HAPKIDO

Work package 3 – Deliverable 3.3

Quantum Safe Public Key Infrastructure transition – applicability of existing (IT) governance models

Olivier Rikken, Lærke Christiansen, Marijn Janssen & Nitesh Bharosa

Summary

The Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations (HAPKIDO) project aims to develop a roadmap for the transition to quantum-safe Public Key Infrastructures (PKIs). The transition demands that organizations collectively tackle technical challenges, as well as governance challenges. Previous HAPKIDO deliverables (e.g. D3.1 – Governance Challenges) describe the governance challenges in detail. Examples include complex PKI systems and interoperability, the perceived lack of urgency, knowledge gaps in the impact of quantum computing on PKI, the progression of quantum computing, lack of in-house management support, and the unclear ownership and operating institution. As part of the HAPDKIDO deliverables, this report zooms in on the applicability of IT Governance models for dealing with these governance challenges. The objective is to evaluate the applicability of governance mechanisms provided in the literature for facilitating the transition towards Quantum Safe (QS) PKI. Attention was given to how the governance mechanisms can strengthen each other, and how system dynamics models should be developed to understand their interdependencies.

For this research, a mix of two research instruments was used. First, a systematic literature review has been performed. The second instrument was conducting interviews with 10 actors involved in various positions as stakeholders within the QS PKI transition. The interviews were semi-structured, with fixed questions, but there was also room for elaboration.

The findings indicate that the governance of the transition can be set up using a wide range of mechanisms and tools on various levels. Some mechanisms, like subsidies and clear set deadlines for implementation, can provide transition incentives for an organization. Other mechanisms, like expertise centers, standards, and assessment tools, will eventually create incentives for transitioning to QS PKI as a result of a more complex interplay of governance mechanisms, which in themselves also can and should have reinforcing feedback mechanisms.

We identified 3 primary governance levels for PKI ecosystems regarding the QS PKI transitions: the micro, meso, and macro levels, which all play their role in the transition. Governance mechanisms differ per level, and their needs change over time. The set of governance mechanisms presented in this report can be used to select the appropriate ones given the circumstances and the operating level. It is important to first conduct a risk assessment of the infrastructure, and actions need to be set in motion to initiate this multi-actor transition process.

The most important recommendation is to acknowledge that this transition is not just an IT project, but covers many elements (technical and non-technical) on multiple layers and cannot be managed out of one organization, using one governance theory, and should be the result of collective action and should be adaptive to changing circumstances.

Contents

1. Introduction and background

The year 2025 is proclaimed as the international year of quantum science and technology by the United Nations as it marks the 100th year since the development of quantum mechanics[1]. The discovery of quantum mechanics has revolutionized our understanding of physics and kickstarted many technological advancements. One of these advancements is the quantum computer, significantly increasing the speed of certain calculations, making calculations possible that conventional computers cannot reach in the near future. This can lead to vast opportunities in various fields of research, but it can also lead to risks in current technological infrastructures, including serious risks in the field of cybersecurity.

Especially Public Key Infrastructures (PKIs), a crucial element in our current digital infrastructure, are prone to no longer adhering to acceptable levels of security. The extremely high integration of PKI in all our digital infrastructures and digital economy will lead to profound business continuity risks, national security risks and privacy risks at all levels of society.

1.1 Current developments in Quantum Computing, the need for transition and challenges

The development of quantum computing is going at an unprecedented rate. In 2021, the 100 Qubit barrier was breached, and in 2022, IBM reported the 433-qubit processor and at the end of 2023 reached 1121 qubits, with the expectation to quadruple that amount in 2025 (Choi, 2022). Current projections even scale to 1 million physical qubits around 2030 with thousands of logical qubits[2]. This could mean the current 2048-bit RSA can be broken (Datacard, 2019). Recent developments indicate an ever-accelerating pace of developments in quantum computing[3]. Although there are more factors than just the number of qubits influencing the availability of a quantum computer being able to break current levels of cryptography, they are progressing to a state where cryptography can be broken. A detailed discussion on this exact progress is out of scope of this deliverable, although the absence of and uncertainty around an exact Q date (the day a quantum computer is available that can break current PKI systems) is very highly relevant for this research and the transition process challenges.

Many developments have already started to ensure that, once quantum computers are large and stable enough to be able to compromise current asymmetric public-private key cryptography, we will have the availability of a Quantum-Safe Public Key Infrastructure (QS PKI). Not least, the current release of three new Post-Quantum Cryptography (PQC) algorithms (and more on the way) by the US standardization organization NIST[4] that should now be tested by organizations to look at the effectiveness against the quantum threat. Also, a recently launched handbook provides guidelines for migration to post-quantum cryptography (AIVD, CWI, & TNO, 2024). In many cases, the expectation is that a QS PKI in the near future will rely on a hybrid architecture, meaning that classical cryptographic algorithms are used in combination with PQC algorithms. The required or preferred combination of algorithms is expected to vary based on the installed based and the business processes.

[1] https://quantum2025.org/en/

[2] https://quantumcomputingreport.com/2024-the-year-of-quantum-computing-roadmaps/#:~:text=New%20Roadmaps,qubits%20with%2040%2C000%20physical%20qubits.

[3] https://www.reuters.com/technology/google-says-it-has-cracked-quantum-computing-challenge-with-new-chip-2024-12-09/

[4] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

The transition towards QS PKI – based on PQC standards alone or hybrid architectures – does come with a wide range of socio-technical challenges. As a result of the complexity of the ecosystem(s) in which PKI operates and is managed, combined with the unpredictable timelines of the availability of a quantum computer able to break current cryptography standards, the transition should not be underestimated. It should commence even sooner than one might expect. Threats like store-now-decrypt-later (SNDL), meaning that if encrypted data gets stolen now and can be decrypted as soon as a quantum computer capable of doing so is available, demand higher transition speed (Csenkey & Bindel, 2023; Mosca, 2018). Besides the SNDL threat, there are even more potential operational issues that increase the necessity of immediate action on the QS PKI transition:

> *"Timelines are diffuse, but not only from store-now decrypt later perspective, sometimes practical, e.g., satellites need to be prepared to be capable for the update, this needs to be done now" (Respondent 6 - R6).*

A previous report of the HAPKIDO program identified the following nine challenges in the transition towards QS PKI (Christiansen, Kong, & Bharosa, 2023);

1) complex PKI system and interoperability,
2) perceived lack of urgency,
3) knowledge gaps in quantum computing,
4) lack of in-house management support,
5) unclear QS governance,
6) perceived lack of awareness,
7) no clear ownership and operating institution,
8) lack of policy guidance and
9) need for various stakeholders.

This report builds on previous HAPKIDO reports and deliverables and focuses, amongst others, on the suitability of current governance theories for the QS PKI transition. According to the literature and various experts interviewed for this research, it should not be seen as a regular PKI update:

> *Although it can be seen as a socio-technical project, it is not as straightforward as upgrading from SHA1 to SHA2. E.g., technically different, solutions not there yet, and the uncertainty of the solution is a big difference" (R7).*

> *"Size and the high level of integration in structures make it significantly more complex to facilitate this than a previous PKI update or even the initial setup of the PKI system. Due to the dependency on the PKI systems for digital trust in combination with high-levels of integration in critical processes in our day-to-day lives, it is also not acceptable that the maturity level falls back from e.g. level 8 pre-QS PKI to a lower level post-QS PKI" (R9).*

> *"Much more complex (than the original PKI implementations), (PKI) has become a commodity, like water from the tap" (R10).*

1.2 Objective and structure

As stated in the previous section, the transition to quantum-safe cryptography will be crucial for various cybersecurity reasons. As this transition eventually entails an upgrade of both hardware and software as well as certain security algorithms, one could argue that common IT governance theory principles would be sufficient for the management of the transition from the current PKI to a quantum-safe PKI system.

The objective of this research is to evaluate the applicability of governance mechanisms provided in the literature for facilitating the transition towards QS PKI. Attention is given to how the governance mechanisms can strengthen each other, and a system dynamics model will be developed to understand its interdependencies.

1.3 Research questions

This research focuses on the following research questions in order to reach the objective as stated above:

1) Are existing IT governance theories and mechanisms sufficient for managing the QS PKI transition?
2) What other governance theories and mechanisms could be applicable in managing the QS PKI transition?
3) What would be concrete recommendations regarding the use of mechanisms and tooling to manage the QS PKI transition?

This report is structured as follows. Section two discusses the research approach. Section 3 of this report elaborates on (IT) governance in general and the potential relevance of various theories on the QS PKI transition. In section four, we combine findings regarding the PKI ecosystem, governance theories, and tooling for the governance of a QS PKI transition framework. We also include a brief analysis of analogies of complex transition processes and lessons learned that can be reused in the context of a QS PKI transition. This section also presents the interdependencies of the governance mechanisms and their system dynamics. Section five presents the conclusions of our research, and section six contains various recommendations.

2. Research approach

This research builds on a mix of two research instruments. First, a literature review has been performed. Due to the novelty of the subject and research, the literature was gathered in multiple ways. First, a query search was performed using Google Scholar. The search was done on the keywords: "Quantum (Safe) Cryptography Governance" "Governance of complex IT systems", "Post Quantum Governance" and "Quantum Safe Cryptography and Security". As this is a novel field, also keywords: "IT Governance", "AI governance" or "Commons Governance" were used. Based on the literature found in the query search, we then used the snowballing method, gathering additional research based on the references of the queried literature (Lecy & Beatty, 2012). Finally, we included literature based on the recommendations of various people interviewed. Using a hybrid search strategy (Mourão et al., 2020), we gathered as much relevant literature as possible, whereas literature on QS PKI transition governance is scarce. This resulted in a mix of scientific literature and grey literature.[5]. The results were screened in multiple rounds based on the PRISMA approach (Moher, Liberati, Tetzlaff, & Altman, 2009).

1) Search (based on the keywords described above)
2) Screening title and abstract
3) Screening introduction and conclusion
4) Inclusion in the study

The second instrument was interviews with various actors involved as stakeholders within the QS PKI transition. The interviews were semi-structured, with fixed questions, but there was room for elaboration. A total of 13 questions were addressed, covering questions related to PKI ecosystem characteristics, IT governance theory suitability, analogies to other transitions, and related questions. The interview transcripts were shared with the interviewees for review to provide the opportunity to correct any misinterpretation by the interviewer or add additional comments when deemed fit. The results per interview were not shared with other interviewees to ensure that the questions were not influenced by the answers or input of others. The interviewees were a cross-section from industry, research, and governmental organizations and are all either experts or policy-makers or both in the quantum and/or Public Key Infrastructures field. Table 1 provides an overview of the interview respondents.

Table 1: interview respondents

#	Role	Organizational type
1	Scientist	University (NL)
2	Scientist	University (NL)
3	Director	PKI Industry Service/Product Provider
4	Policy maker	Governmental Institution
5	Policy maker	Governmental Institution
6	Expert	Research Institution
7	Scientist	University (NL)
8	Expert	Research Institution
9	Director	Governmental Institution
10	Expert	Government Implementation Organization

A total of 10 interviews were conducted. The outcomes of the research have been aggregated in the various sections of this report.

[5] Literature created outside the traditional scientific channels, e.g., NIST standards, PQC Migration guidelines and previous HAPKIDO study reports.

3. (IT) Governance

3.1 What is governance

Governance is a broad term that can be approached from various angles and has many descriptions. The applicability of specific governance approaches can depend on the characteristics of the governed system or ecosystem. It can vary from the governance of governments and politics on various levels (Fukuyama, 2013; Grant & Keohane, 2005), to corporate governance (Baker & Anderson, 2010), commons governance (Dietz, Ostrom, & Stern, 2017; E. Ostrom, 1990), data governance (Marijn Janssen & Kuk, 2016; Rosenbaum, 2010) or IT governance (De Haes & Van Grembergen, 2009; P. Weill, 2004; Peter Weill & Ross, 2005; Peter Weill & Ross, 2004) or combinations thereof (M. Janssen & Joha, 2007; Klievink, Bharosa, & Tan, 2016).

Although there are several initial papers and handbooks addressing challenges and recommendations regarding quantum-safe transitions (AIVD et al., 2024; Kong, Janssen, & Bharosa, 2024a, 2024c), the literature on the governance of QS PKI transition is limited (Csenkey & Bindel, 2023; Perrier, 2022), especially in the analysis of the suitability of existing (IT) governance theories. The existing literature suggests that governance of the quantum threat exceeds purely IT governance, which the majority of the interviewees agree with.

In order to analyze the latter, the characteristics of the PKI landscape and elements related to the QS PKI transition were first analyzed.

3.2 PKI ecosystem in relation to governance of transition to QS PKI

Based on the literature study and the interviews, the PKI system is described not as a single system with a single owner or management structure, but as an ecosystem of various parties that jointly form the PKI (eco)system. Furthermore, it is clear that, although they often work based on the same open source technology, procedures and standards, there is no single one PKI system, but a wide range of PKI systems, often organized within sectors such as PKI overheid, within the banking sector, the telecom sector or military sector. Even within a sector, various systems can co-exist.

Certain ecosystems are open, meaning there are no specific boundaries for participation nor specific ownership, whereas others are closed. This characteristic influences the way the ecosystem can be governed. The interviewees generally describe the PKI (eco)system as mixed, open, and closed, depending on the specific PKI system and/or element. The PKI (eco)system is often described as open from a user perspective, a science perspective, and a standards perspective. However, a strictly closed system does exist as well on user levels. Furthermore, it is stated that from a technical supplier perspective, although the ideas are open, there can be multiple barriers to entry.

Regarding the organization of PKI (eco)systems, although there are also differences between the different systems, as stated above, there is no single ownership and thus governance accountability and responsibility. In general, there is no single or overarching authority in control. It is a socio-technical system involving many actors, from standardization bodies like NIST and ESTA, to governance and authorization parties like certificate, verifying, and registration authorities, and technology providers joining various collaboration and advocacy organizations like the CA/browser forum and end users. As one of the respondents stated:

> *"There are interdependencies on others, you cannot do it on your own. There is no one orchestrating party." (R9)*

It thus should be seen as a self-organizing mechanism where, in the system as a whole, there is no overarching party in charge of the governance of the whole system or with an overarching authority.

However, there are various actors that the interviewees mentioned as being more dominant by nature. The Big Tech and browser parties, like Google, Amazon, Microsoft, and Mozilla, were mentioned multiple times in this context. Also, the standardization bodies, specifically NIST, were mentioned as one of the naturally more dominant parties in the ecosystem. Within the Dutch context of PKI Overheid, Logius was also mentioned multiple times. Although these parties were seen as more or even most powerful in this context, as stated before, none of them have absolute governance power.

> *"It is continuous consensus between the parties involved, so more of a self-organizing ecosystem" (R7)*

When looking at PKI as a product or service, the majority of the interviewees indicated that this could be seen as a public (digital) good or common good. Commons or public goods can be defined as "one which is not subject to exclusion and is subject to jointness in its consumption or use" (V. Ostrom & Ostrom, 1979, p. 7). One of the respondents would even go as far as classifying it as a commodity. All interviewees and the literature state that it is indispensable in secure digital environments.

> *PKI has become a commodity, like water from the tap. (R10)*

The products of the PKI system are predominately defined as infinite in theory, although in certain situations, there is a certain scarcity, not so much from the theoretical amount of keys that can be made, but more so from a process perspective that various procedures that ensure the high trust level a safety do not scale easily and thus in a practical sense results into a limited supply.

In many ways, the PKI (eco)systems are systems that supersede organizations, industries, and even nations. As stated, it is a largely self-governing system with many different parties involved. As one of the interviewees stated:

> *On the basis, it is a global ecosystem. However, we need to make agreements at international, national, and lower levels. (R5)*

As such, we can identify multiple layers that apply to the governance of the organizations involved and the ecosystem as a whole. Both the literature and the interviewees mentioned various levels. Levels range from individual organizations, to international standardization institutions, to nation governments (Csenkey & Bindel, 2023; Kong et al., 2024a; Perrier, 2022). The earlier part of the HAPKIDO research already identified three levels: the macro, meso and micro, with different primary focuses on either research and development or implementation (Christiansen et al., 2023). All these levels play a crucial role in various aspects. As such, we also distinguish these levels and their interdependencies from a governance perspective, but within these levels, we identify certain sub-groups as displayed below.

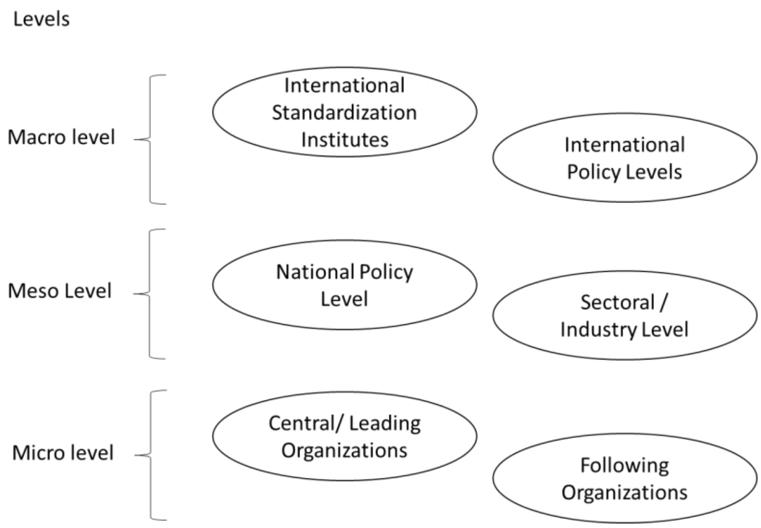

Levels
Macro level
International Standardization Institutes
International Policy Levels
Meso Level
National Policy Level
Sectoral / Industry Level
Micro level
Central/ Leading Organizations
Following Organizations

Figure 1: Governance level PKI (eco)system

On the macro level, we distinguish between international policy levels, e.g., the European Union, that can make and enforce laws and regulations. Another macro-level governance sub-group is the international standardization institutes, within this subgroup organizations like NIST, ESTA, and ISO can be placed, but also, e.g., the CA / Browser forum or international sectoral cooperations like the BIS (Bank for International Settlements). These organizations are not, by definition, always bound to a single country and do not have the authority to declare laws from a legal perspective.

The meso level represents two sub-groups as well, being national governments, with the power to make national laws or who need to translate international law into national laws, and the sectoral or industry organizations groups, which translate international standards into national and sectoral standards and work on intrasectoral agreements.

The micro level represents the organizations that need to implement QS PKI systems. Although all of these organizations need to implement QS PKI, we can distinguish two groups here as well, being central or leading organizations, that, by nature or position in the value chain automatically have a more predominate role, e.g. if multiple other organizations depend on this one due to a crucial role or by the size of the organization or role of the organization being an automatic leader or dominant organization and following organizations. Different organizations on this micro level could also qualify as regular or urgent adopters as described in earlier stages of the HAPKIDO project. (Christiansen et al., 2023).

Altogether, the transition landscape is a complex, dynamic environment, with many actors, a high level of interdependencies, and without clear and strict hierarchical structures. Another complicating factor regarding governance is the lack of a concrete deadline for PKIs to have migrated to a quantum-safe state.

3.3 Relevant governance theories for PKI transition.

Although one could quickly classify the QS PKI transition as a new IT implementation or project, as stressed by multiple interviewees, it is not just a regular IT implementation or update. QS transitions entail new software and hardware, but also new policies, standards, laws, and regulations, which is further complicated by the need for international and cross-sectoral cooperation, due to interdependencies and unclear deadlines. It requires the cooperation of multiple actors at different governance layers, often without being able to exercise formal power over each other. One respondent stated:

"Should not see this just as a technology process, but as a human and cooperation process." (R5) and "It is not only IT!" (R1)

Besides that, to ensure effective organizational change, from an institutional theory perspective, multiple factors and perspectives must be considered. In particular the *regulative perspective*, emphasizing on legal systems, enforcing change by regulation, *the normative perspective*, emphasizing on the moral and ethical systems within organizations, creating change based on duty and responsibilities and moral obligation, and the *cognitive perspective*, emphasizing on the cultural system, focusing on internalizing and value for organization members to embed change (Palthe, 2014; Scott, 2008). These aspects can be approached by one or more layers, e.g. the regulative perspective will be more in play on the macro and meso level, while the cognitive, thus intrinsic motivation, is more present on the micro level, e.g. implementing organizations. Changes in these environments can have their timelines. (Marijn Janssen & Van Der Voort, 2016; Williamson, 1998). Therefore, multiple governance theories, tools, and mechanisms can be applicable for the QS PKI transition.

Although the QS PKI transition is much broader than just an IT transition project, due to the fact that the transition does indeed entails a large technical component, including software and hardware changes, protocol and libraries updates and potentially updates of existing applications that needs to be managed by all organizations, IT governance theory is still eminently viable. One of the most widely accepted IT governance theories at the *organizational level* is by Ross & Weill. They describe IT governance as "the decision rights and accountability framework for encouraging desirable behaviors in the use of IT" (Peter Weill & Ross, 2004, p. 4) and emphasize in their research on creating the right incentives (P. Weill, 2004; Peter Weill & Ross, 2005; Peter Weill & Ross, 2004). This is also described by multiple other scholars as a crucial element within IT governance (Peterson, 2004; Van Grembergen, 2004).

However, the primary focus of IT governance theory is on the organizational level and often reasons from the point of view of an organization with clear decision structures and accountabilities (Van Grembergen, 2004; Peter Weill & Ross, 2005). However, QS PKI transition supersedes organizations, nations and technology. Additionally, scholars (Christiansen et al., 2023; Kong et al., 2024a) and interviewees indicate that decision making, accountability and incentives are often unclear in the broader PKI eco system.

Too much focus on technical design; governance and institutional design needs to be arranged as well (R2). Within the company, this (accountability & decision making) is clear, within the ecosystem not (R3). The QS PKI transition needs to be done in harmony, otherwise it will not work (R5)

Based on the characteristics of the PKI ecosystem, her products and services and the complexity of governance over multiple layers and actors without formal power over each other while jointly in need of action with unpredictable timelines, one also has to look at other governance theories in order to manage the QS PKI transition in the coming years. In particular, governance of common goods, as PKI can be seen as public or common good and collective action theory as this needs to be managed by a wide group of actors in a self-organizing setting.

Olstrom describes governance of commons in her book "Governing the Commons, the evolution of institutions for collective action" (1990). She described eight principles that are elementary to governing commons, being 1) strong group identity and purpose understanding, 2) fair distribution of cost and benefit, 3) fair inclusive decision making, 4) monitoring agreed upon behavior, 5) graduated sanctions for misbehavior, 6, fast and fair conflict resolution, 7) authority to self-govern, and 8) appropriate relations with other groups (E. Ostrom, 1990). She later, together with Dietz and Stern, based on various cases, indicated the importance of adaptive governance to large scale problems to avoid so so-called tragedy of the commons and identified three general principles as most relevant: 1) analytic deliberation, meaning that there is objective information from different angles, 2) nesting, meaning it should be imbedded and enforced top down and bottom up, and 3) institutional variety, meaning that a mix of institutional types like markets, hierarchies, and self-governance and a good mix of actors should be in place to manage these commons effectively (Dietz et al., 2017). Additionally, as there is a clear need for collective action as there is no individual organization in charge, Olson (1965), in the logic of collective action, emphasized the need for clear group incentives to activate in the interest of the group instead of the individual. However the individual incentive should be clear as well as the effect on the collective outcome, otherwise the individual incentive might vanish (Poteete & Ostrom, 2004).

Governance, risk and compliance should be clear for all parties, without governance it is a no go. It needs to be embedded in the law with clear decision-making authority and incentives. (R10)

During the interviews, multiple challenges regarding QS PKI transition governance were mentioned. One of the most commonly mentioned risks was the clear complicating factor that deadlines for implementation are unknown due to the uncertainty of the exact moment that a quantum computer can break current cryptography. This leads to unclear cost benefits for organizations, blocking sense of urgency.

"Cost benefits are not clear for all organizations, as well as deadlines (US has a bit more clear deadlines, but Europe and the Netherlands don't." (R7)

Another risk that was mentioned is the risk of inequality of information or lack of information of understanding of the challenges at hand in the QS PKI transition or no incentives for transition or objective information, e.g. on a nations exact progress of development of quantum computers from a strategic cyber security perspective.

"One of the challenges is objective information, willingly or unwillingly" (R7). Some cyber superpowers might have less incentives for everyone to transition to QS PKIs. (R8)

An important overarching element of these applicable theories is the element of incentives. The QS PKI transition is seen for many as a hygiene factor. One needs to have it in place, but it does not work as motivation for satisfaction. The lack of it will lead to dissatisfaction (Herzberg, Mausner, & Snyderman, 2011).

"For some there will be a direct incentive to transition fast. Some will agree to a very long hybrid period as they don't have a direct incentive, some 'just don't care as it all goes well at the moment right?' ". (R8)

Thus, intrinsic incentives and motivation to change for individuals is low, let alone for the ecosystem that will need to cooperate. Although important, this is often not clear and so far, not described.

Finally, the availability of large-scale quantum computers has a disruptive impact because of the threat on IT security, in particular PKI. Still, timelines are unclear, solutions not readily available and there is a high interdependency of various actors on different levels as well as within levels. A rigid transition plan could lead to inability to adapt to new insights and information. It is thus important to be agile and able to adapt.

"Crypto-agility will become ever more important in the future". (R4) "Crypto-agility needs to be better arranged". (R5)

Agility as mentioned above is not meant in the sense of Agile software development[6], but in flexibility in the whole change and adaptation process for organizations due to many uncertainties. Therefore, adaptive governance will also play a crucial role in the QS PKI transition. Within adaptive governance, elements like "utilizing internal and external capability, decentralized decision-making power, and seeking to inform higher-level decisions from the bottom up" (Marijn Janssen & Van Der Voort, 2016, p. 1) are important strategies.

One does have to realize that, although the above is valid for the PKI systems in general, as there is no single PKI system, but a co-existence of various systems all with their ecosystems of users and actors, it is possible that for some ecosystems a more direct authority-based approach, closer to pure IT governance can be practical, e.g. in military, governmental or closed information exchange systems, while others are much more open and thus require a much more commons governance approach. In all ecosystems and sectors, it will probably be mixed due to 1) the variety of actors involved, 2) a lack of an overarching authority that is in charge of the transition and 3) dependencies on external actors e.g., standards like NIST in closed ecosystems (R10). Additionally, the governance approach can differ per layer of the PKI ecosystem.

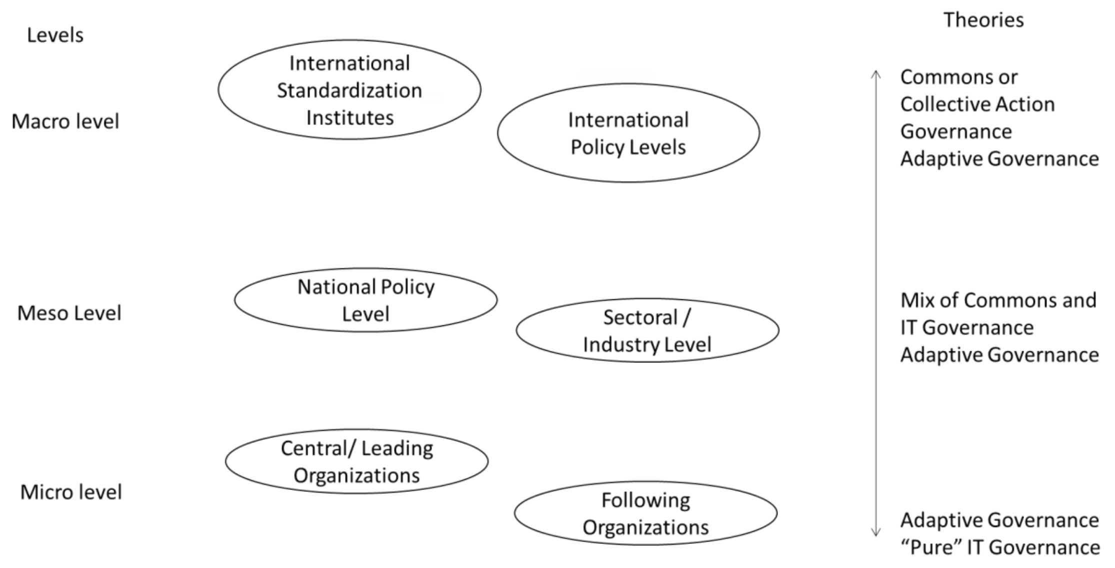
[6] https://agilemanifesto.org/

4. Governance layers, theory, mechanisms, instruments and system dynamics

Section three described the various layers involved in the QS PKI transition and concluded that the governance of the QS PKI transition will need to be managed on various layers. This section describes how the various governance theories match the governance layers based on the characteristics of clarity regarding elements like decision-making, accountability and incentives of the theories compared to the characteristics of the governance levels and which mechanisms and tools could be used per governance layer. Finally, we show how these mechanisms and tools can interact with each other in a dynamic system.

4.1 Theories mapped on the governance layers

When observing the PKI ecosystem (s), as stated in section 2.1, we identify three primary governance levels regarding the QS PKI transitions, the micro, meso and macro levels, that all play a role in the transition. In this section, we plot the governance theories explored in section 2.2 on the identified governance levels. The plot is shown in Figure 2 below.



Levels
Theories
Macro level
International Standardization Institutes
International Policy Levels
Commons or Collective Action Governance Adaptive Governance
Meso Level
National Policy Level
Sectoral / Industry Level
Mix of Commons and IT Governance Adaptive Governance
Micro level
Central/ Leading Organizations
Following Organizations
Adaptive Governance "Pure" IT Governance

Figure 2: predominate (IT) governance theory applicability per level

On the micro level of governance, the individual organizations are represented. Within and between these organizations, a relatively standard authoritarian management style can be handled where transparent decision-making and accountability structures can be set up to implement QS PKI within the companies. Although it does not mean that there cannot be a dependency on, e.g., third-party suppliers for supplying software and hardware needed for the implementation, the implementation itself on this level can be governed using IT governance theory, where the main emphasis is on clear accountability, decision making rights, and incentives.

> *"Within the organization, accountability and decision making are clear, incentives are harder due to unclear deadlines." (R3)*

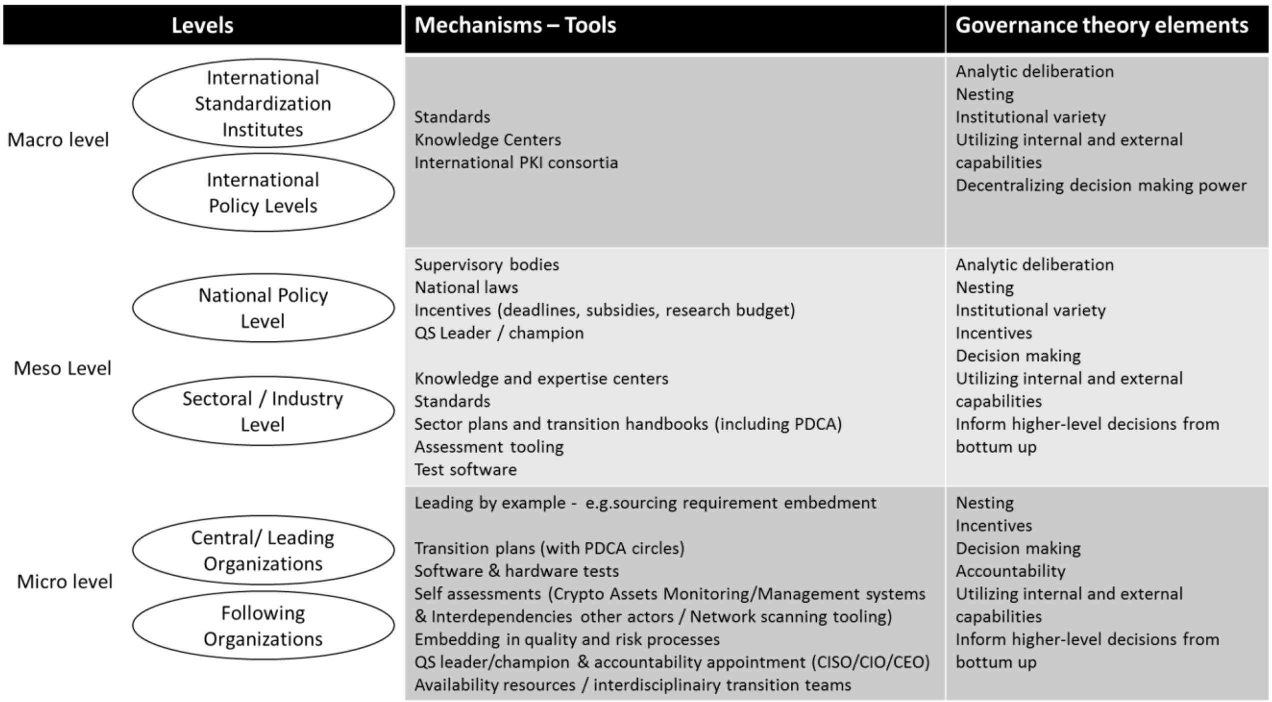
To get to the necessary hardware, software and procedures for implementation on the micro level, input is needed from the higher governance levels and from parties in the same governance level, e.g., standards, agreements, policies etc. At the meso level, in most cases there are no hierarchical relationships, although within certain sectors or industries some hierarchal relationships may be present. Therefore, the predominant governance theory on this level is commons governance and collective action governance as decision-making and accountability is fuzzier than on the micro level. This means there should be more emphasis on analytic deliberation, nesting, institutional variety, and creating incentives that benefit the group, not the individual. However, as the hierarchical relationships can differ per nation and, more specifically, per sector, there can be a mix of governance theories co-existing, where IT governance elements are very much applicable on this level.

On the highest level, the macro level, there is the least authoritarian relationship between the actors involved in the ecosystem. Therefore, the collective action theory and the common sound theory principles will likely be the most useful on this level. Due to the dynamic and uncertain environment in which the QS PKI transition takes place, adaptive governance applies on all levels. The different levels will have to use their internal capabilities and the external capabilities of actors in other layers. Bottom-up information for higher-level decision-making is viable on an organizational level but also between micro and meso levels as well as between micro or meso and macro levels.

When looking at the various theories and levels, one has to conclude that different theories can and need to be used on the different levels, but also that there are interdependencies between the various vertical levels, which leads to system dynamics of governance mechanisms (see section 3.3), where there can be differences within horizontal layers, both between nation states as well as differences per sector.

4.2 Tooling and mechanisms per layer

To contribute to the various governance theory elements described in the previous section, a wide range of mechanisms and tools is identified in both literature (AIVD et al., 2024; Christiansen et al., 2023; Csenkey & Bindel, 2023; Kong et al., 2024a, 2024c; Perrier, 2022) as well as during the interviews. The mentioned tools and mechanisms can adhere to different governance theory elements at various levels and are displayed in Figure 3 below.`



Levels		Mechanisms – Tools	Governance theory elements
Macro level	International Standardization Institutes International Policy Levels	Standards Knowledge Centers International PKI consortia	Analytic deliberation Nesting Institutional variety Utilizing internal and external capabilities Decentralizing decision making power
Meso Level	National Policy Level Sectoral / Industry Level	Supervisory bodies National laws Incentives (deadlines, subsidies, research budget) QS Leader / champion Knowledge and expertise centers Standards Sector plans and transition handbooks (including PDCA) Assessment tooling Test software	Analytic deliberation Nesting Institutional variety Incentives Decision making Utilizing internal and external capabilities Inform higher-level decisions from bottum up
Micro level	Central/ Leading Organizations Following Organizations	Leading by example - e.g.sourcing requirement embedment Transition plans (with PDCA circles) Software & hardware tests Self assessments (Crypto Assets Monitoring/Management systems & Interdependencies other actors / Network scanning tooling) Embedding in quality and risk processes QS leader/champion & accountability appointment (CISO/CIO/CEO) Availability resources / interdisciplinairy transition teams	Nesting Incentives Decision making Accountability Utilizing internal and external capabilities Inform higher-level decisions from bottum up

Figure 3: Tools per governance level

At the macro level, three mechanisms were mentioned multiple times, e.g., standards, knowledge centers and international PKI consortia. Although these all contribute to nesting and institutional variety, they contribute to analytic deliberation by creating objective information resulting from a multi-actor view and the possibility for higher-level decision-making based on bottom-up information. Various consortia are already in place adhering to international PKI consortia, like the CA browser forum, that could also act as knowledge centers. Still, based on the interviews, the role of these knowledge centers should be expanded and cover a broader spectrum regarding the QS PKI transition. Regarding standards, the most predominant development is the selection of three QS algorithms by NIST that the market can now test[7]. During the interviews, it was emphasized that, although the selection of these algorithms is a good start, a lot of work still needs to be done on not only standards for QS PKI algorithms but also standardization of processes and procedures, format of certificates and how to obtain and implement them.

At the meso level, a wide range of governance tools can be implemented. On national governmental or policy subgroups on the meso level, supervisory bodies, national laws and various forms of incentive creating are mentioned. National law can foresee clear deadlines for implementing QS PKI systems, which, given the challenge of unpredictable timelines regarding the exact technical feasibility of a quantum computer, can create better requirements for roadmaps and implementation deadlines. Supervisory bodies can oversee the implementation, although one has to make sure that these can act objectively and independently, as one of the interviewees stated:

> *"This (supervisory bodies) could also pose a danger as it could then become political" (R9).*

Incentives could be created in various ways on the national level as well. Some of the ways mentioned are subsidies for implementation to withstand uncertainty in the cost. Still, also deadlines within the law and, thus risk of non-compliance and research budgets are two mechanisms that are identified.

An even wider range of mechanisms was mentioned within the subgroup of industries or sectors on the meso level. On the macro level, knowledge and expertise centers can play a crucial role in awareness, but even more so, especially as per sector, there will be different requirements and lessons learned in feedback on lessons learned in testing and implementation that others can reuse, clearly contributing to bottom-up information from the individual organizations and can support in utilizing external capabilities to individual organizations. In their role, these sector and national expertise centers can then contribute as actors in bottom-up knowledge sharing on macro levels. Also, on this level, the international standards must be translated to national or sectoral standards. This can be embedded in sector plans and handbooks for QS PKI transition, like the PQC migration handbook published in December 2024 (AIVD et al., 2024), including clear Plan, Do, Check, Act (PDCA) cycles (Pietrzak & Paliszkiewicz, 2015) to have an integrated feedback learning loop on lessons learned in practice. Additionally, the development of assessment tools and PQC testing software for implementation to determine the impact on the organizational level should be part of the governance from a meso level. All these mechanisms adhere to objective information on the national or sector level (analytic deliberation), nesting, and institutional variety. Still, they will also contribute to creating better (group) incentives and clarity in decision-making.

[7] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

A wide range of mechanisms can govern the QS PKI transition at the micro level. All organizations should have transition plans, including internal Plan-Do-Check-Act (PDCA) cycles. Based on the assessment tools and test software, internal assessments and tests should be performed per organization. These assessments should not only focus on the internal inventory of cryptographic assets but also look into interdependency of the cryptographic assets with other actors and creating network scanning tooling to assess the full impact of the organization in their value chain, contributing to possibilities for utilization of external capabilities in the governance of the transition. Multiple interviewees argue that it should become part of the quality assurance and risk management processes within organizations as failure to migrate in time will pose both IT and business continuity risks, preferably performed by multidisciplinary, given the fact that the QS PKI transition supersedes just a technical implementation. Furthermore, it is suggested that, if not already in existence within an organization, a clear accountability system should be introduced, both on operational level (a QS leader or champion) as well as on a strategic level (a CISO/CIO or CEO with QS PKI transition in their portfolio) and resources should be made available, although interviewees do acknowledge that, due to the lack of sense of urgency within organizations, there is often no clear incentive to do so:

> *Many parties see it (QS PKI implementation) as burden, only a few as USP. Need to create an incentive, so even burdened companies can "shine". (R4) "Might need an incident to create awareness". (R5)*

For central/leading organizations, specifically governmental organizations and larger critical central organizations in supply chains, leading by example e.g. by embedding QS requirements in sourcing contracts to their supplier, was mentioned as well.

By implementing the mentioned governance mechanisms on micro level, there is adherence to nesting, clear accountability and decision-making within organizations (including insight in dependency of other organizations) and incentives as described in section 2.2 and 3.1, as well as the possibility to be able to share bottom-up information for higher-level decision making and utilizing internal and external capabilities.

Although one can approach the governance of such a complex transition from a governance theory perspective, often valuable lessons can also be learned from analogies from past complex transitions.

4.3 Analogies: learnings from other transitions

The QS PKI transition was almost unanimously described and acknowledged to be a global transition. Additionally, timelines are seen as unpredictable as the exact availability of quantum computers capable of breaking the current asymmetric public-private key cryptography is unknown, and the timelines can differ per industry or sector and thus per individual PKI systems. During the interviews, the question was asked if the interviewees could give analogies to other global transitions with diffuse timelines and what lessons could be learned from a governance perspective for the QS PKI transition.

Several transitions were mentioned regarding analogies and their lessons. An overview of the lessons per transition mentioned is shown in Table 2.

Table 2: Lessons learned from analogies

Analogy	Lessons mentioned	Related governance mechanism or tools
Energy transition	Providing subsidies	Clear incentives
Climate change	Political willingness	Accountability International agreements
CFC transition	Political willingness, clear impact	Accountability, sense of urgency, global agreements, sourcing requirements
New technology introduction	Do not wait for a incident to happen	Knowledge sharing (analytic deliberation), sense of urgency, incentives
Y2K	Clear impact, clear deadline	Sense of urgency, incentives

Climate related analogies

The most mentioned were climate change and the energy transition, although few lessons from these analogies were mentioned during the interviews. Some of the lessons related to the fact that *political willingness* is crucial and that differences in interests will make it work or fail, also creating incentives, e.g. subsidies was mentioned. The ChloroFluorCarbon (CFC) transition was an example of where this political willingness clearly resulted in worldwide agreements. These agreements were enforced remarkably fast by creating these agreements, with that sense of urgency and clear incentives (e.g., sanctions). Other key factors for success were furthermore clear nesting (governments, civil organizations and industry all working together) and analytic deliberation (consensus that CFCs were the cause of thinning the Ozon layer).[8]

New technology introduction

Although not seen as a particular transition, one respondent compared it to implementation of other new technologies, but crucially side noted that:

> *"it (implementation of new technology and possible consequences) is not new, but for some reason we get caught in the act and act surprised if a problem pops up" (R5)*

Several other interviewees acknowledged this problem in different ways:

> *"Dempt put als kalf verdronken is (Dutch paraphrase meaning we only take action after an incident)" (R2). "We are not the best learners from the past" (R4). "Might need and incident" (R5). "As problem did not yet occur, organizations are hesitant to invest already" (R7).*

The most important lesson here is thus related to analytic deliberation. Although knowledge is present upfront, one should act on it *before* accidents or incidents happen instead of after. Especially given the potential extremely impactful consequences in the QS PKI transition.

Y2K problem

Finally, another often-mentioned analogy was the Y2K problem at the end of last millennium[9]. Although it was a clear example of a worldwide transition without a *clear owner*, there was one crucial difference between this problem and the QS PKI transition: it had a very *clear deadline*, which

[8] https://rapidtransition.org/stories/back-from-the-brink-how-the-world-rapidly-sealed-a-deal-to-save-the-ozone-layer/

[9] https://en.wikipedia.org/wiki/Year_2000_problem

is much more unpredictable in the QS PKI transition. The interviewees see these clear deadlines as important lessons.

"Clear deadlines were set, which lead to incentives for transition" (R1 and R6). "A best practice is US, they have a Qdate. When timelines are diffuse, governments need to set deadlines "(R6). "Most important lesson from previous cases, you cannot start early enough. Some deadlines (e.g. NIST) are set between 2030 and 2035. Transition from SHA 1 to SHA2 already took 10 years, this is much more complex, which is worrying!" (R10)

Looking these analogies, the most important lessons are thus related to clear deadlines that can be set in various policies, leading to transition incentives, knowledge sharing and political willingness. Especially this latter was mentioned as a possible additional challenge:

"The difference for PKI is, sometimes there is a lack of universal driving force, some cyber-superpowers might have less incentives for everyone to transition to QS PKIs" (R8).

Based on this brief analysis of analogies, already several interesting lessons, challenges and additional governance mechanisms were gathered. As this entailed a non structured analysis of analogies, it is useful to further research lessons learned from these types of analogies in future research to identify additional lessons.

4.4 Interdependencies of governance mechanisms and tools (system dynamics)

We identified predominant theories and, tools and mechanisms per governance layer for the QS PKI transition and some first lessons from other transitions. However, the layers and tools cannot be approached or used in an isolated way. Although many of the governance mechanisms and tools can be used in isolation, their in- or output can reinforce each another. Various mechanisms that are being initiated at one level reinforce other mechanisms at the same or other levels. During the interviews, the importance of integrating PDCA cycles was emphasized. This leads to governance elements not only influencing or reinforcing each other, but also forming crucial feedback loops between mechanisms within and over various levels, creating complex system dynamics. Understanding these system dynamics of governance mechanisms is important to identify possible starting points and governance actions and can also help prioritize must-haves and need to have governance actions per sector.

As stated in section 2, incentives are an important overarching governance element. This can be triggered in a direct manner in multiple ways, as shown in Figure 4 below.

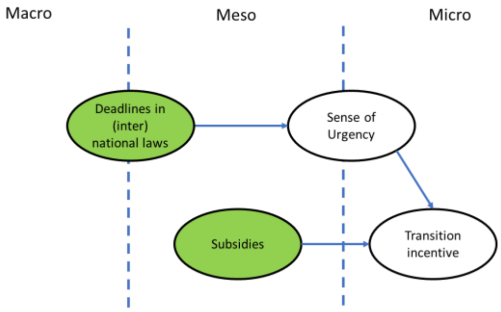


Figure 4: Direct influence on incentives - green balloons indicating (potential) starting points

By creating subsidies (rewards or "carrots") that partially fund QS PKI transitions within companies, one can trigger organizations to start investing in the QS PKI transition. Another direct manner is by threat of non-compliance (fines or "stick"). By implementing deadlines in (inter)national laws on macro or meso level, not adhering will pose the risk of non-compliance and fines, leading to a sense of urgency within organizations and thus incentivizes the transition.

Incentives to transition can also be the result of more complex system dynamics of various governance mechanisms. The interviewees also mentioned various dependencies.

In order to know what incentive we have to have, and thus create sense of urgency, we need to do an inventory of the impact and our crypto assets. (R3)

An example of what such a system dynamic can look like is shown in Figure 5 below.

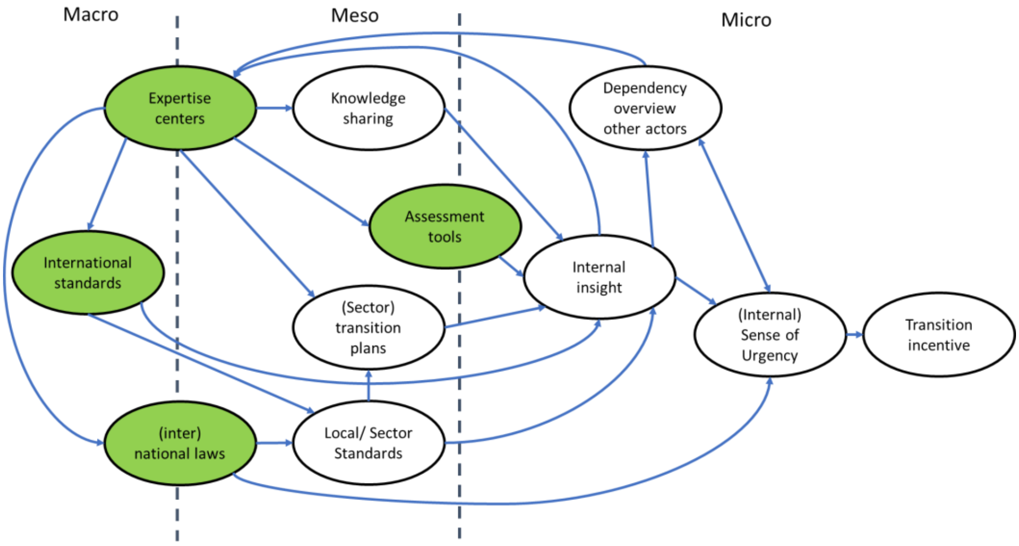


Figure 5: example of system dynamics of governance mechanisms– green balloons indicating (potential) starting points

As shown in Figure 5, expertise or knowledge centers can contribute in the creation of assessment tools provide input for international standards and (inter)national laws. International laws and standards provide input for local or sectoral standards. These local standards can be input for sectoral transition plans. Together, through knowledge-sharing mechanisms, assessment tools and the local standards themselves, they contribute to internal insight for organizations on their vulnerability to lack of transition to a QS PKI. This in itself then can create an (internal) sense of urgency and an incentive for transition.

These internal insights also can also create insight in other actor dependencies, which through a feedback loop of knowledge sharing towards expertise or knowledge centers can lead again to update of standards, handbooks etc., leading to true system dynamics and self-enforcing governance mechanisms. The above might lead to more intrinsic and less hygiene-factor-based motivation as it creates better insights in business impact, not in the least, cost of implementation and benefits of being QS, and not just incentives from a compliance or finance (subsidy) driven perspective.

The figures also show that, although various elements influence each other, one can already start with various governance actions on various levels and there is not necessarily a single starting point. Due to the feedback loop(s), others can then be reinforced and certain actions can later be refined. However, as indicated in the green balloons in both Figure 4 and Figure 5, certain governance mechanisms could be more important starting points as they influence various other governance mechanisms and create higher sense of urgency and and incentives to prepare for and initiate the QS PKI transition.

As there is not just one PKI ecosystem and all can differ in complexity, the number of actors, and the mixture of self-organization vs authoritarian relationships, these system dynamics could differ per sector. Therefore, it should be subject to future research of more detailing, especially per sector. By creating such a system dynamic overview per sector, combined with and actor dependency overview, detailed transition plans can be created per sector.

Finally, due to the dynamic character of the transition and the system dynamics of the governance mechanisms, governance changes over time and it thus continuously needs to be reassessed which mechanisms on what levels are the most useful at that point in time.

5. Conclusion

The QS PKI transition is a transition that is very complex and goes much further than just an algorithm upgrade or an IT project as it can result in true business continuity risks. Additionally, the input needed for the transition is not just technology, but it is about setting standards, procedures, policies and probably even legislation. One needs to understand that the QS PKI transition is not just a regular IT transition or upgrade but poses a business continuity risk as well as a compliance risk (e.g. GDPR) and, therefore, deserves the broader attention of the whole organization that needs to implement it and the ecosystem in which these organizations operate.

Additional complexity is the unpredictable timelines and lack of ready-to-implement solutions, leading to low awareness of the potential impact and, thus low sense of urgency at organizational levels for the QS PKI transition.

With regards to the first two research questions, this research suggests that, although IT governance theory is applicable for the QS PKI transition, due to the complexity and versatility of the transition and the ecosystems wherein the implementation needs to be done, IT governance alone will not suffice. One can use IT governance theory and mechanisms on the micro and meso level, it needs to be supplemented with the theory of commons management and collective action theory, especially in the meso and macro level. It is thus important, not only to steer on accountability and decision making but also on (group) incentives, analytic deliberation, nesting and institutional variety. On all levels, due to the dynamic environment QS PKI operates in, adaptive governance is crucial as well.

One of the most important elements of all layers is incentives. These might not be clear for many stakeholders, often due to unpredictable timelines, the lack of readily available solutions and the unknown impact on the installed. How PQC standards will impact the business processes, the risks, and the transition costs are thus important starting questions that need to be answered to determine the appropriate governance mechanisms.

With regards to the third research question, the governance of the transition can be set up by using a wide range of mechanisms and tools on various levels. Some, like subsidies and clear set deadlines for implementation, can have a direct influence on incentives for transition for organization. Others, like expertise centers, standards and assessment tools, due to the system dynamics of the governance mechanisms, will eventually create incentives for transitioning to QS PKI as result of a more complex interplay of governance mechanisms, which in themselves also can and should have, reinforcing feedback mechanisms.

Governance mechanisms differ per level, and their needs change over time. The set of governance mechanisms presented in this report can be used to select the appropriate mechanism given the circumstances and the operating level. Determine first what are the risks of the infrastructure and what needs governance.

Although the mix of governance theories, mechanisms and elements are applicable to all actors within the PKI ecosystem, one needs to take into account that the exact combination of mechanisms and elements can differ per sector due to the differences in nature of the sector, e.g. in authoritative or more self-organizing relationships between actors and differences in openness per ecosystem.

A complicated challenge could be that not all actors involved have a direct incentive to change and could even be reluctant to migrate to QS PKI systems, hence the importance for collective action and good understanding of the governance system dymanics..

Additionally, there seems to be a lack of universal driving force, as some cyber-superpowers might have less incentives for everyone to transition to QS PKIs

6. Future recommendations for QS governance

This report reveals a wide range of governance theories applicable, as well as mechanisms and tools suitable for managing the QS PKI transition at all levels.

The most important recommendation is to *acknowledge that the transition to quantum-safe cryptography is not just an IT project, but covers many elements (technical and nontechnical*) on multiple layers and *cannot be managed* by a single organization, using one governance theory. Instead, an effective transition strategy demands collective action and should be adaptive to changing circumstances.

It is important to *create clear incentives*. This can be done in a direct way, through *laws* (including setting deadlines and fines for non-compliance) and *(implementation and research) subsidies*. *Creating deadlines* is desirable in the short term to create a clear sense of urgency.

Additionally, due to the interdependencies of multiple governance elements, incentives can be influenced indirectly. Through elements like *knowledge sharing* to create awareness and *expertise centers* to share best practices, and *(inter)national standards and laws* can be crucial starting points. In this way, individual organizations can create insight into the impact of becoming QS (e.g., on costs and benefits) and thus a sense of urgency, creating an internal intrinsic incentive for the QS PKI transition. The lessons learned in the internal impact assessment and tests in themselves should then be used again as a feedback loop in knowledge sharing.

Another way to trigger accountability and incentives for transitioning on the organizational level is to *create clear assignments*, which can be done by having critical or central organizations, like governmental organizations, integrate QS PKI requirements into their sourcing agreements.

At the microlevel, the first handbooks and assessments on QS PKI transition and crypto assets are appearing. The *lessons learned should be used for creating handbooks and migration plans on the meso level, as, based on the insights on an* organizational level, *interdependencies between all the actors* should also become clearer. Also, *additional research* is needed to uncover *lessons learned using analogies* of other global transitions.

Furthermore, seeing if a national supervisory body can be created in time with an independent view and a progress guarding task is recommended. This can either be a public or a public-private supervisory body.

The system dynamics can differ for all PKI ecosystems and change over time. In the short term, it is recommended to *create a system dynamic overview of governance mechanisms and tools per sector, creating insight into who can and should take which governance action at what point*. Multiple of these mechanisms can already be set up in the short term. These system dynamic overviews of governance mechanisms should also be used as input for organizational readiness models for quantum safe transition as described in workpackage 7.1 of the HAPKIDO project (Kong, Janssen, & Bharosa, 2024b), but also, given the dynamic environment of new developments, learnings, and feedback loops, should be updated continuously.

It should thus be clear that there is no *one* starting point from a governance perspective, but *multiple governance mechanisms* should be initiated *at multiple levels* simultaneously.

References

AIVD, CWI, & TNO. (2024). *The PQC Migration HAndbook - Guidelins for migration to post-quantum cryptography* (Revised and Extended Second Edition ed.).

Baker, H. K., & Anderson, R. (2010). *Corporate governance: A synthesis of theory, research, and practice* (Vol. 8): John Wiley & Sons.

Choi, C. (2022). Ibm unveils 433-qubit osprey chip> next year entanglement hits the kilo-scale with big blue's 1121-qubit condor. *IEEE Spectrum*.

Christiansen, L. V., Kong, I., & Bharosa, N. (2023). *Governing the transition to quantum-safe PKIs in the Netherlands: Paving the way for our quantum-safe future.* HAPKIDO,

Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity, 9*(1), tyad001.

Datacard, E. (2019). THE QUANTUM COMPUTER AND ITS IMPLICATIONS FOR PUBLIC-KEY CRYPTO SYSTEMS.

De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management, 26*(2), 123-137.

Dietz, T., Ostrom, E., & Stern, P. C. (2017). The struggle to govern the commons. In *International Environmental Governance* (pp. 53-57): Routledge.

Fukuyama, F. (2013). What is governance? *Governance, 26*(3), 347-368.

Grant, R., & Keohane, R. (2005). Accountability and Abuses of Power in World Politics. *American Political Science Review, 99*(1), 29-43.

Herzberg, F., Mausner, B., & Snyderman, B. B. (2011). *The motivation to work* (Vol. 1): Transaction publishers.

Janssen, M., & Joha, A. (2007). Understanding IT governance for the operation of shared services in public service networks. *International Journal of Networking and Virtual Organisations, 4*(1), 20-34.

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly, 33*(3), 371-377. doi:http://dx.doi.org/10.1016/j.giq.2016.08.011

Janssen, M., & Van Der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly, 33*(1), 1-5.

Klievink, B., Bharosa, N., & Tan, Y.-H. (2016). The collaborative realization of public values and business goals: Governance and infrastructure of public–private information platforms. *Government Information Quarterly*. doi:http://dx.doi.org/10.1016/j.giq.2015.12.002

Kong, I., Janssen, M., & Bharosa, N. (2024a). *Deriving Government Roles for directing and supporting Quantum-safe Transitions.* Paper presented at the Proceedings of the 25th Annual International Conference on Digital Government Research.

Kong, I., Janssen, M., & Bharosa, N. (2024b). *Organizational Readiness Model for Quantum-safe Transition.* HAPKIDO - Project,

Kong, I., Janssen, M., & Bharosa, N. (2024c). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly, 41*(1), 101884.

Lecy, J. D., & Beatty, K. E. (2012). Representative literature reviews using constrained snowball sampling and citation network analysis. *Available at SSRN 1992601*.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine, 151*(4), 264-269.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38-41.

Mourão, E., Pimentel, J. F., Murta, L., Kalinowski, M., Mendes, E., & Wohlin, C. (2020). On the performance of hybrid search strategies for systematic literature reviews in software engineering. *Information software technology, 123*, 106294.

Olson, M. (1965). *Logic of collective action: Public goods and the theory of groups (Harvard economic studies. v. 124)*: Harvard University Press.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*: Cambridge university press.

Ostrom, V., & Ostrom, E. (1979). Public goods and public choices. In *Alternatives for delivering public services* (pp. 7-49): Routledge.

Palthe, J. (2014). Regulative, normative, and cognitive elements of organizations: Implications for managing change. *Management organizational studies, 1*(2), 59-66.

Perrier, E. (2022). The quantum governance stack: Models of governance for quantum information technologies. *Digital Society, 1*(3), 22.

Peterson, R. (2004). Crafting Information Technology Governance. *Information Systems Management, 21*(4), 7-22.

Pietrzak, M., & Paliszkiewicz, J. (2015). Framework of Strategic Learning: The PDCA Cycle. *Management, 10*(2).

Poteete, A. R., & Ostrom, E. (2004). Heterogeneity, group size and collective action: The role of institutions in forest management. *Development change, 35*(3), 435-461.

Rosenbaum, S. (2010). Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. *Health Research and Educational Trust*, 1442-1455. doi:10.1111/j.1475-6773.2010.01140.x

Scott, W. R. (2008). Approaching adulthood: the maturing of institutional theory. *Theory society, 37*, 427-442.

Van Grembergen, W. (2004). *Strategies for Information Technology Governance*: Idea Group Publishing.

Weill, P. (2004). Don't Just Lead, Govern: How best Performing Organisations Govern IT. *MIS Quarterly Executive, 3*(1), 1-17.

Weill, P., & Ross, J. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review, 46*(2), 26.

Weill, P., & Ross, J. W. (2004). IT governance on one page.

Williamson, O. (1998). Transaction Cost Economics: How It Works; Where It is Headed. *De Economist, 146*(1), 23-58.