE Security & Privacy, 2017: p. 14-21.
[13] NIST, Report on Post-Quantum Cryptography, L. Chen, *et al.*, Editors. 2016.
[14] Mosca, M., Cybersecurity in an era with quantum computers: will we be ready? 2015.
[15] Broadbent, A. and C. Schaffner, Quantum cryptography beyond quantum key distribution. Des Codes Cryptogr, 2016. 78(1): p. 351-382.
[16] Mailloux, L.O., C.D. Lewis II, and C. Riggs. Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. 2016.
[17] Bindel, N., *et al.*, Transitioning to a Quantum-Resistant Public Key Infrastructure. 2017.
[18] Barker, W., M. Souppaya, and W. Newhouse, Migration to Post-Quantum Cryptography. 2021.
[19] Panhwar, M.A., *et al.*, Quantum Cryptography: A way of Improving Security of Information. International Journal of Mathematics and Computer Science, 2021. 16(1): p. 9-21.
[20] Sikeridis, D., P. Kampanakis, and M. Devetsikiotis, Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH, in Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies. 2020, Association for Computing Machinery: Barcelona, Spain. p. 149–156.
[21] Burr, W.E. and K.L. Lyons-Burke, Public Key Infrastructures for the Financial Services Industry. 1999.
[22] Huang, J. and D.M. Nicol, An anatomy of trust in public key infrastructure. International Journal of Critical Infrastructures, 2017. 13(2/3).
[23] Al-Riyami, S.S. and K.G. Paterson. Certificateless Public Key Cryptography. 2003. Berlin, Heidelberg: Springer Berlin Heidelberg.
[24] Adams, C. and S. Lloyd, Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations. 1999: Macmillan Technical Publishing.
[25] Paar, C. and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. . 2010: Springer-Verlag Berlin Heidelberg.
[26] Yunakovsky, S.E., *et al.*, Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. EPJ Quantum Technology, 2021. 8(1).
[27] Mavroeidis, V., *et al.*, The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications„ 2018.
[28] Mandviwalla, A., K. Ohshiro, and B. Ji. Implementing Grover's Algorithm on the IBM Quantum Computers. in 2018 IEEE International Conference on Big Data (Big Data). 2018.
[29] Ménard, A., *et al.*, A game plan for quantum computing. 2020, Mckinsey & Company.
[30] Gidney, C. and M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits? 2021.
[31] NIST, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. 2021.
[32] Bernstein, D.J. and T. Lange, Post-quantum cryptography. Nature, 2017. 549(7671): p. 188-194.
[33] TheHagueSecurityDelta, Understanding the Strategic and Technical Significance of Technology for SecurityImplications of Quantum Computing within the Cybersecurity Domain Together. 2019.
[34] Hong, K.-W., O.-M. Foong, and T.-J. Low, Challenges in Quantum Key Distribution, in Proceedings of the 4th International Conference on Information and Network Security - ICINS '16. 2016. p. 29-33.
[35] Gibney, E., The Quantum Gold Rush. 2019.
[36] Accenture, In Quantum We Trust. 2020.
[37] Lovic, V., Quantum Key Distribution: Advantages, Challenges and Policy. Cambridge Journal of Science and Policy, 2020. 1(2).
[38] EuropeanCommission, EU Security Union Strategy. 2020.
[39] EuropeanCommission, The Cybersecurity Strategy. 2021.
[40] TNO, Migration to Quantum-Safe Cryptography: About Making Decisions on When, What and How to Migrate to a Quantum-Safe Situation. 2020.
[41] Boell, S.K. and D. Cecez-Kecmanovic, A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches. Communications of the Association for Information Systems, 2014. 34.
[42] Kitchenham, B. and S.M. Charters, Guidelines for performing Systematic Literature Reviews in Software Engineering. 2007.
[43] Inmark, E., Concept and methodology of Interactive Workshops. 2010.
[44] Baker, J., The Technology–Organization–Environment Framework. Information Systems Theory, 2011: p. 231-245.
[45] Tornatzky, L.G., Fleischer, M. & Chakrabarti, A. K., The Processes of Technological Innovation. 1990, Lexington, Mass.: Lexington Books.
[46] ISARA, Enabling Quantum-Safe Migration with Crypto-Agile Certificates. 2018.
[47] Machatan, A. and D. Heintzman, The Complex Path to Quantum Resistance. 2021.
[48] Wiesmaier, A., *et al.*, On PQC Migration and Crypto-Agility. 2021.
[49] Lindsay, J.R., Surviving the Quantum Cryptocalypse. 2020b.
[50] AccentureLabs, Cryptography in a Postquantum World:: Preparing Intelligent Enterprises Now. 2018.
[51] CSIRO, The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography. 2021, Australia's National Science Agency.
[52] CCC, Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. 2019, Computing Community Consortium
[53] Vermeer, M.J.D. and E.D. Peet, Securing Communications in the Quantum Computing Age: Making the risks to encryption. 2020.
[54] Niederhagen, R. and M. Waidner, Practical Post-Quantum Cryptography. 2017, Fraunhofer Institute for Secure Information Technology.
[55] Menezes, A. and D. Stebila, Challenges in Cryptography. IEEE Security & Privacy, 2021. 19(2): p. 70-73.
[56] ENISA, Post-Quantum Cryptography: Current state and quantum mitigation. 2021, European Union Agency for Cyber Security.
[57] Chen, L. and D. Moody, New mission and opportunity for mathematics researchers: cryptography in the quantum era. Advances in Mathematics of Communications, 2020. 14(1): p. 161-169.
[58] Macaulay, T. and R. Henderson, Cryptographic Agility in Practice: Emerging Use-Cases. 2019.

[59] Tibbetts, J., Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers. 2019, Lawrence Livermore National Laboratory: Center for Global Security Research.
[60] ETSI, Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. 2015.
[61] Thales, Upgrading Existing Security Systems to Agile Quantum-Safe with SafeNet Luna HSMs and SafeNet High Speed Encryptors. 2019.
[62] Sjöberg, M., Post-quantum algorithms for digital signing in Public Key Infrastructures. 2017.
[63] ETSI, CYBER; Migration strategies and recommendations to Quantum Safe schemes. 2020.
[64] Grote, O., A. Ahrens, and C. Benavente-Peces, Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques, in Proceedings of the 9th International Conference on Pervasive and Embedded Computing and Communication Systems. 2019. p. 91-98.
[65] NIST, The Economic Impacts of the Advanced Encryption standard, 1996–2017. 2018.
[66] Petrenko, K., A. Mashatan, and F. Shirazi, Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. Journal of Information Security and Applications, 2019. 46: p. 151-163.
[67] Ma, C., *et al.*, CARAF: Crypto Agility Risk Assessment Framework. Journal of Cybersecurity, 2021. 7(1).
[68] Vermaas, P.E., The Societal Impact of the Emerging Quantum Technologies: A Renewed Urgency to Make Quantum Theory Understandable. Ethics and Information Technology, 2017. 19(4): p. 241-246.
[69] ETSI, Quantum Safe Cryptography; Case Studies and Deployment Scenario. 2017.
[70] Mehrez, H.A. and O.E. Omri, The Crypto-Agility Properties. 2018.
[71] Buchholz, S., *et al.*, 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. 2020, Deloitte Insights.
[72] Peterssen, G., Quantum technology impact: the necessary workforce for developing quantum software. 2020.
[73] Räsänen, M., *et al.*, Path to European quantum unicorns. EPJ Quantum Technol, 2021. 8(1): p. 5.
[74] Lewis, A.M. and M. Travagnin, The Impact of Quantum Technologies on the EU's future policies: Part 2 Quantum communications: from science to policies. 2018, European Commission.
[75] Lewis, A.M., *et al.*, The Impact of Quantum Technologies on the EU's future policies: Part 3 Perspectives for Quantum Computing. 2018, EU Commission.
[76] Lindsay, J.R., Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. Security Studies, 2020a. 29(2): p. 335-361.
[77] Smith, F.L., Quantum technology hype and national security. Security Dialogue, 2020. 51(5): p. 499-516.
[78] Lewis, A.M., The Impact of Quantum Technologies on the EU's future policies: Part 1 Quantum Time. 2017, European Commission.
[79] Logius, Certification Practice Statement (CPS): Policy Authority PKIoverheid for Private Root CA certificates to be issued by the Policy Authority of the PKI for the Dutch government. 2020.
[80] Innovalor, PKIoverheid: Onderzoek naar mogelijkheden om gebruik te vergroten bijvoorbeeld via verplichtstelling. 2019.
[81] EuropeanCommission, Digital Government Factsheet 2019: The Netherlands. 2019.