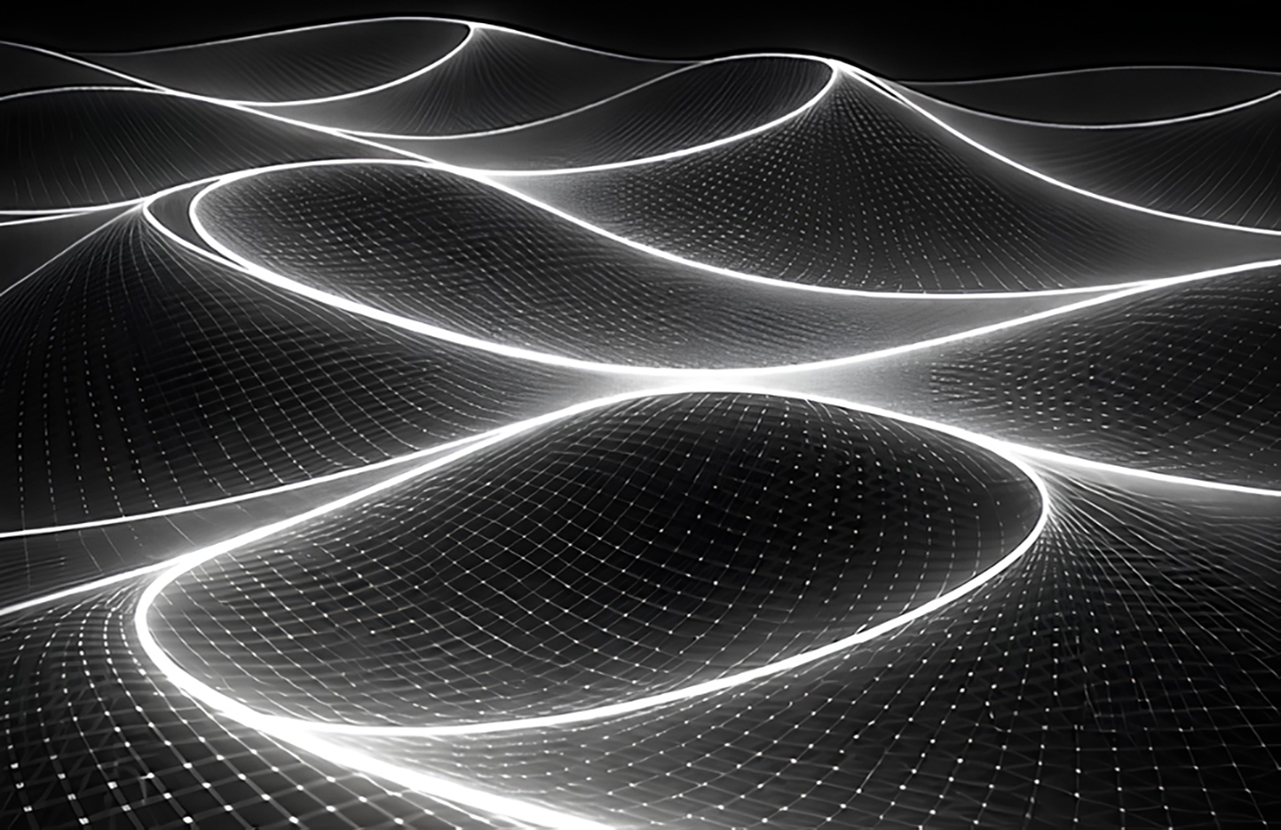
Moving to the Quantum Era

A Stage-Based Growth Approach for Organizations Navigating the Transition to Post-Quantum Cryptography

I. Kong



Moving to the Quantum Era

A Stage-Based Growth Approach for Organizations
Navigating the Transition to Post-Quantum Cryptography

Dissertation

For the purpose of obtaining the degree of Doctor
at Delft University of Technology,
by the authority of the Rector Magnificus,
Prof.dr.ir. H. Bijl,
Chair of the Board for Doctorates,
Defended publicly on
Monday, 8th of June 2026 at 17:30

by

Inhee KONG

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus,	chairperson
Prof.dr.ir. M.F.W.H.A. Janssen	Delft University of Technology, promotor
Prof.dr.ir. N. Bharosa	Delft University of Technology, promotor

Independent members:

Prof.dr. F.C. Bernardini	Fluminense Federal University
Prof.dr. S. Fehr	CWI Amsterdam & Leiden University
Prof.dr. J.R. Ortt	Delft University of Technology
Prof.dr.ir F.E.H.M. Smulders	Delft University of Technology
Prof.dr. P.E. Vermaas	Delft University of Technology

Keywords: Quantum-safe, Post-Quantum Cryptography, Public Key Infrastructure, Information Security, Growth Model, ISM-MICMAC, Transition Challenges, Transition Capabilities

Printed by: Drukkerij Haveka
Cover by: Ini Kong & Niek van Luijn

ISBN: 978-94-6384-970-8

An electronic version of this dissertation is available at: http://repository.tudelft.nl

"I wish it need not have happened in my time," said Frodo.

"*So do I,"* said Gandalf,
"*And so do all who live to see such times.*
But that is not for them to decide.
All we have to decide is what to do with the time that is given us."

J.R.R. Tolkien
From The Fellowship of the Ring, 1954

Table of Contents

Summary

In today's data-driven world, Public Key Infrastructures (PKIs) establish a secure and trusted environment for digital interactions. From financial systems and government networks to energy grids and telecommunications, critical information infrastructures depend on PKIs for secure digital communication and information exchange. With a set of hardware, software, policies, and procedures, PKIs play a crucial role in providing a security framework that manages digital identities between devices, applications, users, and networks. For current classical computers, PKIs are generally considered to be secure and remain practically impossible to break with the use of today's widely used cryptographic algorithms, such as RSA (Rivest-Shamir-Adleman), DHKE (Diffie-Hellman key exchange), and ECC (Elliptic Curve Cryptography). However, with a cryptographically relevant quantum computer (CRQC) on the horizon, these algorithms will no longer be secure.

To address the threats posed by cryptographically relevant quantum computers, solutions based on Post-Quantum Cryptography (PQC) are being developed, which experts believe will be difficult for both current classical computers and quantum computers to solve. After years of research, the National Institute of Standards and Technology (NIST) announced an ongoing set of standards for PQC in August 2024. However, preparation is needed to transition the existing PKIs to become quantum-safe (QS). A newly standardized solution based on PQC algorithms cannot be implemented overnight due to multiple technological dependencies that facilitate the PKI systems. Likewise, there are uncertainties surrounding the development of QS technology, including hardware and software that can run QS cryptographic solutions. Many organizations find themselves without a clear direction, and there is limited knowledge available for QS transition.

As organizations become dependent on the digital environment, it is more important than ever to recognize the systematic risks of quantum computing threats that can affect the entire ecosystem. With essential services across critical infrastructures that depend on PKIs, the topic of QS transition remains relevant and crucial for maintaining national security and public safety. This research, with a focus on PQC, aims to identify the key challenges involved in QS transition and to provide a stage-based growth model for organizations looking to transition to QS PKIs. To achieve this aim, the main research question for the research has been formulated: "*What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems?" T*o answer the main research question, four sub-questions have been developed.

The research has been structured into four phases, with each phase corresponding to one of the four sub-questions. The first phase of the research gathers insights on the socio-technical transition challenges, and the second phase of the research examines dependencies between transition challenges to identify different stages of growth model. The third phase of the research investigates the transition capabilities needed across organizations to move from one stage to the next. The fourth and last phase of the research evaluates the relevance and usefulness of the content of the growth model. In doing so, this research assesses whether the growth model aligns with the needs of experts and practitioners and can serve as a useful tool for organizations to transition towards QS. Using a mixed-method approach, the latter phase of the research is further contextualized and builds on the findings of the earlier phases of the research. The details of each phase are further described.

In the first phase of the research, knowledge and insights into the PKI systems in the context of QS transition were gained by investigating the transition challenges that organizations are struggling with. This phase addressed sub-question 1: *"What are the challenges that hinder organizations in transitioning toward QS PKI systems?"* Using a systematic literature review (SLR), this research identified challenges that may hinder organizations from transitioning their existing PKI systems. After identifying transition challenges in the literature, the list of transition challenges is refined using semi-structured interviews with experts and practitioners in the PKI systems in the Dutch public sector. By combining both the results from the literature and practice, the refined list of 15 transition challenges is derived in the research to understand key socio-technical challenges that may hinder organizations from transitioning their PKI systems to QS ones.

The list of 15 socio-technical transition challenges has been categorized into three distinct categories. In the technological category, the transition challenges are: Availability of QS Standardization, No QS standards & selection, No Reliable & Secure QS solution, Non-PQC systems (e.g., Certificate Authorities (CAs) & Users), and No Availability of QS Hardware & Software. In the organizational category, the transition challenges are: Lack of Urgency within Organization, No Business case for QS Transition, Knowledge Needs within Organizations, Lack of Technical Skills & Qualified Personnel, and No QS Governance within Organization. In the Ecosystem category, the transition challenges are Complex Technical Interdependencies, Lack of Collaboration, Lack of Urgency in the Ecosystem, No QS Governance in the Ecosystem, and Lack of Policy & Regulations for QS Solutions. The results for the list of transition challenges for QS transition indicate

that transitioning existing infrastructures remains complex, and these challenges are socio-technical.

Moreover, the main premise of this research is that organizations need to grow through a series of stages to address transition challenges. The second phase of the research addressed sub-question 2: *"What are the different stages in the growth model and discontinuities for QS PKI systems?"* Since a growth model is context-specific and tailored to fit its objective, previous research on the growth model does not provide a systematic way to derive different stages of growth models for QS transition. Likewise, the concept of *discontinuity* is used to distinguish different stages, which is largely overlooked and not explicitly addressed in existing growth models. Thus, this research is the first to develop a stages of growth model that is grounded in QS transition challenges. By applying the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC), this research presents a novel approach in identifying different stages of the growth model and the list of discontinuities.

With a series of 10 workshops held across organizations in the Dutch public sector, the ISM-MICMAC approach examines dependencies between transition challenges and provides a systematic way to prioritize these challenges in a structural hierarchical model. The hierarchical set of interrelated challenges provides an initial basis for structuring the stages of the growth model. Building on this empirical foundation, discontinuities are derived from the challenges in the ecosystem. These discontinuities represent boundary markers between stages in the growth model and act as necessary conditions that must be met in the ecosystem to move from one stage to the next. By serving as a forward-looking tool, the stages of growth model can be used to provide long-term guidance as organizations search for insights through periods of uncertainty and transformation. For organizations, an overview of QS transition in five stages of the growth model shows the current baseline and what may be needed to move from one stage to the next.

The five stages of the growth model for QS transition include: Stage 1 QS awareness, Stage 2 QS assessment, Stage 3 QS preparation, Stage 4 QS implementation, and Stage 5 QS adaptation. The results showed that QS transition cannot be achieved in silos; organizations need to navigate changes in the ecosystem to collectively move toward QS. This was evident from the list of *discontinuities* identified in this research. In Stage 1, discontinuities include *the acknowledgement of systematic risks and vulnerabilities posed by the quantum threat* and *a finalized list of PQC standards*. In Stage 2, discontinuities include *the establishment of a steering committee and international working groups for QS transition,* and *the*

establishment of a testing environment for QS cryptographic solutions. In Stage 3, discontinuities include *the development of policies & regulations that support QS transition*, and *the availability of selected QS cryptographic solutions validated through testing*. In Stage 4, discontinuity includes *the availability of QS cryptographic solutions in HSM & Certificate Issuance software (CAs)*. In Stage 5, discontinuities include *the availability of lessons learned and best practices from the Implementation of QS cryptographic solutions,* and *the establishment of a cross-organizational coordination mechanism for QS cryptographic solutions.*

In the third phase of the research, the list of transition capabilities was identified across organizations. In this research, the term QS *transition capability* refers to the ability that organizations need to develop in each stage to move from one stage to the next to achieve quantum safety. The third phase focused on addressing sub-question 3, *"What capabilities are needed across organizations for QS PKI systems?"* The list of key actions needed for each stage is derived from the challenges at the organizational level and has been translated to the list of transition capabilities. The list of transition capabilities is categorized into *Sensing, Seizing, and Transforming* based on the Dynamic Capability Theory. First, transition capabilities at Stage 1 and Stage 2 are categorized as *Sensing* capabilities that detect opportunities and assess threats. Second, transition capabilities at Stage 3 and Stage 4 are categorized as *Seizing* capabilities that mobilize resources to capture value from identified opportunities and respond to threats. Last but not least, transition capabilities at Stage 5 are categorized as *Transforming* capabilities that maintain competitiveness through protecting and reconfiguring their intangible and tangible assets.

As changes occur in the ecosystem for QS transition, organizations need to develop transition capabilities so that they are prepared to move with the ecosystem. The transition capabilities are identified through actions needed in organizations at the inter-organizational and intra-organizational levels. At the inter-organizational level, organizations include government agencies that apply national regulations and/ standards (e.g., ministries, Logius, National Cyber Security Centre (NCSC)), organizations that manage and operate critical infrastructures across and within sectors in a national context (e.g., the Central Bank of the Netherlands*, De Autoriteit Financiële Markten (AFM),* KPN, vendors, etc.). At the intra-organizational level, organizations include public and private entities that do not necessarily operate or manage critical infrastructures but rather rely on the services provided by these infrastructures (e.g., government agencies, banks, tax offices, hospitals, service providers, and other small and medium enterprises (SMEs)).

For organizations at the inter-organization level, QS transition capabilities include: At Stage 1, an ability to engage and discuss the development of QS cryptographic solutions across industry, academia, and government. At Stage 2, an ability to establish a national QS governance framework and an ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms. At Stage 3, an ability to integrate QS cryptographic solutions validated through testing into certified hardware and software, and an ability to create and update sectoral guidelines to support QS transition. At stage 4, an ability to modify existing systems with QS cryptographic solutions and an ability to facilitate cross-organizational knowledge sharing & skill development for QS transition. At Stage 5, an ability to coordinate cross-sectoral adaptive responses to address evolving security threats and challenges.

For organizations at the intra-organization level, QS transition capabilities are as follows: At Stage 1, an ability to raise awareness and align stakeholders to implement QS cryptographic solutions. At Stage 2, an ability to assess evolving risks, readiness, and the impact of quantum threats on the organization's business processes. At Stage 3, an ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition. At Stage 4, an ability to implement QS cryptographic solutions in a small-scale environment before deployment, and an ability to upskill employees and share knowledge across departments to manage the implementation of QS cryptographic solutions. At Stage 5, the ability to integrate QS cryptographic solutions in a scaled environment across all systems, and the ability to monitor, adapt, and adjust security practices to changes in the external environment.

The fourth and the last phase of the research addressed sub-question 4, "*To what extent is the growth model for QS transition relevant and useful for organizations?"* Due to an early stage of QS transition when writing this dissertation, quantum safety in the ecosystem has not yet been realized. Likewise, the developed stages of the growth model do not aim to describe what is known but rather identify the stage organizations are at. The model serves as a forward-looking tool that can guide organizations through periods of uncertainty and transformation. The growth model is evaluated in two parts. The first part of the evaluation assessed whether the model captures the relevant key socio-technical challenges and actionable guidance needed for QS transition. The second part of the evaluation assessed whether the growth model aligns with the needs of experts and practitioners and can serve as a useful tool for organizations.

The first part of the evaluation assessed the *relevance* of the growth model based on contextual relevance, topical relevance, cognitive relevance, and actionability. The contextual relevance refers to the level of essentiality of actions. The results showed that nine actions were considered highly essential: 1. Raise awareness on the importance of implementing QS cryptographic solutions, 2. Define clear roles, responsibilities, and decision-making structure for QS governance, 3. Conduct assessments to identify the level of risk, readiness, & impact for QS transition, 4. Develop certified hardware and software that are suitable with QS cryptographic solutions, 5. Develop relevant sector-wide guidelines that support QS transition, 6. Migrate non-PQC systems of CAs to selected QS cryptographic solutions, 7. Modify non-PQC part of the existing systems on a smaller scale with QS cryptographic solutions, 8. Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems and 9. Monitor, adapt, and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes. The results showed that most actions were essential for organizations that viewed QS transition as an important business case. For PKI users, the essentiality of actions differed depending on their risk appetite, business case, and available budget.

The topical relevance indicates how well the actions addressed the organization's needs. These include actions like: 1. Conduct assessments to identify the level of risk, readiness, & impact for QS transition, 2. Develop relevant sector-wide guidelines that support QS transition, 3. Migrate non-PQC systems of CAs to selected QS cryptographic solutions, 4. Facilitate an expertise center for QS transition to share knowledge and skills needed for QS transition, 5. Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems and 6. Monitor, adapt, and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes. The results showed that actions depended on the roles and responsibilities of organizations in the ecosystem. While some actions were of higher priority to regulatory organizations and CA, PKI users didn't view it as their primary responsibility and stated that decisions should be made at the central level of the government, which they would follow.

The cognitive relevance indicates the extent to which the list of actions contributes to the growth of becoming a QS. The results showed that all actions in the model contribute to the growth of becoming a QS. As the participants unanimously agreed that the list of actions in the growth model contributes to the growth towards becoming QS, three key insights have been shared to prepare for QS

transition. First, there needs to be a focus on the organizational aspects of QS transition. Second, many questions about the testing environment are left unanswered, which also signals ongoing uncertainty and organizations' concerns about the potential risks involved in the QS transition. Third, integration of knowledge across organizations is needed to learn from the experiences and best practices in the industry. For regulatory organizations, collaboration may also extend to the EU level, where member states can share knowledge and the process towards their transitions to PQC. However, differences in efforts and decisions on transition may also be witnessed across the jurisdictions, as different national rules and policies may apply.

Moreover, the actionability of actions was assessed to understand which actions can be realized at each respective stage. While the actions at Stage 1 of the growth model for QS transition scored high on actionability, actions at later stages scored low on actionability. Due to a lack of a clear timeline, it was difficult for experts and intended users of the growth model to indicate whether the actions at the later stage of the growth model are actionable. The low actionability also indicated that there needs to be a coordinated approach to realize these actions stage by stage for QS transition. For actions that were not actionable at an earlier stage, three key insights were shared to prepare for QS transition. First, no regret moves (e.g., assessing supply chain dependencies, reviewing cryptographic policies, conducting risk assessment) can still take place, and organizations need to understand their infrastructures to prepare for QS transition. Second, vendor communication needs to occur so that expectations for QS products and services are discussed (e.g., pre-tender negotiations, provincial acceptance with conditions). Third, training and support are needed to collectively become QS.

The second part of the evaluation assessed the *usefulness* of the growth model based on four dimensions from the Technology Acceptance Model (TAM) framework, which are perceived usefulness, perceived ease of use, attitude toward use, and behavioral intention to use. First, the perceived usefulness indicated how useful the growth model is in addressing QS transition challenges. The results indicated that the growth model is useful in addressing QS transition challenges. While recognizing that not all actions and the details in the model have to be followed, the usefulness of the model lies in providing a system-level overview, recognizing QS transition challenges. Second, the perceived ease of use indicates how easy it would be to use the model. The results showed that the growth model is easy to use and flexible, allowing it to be tailored to different usage intentions. The

growth model also provided the right level of abstraction, capturing socio-technical transition challenges for QS transition that organizations need to prioritize.

Third, the attitude towards use indicates how well the model aligns with the current needs. The results showed that the model meets the current needs of organizations for CA and a moderate level of alignment for PKI users. Since changes in the ecosystem (e.g., QS technology, regulations, and other business needs) can influence prioritization, the model provided a good overview for organizations. The results indicated that the model would be useful for roles involving awareness, business continuity, transition planning, and change management, as the model is considered to be too high-level for project managers. Fourth, the behavioral intention to use refers to how likely one is to incorporate the model in work. The results indicated that organizations have intentions to incorporate the model in their work. For CAs, it is important to discuss the topic of QS transition in the ecosystem, as multiple stakeholders are needed to facilitate their cross-organizational business processes. While this was also true for PKI users in the public sector, many decisions still need to be made at the central level, so they will follow the lead.

Going forward, this research is the first to develop a growth model for supporting organizations in their QS transition, grounded in QS transition challenges and how organizations can collectively become QS. By dissecting QS transition into a series of stages, the growth model translates the complexity of achieving quantum safety into a high-level overview that both experts and non-experts can understand. While discontinuities signal that organizations need to navigate changes in the ecosystem, they need to identify the current stage they are in and develop transitional capabilities so that they can be ready to move with the ecosystem. The list of QS transition capabilities shows capabilities that may be needed across organizations at the inter-organizational level and intra-organizational level. For practitioners, the findings of this research imply that achieving quantum safety in PKI systems that many critical infrastructures depend on must be collectively achieved to stay secure and compliant. The growth model can be tailored to different organizations and can further be used as a guidance tool and communication instrument within organizations and across organizations. In doing so, the result of this research not only helps organizations to move to the quantum era but also helps in maintaining their strategic fit over time with the evolving challenges in the security landscape.

The research concludes with recommendations for future research directions on the topic of QS transition. The potential research streams can be divided into conceptual, empirical, and practical. In the conceptual category, three future research avenues are identified. First, future research can investigate the list of QS

transition capabilities at each stage of the growth model to better understand how these capabilities can be developed within and across organizations. Second, future research can explore institutional change and risk governance to understand how institutions evolve their security landscape and how organizations respond to long-term threats posed by disruptive technological triggers**.** Third, future research may investigate how PQC can be integrated with QKD and offer new insights into safeguarding digital communication and information exchanges. The list of socio-technical transition challenges and the stages of growth model for QS transition presented in this research may provide a starting point that is relevant to QKD and can also be further extended.

In the empirical category, three future research avenues can be explored. First, future research could extend the list of QS transition challenges and how these challenges were addressed. Second, the research can further validate the discontinuities per stage in the growth model and actions needed across organizations. As QS transition remains in its early stages at the time of this research, the work concludes with an evaluation on the relevance and usefulness of the model, as an empirical evaluation of the application of the model was not yet possible. An empirical evaluation of the model can further contribute to theory building with a stronger empirical foundation, which may lead to new insights on QS transition. Third, additional research can be conducted in other contexts and applied to growth models in various sectors and countries. This may provide comparative perspectives (e.g., similarities and differences in QS transition processes) and strengthen empirical investigation from multiple cases on PKI systems.

In the practical category, three future research avenues are suggested. First, future research can further improve the growth model and stage-specific actions across different organizations into clear, step-by-step guidance that organizations can follow for practical implementation. Second, research can be conducted to integrate new insights and knowledge gained from the growth model into existing security frameworks. Organizations may further enhance widely used governance models and standards such as COBIT, NIST CSF, and ISO27001, to support more informed decision-making and better coordination across security practices. Third, the research can further advance the topic of cryptographic agility in organizations' security strategies and examine how organizations can implement long-term cryptographic change. Last, more research is needed to examine how practical initiatives in organizations, such as targeted training, knowledge sharing practices, and integration of tools, can support a robust security posture in the quantum era.

Samenvatting

Public Key Infrastructures (PKIs) zorgen voor een veilige en betrouwbare omgeving voor digitale interacties in de huidige datagedreven wereld. PKIs worden gebruikt in tal van netwerken, inclusief financiële, overheids-, energie- en telecommunicatienetwerken. Kritieke informatie-infrastructuren zijn afhankelijk van PKI's voor veilige digitale communicatie en informatie-uitwisseling. Met een combinatie van hardware, software, beleid en procedures spelen PKI's een essentiële rol in het bieden van een beveiligingsraamwerk dat digitale identiteiten beheert tussen apparaten, applicaties, gebruikers en netwerken. Voor de huidige klassieke computers worden PKI's over het algemeen als veilig beschouwd en zijn ze in de praktijk vrijwel niet te breken met de huidige veelgebruikte cryptografische algoritmen, zoals RSA (Rivest-Shamir-Adleman), DHKE (Diffie-Hellman key exchange) en ECC (Elliptic Curve Cryptography). Echter, met de komst van een cryptografisch relevante kwantumcomputer (CRQC) zullen deze algoritmen niet langer meer veilig zijn.

Om de dreigingen van cryptografisch relevante kwantumcomputers aan te pakken, worden oplossingen ontwikkeld op basis van Post-Kwantum Cryptografie (PQC). Experts verwachten dat PQC moeilijk op te lossen zijn voor zowel klassieke als kwantumcomputers en daarom geschikt zijn voor kwantumveilige (QS) systemen. Na jaren van onderzoek heeft het National Institute of Standards and Technology (NIST) in augustus 2024 een reeks standaarden voor PQC aangekondigd. Echter, een nieuw gestandaardiseerde PQC-oplossing kan niet van de ene op de andere dag worden geïmplementeerd, vanwege de vele technologische afhankelijkheden binnen PKI-systemen. Daarnaast bestaan er onzekerheden rond de ontwikkeling van QS-technologie, waaronder hardware en software die QS-cryptografie ondersteunen. Veel organisaties missen hierdoor een duidelijke richting en beschikken over beperkte kennis over de QS-transitie.

Omdat essentiële diensten binnen kritieke infrastructuren afhankelijk zijn van PKI's, is de QS-transitie een relevant en cruciaal onderwerp voor nationale veiligheid en publieke veiligheid. Dit onderzoek richt zich op het identificeren van belangrijke uitdagingen in de QS-transitie, met een focus op PQC, en op het bieden van een op stadia gebaseerd groeimodel dat organisaties ondersteunt bij de transitie naar QS-PKI's. Hiervoor is de volgende hoofdonderzoeksvraag geformuleerd: *"Wat zijn de belangrijkste uitdagingen en welke groeistadia kunnen organisaties volgen om te migreren naar kwantumveilige (QS) PKI-systemen?"* Om deze vraag te beantwoorden zijn vier deelvragen opgesteld.

Dit onderzoek is opgebouwd in vier fasen, waarbij elke fase correspondeert met één van de deelvragen. In de eerste fase worden de socio-technische transitie-uitdagingen onderzocht. In de tweede fase worden afhankelijkheden tussen deze uitdagingen geanalyseerd om op basis daarvan een model gebaseerd op verschillende groeistadia te ontwikkelen. De derde fase onderzoekt welke transitieve vaardigheden organisaties nodig hebben om van het ene naar het volgende stadium te bewegen. In de vierde en laatste fase worden de relevantie en bruikbaarheid van het groeimodel geëvalueerd. Hierbij wordt gekeken of het model aansluit bij de behoeften van experts en praktijkprofessionals en bruikbaar is als hulpmiddel voor QS-transitie. Met een aanpak op basis van verschillende onderzoeksmethoden bouwt deze fase voort op de eerdere resultaten en geeft deze verder context.

In de eerste fase is kennis opgedaan over PKI-systemen in de context van de QS-transitie door het onderzoeken van transitie-uitdagingen. De eerste deelvraag is dan ook: *"Welke uitdagingen belemmeren organisaties in de transitie naar QS PKI-systemen?"* Via een systematische literatuurstudie (SLR) zijn relevante uitdagingen geïdentificeerd. Vervolgens zijn deze verfijnd via semigestructureerde interviews met experts uit de Nederlandse publieke sector. Door literatuur en praktijk te combineren is een set van 15 socio-technische transitie-uitdagingen vastgesteld.

De transitie-uitdagingen zijn ingedeeld in drie categorieën. In de technologische categorie vallen de beschikbaarheid van QS-standaarden, het gebrek aan duidelijke standaarden en selectiecriteria, het ontbreken van betrouwbare en veilige QS-oplossingen, het bestaan van niet-PQC systemen (zoals Certificate Authorities en gebruikers), en het tekort aan QS-hardware en software. In de organisatorische categorie gaat het om een gebrek aan urgentie binnen organisaties, het ontbreken van een businesscase voor QS-transitie, onvoldoende kennis binnen organisaties, een tekort aan technische vaardigheden en gekwalificeerd personeel, en het ontbreken van QS-governance binnen organisaties. In de ecosysteemcategorie spelen complexe technische afhankelijkheden, een gebrek aan samenwerking, een gebrek aan urgentie binnen het bredere ecosysteem, het ontbreken van QS-governance op ecosysteemniveau, en een tekort aan beleid en regelgeving een belangrijke rol. Samen laten deze transitie-uitdagingen zien dat QS-transitie een complexe socio-technische uitdaging is.

De tweede fase richtte zich op de vraag: *"Welke groeistadia en discontinuïteiten bestaan er voor QS PKI-systemen?"* Op basis van de ISM-MICMAC-methode zijn afhankelijkheden tussen uitdagingen geanalyseerd die gevonden zijn in workshops met Nederlandse publieke organisaties. Dit resulteerde in een hiërarchisch model van uitdagingen dat de basis vormt voor de groeistadia.

Discontinuïteiten zijn als grensvoorwaarden tussen stadia in het groeimodel en laten zien dat je van een stadium naar een ander stadium kunt gaan. In de groeistadia wordt aangegeven aan welke voorwaarden in het ecosysteem vervuld moeten zijn om door te kunnen groeien naar een volgend stadium. Het groeimodel bestaat uit vijf stadia: 1. QS-bewustwording, 2. QS-beoordeling, 3. QS-voorbereiding, 4. QS-implementatie, 5. QS-adaptatie. De resultaten laten zien dat de QS-transitie niet geïsoleerd kan plaatsvinden; samenwerking binnen het ecosysteem is noodzakelijk.

In de derde fase is de volgende vraag onderzocht**:** *"Welke capaciteiten zijn nodig voor QS PKI-systemen?"* De benodigde capaciteiten zijn afgeleid van organisatorische acties, die op hun beurt zijn gebaseerd op de uitdagingen op organisatorisch niveau. Deze kernacties per fase zijn vervolgens vertaald naar een lijst met transitieve capaciteiten. Op basis van de Dynamic Capability Theory zijn deze capaciteiten ingedeeld in drie typen: sensing, seizing en transforming. De transitieve capaciteiten in Stadia 1 en 2 worden geclassificeerd als sensing-capaciteiten**,** die gericht zijn op het detecteren van kansen en het inschatten van bedreigingen. Transitieve capaciteiten in Stadia 3 en 4 vallen onder seizing-capaciteiten, die zich richten op het mobiliseren van middelen om waarde te benutten uit geïdentificeerde kansen en om te reageren op bedreigingen. Tot slot worden de capaciteiten in Stadia 5 geclassificeerd als transforming-capaciteiten**,** die gericht zijn op het behouden van concurrentievermogen door het beschermen en herstructureren van zowel immateriële als materiële activa.

De vierde en laatste fase van het onderzoek richtte zich op deelvraag 4: *"In hoeverre is het groeimodel voor QS-transitie relevant en bruikbaar voor organisaties?"* Omdat QS-transitie zich nog in een vroege fase bevindt op het moment van dit onderzoek, was het nog niet mogelijk om kwantumveiligheid in de praktijk te realiseren. Het ontwikkelde groeimodel is daarom niet bedoeld om vast te leggen wat al bekend is, maar juist om te bepalen in welk stadium organisaties zich bevinden en volgende stappen te suggereren. Het model fungeert daarmee als een toekomstgericht instrument dat organisaties kan ondersteunen om kwantumveilig te worden**.**

Het groeimodel is in twee delen geëvalueerd. Het eerste deel onderzocht of het model de relevante socio-technische uitdagingen en bruikbare handvatten voor QS-transitie goed weergeeft. In het tweede deel werd geanalyseerd in hoeverre het model aansluit bij de behoeften van experts en praktijkprofessionals en of het bruikbaar is als hulpmiddel voor organisaties in hun transitie naar QS.

In het eerste deel van de evaluatie zijn vier dimensies onderzocht: contextuele relevantie, thematische relevantie, cognitieve relevantie en

actiegerichtheid. Contextuele relevantie verwijst naar de mate waarin acties als essentieel worden gezien. De resultaten lieten zien dat negen acties als zeer essentieel werden beoordeeld: (1) het vergroten van bewustwording over het belang van QS-cryptografie, (2) het definiëren van duidelijke rollen, verantwoordelijkheden en besluitvormingsstructuren voor QS-governance, (3) het uitvoeren van assessments om risico, gereedheid en impact van de QS-transitie te bepalen, (4) het ontwikkelen van gecertificeerde hardware en software die geschikt zijn voor QS-cryptografie, (5) het opstellen van sectorbrede richtlijnen ter ondersteuning van de QS-transitie, (6) het migreren van niet-PQC-systemen van Certificate Authorities naar geselecteerde QS-oplossingen, (7) het aanpassen van delen van bestaande systemen op kleinere schaal met QS-cryptografie, (8) het afronden van de adoptie van QS-oplossingen binnen alle systemen op grote schaal, en (9) het monitoren en aanpassen van beveiligingspraktijken om snel te kunnen inspelen op nieuwe inzichten en veranderingen in regelgeving en technologie.

Uit de resultaten blijkt dat deze negen acties vooral als essentieel worden gezien door organisaties die QS-transitie als een belangrijk strategisch vraagstuk beschouwen. Voor PKI-gebruikers verschillen de te nemen acties per organisatie, afhankelijk van risicobereidheid, businesscase en beschikbare middelen.

De thematische relevantie geeft aan in hoeverre de acties aansluiten bij de behoeften van organisaties. Hierbij gaat het onder andere om het uitvoeren van risico- en impactanalyses, het ontwikkelen van sectorbrede richtlijnen, de migratie van systemen van Certificate Authorities naar QS-oplossingen, het opzetten van een expertisecentrum voor kennisdeling, het opschalen van QS-adoptie en het continu monitoren en aanpassen van beveiligingsmaatregelen. De resultaten laten zien dat de relevantie van de te nemen acties sterk afhankelijk is van de rol van organisaties binnen het ecosysteem. Waar sommige acties prioriteit hebben voor regulerende organisaties en Certificate Authorities, beschouwen andere organisaties deze vaak niet als hun primaire verantwoordelijkheid en geven zij aan dat besluitvorming op centraal overheidsniveau moet plaatsvinden.

De cognitieve relevantie geeft aan in welke mate de lijst met acties bijdraagt aan de ontwikkeling richting kwantumveiligheid. De resultaten laten zien dat alle acties in het model bijdragen aan deze groei. Omdat de deelnemers unaniem aangaven dat de acties in het groeimodel bijdragen aan de transitie naar QS, zijn drie belangrijke inzichten geformuleerd ter voorbereiding op de QS-transitie. Ten eerste moet er meer belang worden gegeven aan de organisatorische aspecten van de QS-transitie. Ten tweede blijven er veel vragen over de testomgeving onbeantwoord, wat eveneens wijst op aanhoudende onzekerheid en op de zorgen van organisaties

over de mogelijke risico's van de QS-transitie. Ten derde is integratie van kennis tussen organisaties noodzakelijk om te leren van ervaringen en best practices binnen de sector. Voor regulerende organisaties kan deze samenwerking zich bovendien uitbreiden naar EU-niveau, waar lidstaten kennis en ervaringen met hun PQC-transitie kunnen delen. Tegelijkertijd kunnen er verschillen blijven bestaan in aanpak en besluitvorming tussen jurisdicties, omdat de nationale regels en het nationale beleid kunnen verschillen.

Daarnaast is de actiegerichtheid van de acties beoordeeld om te bepalen welke acties in elke fase daadwerkelijk uitvoerbaar zijn. Waar de acties in stadium 1 van het groeimodel voor QS-transitie hoog scoorden op actiegerichtheid, was dit bij latere stadia duidelijk lager. Door het ontbreken van een duidelijke tijdslijn vonden experts en beoogde gebruikers het lastig om te beoordelen of acties in latere fasen daadwerkelijk uitvoerbaar zijn. De lage actiegerichtheid wijst er bovendien op dat een gecoördineerde aanpak nodig is om deze acties stap voor stap te realiseren. Voor acties die in eerdere fases nog niet uitvoerbaar zijn, zijn drie belangrijke inzichten geformuleerd ter voorbereiding op de QS-transitie. Ten eerste kunnen zogenoemde *no-regret moves* (zoals het analyseren van afhankelijkheden tussen organisaties, het herzien van cryptografisch beleid en het uitvoeren van risicoanalyses) al wel worden uitgevoerd, zodat organisaties hun infrastructuur beter begrijpen en zich voorbereiden op de QS-transitie. Ten tweede is communicatie met hardware- en softwareleveranciers noodzakelijk om verwachtingen rondom QS-producten en -diensten af te stemmen, bijvoorbeeld via pre-tendergesprekken. Ten derde zijn training en ondersteuning nodig om de transitie naar QS gezamenlijk te kunnen realiseren.

Het tweede deel van de evaluatie beoordeelde de bruikbaarheid van het groeimodel op basis van vier dimensies uit het Technology Acceptance Model (TAM): de ervaren bruikbaarheid, ervaren gebruiksgemak, houding ten opzichte van gebruik en de gedragsintentie tot gebruik. Ten eerste liet de ervaren bruikbaarheid zien in hoeverre het groeimodel helpt bij het overwinnen van QS-transitie-uitdagingen. De resultaten geven aan dat het model hierin waardevol is. Hoewel niet alle acties en details strikt gevolgd hoeven te worden, ligt de meerwaarde vooral in het bieden van een systemisch overzicht van de belangrijkste uitdagingen.

Als tweede dimensie geeft het ervaren gebruiksgemak aan hoe eenvoudig het model in gebruik is. De resultaten laten zien dat het groeimodel eenvoudig en flexibel is, waardoor het kan worden aangepast aan verschillende gebruiksdoelen. Daarnaast biedt het model het juiste abstractieniveau door de relevante socio-

technische uitdagingen van de QS-transitie inzichtelijk te maken en te helpen prioriteren.

De derde dimensie laat de houding ten opzichte van het gebruik zien in hoeverre het model aansluit bij de huidige behoeften. De resultaten tonen aan dat het model goed aansluit bij de behoeften van Certificate Authorities en een redelijke mate van afstemming biedt voor andere organisaties. Omdat ontwikkelingen in het ecosysteem, zoals QS-technologie, regelgeving en bedrijfsbehoeften, de prioritering kunnen beïnvloeden, biedt het model vooral een nuttig overzicht voor organisaties. Het model sluit met name goed aan bij rollen die zich richten op bewustwording, businesscontinuïteit, transitieplanning en verandermanagement, maar is mogelijk te abstract voor projectmanagementdoeleinden.

Ten slotte verwijst de dimensie over gedragsintentie tot gebruik naar de bereidheid om het model daadwerkelijk toe te passen. De resultaten laten zien dat organisaties van plan zijn het groeimodel in hun werkzaamheden te gebruiken. Voor Certificate Authorities is het daarbij belangrijk om QS-transitie actief te bespreken binnen het ecosysteem, aangezien andere organisaties nodig zijn om kwantumveiligheid te realiseren. Dit geldt ook voor PKI-gebruikers in de publieke sector, al moeten veel beslissingen daar nog op centraal overheidsniveau worden genomen, waardoor zij in de praktijk vaak het beleid zullen volgen.

Dit onderzoek het eerste onderzoek dat een groeimodel heeft ontwikkeld ter ondersteuning van organisaties in hun transitie naar kwantumveiligheid. Het groeimodel is gebaseerd op de bijbehorende transitie-uitdagingen en de manier waarop organisaties gezamenlijk QS kunnen worden. Door de QS-transitie op te splitsen in een reeks fasen, vertaalt het groeimodel de complexiteit van het realiseren van kwantumveiligheid naar een abstract overzicht dat zowel experts als niet-experts kunnen begrijpen. Discontinuïteiten geven daarbij aan dat organisaties veranderingen in het ecosysteem moeten navigeren. Tegelijkertijd moeten zij hun huidige fase bepalen en transitieve capaciteiten ontwikkelen, zodat zij kunnen meebewegen met deze veranderingen. De lijst met QS-transitiecapaciteiten laat zien welke capaciteiten nodig kunnen zijn op zowel interorganisatorisch als intra-organisatorisch niveau. Voor praktijkprofessionals betekent dit dat het realiseren van kwantumveiligheid in PKI-systemen, waarvan veel kritieke infrastructuren afhankelijk zijn, collectief moet gebeuren om veilig en compliant te blijven. Het groeimodel kan worden aangepast aan de wensen van organisaties en kan worden gebruikt als richtlijn en communicatiemiddel binnen en tussen organisaties. Daarmee helpt dit onderzoek organisaties niet alleen om de overstap naar de

kwantumveiligheid te maken, maar ook om hun strategische afstemming te met het veranderende beveiligingslandschap.

Het onderzoek wordt afgesloten met aanbevelingen voor toekomstige onderzoeksrichtingen rond QS-transitie. Deze kunnen worden onderverdeeld in conceptueel, empirisch en praktisch onderzoek. Binnen de conceptuele categorie zijn drie richtingen geïdentificeerd. Ten eerste kan toekomstig onderzoek zich richten op de verdere uitwerking van QS-transitiecapaciteiten per fase van het groeimodel, om beter te begrijpen hoe deze binnen en tussen organisaties ontwikkeld kunnen worden. Ten tweede kunnen institutionele veranderingen en risicomanagement worden onderzocht, om inzicht te krijgen in hoe instituties hun beveiligingslandschap aanpassen en hoe organisaties reageren op lange termijn bedreigingen veroorzaakt door disruptieve technologische ontwikkelingen. Ten derde kan worden onderzocht hoe PQC kan worden geïntegreerd met QKD, wat nieuwe inzichten kan bieden in het beveiligen van digitale communicatie en informatie-uitwisseling. De in dit onderzoek gepresenteerde socio-technische transitie-uitdagingen en groeistadia kunnen hierbij dienen als relevant startpunt dat ook verder kan worden uitgebreid in relatie tot QKD.

Binnen de empirische categorie zijn eveneens drie toekomstige onderzoekrichtingen te onderscheiden. Ten eerste kan toekomstig onderzoek de lijst met QS-transitie-uitdagingen uitbreiden en onderzoeken hoe deze in de praktijk kunnen worden aangepakt. Ten tweede kan het model verder worden gevalideerd door de discontinuïteiten per fase en de benodigde acties binnen organisaties te toetsen. Omdat QS-transitie zich nog in een vroeg stadium bevindt, is dit onderzoek afgesloten met een evaluatie van de relevantie en bruikbaarheid van het model; een empirische toepassing kon nog niet worden uitgevoerd. Een dergelijke empirische validatie kan echter bijdragen aan theorievorming met een sterkere empirische basis en mogelijk nieuwe inzichten opleveren over QS-transitie. Ten derde kan aanvullend onderzoek worden uitgevoerd in andere contexten, sectoren en landen, om vergelijkende perspectieven te bieden (zoals overeenkomsten en verschillen in QS-transitieprocessen) en empirisch onderzoek op basis van meerdere PKI-cases te versterken.

Binnen de praktische categorie zijn eveneens drie richtingen voorgesteld. Ten eerste kan toekomstig onderzoek het groeimodel verder verfijnen tot concrete, stapsgewijze richtlijnen die organisaties kunnen gebruiken voor implementatie. Ten tweede kan worden onderzocht hoe inzichten uit het groeimodel kunnen worden geïntegreerd in bestaande beveiligingsraamwerken. Organisaties kunnen bestaande modellen en standaarden zoals COBIT, NIST CSF en ISO27001 verder versterken

om betere besluitvorming en coördinatie binnen beveiligingspraktijken te ondersteunen. Ten derde kan het onderzoek bijdragen aan de verdere ontwikkeling van cryptografische wendbaarheid binnen beveiligingsstrategieën en aan het begrijpen hoe organisaties langdurige cryptografische veranderingen kunnen implementeren. Tot slot is verder onderzoek nodig naar hoe praktische initiatieven binnen organisaties, zoals gerichte training, kennisdeling en de integratie van tools, kunnen bijdragen aan een robuuste beveiligingspositie.

Preface

When I first moved to the Netherlands for my master's degree, I had no idea what the journey would look like. I did not know I would move from Nijmegen, Utrecht to Delft, three beautiful cities across three provinces that each offered their own chapter. I did not know I would intern at a provincial government, begin a PhD, visit (inter)national organizations in The Hague, and be invited to speak at events and companies I once admired from afar. For this, I am deeply grateful.

Many stories could be told. But what feels most important right now is to pause and reflect on the journey that shaped both the work presented here and the person I became while completing it. When I began my PhD, I stepped into a field that was entirely new to me. The topics, such as post-quantum cryptography, information systems, and quantum computing technology, were far outside my original expertise. Yet, these topics sparked a curiosity that I could not ignore.

What began in wonder, though, soon became a test of perseverance, confronting in the face of unexpected challenges. I wrestled with a steep learning curve, countless hours of revision, and the subtle gnaw of imposter syndrome. Long hours of solitude carried the weight of my struggles, and some days ended with nights of quiet tears. Through it all, I came to realize that every journey holds its own lessons, and the value we find depends on how we embrace them. This journey toward independence as a researcher became a rare gift that I chose to embrace wholeheartedly, unfolding insights and lessons I could not have anticipated.

Each struggle not only taught me the skills needed to be an independent researcher but also offered insights that deepened my understanding of myself. Through recognizing my strengths, building resilience, and confronting my limitations with honesty and remaining humble, these experiences shaped me not just as a researcher but as a person. I came to learn that growth does not come from repetition alone but from pushing yourself beyond the familiar, reflecting deeply, challenging assumptions, and allowing myself to be challenged in return.

Now, I can stand firmly on this foundation. As a person, I have learned to navigate the tides of struggles instead of pushing against them. I have grown to embrace challenges, to find strength in vulnerability, and to navigate uncertainty with resilience. I have come to appreciate the value of being a connector and bringing together ideas and data while actively participating in the exchange of knowledge within and beyond research communities.

As a researcher, I am contributing to a growing body of knowledge and welcome others to shape it further, with the hope that our collective efforts will create meaningful societal impact. I learned that being a researcher is more than just

enthusiasm for the work. It also involves communicating it, advocating for it, and helping others see its value.

With this dissertation, I close a journey that taught me to look beneath the surface, to stay humble, and to move forward with patience and resilience. The challenges, lessons, and reflections gathered will travel with me and continue to shape the work still to come. I hope that the research presented here carries its own weight and that the experiences behind it contribute to the ongoing transition to Post-Quantum Cryptography in the years ahead.

For now, I offer these pages as a record of the journey and as a quiet testament to what it has taught me, as I prepare for the steps that follow. I hope this work brings insight, clarity, and perhaps a moment of reflection.

Warm regards,
Ini Kong

Acknowledgements

Through rain and shine, I've received guidance and encouragement from those around me. I want to dedicate this page to those who accompanied me on this journey. I want to acknowledge these special people and express my deepest gratitude. Without you, I would not be here today.

Mentors come in many forms, but there is no doubt that they leave a lasting impact on our lives and guide the steps we take.

First and foremost, I want to thank my mentor, **Marijn Janssen**, whose forward-thinking guidance and support for independent thinking have profoundly shaped my journey. He not only fueled my curiosity for research but also offered thoughtful insights and guidance at every step. With his keen insights into the strengths of PhD researchers and a thoughtful balance of guidance and trust, he provided me with the confidence and space to reflect, explore, and grow as a researcher. His support encouraged me to embrace challenges, learn from them, and cultivate my own perspectives, shaping the way I think, learn, and grow academically and professionally. I carry these lessons with me, and I aspire to one day become a mentor who empowers others with the same trust and encouragement that he so naturally gave.

Second, I want to thank my mentor, **Nitesh Bharosa**, whose depth of knowledge and experience brought a deeply collaborative spirit to my journey, one that continually reminded me that research does not exist in isolation. Through our shared discussions, sparring sessions, and problem-solving, he challenged me to refine my thinking, pay attention to detail, and articulate my ideas with clarity and rigor. His guidance taught me to balance precision with vision, to see the trees without losing sight of the mountain. Working closely with him has shaped not only how I approach research but also why I pursue it, teaching me that open dialogue and collective effort, guided by high standards, can push one to grow far more than one might expect.

Complementing my mentors in academia, I would also like to express my sincere gratitude to my mentor in practice, **Albert de Ruiter**. Thank you for the opportunities to engage directly with the topics and for giving me the space to grow within the PQC and PKI community. Through your professionalism, your keen business acumen, and the humility with which you share your knowledge and understanding, I have gained insights that have been truly invaluable to me. Always willing to listen and engage, you have created an environment where ideas are shared openly and thoughtfully, fostering collaboration and growth. I am grateful for your

guidance in showing the value of connecting ideas and promoting meaningful knowledge exchange across research communities and practical applications.

Moreover, I want to extend my heartfelt thanks to the **HAPKIDO project team.** Thank you for your support throughout these years, **Alessandro Amadori, Andre Smulders, Dayana Spagnuelo, Gabriele Spini, Julia Kastner, Michele Marcus, Manon de Vries, Rene Bakker, Serge Fehr, Yoram Meijaard,** and **Yu-Hsuan Huang.** This work would not have been possible without your dedication.

I want to highlight our research partners at **CWI, KPN, Logius, Microsoft, NWO,** and **Zynyo** for their essential contribution. Through both challenges and successes, your trust and willingness to share knowledge created an environment in which both the research and the people involved could thrive. I am grateful for the shared effort and sense of community that carried this project forward.

Appreciation is also extended to the individuals in practice for their guidance and generous contributions of time and expertise. Thank you, **Anita Wehmann, Dimitri van Esch, Lizzy Polman, Oscar Koeroo, Paul van Brouwershaven,** and **Pieter Schneider,** for providing the opportunity to exchange knowledge and for the support that has helped bring this research to light. Your engagement and commitment to the topic have been inspiring and have strengthened the impact of this work.

Along this journey, I had the privilege of learning from fellow PhD researchers at TPM, past and present, with whom I shared this path and broadened my horizons: **Antonia Sattlegger, Antra Ewa Abbas, Cathleen Parsons, Cilia Baanstra, Davide Di Staso, Ema Gusheva, Esra Zorer, Gilang Ramadhan, Hong Yan, Íñigo Martínez de Rituerto de Troya, Jessie Lou, Josephine Vos, Julia Barashkov, Lærke Christiansen, Liubov Pilshchikova, Louise van der Peet, María Palacios Barea, Prachi Bagave, Reni Sulastri, Sem Nouws, Steven Yoo, Wendy van Donge, Wiebke Hutiri,** and **Wirawan Agahari.**

I would also like to extend my gratitude to the faculty and staff members. Thank you for your support and for sharing your expertise during this journey. Thank you, **Aaron Ding, Anneke Zuiderwijk-van Eijk, Boriana Rukanova, Ellen Schwencke-Karlas, Fanny Voets, Fernando Kleiman, Ilse Oonk, Ivo Bouwmans, Jolien Ubacht, Maarten Kroesen, Marcela Tulder De Oliverira, Mark de Reuver, Nicolas Dintzner, Pieter Vermaas, Roel Dobbe, Roland Ortt,** and **Yao-Hua Tan.**

I am also grateful to the many colleagues and experts I met through **PKI** and **PQC consortia, DG.O, EGOV, ICEGOV,** and **ONE conferences,** and during the **International Cyber Security Summer School.** While it is not possible to name

each of you, I am sincerely grateful for your time, your willingness to listen, and your support. These connections made this journey richer and more meaningful.

Moreover, thank you, **Ilse Parra** and **Martha van den Bergh,** with whom I volunteer at the Skilling and Education team for Women4Cyber. You are a source of inspiration. I have always felt welcome and heard. I look forward with great excitement to the next chapter of our work together, strengthening visibility for women in the field of cybersecurity. I would also like to thank **Barbara Meixner** for her support as I navigate my professional path.

Last but not least, I owe special thanks to my friends and family for their understanding and belief in me throughout the challenges and milestones of this research. Home away from home in Berlin, Ho Chi Minh City, Seoul, Toronto, and Vienna has kept me grounded throughout this journey. Thank you for always welcoming me and supporting me. Thank you, **Haein & Aaron, Heather, Hojj, GG, Jennie, Jay, Kyujin, Lyuba, Melodie, Mike, Minji, Pia & Sebastian, Sean, Sunghyun, Sunny,** and **Yujin.**

Thank you, **Hans, Philip & Hien, Rik & Natascha,** and **Wilma.** Our get-togethers always brighten my day and remind me of the joy in connection. Thank you, **Niek**, you have always been my biggest cheerleader. Thank you for your endless support and for giving up countless hours on weekends while I dedicated that time to focus on my research. Special thanks to my cat, **Nami,** who offered moral support in the form of soft purrs and occasional snuggles, reminding me to pause and enjoy the serenity of everyday life.

To **Mom and Dad**, "thank you" are the smallest words to express my gratitude for your support and for always believing in me. From the very beginning, you have encouraged me to follow my curiosity and never give up, even when the path seemed uncertain. Your patience, love, and guidance have been my anchor through every setback and every achievement. I am who I am today because of your sacrifices, your confidence in me, and your constant reminders that I am capable of more than I sometimes believe. I hope to make you proud as I continue to grow both personally and professionally.

List of Figures

List of Tables

Chapter 1 Introduction

This chapter presents the security challenges that may arise with the development of quantum computers and provides an outline of the dissertation with research motivation, objective, and research questions. Section 1.1 introduces the security challenges that may arise in the quantum era in the context of Public Key Infrastructure (PKI). Section 1.2 presents the motivations for the study, and research gaps are addressed in the study. Section 1.3 provides research objectives and research questions. The chapter concludes with section 1.4 with an outline of the dissertation.

Parts of this chapter are based on the following publications:
Kong, I. (2022). Transitioning towards quantum-safe government: Examining stages of growth models for Quantum-safe public key infrastructure systems. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022. https://doi.org/10.1145/3560107.3560182

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). https://doi.org/10.1145/3543434.3543644

1.1 Security Challenges in the Quantum Era

From text messages, emails, to banking transactions, the digital environment has become an integral part of our lives. With the growing activities in the digital realm, protecting information across time and space has become more important than ever. From government services to industries in finance, healthcare, telecommunication, and transportation, secure digital communication and information exchange prevent not only unauthorized access and security issues but also ensure public safety by maintaining continuous operation of essential services, such as financial transactions, utilities (e.g., water and electricity), and traffic control systems, etc. (Covers & Doeland, 2020; Krause et al., 2021; Lewis & Travagnin, 2022; OECD, 2024)

The use of *Public Key Infrastructure* (PKI) no longer makes securing digital communication and information exchange between devices, applications, users, and networks a daunting task. By generating, storing, distributing, and managing digital

certificates that act as digital identities, PKIs provide a high level of accountability, integrity, and confidentiality without the physical presence of individuals, businesses, and government agencies (Adams & Lloyd, 1999; Linn, 2000). With many of the critical infrastructures that are fundamental to the functioning of modern societies heavily depending on PKIs, it is crucial to protect PKIs from evolving security threats to secure our digital infrastructures (ENISA, 2025; European Commission, 2020).

In order to secure communication in the digital environment, PKI relies on *Public Key Cryptography* (PKC), which uses a key pair. The key pair includes one public key that must be verifiably authentic and one private key that must remain private (Adams & Lloyd, 1999). With sufficiently large key sizes, the encrypted information would take longer to decrypt for those who do not possess the key. Today's widely used PKC (e.g., Rivest-Shamir-Adleman (RSA), Diffie-Hellman key exchange (DHKE), and Elliptic Curve Cryptography (ECC)) that PKIs depend on provides the level of protection against hacks and other threats (Csenkey & Bindel, 2023; Mosca & Piani, M, 2023).

The strength of PKC is that it provides a foundation for the PKI environments, keeping the information confidential and secure (Adams & Lloyd, 1999; Linn, 2000; Paar & Pelzl, 2010). While this remains true for security issues that occur today with classical computers, quantum computers with strong enough computational power have the potential to break the entire cryptographic foundational layer that PKIs depend on. This implies that much of today's encryption and cryptographic algorithms may no longer be effective at securing information, and the infrastructures that depend on PKIs may no longer be reliable if security has been compromised.

The advancement of quantum computing technology introduces new security issues beyond vulnerabilities, such as poor passwords, data breaches, phishing scams, and malicious software updates. The Shor's algorithm, introduced in 1994 by Peter Shor, shows that the computational power of a quantum computer could be exponentially faster than a classical computer, and it may no longer be difficult to factor a key pair of large prime numbers (Shor, 1994). Using the quantum properties known as superposition, the quantum bits (qubits) can be a 0, a 1, or something in between, allowing the quantum computer to handle many possibilities to tackle certain problems. The availability of a powerful enough quantum computer can perform calculations and analyze complex cryptographic keys much faster than

today's classical computers, using bits as a basic unit of information, which can only be 0 or 1.

Moreover, a recent article in *Science* discusses the work of a computer scientist named Oded Regev, specifically Regev's algorithm, which could improve the efficiency of Shor's algorithm, albeit with increased memory requirements (Kramer, 2023). For other cryptographic algorithms not affected by Shor's Algorithm, Grover's algorithm can speed up the search process of the keys to decrypt the encryption (Grover, 1996). Since access to communication is needed to break the cryptography, *Store-Now, Decrypt Later* threats can occur with powerful enough quantum computers with data that requires long-term security (AIVD, 2021; Mosca & Piani, M, 2023). From government communications, financial transactions, and healthcare records to classified military information, sensitive data is at risk of future decryption. As digital infrastructure becomes increasingly dependent, this also means that security issues may no longer be limited in scope and impact, affecting public safety and national security.

As quantum computing technology remains a double-edged sword, presenting both opportunities and challenges, a growing ecosystem of quantum innovators is emerging across academia, national labs, and industries. On the one hand, the power of computation holds myriad possibilities for tackling complex problems. While practical application of the quantum computer has not yet been achieved, it was highlighted in 2019 that a 2048-bit RSA integer can be broken in only 8 hours with a 20-million-qubit computer (Gidney & Ekerå, 2021). The recent breakthrough from Google shows that the speed and error correction of the Willow chip perform better than its previous chip, the Sycamore (Castelvecchi, 2024; Google Quantum AI and Collaborators et al., 2024). Likewise, IBM has recently unveiled new quantum hardware and software capabilities that expand quantum algorithms' scale, speed, and accuracy (IBM, 2024). With the ambitions set out in IBM's Quantum Development Roadmap, the development of quantum computers is rapidly advancing in qubit numbers and error-correction techniques.

On the other hand, there is ongoing research on QS approaches that can resist attacks from classical and quantum computers. Two main types include (a) *Post Quantum Cryptography* (PQC) and (b) *Quantum Key Distribution* (QKD). While the former is based on their underlying mathematical principles (e.g., lattice-based, hash-based, etc.), the latter uses principles of quantum mechanics of qubits (e.g., superposition and entanglement) to distribute keys and detect any eavesdropping. With the recent publication of the first set of finalized PQC standards,

the US National Institute of Standards and Technology (NIST) has signaled that quantum threats are inevitable, and it may be crucial for organizations to transition their existing infrastructure to become QS (Alagic et al., 2022; NIST, 2024e).

1.2 Motivation for the Study

Although there are motivations across academia, industries, and government to develop QS solutions, transitioning the existing infrastructures remains complex. First, there are many technical uncertainties surrounding the development of QS solutions. Organizations are unsure which QS cryptographic algorithms will survive the testing phase. Likewise, practical compatibility has not yet been achieved for QS solutions (CCC, 2019; ISARA, 2018; Mashatan & Heintzman, 2021; NIST, 2018). With the selection of QS solutions not yet decided, it is unclear whether organizations need full substitutions or adopt hybrid architectures with both classical cryptographic algorithms and QS cryptographic algorithms combined. While many organizations face uncertain future trajectories, decisions regarding QS transition cannot be made independently due to interoperability and backward compatibility issues.

Second, there are multiple interdependencies among stakeholders, including standards bodies, governments, hardware vendors, software companies, service providers, and PKI users. By maintaining interoperability and backward compatibility, organizations prevent potential service disruptions in the existing infrastructures (CCC, 2019; The Hague Security Delta, 2019; Vermeer & Peet, 2020). However, unlike previous continuous control and maintenance efforts to address security issues, organizations may need to modify their cryptographic layers, which serve as the fundamental building blocks of infrastructure. Given the rigidity of the system, organizations find it difficult to implement changes without careful planning. With a set of roles, security policies, encryption mechanisms, and procedures already in place, there is no simple big bang approach to adopt these solutions without recognizing the complex interdependencies that exist in the installed systems (Barker et al., 2021b; Bindel et al., 2017; Broadbent & Schaffner, 2016).

As stricter EU-wide requirements are imposed on organizations from other policies and regulations (e.g., NIS 2 Directive), organizations may inevitably be held accountable for improving network security and information systems**.** However, it remains difficult for organizations to address all aspects of socio-technical predicaments. With varying levels of urgency, interests, and risk appetites for QS

transition, organizations may need to recognize the sufficient amount of lead time for their transitions and ensure that relevant stakeholders have the knowledge needed (Barker et al., 2021b; Mashatan & Heintzman, 2021; Mulholland et al., 2017; Vermaas, 2017). Likewise, decision-making (e.g., operational and strategic) needs to be adapted to the context and coordinated with relevant stakeholders (Ortt & Van Der Duin, 2008; Van Der Duin & Ortt, 2020). Yet, the uncertainties may result in an iterative, non-linear, and somewhat chaotic process (Dedehayir et al., 2022).

Research Gaps

Limited Research on QS Transition in the Field of Information Systems

As today's widely used cryptographic algorithms may no longer be reliable, new security vulnerabilities and issues from quantum threats raise concerns in the existing infrastructures. These include critical infrastructures across sectors that depend on Public Key Infrastructure (PKI) systems for digital communication and information exchange. Although research on the complexity of information systems is not new, the topic of QS transition is relatively new, and much attention is given to the technical development of QS cryptographic algorithms (Giron, 2023; Joseph et al., 2022; Käppler & Schneider, 2022; M. Kumar, 2022). The study extends knowledge on QS transition using a case study on the current PKI systems and captures various socio-technical challenges to understand the complexity of QS transition that organizations may need to be aware of. While these studies on technical aspects of QS transition provide valuable insights, transitioning the current PKI systems does not remain a technical challenge alone. As a result, previous research provides a partial understanding of how current PKI systems can become QS. Likewise, there is a lack of research on institutional, organizational, and policy aspects of QS transition, which provides limited insight into QS transition.

Lack of Knowledge of QS Transition Capabilities in Organizations

Organizations currently lack knowledge of the complexity of implementing and adopting QS cryptographic algorithms. Although QS cryptographic algorithms are a new technology that may require changes in organizations' operations in the existing business processes, there is little documentation and lessons learned available for organizations. As organizations currently lack knowledge of best practices and strategies for managing QS transition, the study offers practical insights on how organizations can move towards QS situations. The previous transitions (e.g., SHA1-SHA2, IP4-IP6, ECC, etc.) indicate that QS transition may

result in a longer transition time (NIST, 2024e). Due to technological interdependencies of PKIs that facilitate secure digital communication and information exchange, organizations may not be able to transition their existing infrastructures on their own. With varying levels of risk appetite, knowledge, and resources available, the direction for QS transition remains unclear, and organizations are uncertain about what is needed to prepare for QS transition. There is a lack of knowledge on the capabilities that organizations may need to transition their existing PKI systems to become QS.

Lack of Guidance on QS Transition Stages of Growth Model

While the existing security framework on critical infrastructures needs to remain flexible, secure, scalable, and reliable to communicate and exchange information, there is no guidance available for organizations to start the preparation for QS transition. With large numbers of different users, which include individuals, businesses, and other government agencies, QS transition may need to be carefully prepared to avoid potential disruptions. In doing so, the research uses theories on the stages of the growth model to dissect the QS transition into a series of stages. In both research and practice, the stages of growth model has become an important tool for assisting decision-makers. By assessing the current level of organization, the stages of growth model allow organizations to navigate their transition process and move from one stage to the next (Becker et al., 2009; Iversen et al., 1999). For practitioners, the stages of growth models may provide a prescriptive approach for QS transition and prevent possible lock-in and paralysis in transition efforts. Although various stages of growth models are available, the stages of the models are context dependent, and there is no ready-to-use growth model for organizations looking to transition to a QS future.

1.3 Research Objectives & Research Questions

This research aims to identify the key challenges involved in QS transition and to provide a stage-based growth model for organizations looking to transition to QS PKIs. The main research question for this research is: "*What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems?*" To answer the main research question, the following sub-questions have been formulated:

Sub-Question 1: *What are the challenges that hinder organizations in transitioning toward QS PKI systems?*
By answering sub-question 1, the research gains knowledge and insights into the PKI systems in the context of the QS transition. In Chapter 5, the challenges are identified from both research and practice. The list of challenges identified from the literature is discussed in Section 5.3. The list of challenges from the practice is discussed in Section 5.4. The list of challenges has been clustered using the Technology, Organization, and Environment (TOE) framework. By combining both results from the literature and practice, the refined list of challenges is presented to understand key transition challenges that may hinder organizations from transitioning their PKI systems to QS ones.

Sub-question 2: *What are the different stages in the growth model and discontinuities for QS PKI systems?*
By answering sub-question 2, the research develops a stages of growth model for QS transition. In order to extend the theories on the growth model, this research is the first to use the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach to provide a structured and systematic method for deriving different stages of the growth model. In Chapter 6, different stages and discontinuities in the growth model for QS transition are presented. The results from the ISM-MICMAC approach and the synthesized structural hierarchical model for QS transition challenges are discussed in Section 6.2. The five stages of the growth model are explained with a list of discontinuities in Section 6.3.

Sub-question 3*: What capabilities are needed across organizations for transitioning to QS PKI systems?*
By answering sub-question 3, the research identifies the QS transition capabilities required in organizations to progress from one stage to the next. In this research, QS transition capability refers to the ability that organizations need to develop in each stage to move to the next to achieve quantum safety. In Chapter 6, QS transition capabilities are further explored after introducing the five stages of the growth model and discontinuities for QS transition. In Section 6.4, the list of QS transition capabilities is clustered using sensing, seizing, and transforming categories based on Teece's dynamic capabilities. The section extends the discussion on the scope of influence to understand interdependencies across organizations and the process of

growth by learning and learning by growth as organizations move from one stage to the next in the growth model.

Sub-question 4: *To what extent is the growth model for QS transition relevant and useful for organizations?*
By answering sub-question 4, the research assesses the relevance and usefulness of the stages of growth model in gathering insights from experts and practitioners. In Chapter 7, the relevance of the growth model and the details presented are evaluated, as well as its potential usefulness. In Section 7.3.1, relevance is evaluated using dimensions such as contextual relevance, topical relevance, cognitive relevance, and actionability. In Section 7.3.2, the model's usefulness is evaluated using the Technology Acceptance Model (TAM), which encompasses dimensions such as perceived usefulness, perceived ease of use, attitude toward use, and behavioral intention to use.

1.4 Dissertation Outline

The structure of this dissertation is shown in Figure 1.

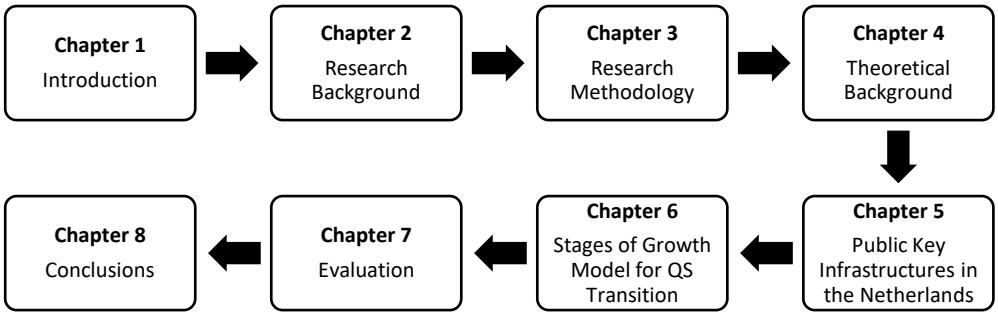


Figure 1: Overview of the Dissertation Chapters

After the Introduction presented in Chapter 1, Chapter 2 provides the technical background on Public Key Infrastructure (PKI), quantum computing technology, quantum threats, and QS transition. The background information on technologies lays the groundwork and presents the technical context for the study. Chapter 3 introduces research philosophy, research methodology, and data collection methods. The chapter describes interpretivism as part of research philosophy and discusses the scope and context of the case study. The overview of data collection methods is provided with examples of systematic literature review, interviews, workshops, and

surveys used in the research. In this chapter, the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach used to derive different stages of the growth model is further explained.

Chapter 4 provides an overview of the theoretical background of this research. The chapter reviews the core theories, such as the Stages of Growth Model and Dynamic Capabilities. The chapter discusses the related work and limitations of the current research. By doing so, the chapter not only highlights gaps in the existing theories and literature but also shows how this research can further extend the theoretical knowledge and provide practical significance to the context of the study. Chapter 5 introduces the case study research in the context of this research, which focuses on Public Key Infrastructure (PKI) in the Dutch public sector. The chapter discusses the significance of PKI services and introduces diverse organizations that are part of the PKI system. By examining PKI systems in the public sector as part of the case study, Chapter 5 answers sub-question 1 and provides in-depth knowledge on QS transition challenges that are involved in the complex PKI landscape.

Chapter 6 gives an overview of the stages of the growth model for QS transition. The first part of the chapter answers sub-question 2 and describes the results of ISM-MICMAC. This is further elaborated as the chapter explains how using a novel approach has been derived at different stages of the growth model. The chapter examines the list of discontinuities that act as the necessary conditions in the ecosystem that must be met and discusses the scope of influence that may exist between organizations across different levels (Ecosystem Level, Inter-organizational Level, and Intra-organizational Level). The second part of the chapter answers sub-question 3 and dives deeper into the actions and capabilities that may be needed in organizations. By using the growth model as a foundation for navigating QS transition, the chapter discusses key actions needed and a list of transitional capabilities that organizations need to develop to move from one stage to the next towards QS PKI systems.

Chapter 7 presents the evaluation process of the stages of the growth model. By outlining the importance of assessing the relevance and usefulness of the model, Chapter 7 answers sub-question 4 with the insights gained from the evaluation of the growth model. Chapter 7 discusses how feedback was received, and data were gathered for the evaluation process. Since the QS transition is at its early stage, the empirical testing and validation of the model are excluded, and focus solely on evaluating the relevance and usefulness of the growth model. The focus lies in providing the growth model as conceptual guidance, and whether practical insights

have been gained from evaluating the model when navigating QS transition processes and identifying the actions needed for organizations. What is not included in the chapter will be further discussed in Chapter 8 on limitations of the research and extend these with recommendations for future research.

The dissertation concludes in Chapter 8, primarily recapitulating the research context and revisiting the research question and goals. In doing so, the chapter provides an overview of the research scope, the motivations behind it, and a summary of the key findings. The findings are presented with emphasis on their contributions to both theoretical knowledge and practical application. By providing a reflection on the study, the chapter not only discusses the limitations of the research but also suggests ways to overcome these limitations, offering recommendations for future research with a focus on the fields of Information Systems and Digital Government. Chapter 8 provides a closure to this study with a reflection on moving forward.

Chapter 2 Background

2.1 Introduction

This chapter introduces the context of the research that focuses on the Public Key Infrastructure (PKI) and Quantum-safe (QS) Transition. The term QS Transition used in this dissertation refers to modifying the existing systems that currently use classical cryptographic algorithms to QS solutions that are based on Post-Quantum Cryptographic (PQC). In Section 2.2, the anatomy of PKI, including Public Key Cryptography (PKC), the technical components of PKI, and how they are operated, is introduced. Section 2.3 explains the development of quantum computers and how their advancement in computational power poses threats to PKIs. This is followed by Section 2.4, which further discusses the need for QS transition using QS cryptographic algorithms based on PQC. Finally, conclusions are drawn regarding the need for a stage-based growth model for organizations looking to transition to QS PKIs.

Parts of this chapter are based on the following publications:
Kong, I., Janssen, M., & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly.* 41(1), 101884. https ://doi.org/10.1016/j.giq.2023.101884

Kong, I. (2022). Transitioning towards quantum-safe government: Examining stages of growth models for Quantum-safe public key infrastructure systems. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022. https://doi.org/10.1145/3560107.3560182

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). https://doi.org/10.1145/3543434.3543644

2.2 Public Key Infrastructures

Section 2.2 provides background information on PKI, and it is divided into three sections. Section 2.2.1 introduces Public Key Cryptography (PKC), which is an important part of digital certificates and an encryption method used in the PKI. Section 2.2.2 explains key components of PKI and further elaborates on how PKI is facilitated. Section 2.2.3 discusses Certificate Authority (CA) hierarchy and the associated policies and practices.

Section 2.2.1 Public Key Cryptography (PKC)

In the field of cryptography, cryptographic primitives act as foundational building blocks for ensuring the security of information. For purposes of this study, the first part of section 2.2.1 briefly introduces two main encryption methods, symmetric encryption and asymmetric encryption, also known as Public Key Cryptography (PKC). The second part of this section further focuses on PKC and elaborates on the application of digital signatures in digital certificates that are used in Public Key Infrastructure (PKI).

Encryption Methods

Encryption methods are part of what is commonly known as cryptographic primitives. These are the essential building blocks of tools that function to keep information safe. By changing the information into an encrypted form, encryption allows only those intended to read the information to decrypt it. In a digital environment, the cryptographic key is a string of randomly generated characters represented in binary to encrypt or decrypt the information. Keys are a fundamental part of the encryption and decryption process and are essential for maintaining the security of the cryptographic system. The information is transformed from a plaintext (that is a readable format) to a ciphertext that is an unreadable format and vice versa. The two main encryption methods are illustrated in Figure 2.

In *symmetric encryption*, the data is encrypted and decrypted using the same key for both processes of encryption and decryption. The key is shared between the sender and recipient, so the shared key needs to remain private to communicate securely and decrypt the encrypted data (Adams & Lloyd, 1999; Hunt, 2001). Thus, anyone who intercepts without the matching keys cannot decrypt the information that has been encrypted. In *asymmetrical encryption, also known as public-key cryptography (PKC),* a key pair includes one public key and one private key. While the public key can be shared with anyone and used to encrypt data, the private key is kept secret and used to decrypt the data (Adams & Lloyd, 1999; Hunt, 2001).

These keys are mathematically tied together, so the private key can only decrypt the encrypted information using its corresponding public key.

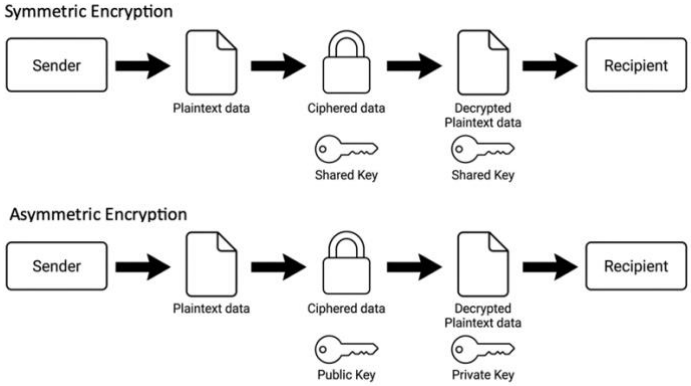


Figure 2. Symmetric Encryption vs. Asymmetric Encryption
Note. Adapted from "Realizing Quantum-Safe Information Sharing" by Kong, Janssen & Bharosa (2024, p.3).

With the set of mathematical principles, the cryptographic keys are generated using algorithms that rely on random number generators to create unique, random, and secure keys. By utilizing symmetric and asymmetric encryption rules and procedures, cryptographic algorithms generate cryptographic keys to prevent unauthorized parties from accessing sensitive and/or vulnerable data (Adams & Lloyd, 1999; Linn, 2000). Since the lengths of key sizes can differentiate the decryption time, longer keys provide greater security, and it can be difficult and expensive for non-key holders to decrypt the encrypted information. The key generation is vital for maintaining the keys to resist brute-force attacks, where an attacker tries all possible key combinations (Adams & Lloyd, 1999; Linn, 2000).

There are cryptographic keys generated with algorithms that are commonly used in different encryption methods. For *symmetric encryption,* one shared key is required, which is commonly used with algorithms such as Advanced Encryption Standard (AES) 128, 192, 256bits. While it is estimated that breaking a 128-bit long AES key using general hardware would take 500 billion years or more, 256-bit long keys are considered highly unbreakable. However, two users who wish to communicate must agree upon a random key in advance since it is challenging to generate and distribute shared keys in private. For *asymmetrical encryption, also known as PKC,* two keys need to be generated for the process, and specific algorithms used for PKC include RSA (Rivest-Shamir-Adleman), Diffie-Hellman

key exchange (DHKE), and ECC (Elliptic Curve Cryptography) (Martin, 2025; Paar & Pelzl, 2010).

Digital Signatures in Digital Certificates

For electric identity management, the process of digital signing maintains the security of encrypted data without being tampered with by an unauthorized party (Bharosa et al., 2015; Lozupone, 2018). By binding one's digital identity to a piece of data, a digital signature that is unique to an entity authenticates the identity of users in digital transactions and verifies the integrity of the signed documents. With the use of PKC, which generates a pair of cryptographic keys and digital signatures, digital certificates act as digital passports (Bindel et al., 2017; Buchmann et al., 2013; Lozupone, 2018)**.** From electronic mail security, financial transactions, electronic filing, and software protection applications, digital certificates verify identities over networks and secure digital transactions and data exchange, providing a foundation for security and trust in the digital environment. Digital signatures in digital certificates provide a high level of security standard for user authentication, and ensure message integrity and non-repudiation (Hunt, 2001; Linn, 2000). These three functions are further explained below.

Authentication: The ownership of a private key is bound to a specific user, and a valid signature shows that the user has sent the message. A digital signature ensures that the entity who signed the document is who they claim to be. Authentication allows users to establish trust between parties when using digital transactions via online banking or exchanging contract documents, etc.

Message Integrity: Once the message is signed, any message-en-route changes will have a different hash value. The content of the signed message or documents may remain unchanged from the moment it was signed. Message Integrity ensures that documents such as financial transactions, legal documents, and other sensitive data remain trustworthy and are prevented from unauthorized modifications.

Non-repudiation: Once the information is signed, non-repudiation prevents the user from denying their involvement in signing a document or message. Non-repudiation provides a legal basis for accountability for contracts, e-signatures, and other legal contexts. Digital signatures can be used as evidence in disputes and make it difficult for entities to withdraw agreements or actions.

Section 2.2.2 Public Key Infrastructure (PKI)

This section briefly outlines the key components of the Public Key Infrastructure (PKI) and explains how a PKI operates to facilitate secure digital communication and information exchange.

Key Components of Public Key Infrastructure (PKI)

With the increasing use of Information Communication Technologies (ICT) and daily activities in the digital environment, Public Key Infrastructure (PKI) has become essential to maintaining the security and reliability of digital communication and information sharing. With a set of hardware, software, policies, and procedures, PKI provides a security framework for modern cybersecurity practices for various applications, including secure digital transactions, web browsing, email communication, software verification, etc. (Bharosa et al., 2015; Buchmann et al., 2013). By managing digital certificates and public-key encryption with services such as key generation, key distribution, and certificate management, PKI ensures the security of digital communication and information exchange with confidentiality, integrity, authentication, and non-repudiation.

Moreover, PKI provides a system of trust between entities in the digital environment across diverse sectors, including but not limited to finance, healthcare, defense, and national government (Innovalor, 2019; Kong et al., 2023, 2024). In the public sector, PKI not only maintains the security of the government information and communication system but also ensures that public services provided by critical infrastructures remain safe, reliable, and accessible. From sharing filing taxes, applying for permits, loans to sharing information with different entities on policy and regulations, PKI facilitates secure digital transactions with a large number of different users between government-to-government, government-to-business, government-to-citizens, and business-to-citizens (Jansen & Ølnes, 2016; Janssen et al., 2009; Kong et al., 2024; Lindgren & Jansson, 2013).

In addition, there are several components that are crucial in facilitating secure digital communication and information exchange. The key components of PKI enable the process of key generation, distribution, storage, usage, revocation, and digital certificate management (Bharosa et al., 2015; Buchmann et al., 2013). These components include Users, Registration Authority (RA), Certificate Authority (CA), Root Certificate Authority (Root CA), and Certificate Repository (CR). With X.509 certificate as a standard, the format of digital certificates is defined, and interoperability is achieved between different systems and applications (Banoth & Regar, 2023; Bharosa et al., 2015; Buchmann et al., 2013; Huang & Nicol,

2017). Figure 3 shows how these components operate digital certification in PKI, and each component is described below.

Users: The users of the PKI system include individuals and/ or organizations that require a secure communication process and identity authentication for digital communication and information exchange with other users.

Certificate Authority (CA): The CA is a trusted entity that issues a digital certificate once RA has verified the user's identity. Then CA signs the certificate using its private key and issues the certificate containing the user's public key, who owns the certificate.

Root Certificate Authority (Root CA): The CAs in the PKI system are tied to *Root Certification Authority* (Root CA), which has the highest authority. Under the Root CA, it is also possible to create several intermediate CAs. The following certificates issued by these intermediate CAs are trusted by the lower-level CA. This is further explained in Section 2.2.3.

Registration Authority (RA): The user submits an application to RA. Then, RA ensures that the identity of the certificate requester user is verified through authentication. The quality of this authentication process determines the level of trust that can be placed in the certificates since RA provides the interface between the user and the CA. CA issues the digital certificates based on RA's recommendation.

Certificate Repository (CR): Once CA digitally signs the certificate, it is issued and placed into a Certificate Repository (CR) to be accessed by users. CR acts as an electronic directory of services where important certification details, such as keys, certificates, and certificate revocation lists, are stored. When a key is lost, a PKI may provide an advanced function, such as a key recovery service, to recover data or messages.

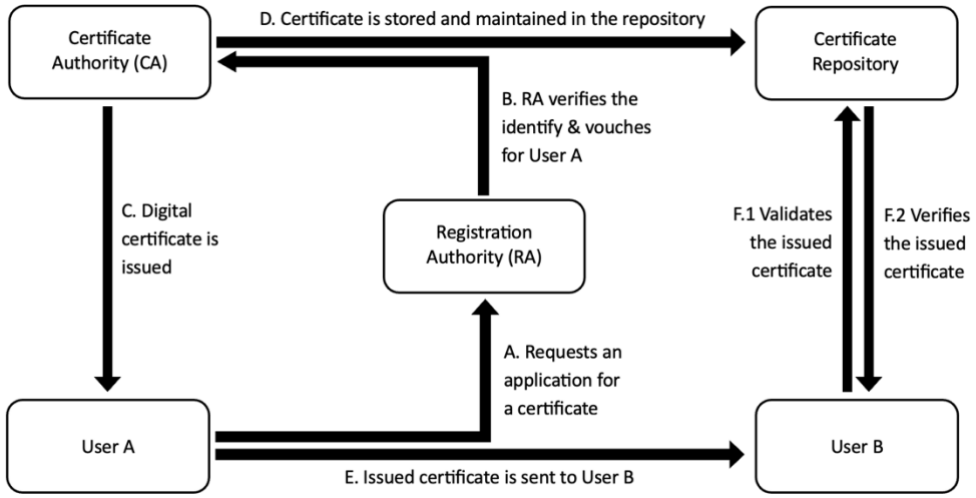


Figure 3. Process of Authenticating Identity Using Digital Certification in PKI
Note. Adapted from Banoth & Regar (2023) and Adam & Lloyd (1999).

The process of authenticating a user's identity using a digital certificate is explained in Figure 3. The explanation of the flow of interactions is as follows.

A. User A submits an application to RA to obtain a certificate from CA
B. RA verifies the validity of the identity and vouches for User A
C. The certificate that is signed by CA is issued to User A
D. The issued certificate is published to the certificate repository
E. The certificate is sent to User B to authenticate & secure the identity of User A
F. User B can verify User A's identity using the certificate to confirm that User A is who they claim to be. User B trusts CA, whose electronic signature validates the details within the certificate

2.2.3 CA Hierarchy & the Associated Policies and Practices in PKI

Certificate Authority (CA) acts as one of the key components of PKI and ensures the chain of trust is formed with a certification path from Root CA to intermediate CAs (Adams & Lloyd, 1999; Linn, 2000). In non-technical terms, all CAs are chained together under the Root CA. Digital certificates that are issued by the Root CA follow a CA hierarchy, and certificates are passed down to several intermediate CAs that are created under the Root CA. At the lower level of the CA hierarchy, end-entity certificates are then issued to people, applications, or devices (Bharosa et

al., 2015; Huang & Nicol, 2017). The certification path in a CA Hierarchy is illustrated in Figure 4.

In PKIs, a well-defined CA hierarchy is crucial in minimizing risks in a certification path. The responsibilities of Root CA are often delegated to intermediate CAs. Yet, the security issues may still arise from the intermediate CAs being compromised. Although the Root CA may remain safe, the certificates issued by intermediate CAs may no longer be trusted for digital transactions. The compromised CAs can issue fraudulent certificates, enabling man-in-the-middle attacks and introducing security issues (explained in Section 2.2.4). Thus, compromised certificates need to be immediately revoked, and the CAs need to publish a Certificate Revocation List (CRL) and the Online Certificate Protocol (OCSP) to inform the users, services, and applications of the compromised status (Bharosa et al., 2015).

In addition, the specific associated policies and practices in a PKI framework govern the issuance and management of digital certificates, outlining the responsibilities of CAs and their users (Albar & Perdana, 2021). Some PKIs operated by trusted third parties require Certificate Policies (CP) and Certificate Practice Statement (CPS), which provide details on practices and standards that a CA follows in issuing, managing, and revoking certificates (Logius, 2024a, 2025a). The CPS must complement the associated policies and comply with current industry standards and regulations, such as those established by the Internet Engineering Task Force (IETF), WebTrust, or other applicable regulatory bodies (Chokhani, S. et al., 2003).

Moreover, there are multiple standards that PKI must follow to facilitate identity verification, certificate lifecycle management, and revocation mechanisms. For example, the X.509 certificates serve as a fundamental component of digital security and play a crucial role in supporting PKI (Chokhani, S. et al., 2003; Cooper, M. et al., 2005). In order to restore security and trust in digital certification, entities need to reissue their certificates with a trusted CAs based on the X.509 standard, which specifies the format of public key certification and serves as secure communication protocols Without X.509, different systems such as (e.g., browsers, apps, and servers) may not be able to communicate and issues in interoperability across systems can be created.

PKIs operate on a trust model where it is essential to establish trust and security in the use of digital certificates. By following the Electronic Identification and Trust Services (eIDAS) regulations, CAs can become a Qualified Trust Service Provider (QTSP) where a high level of security and trustworthiness in electronic

transactions is achieved (European Commission, 2024b; European Union, 2014). The QTSP status provides an additional layer of trust between entities using services where assurance of strong security, legal recognition, and interoperability across borders can be maintained. The standards that QTSPs must meet encourage CAs to implement best practices in terms of security, risk management, and customer service.

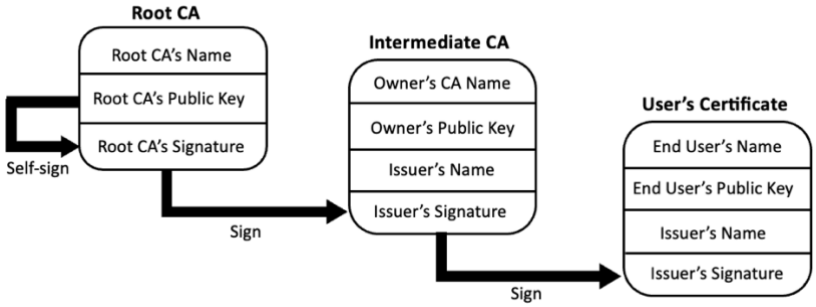


Figure 4. Certification Path in a CA Hierarchy
Note. Adapted from "Realizing Quantum-Safe Information Sharing" by Kong, Janssen & Bharosa (2024, p.4).

2.2.4 Security Risks in Public Key Infrastructures

The secure facilitation of PKIs that enable secure digital communication and information exchange depends on cryptographic keys (explained in Section 2.2.1) and technical components (explained in Section 2.2.2). However, once the keys and CAs become compromised, there are vulnerabilities that may raise security risks in PKIs. When securing digital data, there are three states of risk: data-in-transit, data-in-use, and data-at-rest. The focus of this section is to discuss security risks that are inherent to PKIs. By giving examples of data-in-transit and data-at-rest, security risks in PKIs are briefly introduced to better connect to Section 2.3.2, which discusses the threats posed by quantum computing technology.

As previously described in Section 2.2.1, cryptographic keys are generated using a combination of random number generation and cryptographic algorithms. With a set of large and unpredictable numbers from random number generation, cryptographic algorithms use these numbers to create keys that can be used to encrypt and decrypt information that is difficult to guess (Adams & Lloyd, 1999; Hunt, 2001). This allows the cryptographic keys to resist brute-force attacks where unauthorized entities try to find possible key combinations to break the keys. Once the cryptographic algorithms such as RSA (Rivest-Shamir-Adleman), DHKE

(Diffie-Hellman key exchange), and ECC (Elliptic Curve Cryptography) become weak, it may be possible for these algorithms to be broken with enough effort. Although today's widely used cryptographic algorithms remain largely secure against classical computers, there are inherent security risks for PKIs.

On the one hand, the privacy key secrecy of PKC is crucial to the secure facilitation of PKIs since a private key that is kept secret is only used to decrypt the data that is encrypted with its corresponding public key. By authenticating the identity of users, the digital signature generated using PKC in the digital certificates remains unique to the entity (Adams & Lloyd, 1999; Bindel et al., 2017; Hunt, 2001). In doing so, encrypted data cannot be tampered with by those who are unauthorized without a private key (Buchmann et al., 2013; Lozupone, 2018). With an emphasis on the use of PKC, the loss of the private key may introduce security risks. If someone steals or copies a private key, it becomes possible for others to pretend to be the key owner and decrypt the information that is encrypted. Thus, without the private key secrecy, secure facilitation of PKIs can be compromised.

On the other hand, Certificate Authorities (CAs) are one of the key components of PKI. As a trusted entity, CA issues a digital certificate once the Registration Authority (RA) has verified the user's identity and signs the certificate using its private key. The CA process acts as an important part of the secure facilitation of PKIs (Adams & Lloyd, 1999; Bindel et al., 2017; Linn, 2000). If a CA is compromised, fake certificates can be issued, which can trick users into trusting unauthorized entities. Likewise, flaws in the CA process can also lead to a certificate being issued to those who are not authorized. This may hurt certification integrity and result in entities impersonating others and using certificates. As a result, the entire CA hierarchy (explained in 2.2.3) may also be affected. Once the CA is compromised, the facilitation of PKIs cannot guarantee secure digital communication and information exchange.

Once the cryptographic keys and CAs become compromised, there are vulnerabilities that may raise security risks in PKIs. For example, data-in-transit and data-at-rest can be affected. For Data-in-Transit, the security risks in PKI can occur from message interception and replay attacks, also known as a Man-in-the-Middle attack. These can occur in many different types, such as interruption, interception, modification, and fabrication (Bharosa et al., 2015). The first type, called interruption, is when an attack causes a message sent by a sender to never reach a receiver. The second type, called interception, is when a message is copied and viewed by the attacker. The third type, called modification, is when a message is intercepted and modified before it reaches a receiver. The fourth and last type, called

fabrication, is when an attacker sends an altered message to a receiver and pretends to be a sender without the sender's authorization.

For Data-at-Rest, the stored data on the database, backups, and disks can be instantly decrypted (Bharosa et al., 2015). The information, such as personal data, intellectual property, or financial and health records, can be accessed by unauthorized parties. This would result in full exposure of stored data, even if the data was previously encrypted. With the compromised cryptographic keys and CAs, access can be granted to unauthorized parties and also retrieve encryption keys, backups, and storage (Adams & Lloyd, 1999; Linn, 2000). For organizations that are storing data, the security risks to data-at-rest can lead to not only data loss but also issues related to legal and regulatory violations (e.g., GDPR) and even reputation damage for companies in their business processes.

2.3 Quantum Computing Technologies

Section 2.3 discusses quantum computing technology, and it is divided into three sections. Section 2.3.1 examines the up-to-date development of quantum computers. Section 2.3.2 explains how the advancement of quantum computers poses security threats due to their computational power and Store Now Decrypt Later (SNDL) attack. Section 2.2.3 explains how threats of quantum computers may be relevant to PKIs and affect the current system of digital communication and information exchange.

2.3.1 Development of Quantum Computers

Throughout the 20th century, the development of quantum theory significantly fueled research in the field of quantum computing technology. With the work of scholars including, but not limited to Albert Einstein, Max Planck, Niels Bohr, Richard Feynman and David Deutsch, the knowledge and understanding on quantum mechanics, key concepts and theoretical models of quantum computation have laid the groundwork on the practical application of quantum computers (Bohr, 1913; Feynman, 1948; Heisenberg, 1983; Planck, 1900; Schrödinger, 1926). The theoretical insights have set the stage for today's experimental advancement and contributed to the knowledge of a universal quantum computer.

Over the past decade, the field of quantum computing technology has evolved into one of the promising frontiers of technology. Researchers anticipate that the advancement in quantum computers may become increasingly relevant to diverse scientific and industry domains. The availability of quantum computers may accelerate the optimization process in logistics, finance, and manufacturing,

simulate new properties of materials and medicine, analyze risks and patterns in large datasets and complex modelling (Bova et al., 2021; M. Brooks, 2023; De Wolf, 2017; Dowling & Milburn, 2003; Ménard et al., 2020). The myriads of opportunities from the technology may be used to address complex real-world problems.

Due to the quantum properties known as *superposition,* quantum computers process information differently from classical computers. While classical computers use bits as the basic unit of information, representing either 0 or 1, quantum computers use qubits representing 0, 1, or both. Although a fully functioning quantum computer is not yet available, one of the latest breakthroughs includes Google's new quantum computing chip called Willow (Google Quantum AI and Collaborators et al., 2024). After the Sycamore quantum computing chip, which was introduced in 2019, the Willow chip has improved in speed and error correction (Bravyi et al., 2024; Google Quantum AI and Collaborators et al., 2024; Putterman et al., 2024). In under five minutes, the Willow ship can perform a standard benchmark computation which would otherwise take 10 septillion years for today's fastest supercomputers.

Since minimizing calculation errors and improving error corrections are essential for robust quantum systems, research is ongoing to shield qubits from noise and decoherence (Sood & Chauhan, 2024). According to the ambitions set out in IBM's Quantum Development Roadmap, the company aims to achieve error-corrected quantum systems by 2029 (AbuGhanem, 2025; IBM, 2024). From breaking the 127-qubit Eagle chip with the 433-qubit Osprey processor in just over a year, IBM has recently introduced the company's latest version of an advanced quantum processor, IBM Quantum Heron (Daley et al., 2022; Kim et al., 2023). While these processes have been designed for different computing tasks, the new quantum hardware and software capabilities aim to utilize the latest technology to perform quantum calculations and expand the scale, speed, and accuracy of quantum algorithms (AbuGhanem, 2025; IBM, 2024).

2.3.2 Quantum Threats

The research on quantum computing continues to accelerate, and the computational power of quantum computers will soon outcompete classical computers. One of the fundamental principles of quantum mechanics that contributes to the computational power of quantum computers is known as *Superposition. Superposition* allows qubits to exist in multiple states simultaneously, to be in 0, 1, or something in between (Gibney, 2019; Mavroeidis et al., 2018). With such ability in qubits, quantum computers can perform parallel computations and explore many possible

solutions at once. As the number of qubits increases, the computational power of quantum computers may also grow exponentially, which can evaluate all possibilities for problems with an enormous solution space.

Another fundamental principle of quantum mechanics is known as *Entanglement*. Quantum drastically enhances its computational power for certain problems. *Entanglement* allows two or more qubits to stay linked, and the state of one qubit can directly affect the states of other qubits (M. Brooks, 2023; Gibney, 2019; Mavroeidis et al., 2018). Despite the distance that may separate qubits, the ability allows qubits to be entangled and enables quantum computers to determine the state of other qubits by measuring the state of just one qubit. While this complex correlation cannot be achieved with classical bits, the properties of qubits can enable it and further enhance the computation power of a quantum computer, making it more reliable (M. Brooks, 2023; Memon et al., 2024). As entangled qubits are used to share information and enhance error correction, solving complex problems may become easier, and the system may become more resistant to errors.

By taking advantage of quantum properties, quantum computers have the potential to introduce new security threats. According to Peter Shor, it would no longer be difficult and time-consuming for quantum computers to factor a key pair of large prime numbers (Shor, 1994). Using Shor's algorithm, quantum computers can theoretically break today's security measures that are initially assumed to be intractable for classical computers. For cryptography, today's widely known PKC encryption methods and algorithms, such as RSA, DHKE, and ECC, will no longer be strong enough to provide security against quantum computers (Csenkey & Bindel, 2023; Mosca & Piani, M, 2023; Paar et al., 2024; Shor, 1994). The recent publication of Regev's algorithm in *Science,* which may improve the efficiency of Shor's algorithm further, raises concerns for the quantum threats (Kramer, 2023).

For encryption methods and algorithms not affected by Shor's algorithm, Grover's algorithm offers quantum computers to speed up the search process of an unstructured database (Grover, 1996). While classical computers cannot perform such shortcuts, quantum computers can theoretically perform an extensive brute-force search and benefit from faster searches using Grover's algorithm (Mandviwalla et al., 2018). With the quadratic improvement in their search time, symmetric encryption methods and algorithms such as AES 128, 192, 256 bits that use the same key for encryption and decryption are no longer secure against quantum computers (Grover, 1996). The security level of symmetric encryption and algorithms is estimated to halve, as a 128-bit key would only offer 64 bits of security.

Although quantum computing technology is still in its early stages, quantum computer-based threats can still occur today. With the threat known as *Store Now Decrypt Later,* encrypted data can be harvested today and be stored until a quantum computer becomes capable enough to decrypt the encrypted data (AIVD, 2021; Mavroeidis et al., 2018; Mulholland et al., 2017). For data that requires long-term security in the next 10-20 years, the threats can occur today and make the data vulnerable since the data-at-rest can still be of use once adversaries decrypt the data (Barker et al., 2021b; Mavroeidis et al., 2018; Yunakovsky et al., 2021). It also remains difficult for organizations to ensure security on the stolen data, as no forensic evidence may be left to check whether the information has already been harvested and stored by malicious adversaries to be decrypted later.

2.3.3 Quantum Threats on PKI

While many security issues occur today from poor passwords, data breaches, phishing scams, and malicious software updates, the computational power of quantum computers introduces security issues that threaten the entire foundation of cryptographic systems (Kong et al., 2024; Mavroeidis et al., 2018; Mulholland et al., 2017; Paar & Pelzl, 2010). As research on quantum computing technology continues to advance, leveraging algorithms such as Shor's algorithm allows quantum computers to make the entire security framework of PKIs that facilitate secure digital communication and information exchange insecure (Shor, 1994). This poses a significant threat across critical infrastructures that rely on PKIs as, and the services provided by these infrastructures may no longer be secure and reliable against quantum computing threats.

Using Shor’s algorithms, a cryptographically relevant quantum computer (CRQC) can efficiently factor large integers and solve the discrete logarithm problems in PKC algorithms. Since PKIs are based on PKC encryption methods and algorithms such as RSA, DHKE, and ECC, the presence of sufficiently powerful quantum computers can make the key exchange process in PKIs no longer secure (AIVD, 2021; Csenkey & Bindel, 2023; Mosca & Piani, M, 2023; Yunakovsky et al., 2021). This raises security risks on PKI as the entire cryptographic foundations on which PKIs are built become vulnerable. By interfering with the key extraction process, adversaries can retrieve a private key that corresponds to their public key to decrypt the data that has been encrypted. Although the PKIs have been proven to secure digital transactions against classical computers, this may not be the case with the advancement of quantum computers.

Moreover, if the algorithms underpinning digital certificates become vulnerable, a well-defined CA hierarchy is intended to minimize risks in certification management. Digital signatures in digital certificates will no longer provide a high level of security standard and ensure authentication, message integrity, and non-repudiation. The quantum threats in PKIs could undermine confidence in CAs and affect the chain of trust that is established with a certificate hierarchy over networks (Albar & Perdana, 2021; Giron, 2023; Vogt & Funke, 2021). Once the encryption of a certificate is compromised, it may lead to the immediate revocation of compromised certificates, and the validity of existing certificates will remain in question. Likewise, CAs that play a crucial role in PKIs may no longer provide trust services in verifying the legitimacy of entities and establishing trust between entities.

In addition, with the *SNDL* threat, adversaries may access the data in transit and stored data. Let's unpack both scenarios. First, data in transit is the classic SNDL scenario. An adversary sits on a network connection (like a wiretap on the internet backbone) and passively records all the encrypted traffic flowing between two points. In the data at rest scenario, an adversary breaches a server but finds the database is encrypted yet steals the encrypted files anyway. If the file was encrypted using a mechanism that relies on quantum-vulnerable cryptography, they can decrypt it once CRQCs arrive. To be precise, in the SNDL scenarios, the adversary accesses and copies the ciphertext (the scrambled data). They do not access the plaintext (the readable information) until the 'Decrypt Later' phase occurs, using a CRQC.

With the increasing dependence on PKIs in the existing infrastructures, security issues from quantum threats may no longer be limited in scope and impact, affecting public safety and national security. For example, sensitive and confidential data that require long-term security, including personal data, health records, financial transactions, classified military information, and intellectual properties, may be at risk if they are not adequately protected (Kong et al., 2023, 2024). It would be inevitable that quantum threats extend across diverse sectors, various sectors where data-at-rest is no longer protected with the current cryptographic methods.

2.4 Quantum-safe (QS) Transition

Section 2.4 discusses the topic of Quantum-safe (QS) transition. The term QS Transition used in the dissertation is defined as transitioning existing systems from using classical cryptographic algorithms that are non-Post-Quantum Cryptographic (PQC) to systems that use PQC-based QS solutions in the existing systems. Section 2.4.1 introduces the emergence of standards and Post-Quantum Cryptography (PQC). Section 2.4.2 discusses potential solutions that may address quantum threats

with two main QS approaches, which include Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Section 2.4.3 highlights the complexity of QS transition in the context of PKI.

2.4.1 Emergence of Standards, NIST & PQC standards

Various cryptographic algorithms such as AES, SHA-2, SHA-3, RSA, DHKE, and ECC are widely used today to provide underlying security protocols for digital communication and information exchange. Since not all algorithms are secure or efficient, standards for cryptographic algorithms provide systems with a consistent security baseline. In doing so, standards define how different cryptographic algorithms can be used in practice for different use cases and allow organizations to use algorithms that are strong enough to prevent unauthorized parties from accessing sensitive and/or vulnerable data (Adams & Lloyd, 1999; Hunt, 2001). Thus, it would be difficult to maintain secure digital communication and information exchange without standards.

In addition, standards ensure that algorithms are used across governments and industries with a common framework that provides operational and service delivery. By defining acceptable key sizes and maintaining interoperability with different systems, standards clarify parameter choices and encoding rules to ensure that systems are secure and universally compatible. PKIs provide a framework of policies, software, and hardware that support secure digital identity and communication (Adams & Lloyd, 1999; Hunt, 2001; Linn, 2000). To ensure a system of trust between entities in the digital environment, PKIS must maintain consistency, quality, and safety between applications, devices, users, and/or networks. By aligning with global standards that meet minimum security guarantees, different entities can work together and communicate seamlessly.

The National Institute of Standards and Technology (NIST) is responsible for developing and maintaining cybersecurity standards across the federal government in the U.S. The documents regarding standards and guidelines published by NIST (e.g., NIST SP 800-53, NIST Cybersecurity Framework (NIST CSF)) are adopted internationally and have wide applicability across diverse sectors (Joint Task Force Interagency Working Group, 2020). What differentiates NIST from Standard Development Organizations (SDOs) (e.g., ISO, ETSI, ANSSI, or IEEE) is that NIST standards are developed in an open process and public competitions (e.g., AES, SHA-3, PQC) with transparency and years of public scrutiny (Alagic et al., 2022, 2025; NIST, 2024e). Other standard bodies and hardware and software

vendors (e.g., Microsoft, Intel, AWS, Cisco) incorporate decisions and build products aligned with NIST.

Instead of organizations reinventing their own cryptographic algorithms, shared standards reduce cost and ensure security, interoperability, and compliance. Since standards have been carefully reviewed and tested, products and services that have these standards are established with benchmarks for safety, reliability, and performance. For weak and broken cryptographic algorithms, efforts are made to retire weak standards (e.g., DES, SHA-1) and introduce stronger standards (e.g., AES, SHA-2, SHA-3). The evolution process of different standards for cryptographic algorithms shows that standards need to be maintained and updated with evolving security threats. For example, moving from SHA-1 to SHA, or from DES to AES, shows that standards evolve to protect new emerging threats.

Moreover, in 2016, NIST issued a call for proposals to develop cryptographic algorithms that can safeguard against new threats posed by quantum computers (explained in Section 2.3.2 and Section 2.3.3) (NIST, 2016). The cryptographic algorithms based on Post-Quantum Cryptography (PQC) are considered secure against quantum computers (Barker et al., 2021b; ENISA, 2022; Käppler & Schneider, 2022; NIST, 2024e). The first set of NIST PQC standards (e.g., FIPS 203, 204, 205) was announced in 2024, and the final draft of FIPS 206 is expected in late 2025 (NIST, 2024c, 2024b, 2024d). Figure 5 shows NIST PQC milestones and timeline. Since the initial PQC standardization, standard bodies such as ETSI announced the launch of its post-quantum security standard to enhance security mechanisms (e.g., ETSI TS 104 015), and government agencies (e.g., ENISA, EC, CISA) are currently working on providing policy advice and certification schemes aligning with the NIST PQC standards (CISA, 2023; ENISA, 2025; European Commission, 2024a).

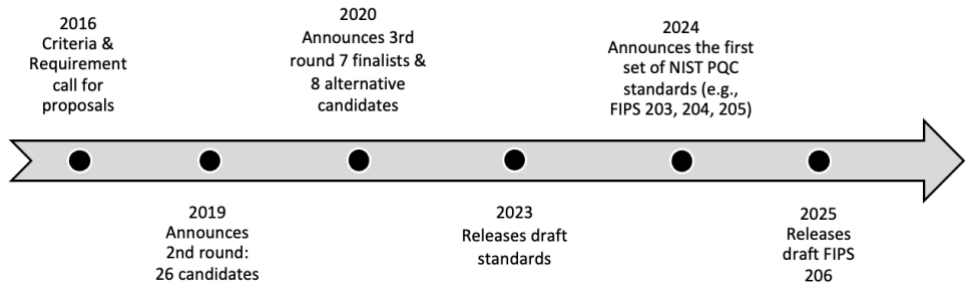


Figure 5. NIST PQC Milestones & Timeline
Note. Adapted from "NIST PQC-The Road Ahead," by Moody (2025, p.3).

2.4.2 State of the Art QS Cryptographic Algorithms: PQC & QKD

With the ever-increasing dependencies in the digital environment, security threats posed by quantum computers in digital communication and information exchange may have a cascading effect across sectors, affecting national security and public safety. The increased research and interest in maintaining privacy, trust, and security in an interconnected world have led organizations across academia, industries, and government to work on QS cryptographic algorithms that can be secure against both classical and quantum threats. The two main QS approaches include Quantum Key Distribution (QKD) & Post-Quantum Cryptography (PQC).

The first approach is called Quantum-Key Distribution (QKD). This solution is a hardware-based approach using the properties of quantum bits (previously discussed in Section 2.3.2). Unlike traditional key distribution methods, QKD uses quantum mechanics, such as *Superposition* and *Entanglement,* to securely distribute encryption keys between two parties (e.g., sender and receiver). During the key exchange process, any eavesdropping attempt can be identified, and QKD can be used to detect whether information has been corrupted and/or intercepted (AIVD, 2024; Lovic, 2020; Sabani et al., 2022). While the approach provides a solution that can ensure a higher level of security, a quantum infrastructure is needed, starting with a quantum channel such as a fiber-optic cable, where photons can be used to encode the information.

While the research on QKD is rapidly evolving and offers a solution to unparalleled security using the laws of quantum mechanics, limitations exist in its scalability and infrastructure requirements (Aquina et al., 2025; Lovic, 2020; NSA, 2024). QKD cannot be adopted in the existing infrastructures due to short distances and key exchange rate constraints. Additionally, a manual authentication process may be needed for non-secure endpoint installations as authentication is not yet supported with the current QKD approach. Moreover, the application of QKD requires a quantum infrastructure, new specialized hardware that does not fit into the existing infrastructures, likely resulting in high costs of delicate equipment (AccentureLabs, 2018; Aquina et al., 2025; Lovic, 2020; NSA, 2024).

The second approach is called Post-Quantum Cryptography (PQC). There are different approaches to this solution, such as code-based, hash-based, and lattice-based cryptography (ENISA, 2022; Käppler & Schneider, 2022; NIST, 2024a). Although it is based on PKC, QS solution algorithms based on PQC is considered safe against quantum threats. The theoretical groundwork for PQC began when the researchers started to recognize the potential of quantum threats in the mid-1990s (e.g., Shor's algorithm). Yet, the initiative to evaluate and standardize QS

cryptographic algorithms based on PQC did not start until 2016. In 2022, the US National Institute of Standards and Technology (NIST) selected four QS cryptographic algorithms based on PQC which include CRYSTALS-KYBER for public key encryption and CRYSTALS–Dilithium, SPHINCS+, and FALCON for digital signatures. (Alagic et al., 2022, 2024; L. Chen et al., 2016; NIST, 2024a).

The first set of finalized PQC standards was announced (e.g., FIPS 203-205) in 2024, with FALCON pending its standardization (NIST, 2024d, 2024b, 2024c). Currently, the PQC approach holds an advanced theoretical basis with ongoing research on key sizes, efficiency, and performance. Since the PQC approach still requires intensive computation, the QS solution algorithms are not yet suitable for large-scale commercial use and cannot be implemented in the existing infrastructures (NIST, 2021; 2016). However, PQC approach does not need new infrastructures like QKD approach and is largely accepted as an alternative to the existing algorithms once they are fully tested for their efficiency and performance in different use cases (Barker et al., 2021a, 2021b)

Although this paper recognizes the potential of QKD as a QS approach, this research focuses on PQC. As mentioned earlier, the specialized hardware and new infrastructure needed for QKD are not yet available. Meanwhile, PQC can be implemented without significant changes to the existing infrastructures, making PQC a more accessible and cost-effective solution to be used for various applications (e.g., digital signatures, secure communication, public key encryption). Second, QKD research still needs to bridge the gap between theory and practice to realize broader adoption. With PQC moving closer towards standardization, implementation, and adoption in the existing infrastructures, different approaches to PQC-based solutions show that PQC is a mature algorithm that is based on PKC, where its security and effectiveness have been proven.

2.4.3 QS Transition & Challenges in the Context of PKI

In order to safeguard against the quantum threats, PKIs in the existing infrastructures need to implement and adopt QS cryptographic solution based on PQC. With the list of four QS cryptographic algorithms (e.g., CRYSTALS-KYBER for public key encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures) research on practical compatibility needs to take place to check the efficiency and performance of these algorithms (Alagic et al., 2022; Barker et al., 2021b). However, a simple drop-in method cannot change PKIs and substitute these solutions. Transitioning the existing infrastructures without preparation may create

interoperability and backward compatibility issues (Barker et al., 2021b; Bindel et al., 2017; Broadbent & Schaffner, 2016).

Moreover, PKIs are installed systems with path dependencies with a set of roles, security policies, encryption mechanisms, and procedures (Barker et al., 2021b; Liu et al., 2025; Mashatan & Heintzman, 2021). Multiple stakeholders with various roles, including governments, standards bodies, hardware vendors, software companies, service providers, and PKI users, make PKIs difficult to change (CCC, 2019; The Hague Security Delta, 2019; Vermeer & Peet, 2020). With QS transition in its early stage, there is a void in knowledge on how to transition toward QS PKI systems (Barker et al., 2021b; Mashatan & Heintzman, 2021; Mulholland et al., 2017; Vermaas, 2017). Organizations are unprepared and do not know where to begin the QS transition.

In addition, there are many uncertainties for QS transition as organizations do not know whether full substitution of QS solutions or hybrid solutions (that include both classical and QS algorithms) is needed (Barker et al., 2021b; De Wolf, 2017). Perhaps, QS transition may require the hardware and software to be changed to meet the requirements (Barker et al., 2021b; ENISA, 2022). With the interdependencies among organizations in the PKI systems, organizations may have different starting points, interests, and expectations (Bharosa et al., 2015; CCC, 2019; The Hague Security Delta, 2019; Vermeer & Peet, 2020). As QS transition remains complex, a high degree of decision-making, coordination, and leadership efforts may be required for the transition processes.

According to Mosca (2015), the transition timeline raises important considerations for the existing infrastructures, as QS transition may need to be planned as soon as possible to prevent potential risks. Although the transition time required for organizations may vary depending on risk appetite, cryptographic assets, the lifespan of technology in PKIs, and the resources available, it is estimated that an average of 10+ years may be needed for organizations to fully transition to QS PKI systems (CCC, 2019; Macaulay, & Henderson, 2019; Vermeer & Peet, 2020). In Mosca's Theorem, the following three variables are explained below to determine the timeline of QS transition.

X = the security of shelf-life (The time the information remains confidential)
Y = the transition time (The time it takes for organizations to transition)
Z = the collapse time (The time when the quantum computer is realized)

The sum of two variables, X and Y, is the estimated time the organization would need to transition to a QS PKI transition. It is assumed that data is vulnerable for the full shelf life (e.g., X), and the data is still under a potential harvesting of SNDL attack until the migration is completed (e.g., at the end of Y). Thus, if the sum of time (e.g., X and Y) takes longer than the time Z, the theory states that the system will no longer be protected against quantum-computing-based threats (Mosca, 2015).

2.5 Chapter Conclusion

This chapter provides background information on Public Key Infrastructures (PKI) and quantum computing technology. In doing so, the chapter sets the tone for the context of this research on QS transition. The chapter introduces PKI by explaining how PKIs manage digital certificates, which act as digital passports for users in the digital environment. With the use of Public Key Cryptography (PKC), a pair of cryptographic keys and digital signatures in the digital certificates allows a high level of security standard for user authentication and ensures message integrity and non-repudiation.

Although there are inherent vulnerabilities in PKIs that may raise security risks, the chapter highlights that facilitations of PKIs are generally considered secure, and PKCs remain practically impossible for current classical computers to break. However, this is no longer the case with the advancement of quantum computing technology. The cryptographic foundations based on PKC that provide a security framework are no longer safe, as the computational power of quantum computers can solve complex problems exponentially faster and explore possibilities simultaneously.

The chapter introduces the emergence of standards and Post-Quantum Cryptography (PQC) and further discusses the state-of-the-art development for two main areas of solutions for becoming QS, which are Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). While this research acknowledges the potential possibilities of QKD, the chapter emphasizes that the focus of this research is on PQC, which is based on the standards announced by the National Institute of Standards and Technology (NIST). The chapter concludes with various challenges that may exist in PKIs due to uncertainties regarding QS transition. With essential services across critical infrastructures that depend on PKIs, the topic of QS transition remains relevant and crucial.

While it is difficult for organizations to transition their existing infrastructures due to technical complexities, changes in the PKIs cannot be made with a big-bang approach. Likewise, no clear QS cryptographic solutions are yet

available based on PQC for organizations to adopt and implement in their systems. Thus, QS transition remains complex and requires careful planning. Going forward, this research aims to identify the key challenges involved in QS transition and to provide a stage-based growth model for organizations looking to transition to QS PKIs. To achieve this aim, the main research question for the research has been formulated: "*What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems?"*

Chapter 3 Research Methodology

3.1 Introduction

This chapter introduces the research approach for this study and clarifies how data is collected and analyzed using the chosen research philosophy, methodology, and data collection methods. The chapter sets the stage to align research aims and provide context for the results presented in the later chapters of the dissertation. In Section 3.2, the research philosophy is discussed with a focus on interpretivism and how interpretivism fits with the research. In Section 3.3, an overview of data collection and analysis using mixed methods is explained. In Section 3.4, the case study approach is explained as the research methodology used in this research. The chapter concludes in Section 3.5.

Parts of this chapter are based on the following publications:
Kong, I., Janssen, M., & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition. In: CEUR Workshop Proceedings. 3449.

Kong, I. (2022). Transitioning towards quantum-safe government: Examining stages of growth models for Quantum-safe public key infrastructure systems. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022. https://doi.org/10.1145/3560107.3560182

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). https://doi.org/10.1145/3543434.3543644

3.2 Research Philosophy: Interpretivism

Section 3.2 introduces interpretivism as the selected research philosophy, and it is divided into two sections. Section 3.2.1 provides a brief overview of research philosophy. Section 3.2.2 discusses interpretivism as a selected research philosophy and why interpretivism is appropriate for this research.

3.2.1 An Overview of Research Philosophy

Research Philosophy provides a foundational belief that influences researchers in how they approach the research and shows their view on the nature of knowledge and reality that underpin the research process (Guba & Lincoln, 1994; Saunders et al., 2019). By establishing ontology (the nature of reality) and epistemology (the nature of knowledge), the researchers can position their ontological stance that concerns the nature of reality and epistemological stance that questions how researchers know what they know and discusses what constitutes reality (Guba & Lincoln, 1994). The details on ontology and epistemology of the chosen research philosophy can guide the development of research questions and clarify the goals of the research.

Moreover, a research methodology determines how researchers go about finding out about the reality, and methods provide details on the tools and techniques used during the research process to know about the reality. By understanding the research philosophy, researchers can shape research design and how knowledge is generated and understood. In doing so, they can align the design of the research with appropriate methodologies and methods (Guba & Lincoln, 1994; Yin, 2018). There are various types of research philosophies, including positivism, interpretivism, critical realism, pragmatism, and constructivism (Guba & Lincoln, 1994). Going forward, positivism and interpretivism are briefly discussed as two dominant research philosophies in the field of Information Systems (IS) that offer different perspectives.

One of the dominant IS research philosophies is *Positivism* (W. Chen & Hirschheim, 2004; Orlikowski & Baroudi, 1991). In Positivism, the nature of reality comprises one single reality and truth. The nature of knowledge is achieved through objective knowledge and measurable properties, which can be verified through observation and experiments (Niehaves & Becker, 2006; Weber, 2004). Since an objective reality can be measured and analyzed, positivist researchers emphasize verification of hypotheses, statistical generalizability, and highly structured quantitative variables. The reality is believed to be measured and explained through quantifiable observations (Guba & Lincoln, 1994; A. S. Lee, 2004)

Another dominant IS research philosophy is Interpretivism (Baskerville & Pries-Heje, 2010; Walsham, 1995) . In interpretivism, it is argued that there are multiple realities and truths rather than one. The realities are constructed through individual and collective interactions, including the shared knowledge (Guba & Lincoln, 1994; A. S. Lee, 2004). The interpretivist researchers see that the nature of knowledge is constructed by people through their own experiences and reflections on those experiences (Myers & Klein, 2011; Orlikowski, 1992). The methodology of interpretivism uses mainly qualitative methods, emphasizing inter-subjective knowledge and interpretation (Guba & Lincoln, 1994; A. S. Lee, 2004)

3.2.2 Research Philosophy: Interpretivism

The selected research philosophy for this study is Interpretivism. Since there is a set of established frameworks for technology applications, policies, and practices, as well as various actors and stakeholders involved in the secure facilitation of the infrastructures, the interpretivist approach allows the researcher to gather in-depth analysis. As reality that is socially constructed may vary from one context to another, analyzing perspectives of diverse experts and practitioners may serve as a vital lens in exploring the details of the context of the study. The interpretivist approach often employs diverse methods such as interviews, focus groups, and workshops to gather results of the research (Guba & Lincoln, 1994; Myers, 1997; Walsham, 1995). The results of such qualitative and quantitative methods can extensively capture the subjective views and experiences of relevant experts and practitioners.

Building on the interpretivist philosophical stance, the methodologies and methods used to conduct research are designed to capture the richness of human experience and the complexity of social interactions. The existing infrastructures have organizations and system structures that are interdependent, artificial, and purposefully designed (Alter, 2008; Baskerville & Pries-Heje, 2010; Orlikowski, 1992). Due to the importance of highlighting varying contexts and diverse factors, a deeper understanding of the context of QS transition and the complexities in existing infrastructures may be needed. For organizations that are looking to transition their existing infrastructures to become quantum-safe, conceptual insights across different organizations may provide an understanding of the conditions and capabilities that organizations may need for QS transition trajectories. Such a comprehensive and overarching view of QS transition may provide organizations with relevant and actionable guidance.

3.3 Research Approach

Section 3.3 provides an overview of the research approach. Section 3.3.1 discusses the development of the theoretical framework that is used in the research. Based on Gregor's The Nature of Theory in Information Systems, Type V Theory for Design and Action is used as a relevant foundational theory for the research. Section 3.3.2 introduces a sequential mixed-methods case study, which is divided into four phases of the research. Section 3.3.3 discusses the suitability of a case study for examining PKI systems in the context of QS transition. Section 3.3.4 presents the case study design, highlighting a single case study with multiple embedded units of analysis used in the framework.

3.3.1 Foundational Theories

Section 3.3.1 introduces theories that serve as foundational theoretical frameworks. Based on the different types of theories from Gregor's The Nature of Theory in Information Systems, the research focuses on Type V Theory for Design & Action, which serves as a relevant foundational theory for the research. An overview of the theoretical framework for the research is shown to indicate how Type V Theory for Design & Action provides a theoretical framework for core theories (explained in Section 4.2 and Section 4.3) used in the research.

Nature of Theory in Information Systems

By understanding theory in Information Systems, the overall intent of the research may be clarified, and coherence with the research objective can be built (Gregor, 2006). The researcher can better align with different research methods and build a stronger theoretical framework, which may contribute to the existing knowledge. It is crucial to examine information systems with socio-technical aspects as the intersection of knowledge on both social and technical aspects of the systems is needed to make theoretical and practical contributions (A. S. Lee, 2004). By specifying whether the research is intended for analyzing, explaining, predicting, or guiding design and action, the research can be addressed with appropriate theoretical aims (Gregor, 2006). There are five different types of IS theories introduced in The Nature of Theory in Information Systems: 1. Theory for analyzing, 2. Theory for explaining, 3. Theory for predicting, 4. Theory for explaining and predicting, and 5. Theory for design and action (Gregor, 2006)

According to Gregor (2006), Type I Theory for Analyzing identifies, organizes, and categorizes key concepts or constructs in the research, and provides foundations to understand what exists. Type II Theory for Explaining identifies

causal relationships and mechanisms but does not provide predictions on the future. Type II theories explain why and how phenomena occur (e.g., processes and systems). Type III Theory for Predicting forecasts what may happen in specific phenomena without providing a causal explanation. With the use of statistical or mathematical models, Type III theories can provide decision-making and planning where outcome predictions need to be made. Type IV Theory Explaining and Predicting combines the strength of both Type II and Type III to provide a causal explanation of why certain outcomes occur and some future events may be anticipated. Type V theory for design and action prescribes practical guidance for processes and systems with the aim of implementing change to achieve desired goals.

Theory for Design and Action

For this research, the aim is to identify the key challenges involved in QS transition and to provide a stage-based growth model for organizations looking to transition to QS PKIs. Due to the early-stage research on QS transition, there is a lack of knowledge available on how organizations can transition their existing infrastructures to become QS. To address this aim, the research needs a comprehensive view of both the problem and the solution in the context of QS transition. Thus, the research first examines the socio-technical aspects of PKI systems and builds initial knowledge of QS transition challenges. In doing so, socio-technical transition challenges are identified in the case of PKI systems to understand the challenges that organizations are struggling with when transitioning their existing infrastructures.

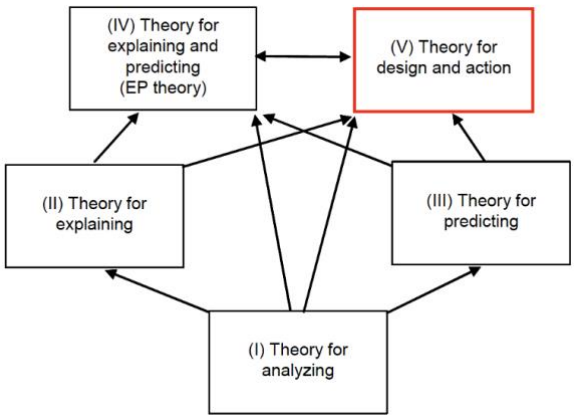


Figure 6. Interrelationships Among Different Theory Types for the research
Note. Adapted from "The Nature of Theory in Information Systems" by Gregor (2006, p. 630).

Moreover, Type V Theory for Design and Action builds on the background that has been examined in the context of QS transition. By building on the socio-technical transition challenges that have been identified in the first part of the research, this research further investigates *what should be done* so that actionable guidance on QS transition can be provided for organizations to overcome the challenges and move to a QS PKI. Type V Theory for Design and Action provides a theoretical lens that is not only based on the complex phenomena of QS transition in the case study of Dutch PKI systems in the public sector but also prescribes practical solutions on what organizations may need to do to progress with their transitions to achieve quantum-safety. Figure 6 shows the interrelationship among different theory types and specifies the theory type used in the research. The theory used in this research is indicated in red.

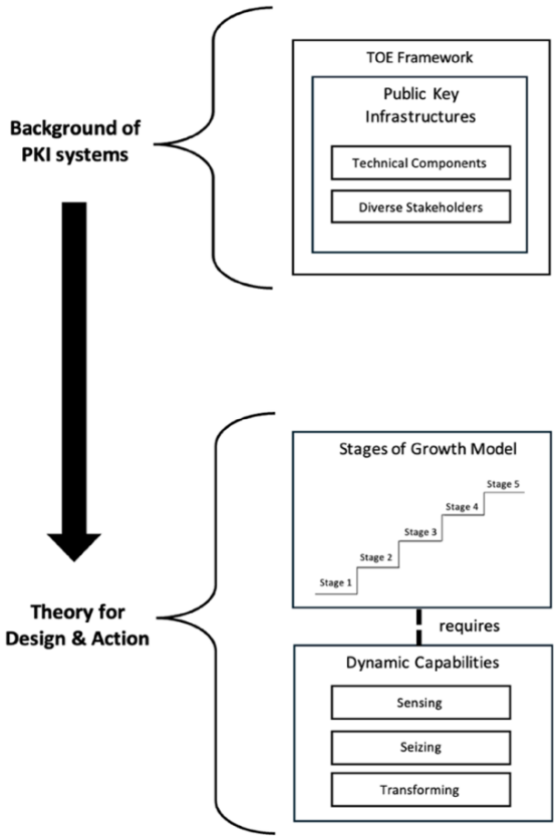


Figure 7. Overview of the Theoretical Framework Used in this research

Figure 7 shows an overview of the theoretical framework used in the research. In order to develop a theoretical framework, Type V theory for design and action is used. The TOE framework has been used to explore the multiple aspects of PKI systems. By taking technical components and diverse stakeholders that are inherent in PKI systems, the context of QS transition has been examined. In doing so, socio-technical transition challenges are identified to provide a list of factors that are relevant for organizations transitioning PKI systems to become QS. By building on the background of PKI systems, theories such as the Stages of Growth Model and Dynamic Capabilities were used in the research as core theories for the Type V theory for design and action. Based on the stages of growth model, the main premise of this research is that QS transition is composed of a series of stages, and organizations need to grow from one stage to the next to address socio-technical transition challenges. The dynamic capabilities theory (DCT) further provides a lens for examining what capabilities organizations may need to develop when changes occur in the ecosystem. In doing so, dynamic capabilities for QS transition allow organizations to do the right things and build their competitive advantage against evolving security threats in the quantum era.

3.3.2 Four Phases of Mixed Methods

To address the main research question, *"What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems?"* formulated in Section 1.3, a mixed methods approach is used to collect and analyze data. In doing so, the strength of each method is maximized, and the weakness is minimized(Creswell & Plano Clark, 2011; Creswell & Poth, 2018). While qualitative methods provide detailed information about the context of the case and problem that the research aims to investigate, quantitative methods measure specific variables or patterns related to the case (Creswell & Plano Clark, 2011). The combination of different methods, such as desk research, secondary data analysis, interviews, and workshops, is used in the research. By narrowing down the scope of research using a case study, the researcher can explore the phenomenon and further examine it. The case study not only contributes to theoretical knowledge but also offers practical insights as the findings are relatable and actionable for practitioners, bridging the gap between research and practice. Section 3.3.2 and Section 3.3.3 provide more details on the case study regarding the PKI systems in the public sector in the context of QS transition.

As one of the three approaches to conduct mixed methods, the sequential approach has been applied in this study to expand on findings from one research

method to other research methods (Creswell & Plano Clark, 2011; Creswell & Poth, 2018; Morse & Niehaus, 2016). The multiple methods used in the research are connected in sequence to address the research questions. By collecting multiple forms of data, which include both qualitative and quantitative methods, the earlier phase of research can be used to contextualize the later phase of the research. Each phase of the research can also be triangulated to scrutinize the results obtained and generate new knowledge. By undertaking mixed methods with a sequential procedure, different forms of data provide a detailed exploration and connect the results of each phase to build a comprehensive understanding of the research. The mixed methods allow researchers to dive deeper into the topic of research (Creswell & Plano Clark, 2011; Morse & Niehaus, 2016). As the researcher employs various methods and multiple data sources, the results provide more evidence and offer insights that could have otherwise been overlooked (Creswell & Plano Clark, 2011; Morse & Niehaus, 2016). Figure 8 shows an overview of the mixed methods used in the research in four phases to answer the main research question.

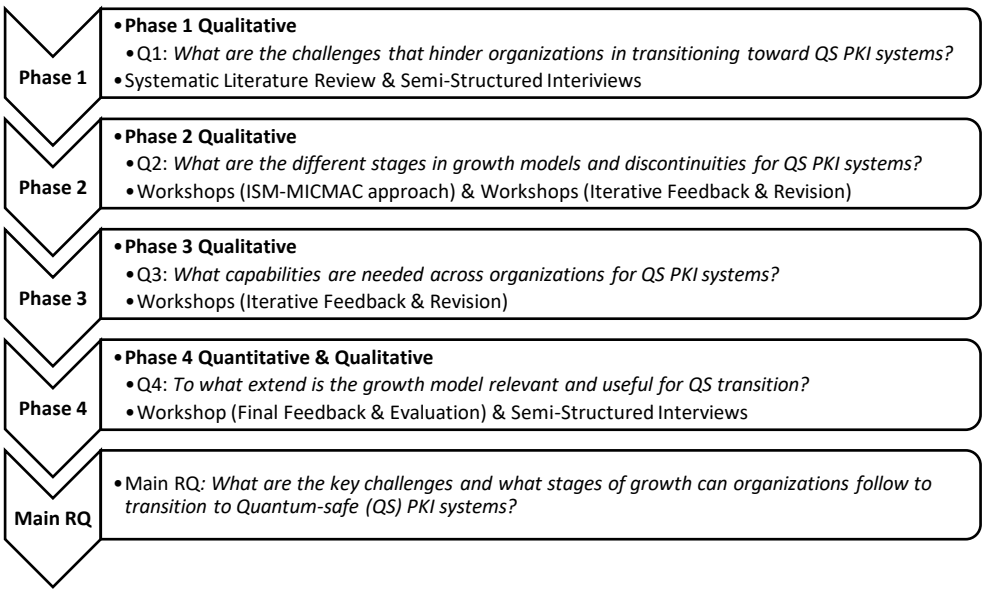


Figure 8. Overview of Mixed Methods Used in the Research

In Phase 1, a systematic literature review is conducted to gain contextual understanding of the topic of QS transition and challenges that may hinder organizations from transitioning PKI systems. The list of QS transition challenges is identified and clustered using Technology, Organization, and Environment (TOE

framework) in Section 5.3. After gaining an understanding of transition challenges in the literature, semi-structured interviews were conducted to focus on transition challenges in practice using a case study related to the Dutch PKI systems in the public sector (as explained in Section 3.3.3). The results from both the literature and the interviews provide a refined list of QS transition challenges.

In Phase 2, a series of workshops is organized to apply the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach (as explained in Section 3.4.2). The ISM-MICMAC approach provides a systematic and structured process to gain contextual understanding of transition challenges from a multifaceted lens of different organizations in the PKI systems. The refined list of challenges for the QS transition is used as input to the ISM-MICMAC approach. One of the core theories, the stages of growth model theory (as explained in 4.2), is used to investigate a series of stages of the growth model in the context of QS transition. The results of the ISM-MICMAC approach provided an initial basis for structuring different stages of the growth model for the QS transition.

Building on this empirical foundation, discontinuities are derived from the challenges at the ecosystem level. The list of discontinuities represents boundary markers between stages in the growth model and acts as necessary conditions that must be met in the ecosystem to move from one stage to the next. Due to complex dependencies, organizations in the ecosystem also needed to take part in their preparation, and QS transition cannot be addressed in isolation. The challenges at the organizational level are further translated into actions needed across inter- and intra- organizational levels to address challenges at each stage.

In Phase 3, a series of workshops has been organized to identify a list of key actions needed across different organizations. During this phase, the participants provided feedback on the details of the growth model and checked for any missing information that is relevant to the topic of QS transition. Another core theory, dynamic capabilities theory (as explained in 4.3), is used to examine transition capabilities that organizations may need in order to move from one stage to the next in the growth model for QS transition. In doing so, the list of actions needed across organizations has been translated to the list of transition capabilities needed per stage. Through an iterative process, the results are synthesized to answer sub-question 3.

In Phase 4, a final workshop and a series of interviews have been organized to evaluate the growth model that has been developed. During this phase, the details on the growth model are revisited with experts and relevant practitioners to assess relevance and usefulness, which answers sub-question 4. The evaluation workshop and interviews allowed the researcher to highlight any gaps that were still missing

in the model. The results of the workshop and interviews are collected to check whether the developed growth model is relevant and useful in practice. Further details on the workshop and interviews are discussed in Section 3.4.3, and the results of the evaluation can be found in Chapter 7. After Phase 4, the answers to sub-questions 1 to 4 are synthesized to answer the main research question.

Section 3.3.3 Relevance & Application of Case Study

In the field of Information Systems (IS), the case study research was proven valuable (Walsham, 1995). Since the case study aims to develop a novel, accurate, and robust theory that emerges from the collected data, it can address theoretical gaps when existing theories are inadequate in solving the problem of the research context (Eisenhardt, 1989; Eisenhardt & Graebner, 2007) Despite the prior constructs that may guide the investigation, no relationship between constructs is assumed, and a case study is used to provide a grounded way to generate and refine the theories with the evolving nature of the IS (Eisenhardt, 1989). If certain constructs are proven to be valuable as the research progresses, the specification of constructs can be closely revisited.

Moreover, a single case study with multiple embedded units of analysis is selected to answer the main research question, "*What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems?*" Although multiple case studies offer comparative perspectives, a single case study can be appropriate when the objective of the research is to analyze the context of the research and gather deeper insights, which may be critical to the theory (Eisenhardt, 1989; Eisenhardt & Graebner, 2007). Figure 9 shows basic types of design for case studies, and the selected type for this research is boxed in red.

According to Yin (2018), a single case study is appropriate when the case represents a) a critical test of existing theory, b) extreme or unusual circumstances, or c) a common case that serves revelatory or longitudinal purposes. The topic of research on QS transition, the case of PKI system, serves as a revelatory case as it is an explorative study that aims to build initial knowledge on a new phenomenon. There is no established theory on QS transition that currently exists. The unit of analysis should define what the case is and ensure that these are clear and correctly identified (Yin, 2018). With a single case study in the research, the unit of analysis is the QS transition process. With different organizations in the ecosystem, multiple units of analysis of QS transition process are embedded, and sub-units, such as different stages of QS transition and capabilities, are examined.

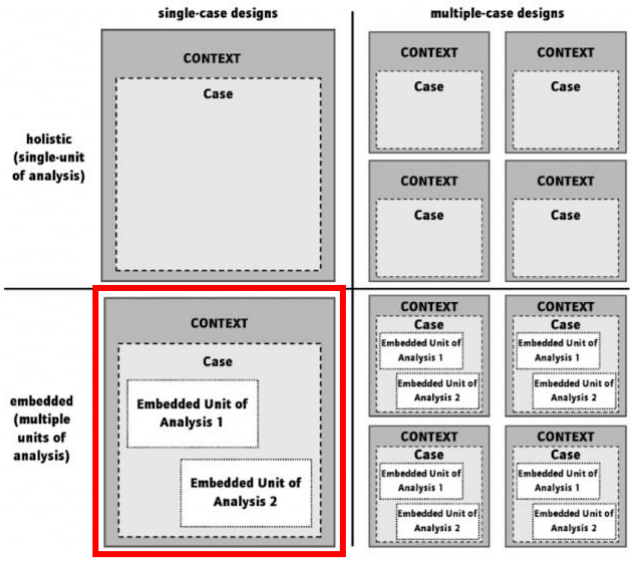


Figure 9. Basic Types of Designs for Case Studies
Note. Adapted from "Case Study Research and Applications" by Yin (2018, p. 48).

Furthermore, a wide variety of data can be collected using multiple means of data collection, such as documentation, archives, interviews, workshops, and/or secondary data (Eisenhardt, 1989). Using multiple sources of data allows for data triangulation, which strengthens the depth of analysis and reduces biases in the research (Carter et al., 2014; Denzin, 2012). Within the context of QS transition, the case of the PKI system is selected to investigate the complex technical and governance aspects of the existing infrastructures and gain knowledge on how organizations can transition towards QS PKI systems. A mixed-methods approach is employed to provide a robust framework for exploring QS transition. By conducting various methods of data collection and analysis, the selected case is further examined in the context of research. The case study design is discussed further in Section 3.3.2.

Section 3.3.4 Case Study Design

The work of Eisenhardt (1989), *Building Theories from Case Study Research,* is followed to carefully design a case study research. The case study design allows for an in-depth exploration of the chosen subject within its real-life context and sets a clear guideline for generalization of the evidence that is obtained from the case studies (Eisenhardt, 1989). Depending on the goal (explanatory, descriptive, and investigative case study) and the size of the case study (single case study or multi-

case study), the case design can be further designed (Creswell & Plano Clark, 2011; Creswell & Poth, 2018; Yin, 2018). Thus, it is important to clarify the objectives of the case study research and carefully select the cases that are being investigated.

In addition, theoretical sampling is used for case study selection to choose cases which are likely to replicate or extend the emergent theory" (Eisenhardt, 1989, p. 537). In the context of the research on QS transition, the case of PKI systems in the Dutch public sector is selected as a single case study. Since QS transition is relatively new and there is a lack of research on the topic, the case is considered not only unique but also critical due to the security threats posed by quantum computing technology. By having a single case study, the case can analyze QS transition at the ecosystem and provide actionable guidance to diverse organizations that are part of the secure facilitation of PKI systems. Rather than testing the results of the single case study, the results may be used to extend the existing theories on the topic of research.

With the focus of the case study on PKI systems in the Dutch public sector, the process of QS transition is selected as the unit of analysis**.** Since the research takes an ecosystem perspective, the embedded multiple units of analysis are chosen to recognize QS transition processes across organizations with diverse perspectives. The integration of multiple units of analysis in one case study serves to build a deeper understanding of the case (Yin, 2018). The embedded multiple units of analysis in the case study ensure that transitions across different organizations are captured. Within the embedded multiple units of analysis on QS transition processes, sub-units such as different stages and capabilities are chosen to further examine these within the units of analysis.

In order to sufficiently gather different perspectives of the PKI systems, theoretical sampling is used to select multiple embedded units of analysis in the study. With the technical complexities and interdependencies that are inherent in PKI systems, there is a need to analyze different QS transition processes with organizations across the ecosystem. Thus, organizations that are part of the Dutch government's information infrastructure that use PKIoverheid certificates need to be included. The multiple organizations for the case include PKI users (e.g., Tax authority, Chamber of Commerce, banks), organizations that create and establish standards or regulations (e.g., NIST, ETSI, etc.), organizations that manage and operate PKI systems (e.g., Logius, Ministry of Internal Affairs), and organizations that provide external expertise (e.g., Qualified Trust Service Providers, hardware vendors, and software companies).

Moreover, the use of mixed methods is suitable for research that is taking a system-level view to develop a more complete understanding of the problem (Creswell & Plano Clark, 2011; Creswell & Poth, 2018). Since the single case study on PKI systems in the Dutch public sector with multiple embedded units of analysis needs to be examined, a mixed methods approach is used to collect and analyze the data (explained in Section 3.4). In the context of the research, the technical complexity of PKI systems and interdependencies that exist across different organizations require an understanding of both the socio-technical aspects of QS transition. By drawing on the strength of each method, the combination of qualitative and quantitative data provides the research with deeper insights into QS transition. For example, interviews and workshops are used to collect qualitative data, and surveys are used to collect quantitative data.

3.4 Research Methods Used in the Research

Section 3.4 describes methods used in the research. Section 3.4.1 describes the process of a systematic literature review and discusses the results obtained. Section 3.4.2 explains how interviews were conducted and how the data from the interviews were used in the research. Section 3.4.3 provides details on the workshop and how different workshops were conducted in the research. Section 3.4.4 describes the process of ISM-MICMAC Analysis used in Workshops, and Section 3.4.5 explains how the survey was used in this workshop as a systematic method for collecting data and as an evaluation criterion.

3.4.1 Systematic Literature Review

As part of the research, a systematic literature review (SLR) was conducted to gain deeper insights into QS transition challenges that organizations may encounter when modifying their existing infrastructures. The SLR is a process-oriented research method that reviews the previous work on the relevant research topic and provides deeper research directions (Boell & Cecez-Kecmanovic, 2014). With a structured and replicable process to search and analyze the existing body of literature, all relevant studies related to QS transition and PKI systems can be reviewed without selection bias. The SLR raises research and practical implications for QS transition and builds knowledge on the current PKI systems.

By using the keywords such as “post-quantum cryptography challenge,” “quantum-safe cryptography challenge,” and “quantum-safe transition challenge, a comprehensive literature search was conducted on Google Scholar, Mendeley, ScienceDirect, Scopus, and SpringerLink. The search results identified a total of

2266 articles. After screening the titles and abstracts of each paper, we selected 154 articles and excluded 19 duplicate articles. Of the remaining 135 articles, 93 were deemed irrelevant and excluded after full-text review. As a result, 42 articles were selected for the review. As a result, 42 articles were selected for the review. Upon evaluating these articles, we identified the list of QS transition challenges. Figure 10 shows the process of SLR conducted in this research. The Technology, Organization, and Environment (TOE) framework was used to categorize the diverse transition challenges with a well-established structure (further explained in Section 5.3).

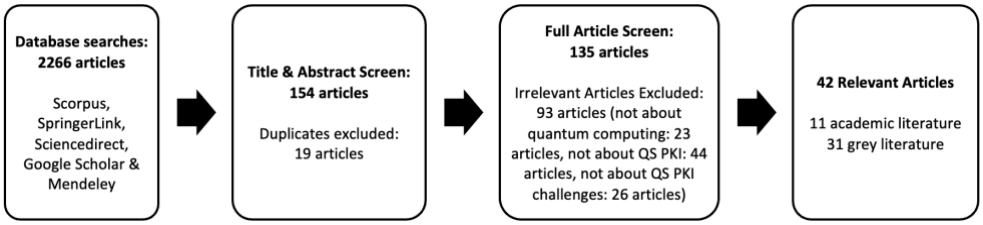


Figure 10. Process of Systematic Literature Review

Section 3.4.2 Semi-Structured Interviews

The interviews with experts and practitioners from organizations that are part of the PKI systems were conducted to understand the challenges in practice. Given the early-stage nature of QS transition, it was crucial to extend the results found from the literature and understand QS transition challenges in practice with multiple perspectives of experts and practitioners. Moreover, the interviews with organizations in the PKI systems provide deeper insights into the topic of QS transition and the practical implications of the results obtained from SLR. To conduct the semi-structured interviews, purposive sampling was used to select organizations that are part of the PKI systems in the Dutch government that use government certificates. Due to the early stage of QS transition, a limited number of experts and practitioners were available to provide the knowledge and experience regarding the topic of research.

The interviews with stakeholders include PKI users (e.g., Tax authority, Chamber of Commerce, Banks), organizations that manage PKI systems (e.g., Logius, Ministry of Internal Affairs), and organizations that provide external expertise (e.g., Qualified Trust Service Providers). The interviewees were selected based on availability and the expertise they have within their organizations. The interviewees' expertise includes enterprise architects, policy, and organization management etc. This would also allow us to gain a balanced overview of how

different stakeholders view the QS transition in the PKI system and be able to compare the findings. Table 1 shows the list of 12 interviewees. There were four experts from government agencies, one expert from a bank, two experts from research institutes, one expert from the tax office, two experts from software companies, and one expert from a service provider. The examples of interview protocol can be found in Appendix B.

Table 1. List of Respondents for the Interviews in Phase 1

#	Role	Organization	Perspective
1	Chief Architect	Government Agency	Regulatory organization
2	Information Sharing Architect	Bank	PKI user
3	Change Manager	Government Agency	Regulatory organization
4	Policy Officer	Government Agency	PKI user
5	Strategic Advisor	Research Institute	External expert
6	Chief Technology Officer	Service Provider	External expert
7	Enterprise Architect	Tax Office	PKI user
8	Cryptographer	Research Institute	External experts
9	Policy Coordinator	Government Agency	Regulatory organization
10	General Manager	Software Company	External expert
11	Software Developer	Software Company	External expert
12	Vice President of Operations	Service Provider	External expert

Note. Adapted from "Realizing quantum-safe information sharing" by Kong, Janssen & Bharosa (2024, p.5).

Moreover, a series of semi-structured interviews has been conducted in Phase 4 as part of the evaluation (explained in Section 3.4.3). The evaluation of the research ensures that the developed stages of the growth model are shaped by the needs and experiences of practitioners, where feedback is representative of the intended user base. Given the early stage of the growth model and the trajectories of QS transition, gathering multiple perspectives and insights from experts and practitioners was crucial. However, only one workshop was organized as a final evaluation due to the lack of experts and practitioners in the field of QS transition who are affiliated with the public sector. Thus, additional interviews were conducted to provide perspectives and feedback on the growth model and QS transition. The content of the interviews followed the evaluation approach outlined in Section 7.2. Table 2 shows the list of respondents for the interviews. The details of the results obtained

from the evaluation workshop on the relevance and usefulness of the stages of growth model for QS transition can be found in Section 7.3

Table 2. List of Respondents for the Interviews in Phase 4

#	Role	Organization	Perspective
1	Change Manager	Government Agencies	Regulatory organization
2	CISO	Government Agencies	PKI user
3	Strategic Advisor	Government Agencies	Regulatory organization

3.4.3 Workshops

The workshops provide interactive sessions to bring multiple parties together to share knowledge and collaborate on problem-solving. The workshops can be used to engage in structured activities to explore and provide feedback on specific aspects of the research. In this research, the workshops were used to bring together experts and practitioners relevant to the PKI systems in the public sector. In doing so, the workshops captured diverse perspectives of participants to discuss the QS transition in the PKI systems. For researchers, the workshops provide a flexible method to build consensus and facilitate collaborative discussion.

Since participants can clarify concepts discussed during the workshops, new ideas and strategies can be generated from reflecting on their own knowledge and experience and learning from each other. In order to understand complex issues for QS transition, multiple viewpoints were needed from various participants. Thus, the workshop allowed the researchers to invite experts and practitioners from different backgrounds to ensure that the discussions do not remain in a homogenous environment. The workshop allowed active dialogue between participants and strengthened the quality of discussions. Ten workshops were organized and can be divided into three types of goals, which were exploratory workshops, Iterative feedback and revision workshops, and a final evaluation workshop.

The exploratory workshops focused on understanding the topic under study. In the context of this study, this included identifying challenges, conducting analysis using the ISM-MICMAC approach, and gathering information to develop the growth model. The iterative feedback and revision workshops focused on reviewing the findings of the outputs from the previous workshops. The workshops were organized to enable the discussion and further refine the results based on the expert and practitioner's perspectives. The final evaluation workshop focused on assessing the relevance and usefulness of the growth model developed in the research. The workshop also provided an opportunity to share the opinions of experts and intended users. This allows the researcher to reflect on the results and gather suggestions for

further refinement and the next steps. The details of each goal of the workshops are explained below.

The goal of Workshops 1 to 4 was to apply the ISM-MICMAC approach and prioritize QS transition challenges and identify different stages of the growth model. After the stages were identified, Workshops 5 to 9 were organized to refine the results and determine the actions needed for each stage to address QS transition challenges. Through an iterative process, participants provided feedback to revise the growth model. An additional Workshop 10 has been organized to provide an evaluation of the growth model for QS transition. The participants of the workshops had either a prior technical background or knowledge and experience from industry, government, or academia. With the stakeholders who are willing to provide the information and conduct the workshops, various stakeholders in the PKI system are selected in the process as participants to ensure heterogeneity. The list of workshops conducted in the research is shown in Table 3, and more details about each workshop are explained below.

Table 3. List of Workshops

#	Goals	Organizations Participated	Date Conducted
1	ISM-MICMAC (Challenges & Stages)	Government Agencies	25/01/2023
2		Government Agencies	14/02/2023
3		Service Providers	14/02/2023
4		Financial Institutions	10/05/2023
5	Iterative Feedback & Revision (Discontinuities & Key Actions per Stage)	Government Agencies/ Private Companies/ Research Institutes/ Financial Institution	14/062023
6		Government Agencies/Private Companies/ Research Institutes/ Financial Institutions	14/06/2023
7		Government Agencies/Private Companies/ Research Institutes/ Financial Institutions	07/11/2023
8		Government Agencies	22/02/2024
9		Government Agencies/Private Companies/ Research Institutes/ Financial Institutions	16/10/2024
10	Final Evaluation	Government Agencies/ Service Providers/ Research Institutes	12/03/2025

From Workshops 1 to 4, the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach was used to further examine contextual relationships between the list of QS transition challenges. In doing so, participants can share their insights and extend the discussion on QS transition challenges that organizations may need to consider when implementing and adopting QS solutions. While ISM can analyze the interrelationships between the

factors that influence the system, the MICMAC classifies factors based on driving power and dependence power. The MICMAC approach is used to classify these factors and validate the results obtained from the ISM analysis (Gorane & Kant, 2015; Warfield, 1974).

In the context of this research, the ISM-MICMAC approach (as explained in Section 3.4.4) examines the relationship between the list of QS transition challenges and categorizes these challenges per driving and dependency power (Attri & Sharma, 2013). The results show dominant challenges and clarify challenges that need to be addressed with priorities. To conduct the workshops, purposive sampling was used to identify organizations relevant to PKI systems. The steps of the ISM-MICMAC approach can be found in Appendix C. The ISM-MICMAC results in a list of challenges that need to be addressed to become QS, with priorities at different stages (as explained in Section 6.2.3). These results were synthesized, and a hierarchical set of interrelated challenges provided an initial basis for structuring different stages of the growth model.

However, strong interdependencies among the challenges at each stage made it difficult to translate the findings into actionable guidance. Building on the empirical work from the ISM-MICMAC approach, discontinuities are derived from the challenges at the ecosystem-level. These discontinuities represent boundary markers between stages and act as necessary conditions for the ecosystem to move from one stage to the next. The challenges at the organizational-level are further translated into the list of actions needed across inter- and intra- organizational levels to address challenges at each stage.

Workshops 5 to 9 were organized to refine the discontinuities and the key actions needed across organizations. The iterations of the growth model are shown in Appendix D. The workshops provided practitioners and experts with opportunities to share their insights on the iterated growth model and to determine whether additional revisions are needed. The research focused on gaining insights from a smaller number of participants and conducted multiple iterative workshops over time to build on the previous insights. This approach was adopted due to the limited availability of participants with sufficient knowledge and experience in QS transition. The identified key actions across different organizations were further translated into a set of transition capabilities (as shown in Table 16) required within each organization at each stage.

For Workshop 10, relevant practitioners from organizations in PKI systems in the Dutch public sector were invited to evaluate the growth model for QS transition. The evaluation workshops ensure that the developed stage model is not

only informed by research but also shaped by the needs and experiences of practitioners, where feedback is representative of the intended user base. In doing so, insights into the relevance and usefulness of the stages of growth model for QS transition were gathered. The feedback from experts and practitioners was also used to highlight the implications of QS transition and discuss potential transition efforts for QS transition moving forward. The qualitative feedback from the workshop was complemented with a structured survey that was embedded within the workshop. The details on the evaluation workshop can be found in Chapter 7.

3.4.4 ISM-MICMAC Analysis Used in Workshops

The Interpretive Structural Modelling was introduced by Warfield (1974) to structure a set of factors in complex issues into a systemic hierarchical model. By identifying relationships among factors, unclear mental models of factors are put into a hierarchy (Attri et al., 2013). ISM is not only used for long-term planning with its high level of abstraction, but also for analyzing details of systems and processes in various fields. Multiple studies have been used to analyze important factors with the use of ISM in the field of strategic planning, decision making, and process engineering (Devi K et al., 2021; Goel et al., 2022; Sivaprakasam et al., 2015). The inter-relationships of criteria and their different levels can systematically structure this relationship between factors into a hierarchical model.

The use of transitive inference in the ISM may reduce the relational queries of the factors while considering all possible relations between factors. In order to respond to a series of relational queries between factors, participants taking part in the discussion need to be familiar with the topic and have enough understanding of the context. Through interdisciplinary and interpersonal communication, participants discuss interactively one question at a time to examine the relationship between factors. By providing a space for participants to reflect on each factor, participants share how different factors may or may not address the problem in the context. The results from the ISM show a structured graphical representation of the factors and serve as a learning tool to gain a deeper understanding of the problem context.

In addition to ISM, the use of Matrice d'Impacts Croisés Multiplication Appliqués à un Classement (MICMAC) evaluates the relationship between the factors according to their driving power and dependence power (Duperrin & Godet, 1973). The MICMAC analysis can validate the results obtained by ISM and classify the factors using four categories: autonomous, dependent, linkage, and independent (explained in Section 6.2.1). The integrated ISM-MICMAC analysis is well

documented in various domains such as supply chain management, industry 4.0 adoption (Godinho Filho et al., 2022; Janssen et al., 2019; P. Kumar et al., 2021; Mishra & Sharma, 2015; Ranjan et al., 2024; Singh et al., 2023). The results of the ISM-MICMAC analysis show influences among factors that were previously unclear and allow researchers to gain insights into the relations of factors on complex issues systematically. The steps of the ISM-MICMAC approach are shown in Appendix B.

3.4.5 Survey Used in Workshop

A survey was used in this research as a systematic method for collecting data and acted as an evaluation criterion for researchers to understand the opinions of participants and gather feedback from their knowledge and expertise. The qualitative feedback from the workshop was complemented with a structured survey that was embedded within the workshop. Since multiple participants in the workshop give better insight into the ecosystem perspectives than a single person, a survey was conducted during the workshops. In the context of the research, validating the outcome and measuring whether the QS transition has occurred or not in accordance with the model cannot be done due to the early stage of QS transition. Thus, surveys were used in the workshop focused on assessing the relevance and usefulness of the growth model developed in the research.

This allowed the researchers to understand participants' perceptions of whether the growth model developed in the research is relevant and useful for the intended users. More details on the survey and evaluation approach can be found in Chapter 7. By capturing the reflection and feedback of participants who are experts and intended users of the growth model, the survey provided ways to inform the research with improvements and next steps for the model. Likewise, the survey in workshops not only presented as a way to measure and collect data but also created a feedback loop for the growth model for QS transition and provided a shared learning process for participants to think about their strategies to further align with the challenges and needs of their organizations. The survey used in the workshop also allowed researchers to triangulate findings to ensure both depth and reliability of the workshops conducted.

3.5 Chapter Conclusion

Since the existing infrastructures already have systems in place with a set of established frameworks for technology, policies, and practices, interpretivism was chosen as an appropriate research philosophy to gather the insights across different

organizations with diverse perspectives of experts and practitioners. An overview of the theoretical framework used in this research is provided to clarify the overall intent and better align with different research methods. Based on Gregor's The Nature of Theory in Information Systems, the research uses Type V Theory for Design and Action. By taking technical components and diverse stakeholders that are inherent in PKI systems, the context of QS transition is examined. The research identifies socio-technical transition challenges that are relevant for organizations transitioning PKI systems to become QS. By building on the background of PKI systems, Type V Theory for Design and Action further provides a prescription on what actions may be needed in organizations to address challenges and move towards QS transition. Type V Theory answers *what should be done* from what is in the context of research.

The technical complexity of PKI systems and interdependencies requires an understanding of both the socio-technical aspects of QS transition. The chapter introduced a sequential mixed-method approach with four phases of the research to collect and analyze the data. By expanding on findings from the earlier phase of research, the latter phase of the research is contextualized. The knowledge of relevant experts and practitioners on QS transition and complexities in the existing infrastructures was captured using diverse methods, such as interviews, workshops, and surveys. By drawing on the strength of each method, the combination of qualitative and quantitative data provides the research with deeper insights into the QS transition. For example, interviews and workshops are used to collect qualitative data, and surveys are used to collect quantitative data. The results of each phase build a comprehensive understanding of the topic of research.

In Phase 1, the results from both the literature and interviews provide a refined list of QS transition challenges. After gaining an understanding of transition challenges in the literature, semi-structured interviews have been conducted to focus on transition challenges in practice, using a case study related to the Dutch PKI systems in the public sector. The list of QS transition challenges is identified and clustered using the Technology, Organization, and Environment (TOE) framework.

In Phase 2, the list of transition challenges is applied to identify different stages of the growth model for QS transition. A series of workshops was organized and used the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach to provide a systematic and structured process to prioritize the identified challenges. The hierarchical set of interrelated challenges provided an initial basis for structuring the stages of the growth model. Building on this empirical foundation, discontinuities are derived from the

challenges in the ecosystem. These discontinuities represent boundary markers between stages in the growth model and act as necessary conditions that must be met in the ecosystem to move from one stage to the next. The challenges at the organizational level are translated into actions needed to address challenges at each stage.

In Phase 3, another series of workshops was organized to determine key actions needed across organizations at each stage. From these key actions, a list of transition capabilities was compiled. One of the core theories, the dynamic capabilities theory, is used to examine transition capabilities that organizations may need to move from one stage to the next in the growth model. Through an iterative process, the results have been synthesized to further revise the list of actions and the list of transition capabilities needed across organizations.

In Phase 4, the details on the growth model have been revisited with experts and relevant practitioners. The evaluation workshop and interviews allowed the researcher to highlight any gaps and check whether the developed growth model is relevant and useful in practice. The relevance of the growth model was assessed to determine whether the model captures the relevant key socio-technical transition challenges and provides actionable guidance for QS transition. The usefulness of the growth model is assessed to determine whether the growth model aligns with the needs of experts and practitioners and can serve as a useful tool for organizations transitioning towards QS.

Chapter 4 Theoretical Background

4.1 Introduction

This chapter provides the theoretical background used in the research. Building on the foundational theories explained in Section 3.3.1, the theoretical background of the two core theories is presented in Sections 4.2 and 4.3. In Section 4.2, the Stages of Growth Model is introduced as one of the core theories, and key theoretical gaps from related work are discussed. In Section 4.3, another core theories on organizational capabilities with the focus on dynamic capabilities are introduced, and key theoretical gaps from related work are discussed. The chapter ends with the conclusion in Section 4.4.

Part of this chapter is based on the following publication:
Kong, I. (2022). Transitioning towards quantum-safe government: Examining stages of growth models for Quantum-safe public key infrastructure systems. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022. https://doi.org/10.1145/3560107.3560182

4.2 Core Theory 1: Stages of Growth Model

This section introduces the Stages of Growth Model and discusses the related work on the stage model theory. Section 4.2.1 introduces Stages of Growth Model and highlights areas where these theories have been useful. Section 4.2.2 presents the related work on the Stages of Growth Model in the context of public sector service provisions. Section 4.2.3 discusses limitations of the current research on Stages of Growth Model.

4.2.1 Stages of Growth Model

In the field of information Systems (IS), stages of growth models or *stage models* have become an important topic in both research and practice. It is also referred to as a *stage of growth* or *stage models* (Layne & Lee, 2001; Prananto et al., 2003; Solli-Sæther & Gottschalk, 2010). The earlier growth models develop an understanding of the evolution of information technology and show how technologies evolved in organizations (Gibson & Nolan, 1974; Nolan, 1973). One of the notable examples of the model is proposed by Richard Nolan in 1973 concerning the general approach to IT in business. Nolan's Stages of Growth Theory introduces how IT evolves in organizations in six stages, which are known as

initiation, contagion, control, integration, data administration, and maturity (Gibson & Nolan, 1974; Nolan, 1973, 1979).

With a series of stages, the model provides a roadmap for further organizational development. For organizations, there can be different focal points in stages, ranging from reducing cost, ensuring data protection and regulatory compliance, to coordinating data management strategies for information security. Whether its for addressing interoperability across different departments to managing security risks with evolving threats and regulatory requirements, the stages of the growth model shows how organizations evolve and address new tasks and problems to move from one stage to the next (Kazanjian & Drazin, 1990). The concept of *discontinuity* depicts the separation of stages as organizations move between stages (Janssen & van Veenstra, 2005; Klievink & Janssen, 2009).

As organizations grow in stages, the discontinuities act as boundary markers that distinguish one stage from the next and set the stage for the next phase of growth. Each stage of the growth model allows organizations to describe their processes and evaluate their performance through self-assessment (Fontana et al., 2018). The models can assess the current level (as-is situation) of an organization to the desired level (to-be situation) in distinct stages (Becker et al., 2009; Iversen et al., 1999). By identifying each stage, organizations can provide guidelines for actionable steps and future improvements (Gottschalk, 2009; Kazanjian & Drazin, 1990). The stages of growth model provides a structured overview of organizations by conceptualizing its evolution over time (Caralli et al., 2012; Mettler & Rohner, 2009).

Nolan's contribution lies in the foundational idea that organizational capability develops through a series of stages and may require different responses depending on the stages. Since the initial conception of the Stage of Growth Theory in the early 1970s, many variants of the models have appeared based on a sequence of stages. The growth models have been applied to various research domains including business process management (de Bruin et al., 2005; J. Lee et al., 2007; Niehaves et al., 2013), platform business (Kim & Yoo, 2019) health care (P. Brooks et al., 2015; De Carvalho et al., 2016), knowledge management (Gottschalk & Khandelwal, 2004), project management (Brookes et al., 2014), and e-government (Janowski, 2015; Janssen & van Veenstra, 2005; Klievink & Janssen, 2009; Rooks et al., 2017).

Moreover, the stages of the growth model are useful in managing information systems and assisting decision makers in practice. There are several benefits to using the stages of growth model. First, the model provides a high-level overview to guide organizations transitioning from one stage to the next. The

overview of the transition in stages allows organizations to develop strategies. Second, the model provides a framework that organizations use to assess their current state of information systems. By identifying the stage they are in, organizations can understand the need at each stage and allocate resources. Third, the model acts as a communication tool to share knowledge. By recognizing the organizational needs, the model allows organizations to discuss their transition process and highlights areas for continuous improvement.

Among practitioners, the Quality Management Maturity Grid proposed by Crosby (1980) has influenced various applications of the maturity model. One of the well-known models is called Capability Maturity Model (CMM), which was introduced by the Software Engineering Institute (SEI) of Carnegie Mellon University. (Paulk et al., 1993). The CMM was adopted by software companies and consultants to measure and improve the development process of businesses. Organizations grow through their maturity levels and follow a structured process to meet deliverables and improve their performance. Building on the conceptual foundation of CMM, the later works were adopted for broader maturity model development (e.g., de Bruin et al.,(2005) and Vitharana and Mone (2008)). By assessing their processes, organizations can adjust and respond more effectively to the changes in the industry.

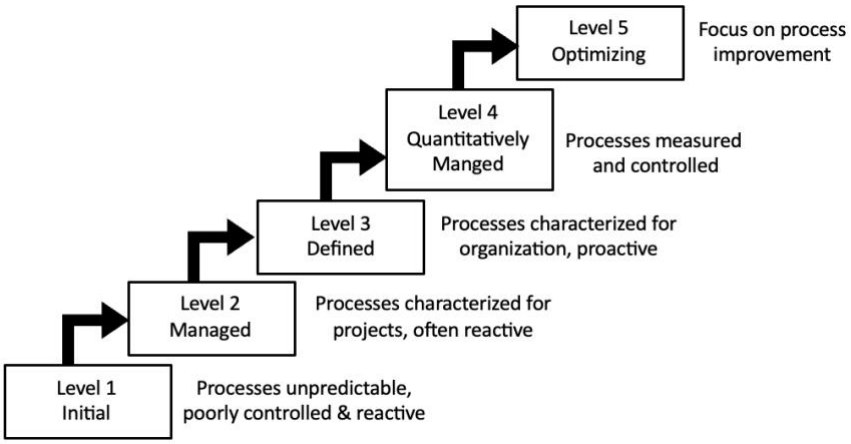


Figure 11. Example of Capability Maturity Model Integration
Note. Adapted from "Software Engineering Institute" by Paulk et al (1993, p. 8*)*.

Over the years, the model called Capability Maturity Model Integration (CMMI) has also been introduced (Rassa et al., 2002). The CMMI model provides a structured framework for organizations with a roadmap for process improvement. An example

of CMMI is shown in Figure 11. Organizations can improve process maturity and streamline their operations to develop better products and services. The CMMI model can be applied to different software, hardware, and service development across industries (Chrissis et al., 2011; Poeppelbuss et al., 2011; Rassa et al., 2002). The five maturity stages outlined in CMMI allow organizations to implement systematic approaches. By identifying potential risks and developing strategies, CMMI ensures that organizations focus on long-term growth and remain resilient in a dynamic environment.

The stages of growth models in research and practice show three main objectives: Descriptive, Prescriptive, and Comparative (Becker et al., 2009; de Bruin et al., 2005). While the models show different objectives, the maturity levels in the model act as a good indicator in navigating their process and understanding the changes that occur around the organizations. For descriptive purposes, the organization or process's current level (as-is situation) is evaluated and used as a diagnostic tool. For the prescriptive purpose, the desired maturity levels are identified, and guidance on how organizational improvement measures (specific and detailed course of action) should take place. For comparative purposes, the maturity levels of organizations are compared for a comparative analysis (benchmarking) (Becker et al., 2009; de Bruin et al., 2005).

4.2.2 Related Previous Work on the Stages of Growth Model

Since Nolan proposed the stages of growth model more than fifty years ago, many variants of the model with different objectives and stages have appeared in academic literature. Several models have been further applied in the context of e-government to monitor and improve public sector service provisions (Layne & Lee, 2001; Prananto et al., 2003; Solli-Sæther & Gottschalk, 2010). The extensive development of growth models has been developed as an approach to monitor and improve public sector service provisions. The growth models act as a framework that can guide stages of technological maturity in government and identify capabilities that are required to move from one stage to the next. Table 4 outlines the literature on e-government growth models in the past two decades.

The literature shows that there are various applications among e-government growth models depending on its objectives. The model of Layne and Lee (2001) focuses on service provision by municipalities to citizens and businesses. The growth model looks at e-government maturity in terms of technology, supply, and organizational integration. This is similar to growth models presented by Hiller and Bélanger (2001) and Moon (2002) that propose e-government maturity in the

development of electronic services and democratic participation. Although the work focuses on the same application in the development of electronic services and democratic participation, the growth model from the work of Siau and Long (2005) is different from the previously mentioned models.

Table 4. Comparison of Previous Work: Stages of Growth Models in E-Government

Scholars	Application	Stages
Layne & Lee (2001)	Fully functioning e-government	Catalogue, Transaction, Vertical integration, Horizontal integration
Hiller & Bélanger (2001)	Electronic public services & democratic participation	Information dissemination, Two-way communication, Integration, Transaction, Participation
Moon (2002)	Electronic public services & democratic participation	Web presence, Interaction, Transaction, Transformation/ Integration, Participation
Siau & Long (2005)	E-government	Web presence, Interaction, Transaction, Transformation, e-democracy
Janssen & van Veenstra (2005)	Development of information architectures	No integration, One to one integration, Warehouse architecture, Broker architecture, Orchestrated broker architecture
Andersen & Henriksen (2006)	Online services in public sector	Cultivation, Extension, Maturity, Revolution
Gottschalk & Solli-Sæther (2006)	IT outsourcing relationship	Cost stage, Resource stage, Partnership stage
Gottschalk & Solli-Sæther (2008)	E-government interoperability	Work process stage, Knowledge sharing stage, Value Creation stage, Strategy Alignment stage
Klievink & Janssen (2009)	Joined-up government	Stovepipes, Integrated organizations, Nationwide portal, Inter-organizational integration, Demand-driven, joined-up government
Lee (2010)	Review of 12 growth models	Presenting, Assimilating, Reforming, Morphing, E-governance
Kalampokis, Tmabouris & Tarabanis, (2011)	Open government data	Aggregation of government data, Integration of government data, Integration of gov data with non-gov formal data, Integration of gov data with non-gov formal and social data
Janowski (2015)	Digital government evolution	Digitization, Transformation, Engagement, Contextualization
Favaretto & Melrelles (2015)	ICT/IS initiatives in modern organizations	Initiation, Contagion, Control, Integration, Data Administration, Maturity
Rooks, Matzat & Sadowski (2017)	E-government	Information provision, Requests for permits and documents, Personal service delivery, E-democracy

Lemke et al (2020)	Smart government	Catalogue, Transaction, Vertical Integration, Horizontal Integration, Provident

In addition, the work of Kalampokis, Tambouris, and Tarabanis (2011)introduces a four-stage growth model that provides a roadmap for Open Government Data re-use and evaluation of online public service development. This is different from the growth model of Rooks et al. (2017) that describes the development of e-government in four stages, and the growth models from Andersen and Henriksen (2006), Gottschalk and Solli-Sæther (2008) and Janowski (2015) , which also have four stages. Although there are the same number of stages in the growth models, the application and objectives of the models all vary from one another. Also, the work of Siau and Long (2005) and Rooks et al. (2017) both call the last stage as *e-democracy*. However, the number of stages differs from one another, and the objectives of applications also vary.

Moreover, the literature on the e-government growth model often extends the existing growth models from previous work. The work of Gottschalk and Solli-Sæther (2006) focuses on IT outsourcing relationships and identifies three stages, which include the cost stage, the resource stage, and the partner stage. Their other work such as of Gottschalk and Solli-Sæther (2008) discusses the stages of e-government interoperability, which is based on the literature on systems interoperability and builds on the existing growth models (Gottschalk & Solli-Sæther, 2008). Similarly, Favarettp and Melrelles (2015) build upon Nolan's growth model (1979) to develop a measurement of the ICT/IS initiatives in organizations and an evaluation of emerging technology. Also, both models presented in the work of Siau and Long (2005) and Lee (2010) use a meta-synthesis approach by developing new growth models from existing models.

4.2.3 Limitations of the Stages of Growth Model

As the work of King and Kraemer (1983) addressed criticisms towards the growth model proposed by Nolan (1979), many of the criticisms hold true for the stages of growth models today and are controversially discussed within the academic community (Poeppelbuss & Roeglinger, 2011; Raber et al., 2013). One of the criticisms surrounding the stages of growth models is that the process of how technologies have evolved and continue to evolve in organizations is much more complex in practice (de Bruin et al., 2005; King & Kraemer, 1983). While some argue that stages may not be skipped due to difficulty in implementing changes in the services (Kazanjian & Drazin, 1990; J. Lee, 2010), others state that organizations

can skip one or more stages if the right capabilities are addressed for the higher stages (Klievink & Janssen, 2009).

Moreover, the classification of the stages and what is being classified depends on the context and objective of the model. The table shows how different growth models are incongruent. While one model is a three-stage growth model, others consist of five or more stages in their models. Even when the application of growth models may be similar, the number of stages of growth models differs from one another. The classification depends on the objective of the model and what is being classified (Janssen & van Veenstra, 2005; Klievink & Janssen, 2009). This means that the growth models cannot be used universally, as they are designed to meet specific objectives, and the concept of maturity may vary depending on these objectives. In the context of this research, existing models do not offer a silver bullet to guide organizations in their transitions (Klievink & Janssen, 2009; Maheshwari et al., 2011).

Furthermore, there is a lack of a theoretical base when deriving different stages in the models (de Bruin et al., 2005; Thordsen & Bick, 2023). While there are models that are exceptions to this criticism (e.g., with the concept of *discontinuity* introduced by the work of Janssen and van Veenstra (2005) and Klievink and Janssen (2009) and the work Siau and Long (2005) that sees *stages* as gradual *leaps*), the majority of the models do not have a systematic approach in deriving different stages of the models. Likewise, the existing growth models overlook the concept of *discontinuity* that is used to classify different stages, and they do not incorporate it into the growth model. There is no theoretical framework on how to reach and define different stages, and no predefined method was available. Thus, this research is the first to develop a stages of growth model that is grounded in QS transition challenges. By applying Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC), this research presents a novel approach in identifying different stages of growth model and the list of discontinuities.

4.3 Core Theory 2: Organizational Capabilities

This section introduces the concept of organizational capabilities and discusses the related work. Section 4.3.1 introduces the concept of organizational capabilities with a focus on dynamic capabilities and highlights areas where these theories have been useful. Section 4.3.2 focuses on dynamic capabilities and presents the related work. Section 4.3.3 discusses limitations of the current research on dynamic capabilities.

4.3.1 The Concept of Organizational Capabilities

In the field of strategic management and organization theory, various scholars have defined the concept of organizational capabilities in different ways. Notably, the term, organizational capability is widely understood as an *ability* of an organization to deploy its tangible (inventories, financial capital, products) or intangible resources (e.g., joint ventures, firm culture, trademarks) to perform a task or to improve existing performance (Teece et al., 1997). Likewise, the work of Dosi, Nelson and Winter (2000) states that organizational capabilities are defined as a firm's *ability* to perform effectively to solve organizational problems. The concept of organizational capabilities often focuses on attributes that contribute to their unique organizational processes. Others conceptualize organizational capabilities as an organization's *routine* or *process* to improve organizational performance (Eisenhardt & Martin, 2000).

The initial work of Penrose's Theory of Growth of the Firm (1959) provides a foundational insight into how firms leverage resources for growth. The *resource-based view* (RBV) of the firm conceptualizes organizational capabilities as firm-specific resources and routines that contribute to competitive advantage (Barney, 1991; Penrose, 1959, 1995). The classical RBV perspectives view a firm as a collection of productive resources that develops based on its resources and their utilization (Penrose, 1959). The organizational resources and capabilities are something rare, valuable, and non-substitutable, which form the basis for a firm's sustained competitive advantage (Barney, 1991). The research on RBV further argues that a firm's activities rest on the resources it controls, and patterns of organizations are influenced by various capabilities (Richardson,1972).

However, the perspective on RBV has been criticized for its inability to explain intangible resources and the dynamics of a firm's development in a changing external environment (Barney, 1991; De Toni & Tonchia, 2003; Teece & Pisano, 1994). Since the work on RBV, different perspectives have shaped the field of strategic management research and practice concerning an organization's growth and capabilities (Nelson & Winter, 1982; Richardson, 1972). As an extension of the

RBV, the concept of dynamic capabilities has been introduced to explain how resources evolve to ensure growth and how organizations create resources in a changing environment. The dimensions of dynamic capabilities are seen as sources of advantage and explain how combinations of competences and resources (value, rareness, imitability, and substitutability) can be developed, deployed, and protected in organizations.

Moreover, the routines alone cannot perform in a highly competitive environment as these tend to adapt too slowly to changes (Teece, 2007; Teece et al., 1997). By modifying and reconfiguring existing intangible or tangible assets, organizations can further create new strategic assets (such as technology, collaboration, capability, and complementary assets) (Helfat et al., 2007; Teece, 2007). The work of Teece (1997) terms dynamic capabilities as an organization's capability that can effectively address the rapidly changing environment. The concept of dynamic capabilities is crucial not only for organizations to reinvent and go through a transformation but also to reintroduce operational activities that meet the changing environment (Eisenhardt & Martin, 2000; Teece, 2007; Winter, 2003).

As organizations need to adapt to new situations and address new emerging challenges, the literature on dynamic capabilities has provided deeper implications for strategic management practice. The studies on dynamic capabilities extend from analyzing and improving business performance, driving innovation, to ensuring resilience in an ever-evolving marketplace. While ordinary capabilities focus on doing things right, dynamic capabilities focus on doing the right things, which find opportunities and facilitate innovation. (Teece, 2014; Teece et al., 2016). The ordinary capabilities enable organizational performance, and dynamic capabilities ensure that ordinary capabilities perform in an uncertain and constantly changing environment (Teece, 2014; Teece et al., 2016)

4.3.2 Related Previous Work on Dynamic Capabilities

The work of Teece and Pisano (1994) defines it as the ability of organizations to gain, integrate, and transform resources for changing environments (Teece et al., 1997; Teece & Pisano, 1994). Building on the definition, Teece (2007) further emphasizes the importance of micro foundations, such as routines, processes, and managerial actions that serve as the building blocks of dynamic capabilities**.** In order to detect, create, and seize opportunities, it is necessary to monitor the environment and sustain the performance of organizations, which allows firms to sense, seize, and transform opportunities (Teece, 2007). These include: 1. an ability to sense and shape opportunities and threats, 2. an ability to seize opportunities, and 3. an ability

to maintain competitiveness through protecting, enhancing, and reconfiguring intangible and tangible assets.

Moreover, Teece (2014) further explains that such abilities are crucial to align strategy and achieve performance outcomes. The work of Teece (2014) and Teece (2016) further makes a distinction that when traditional capabilities focus on doing things right, dynamic capabilities focus on doing the right things and hold the view of evolutionary fitness, which finds opportunities and facilitates innovation (Teece, 2014; Teece et al., 2016). In the context of a rapidly changing environment with innovation and deep uncertainties, building dynamic capabilities is crucial as it can help firms to navigate. He emphasizes the role of managers as active agents, and dynamic capabilities are key to maintaining competitiveness (Teece et al., 2016). The work of Teece (2018) further states that sensing, seizing, and transforming abilities need to be implemented in a practical system where a set of routines, processes, and organizational structures in a firm are maintained and aligned.

Furthermore, the work of Eisenhardt and Martin (2000) distinguishes organizational capabilities into two different capabilities: ordinary capabilities and dynamic capabilities. They argue that while ordinary capabilities enable organizational performance and maintain services and products, dynamic capabilities invoke the changes to ensure ordinary capabilities perform (Eisenhardt & Martin, 2000). Since organizations achieve performance through repetitive and standardized routines, dynamic capabilities are processes that can achieve resource configuration to meet market change. Through this, organizations are able to create, extend, or modify their resource base and affect the quality of the ordinary capabilities, which influence the performance of the firm (Eisenhardt & Martin, 2000). This perspective consists of strategic and organizational processes such as alliancing, product development, and strategic decisions that create value for firms.

In addition, Winter (2003) presents a different categorization of organizational capabilities in relation to the concept of organizations' routines. Winter defines capabilities as behavior that is learned, highly patterned, repetitious, and founded in part on tacit knowledge (Winter, 2003, p. 991). While the capabilities in the zero level have an emphasis on activities of firms that allow earning a living in the short term, the first-order capabilities focus on the domain of scale and markets (e.g., new product development and performance). This includes creation, modification, and combination of lower-level operational capabilities (Winter, 2003). The higher-order capabilities depend on the investments and strategic competition, which facilitate the first-order capabilities. Winter points out that these higher-order capabilities are embedded in the less visible part of the processes and

support decision-making in organizations relating to investment and resource allocation.

The work of Zollo and Winter (2002) further connects the dynamic capabilities with the creation and utilization of knowledge. They state that dynamic capabilities derive from three learning mechanisms, such as 1. experience accumulation, 2. knowledge articulation, and 3. knowledge codification (Zollo & Winter, 2002). They explain how these learning mechanisms can generate and sustain the development of dynamic capabilities. The work of Wang and Ahmed (2007) identifies three components of dynamic capabilities: 1. adaptive capability, identifying and capitalizing on emerging market opportunities, 2. absorptive capability, integrating and translating the learning and external information into the firm's embedded knowledge, 3. innovative capability, aligning strategic, innovative orientation with innovative behaviours and processes (Wang & Ahmed, 2007).

Table 5. Overview of Different Definitions & Components of Dynamic Capabilities

Scholars	Definition	Components
Teece et al. (1997)	an ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments (as a form of competitive advantage)	Update, Reconfigure, Recombine
Eisenhardt & Martin (2000)	a set of specific and identifiable strategic organizational routines whose nature varies with the degree of market dynamism	Creating, Integrating, Recombining, Releasing
Zollo & Winter (2002)	a learned and stable pattern of collective activities through which the organization generates and modifies its operating routines systematically to improve their efficiency	Experience accumulation, Knowledge articulation, Knowledge codification processes
Teece (2007)	an ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments	Sensing, Seizing, Transforming
Helfat et al. (2007)	the capability of an organization to purposefully create, extend, or modify its resource base	Deployment of resources in a firm, Search, Selection, and Creation of resources
Wang & Ahmed (2007)	a firm's capacity to deploy resources, usually in combination, and encapsulate both explicit processes and those tacit elements (such as know-how and leadership) embedded in the processes	Adaptive capabilities Absorptive capabilities Innovative capabilities

Easterby-Smith, Lyles & Peteraf (2009)	higher-level capabilities which provide opportunities for knowledge gathering and sharing, continual updating of the operational processes, interaction with the environment, and decision-making evaluations	Variety of forms and involve different functions: learning processes, balancing exploration and exploitation processes, a knowledge management infrastructure
Pandza & Thorpe (2009)	an organizational process accountable for the creation of novel knowledge that significantly deviates from a firm's existing knowledge trajectories	creative search, Initial sense-making, strategic sense-making
Teece (2014)	an ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environment (e.g., to drive strategy alignment and enterprise performance)	Sensing, Seizing, Transforming
Teece (2016)	an ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environment (e.g. to manage uncertainties in the environment and rapid innovation)	Sensing, Seizing, Transforming
Teece, Peteraf & Leih (2016)	A firm´s capacity to innovate, adapt to change, and create change that is favorable to customers and unfavorable to competitors	Identification, development, co-development, and assessment of technological opportunities, Mobilization of resources to address needs & opportunities, Continued renewal
Teece (2018)	an ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environment (e.g., with routines and organizational processes)	Sensing, Seizing, Transforming

The internal learning mechanisms from Zollo and Winter (2002) and the second type of component of absorptive capability from Wang & Ahmed (2007) extend the discussion on dynamic capabilities and connect to how organizations develop routines that support adaptation and learning-based capabilities. This relates to the concept of *absorptive capacity*, originating from the work of Cohen and Levinthal (1990). The absorptive capacity enables the firm to recognize, assimilate, and apply external knowledge into its existing routines, thereby supporting the development and renewal of dynamic capabilities (Cohen & Levinthal, 1990; Zahra & George, 2002). It is argued that the higher a firm demonstrates its absorptive capability, the more dynamic capabilities it exhibits (Cohen & Levinthal, 1990; Wang & Ahmed,

2007). For this research, we do not focus on the absorptive capacity and suggest this as further research.

Furthermore, the work Easterby-Smith, Lyles & Peteraf (2009) states that dynamic capabilities can be created when top management provides a vision for processes. With various forms and functions, the higher-level capabilities provide other operational processes, interactions, and decision-making evaluations (Easterby-Smith et al., 2009). The work of Pandza and Thorpe (2009) argues that experimental learning is insufficient to explain the existence of dynamic capabilities. There are two cognitive processes introduced, such as creative search and strategic sense-making (Pandza & Thorpe, 2009). The process leading to a creative search and strategic sense-making involves knowledge discontinuities. By encouraging discontinuity from past paths, dynamic capabilities create new knowledge trajectories (Pandza & Thorpe, 2009).

4.3.3 Limitations of Dynamic Capabilities Theory

Despite the wide range of conceptualizations of organizational capabilities and dynamic capabilities, there are some limitations to consider. First, the concept of dynamic capabilities does not have a clear unifying definition, and confusion exists at the theoretical level (Collis & Anand, 2021; Easterby-Smith et al., 2009). Although much of the research on capabilities can be divided into two approaches, either as the ability-based approach (Teece, 2007, 2014; Teece et al., 2016) or the routine-based approach (Eisenhardt & Martin, 2000; Winter, 2003; Zollo & Winter, 2002), there is a lack of agreement in the definitions and components regarding the term. This provides an opportunity to consider diverse definitions and further extend the term in the context of the study.

In addition, there seems to be a lack of empirical evidence that supports the conceptualization of dynamic capabilities over time (Easterby-Smith et al., 2009; Helfat & Peteraf, 2015). Following the work of Teece et al (1997) and Eisenhardt and Martin (2000), the majority of the past literature examines the antecedents and characteristics of organizational capabilities, which largely discuss what constitutes dynamic capabilities in a particular situation (Eisenhardt & Martin, 2000; Teece, 2007, 2014; Teece et al., 2016; Zollo & Winter, 2002). Thus, how organizations evolve and ensure long-term growth may require a closer look at what capabilities are needed over time in the rapidly changing environment (Eisenhardt & Martin, 2000; Winter, 2003; Zollo & Winter, 2002).

Moreover, there is no generic list of dynamic capabilities that can be applied to all types of activities and settings. There is no set of established capabilities that

provide guidelines for practitioners to develop capabilities and reconfigure resources in the context of this research. This results in unclear practical implications for capabilities that organizations may need when implementing and adopting emerging technology. The dynamic capabilities may depend on their intended purposes and the actions that need to be executed. With different units of analysis (e.g., individuals, teams, organizations, etc.) and processes (coordination, learning reconfiguration, etc.), dynamic capabilities need to consider a diverse view and be specified (Arend & Bromiley, 2009; Easterby-Smith et al., 2009; Eisenhardt & Martin, 2000; Helfat et al., 2007; Teece, 2007).

4.4 Chapter Conclusion

The chapter introduces the theoretical background of the Stages of Growth Model and Dynamic Capabilities. In the field of information Systems (IS), the stages of growth models have been used to provide a structured overview of organizations. By conceptualizing their evolution over time, the stages of growth models are useful in managing information systems and assisting decision makers in practice. There are several benefits in using the stages of growth model. First, the growth model provides a high-level overview that organizations can use to develop strategies. Second, the growth model allows organizations to assess their current stage of information systems. By identifying the stage they are in, organizations can understand the need at each stage and allocate resources. Third, the growth model acts as a communication tool to share knowledge and highlights areas for continuous improvement.

However, there is no predefined method available for identifying different stages of the growth model. Since a growth model is context-specific and tailored to fit its objective, previous research on the growth model does not provide a systematic way to derive different stages of growth models. Likewise, the concept of *discontinuity* used to distinguish different stages is largely overlooked and not explicitly addressed in existing growth model. This research addresses this gap by introducing a stage-based growth model for supporting organizations in their QS transition. By using Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC), this research presents a novel approach in identifying different stages of growth model and the list of discontinuities that is grounded in QS transition challenges.

Moreover, Dynamic Capabilities are used in this research. While ordinary capabilities focus on doing things right and enabling organizational performance, dynamic capabilities focus on doing the right things and finding opportunities that

enable ordinary capabilities to perform in an uncertain and constantly changing environment. In the context of QS transition, there is no set of established capabilities that can provide guidelines for practitioners to develop their ordinary capabilities and reconfigure resources. This research further examines actionable guidance needed at each stage of the growth model, which may enable organizations to achieve long-term growth towards quantum safety. In doing so, this research identifies the capabilities through actions needed in organizations and uses the term QS transition capabilities to highlight dynamic capabilities. The list of QS transition capabilities is further categorized into sensing, seizing, and transforming based on Teece (2016).

Chapter 5 Public Key Infrastructures in the Netherlands

5.1 Introduction

This chapter provides an empirical investigation of Public Key Infrastructures (PKIs) in the Netherlands in the context of the QS transition. Section 5.2 introduces the PKI systems in the Dutch public sector and focuses on the Dutch governmental PKI known as PKIoverheid. Section 5.3 gives an overview of a long list of QS transition challenges found in the literature. After discussing the challenges in practice for QS transition in section 5.4, a refined list of QS transition challenges that answers sub-question 1 is presented. The chapter concludes with Section 5.5, providing concluding remarks on the list of QS transition challenges drawn from both literature and practice.

Parts of this chapter are based on the following publications:
Kong, I., Janssen, M., & Bharosa, N. (2024). Navigating through the Unknowns-Readiness Assessment Model for Quantum-safe Transition. Electronic Government: 23rd IFIP WG 8.5 International Conference, EGOV 2024, Ghent-Leuven, Belgium, September 3–5, 2024, Proceedings. p. 438 – 453. https://dx.doi.org/10.1007/978-3-031-70274-7_27

Kong, I., Janssen, M., & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly.* 41(1), 101884. https ://doi.org/10.1016/j.giq.2023.101884

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). https://doi.org/10.1145/3543434.3543644

5.2 PKI systems in the Netherlands

This section introduces PKI systems in the Netherlands and presents QS transition challenges in the literature and practice. Section 5.2.1 provides background information on PKI systems in the Dutch public sector. Section 5.2.2 presents stakeholders in the PKI systems using an example of PKIoverheid.

5.2.1 PKI systems in the Dutch Public Sector

Critical information infrastructure plays a crucial role in facilitating digital transactions and communication. Notably, Public Key Infrastructure (PKI) ensures the security of these services and also supports platforms of other critical infrastructure, including, but not limited to, banking, telecommunication, or national government. By managing the identities of users and the encryption of information in the digital environment, the security framework of PKI secures information across applications and connected devices of individuals, businesses, and government agencies. As governments increasingly use Information Communication Technologies (ICT) and networks to provide accessible governmental information and efficient public services, PKIs have become an essential part of the public sector.

Although it is not always obvious to users and policymakers, PKIs facilitate electronic identification schemes and secure communication and information exchange by enabling user authentication, message integrity, and message non-repudiation services (Innovalor, 2019; Kong et al., 2022). Examples range from sharing information on public policy, regulations, government documents, and forms to maintaining services, filing taxes, applying for permits, studying loans, and receiving social benefits, using PKIs (Coursey & Norris, 2008; Jansen & Ølnes, 2016; Lindgren & Jansson, 2013). In the Netherlands, the main governmental PKI, known as PKIoverheid, provides strong credentials for information sharing using PKIoverheid certificates (Innovalor, 2019; Logius, 2024a, 2025a). Figure 12 illustrates secure information sharing in government using an example of PKIoverheid.

Additionally, PKIoverheid is crucial for the proper functioning of other infrastructures that ensure maintenance, reliability, and safety in government communication and service delivery processes. The certification of PKIoverheid supports various functions, from the authentication of users and organizations and signing documents using digital signatures to setting up digital tunnels for secure message exchange. Logius acts as Policy Authority (PA) and manages service providers that issue and revoke digital certificates for PKIoverheid (Innovalor, 2019; Logius, 2024b, 2025a). With the government as a frontrunner in managing and

regulating the facilitation of a national and cross-sectoral PKI system, there is a high dependency on PKIoverheid, which, like other PKIs, has a high vulnerability to quantum threats.

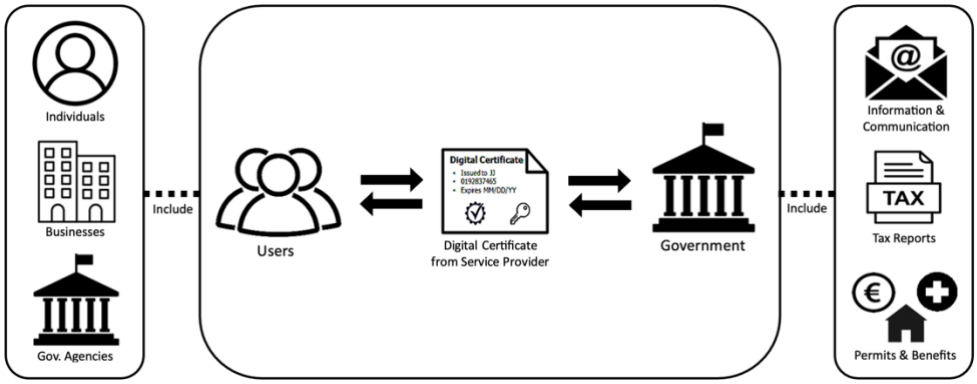


Figure 12. Secure Information Sharing Using Public Key Infrastructure
Note. Adapted from "Realizing Quantum-safe Information Sharing" by Kong, Janssen & Bharosa (2024, p.5).

5.2.2 Stakeholders in PKI systems in the Dutch Government

Although there are different definitions of stakeholders, we will use the most widely known definition of stakeholders as proposed by Freeman (2023) in this proposal. The term stakeholders is defined as "any group or individual who can affect or is affected by the achievement of the organization's objectives" (Freeman, 2023, p. 62). Stakeholders have a particular interest or degree of influence on the operations' achievements. The effective participation of diverse stakeholders is an integral part of IS development (Cavaye, 1995; Hirschheim et al., 1991). While actors who have stakes can become stakeholders, stakeholders are not always actors in the system.

In PKI systems, stakeholders include users (individuals, businesses, and government agencies), external expertise (e.g., QTSPs, hardware vendors, and software providers), governing bodies (e.g., Logius, AT, and Ministry of Interior and Kingdom Relations), and standardization bodies (e.g., NIST, ETSI). With multiple stakeholders in the PKI, the process of identity authentication, authorization, and digital certification is maintained to ensure secure communication and information exchange. The overview of stakeholders in the PKI system in the context of PKIoverheid is illustrated in Figure 13. This figure has been compiled from various sources, including policy documents, reports, and research papers on

PKIoverheid. Thus, it is a high-abstraction version and is intended to show the socio-technical complexity of PKI systems.

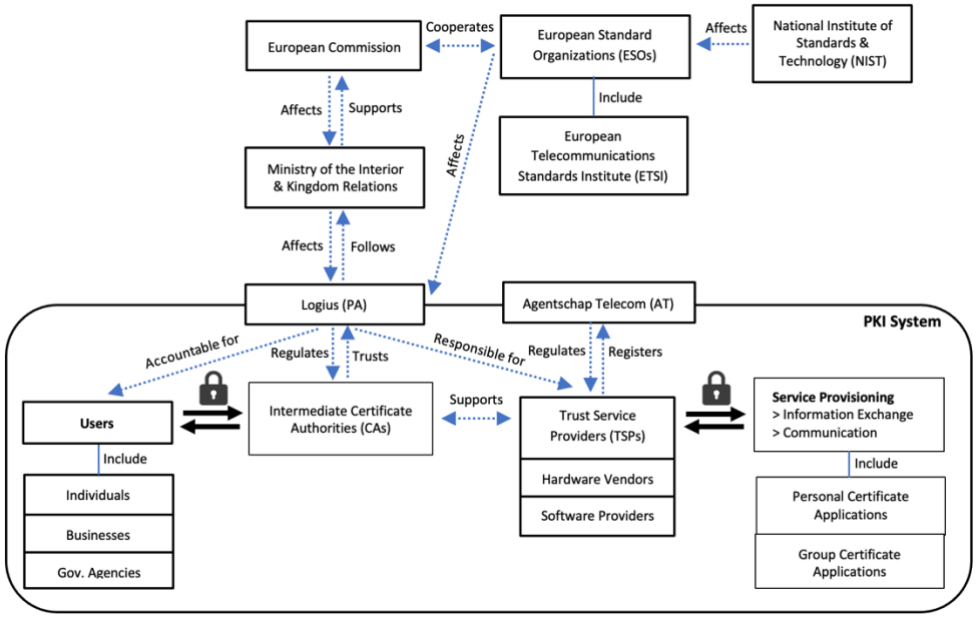


Figure 13. Overview of Stakeholders Involved in PKIoverheid
Note. Adapted from "PhD Proposal" by Kong (2022, p.11).

Governing Bodies

Ministry of Central Government

There are governing policies and regulations that manage the relationship between organizations and their users in PKI. In the context of PKI for the Dutch government, the decisions on strategy and funding lie with the ministry in charge of government-wide ICT solutions, e.g., Ministry of Interior and Kingdom Relations. While EU Directives may require national governments to translate these directives within a set deadline into national laws that organizations must follow, EU regulations such as GDPR and eIDAS are directly applicable to organizations in all EU Member states. Without national transposition, organizations must comply with these regulations, which are proposed by the European Commission and adopted by the European Parliament and the European Council.

Logius

The government organizations have a shared responsibility in the PKI system for the government, e.g., PKIoverheid (Logius, 2025b). While ultimate decisions regarding

the PKI system are made by the Ministry of the Interior and Kingdom Relations (BZK), management of the PKI system lies with Logius as a Policy Authority (PA) (Innovalor, 2019; Logius, 2024b, 2025a). The PA is a unique feature of the national PKI system in the Dutch government. As a PA, Logius defines and maintains the overall governance framework for the PKIoverheid (Bharosa et al., 2015). Logius is also responsible for many shared digital infrastructure services for public administration, such as authentication (DigiD) and data-exchange gateways (Digipoort) (Logius, 2025b).

In the context of PKI for the Dutch government, Logius acts as a supervisory body of the PKI system responsible for managing the entire infrastructure and other external expertise (e.g., Qualified Trust Service Providers (QTSPs)) needed to facilitate the infrastructure. Logius oversees these admissions and monitors compliance with policy and audits (Logius, 2024). In addition, Logius also acts as a Certificate Authority (CA) for the root and intermediate levels of PKIoverheid. These mean that they hold the root CA keys, issues, and manage the certificates (Logius, 2024b, 2025a). Logius plays a unique role as CA-root authority and policy authority. While Logius defines the certificate policy, issues root and intermediate certificates, Logius admits QTSPs for CAs, and supervises them.

Rijksinspectie Digitale Infrastructuur (RDI)

In the Netherlands, Rijksinspectie Digitale Infrastructuur (RDI), also known as the Dutch Authority for Digital Infrastructure, which was initially known as Agentschap Telecom (AT), collaborates with Logius to supervise the QTSPs. As a supervisory authority for digital infrastructure, they are one of the administrative law supervisors. The QTSPs must be registered with AT before they can become an issuer of qualified certificates. Such registration is a legal requirement of eIDAS and applies to all certificates. AT and Logius inform each other and discuss protocol and cooperation related to QTSP, assist upon request and when necessary, provide advice and consultation regarding PKIoverheid (Logius, 2024b, 2025a).

Businesses that operate their own private PKI

For business organizations that use private PKIs to manage their PKI solutions for issuing and managing privately trusted certificates. This form of PKI differs from the example of PKIoverheid shown in Figure 4. The organizations with private root PKI prefer to have all operational aspects of their Private CA, including hosting, maintenance, security, and compliance, secure internal web servers, user access, connected devices, and applications. For example, these organizations in the

financial & telecommunications industries include KPN, T-Mobile, ING, ABN Amro, etc.

Standardization Bodies

National Institute of Standards and Technology (NIST)

A non-regulatory government agency based in the U.S develops technology, metrics, and standards to drive innovation and economic competitiveness. NIST produces standards and guidelines to help federal agencies meet the requirements of the Federal Information Security Management Act. Also, NIST assists those agencies in protecting their information and information systems through cost-effective programs.

European Telecommunications Standards Institute (ETSI)

As a part of the European Standard Organizations (ESO), ETSI is a non-profit enterprise based in Europe whose mission is to produce telecommunications standards throughout Europe. Standards developed by ETSI are adopted by the European Commission as the technical base for directives or regulations.

External Expertise

Qualified Trust Service Providers (QTSPs)

To manage the certification process for millions of applications and connected devices, organizations increasingly rely on Qualified Trust Service Providers (QTSPs) for their services. Under the eIDAS regulations, CAs can become a QTSP providing services such as monitoring and other technical management services, such as key generation and physical identity verification processes (European Commission, 2024b; European Union, 2014). The QTSPs need to follow the ETSI standards framework, and they have to comply with the requirements as stated in eIDAS . The services include In the Netherlands, the list of QTSPs includes Cleverbase, KPN, Digidentity, QuoVadis, etc. (European Parliament and Council of the European Union, 2022). These companies may or may not have their own *hardware vendors* or *software providers*. It would vary depending on their expertise, capital, and human resources available in the organization.

PKI Users

Individuals, Businesses & Government Agencies

The users include individuals (e.g., professionals, non-professionals), businesses (e.g., banks, SMEs), and government agencies (e.g., Tax and Customs

Administration, Chamber of Commerce, Central Statistical Office, other ministries, provincial governments, municipalities etc.) that need access to services that require information exchange and internal & external communication: portals, personalized services from government institutions, services to businesses.

5.3 QS Transition Challenges in Literature

This section discusses QS transition challenges for PKIs found in the Literature. Section 5.3.1 gives an overview of transition challenges in the technological category. Section 5.3.2 gives an overview of transition challenges in the organizational context, and Section 5.3.3 gives an overview of challenges in the environmental context.

The findings and discussion presented in this section draw upon and are adapted from the previous work, 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). https://doi.org/10.1145/3543434.3543644.

To cluster the transition challenges found in the literature on QS transition, the TOE framework was adopted. This is because the TOE framework provides a multi-perspective view that focuses on technology implementation at an organizational level rather than an individual level. Moreover, the inclusion of factors in technological, organizational, and environmental contexts brings 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.

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

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

Environmental Category: 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.

5.3.1 Technology

Technological Category: The list of transition challenges towards a QS PKI system from the literature is shown in Table 6.

Incompatible Legacy System

Two main approaches to achieving QS cryptography are available: Post-quantum cryptography (PQC) and Quantum Key Distribution (QKD). In order to ensure the same level of protection in the legacy systems, however, more research is needed. 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. While PQC may not need new infrastructure, QKD requires quantum infrastructure. With the latter approach, practical compatibility with legacy systems remains a bigger concern.

Not-yet-achieved NIST Standards

The standardization can bolster the use of cryptography and maximize interoperability. 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 (e.g., PQC). 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.

No Universal QS Algorithm

There is relatively little chance that a single QS cryptographic algorithm will be selected as a replacement. 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. Thus, NIST is looking to provide several alternatives (e.g., 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.

Implementation Flaws & Side-Channel Attacks

The changes in the PKI system can lead to implementation flaws and side-channel attacks. These include fault injection attacks, side-channel cryptanalysis, and physical cryptanalysis. 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. 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, but it would also take years for new algorithms to be able to substitute existing algorithms. There is currently no real-world use of QS cryptography, and it has yet to stand the test of time to prove its reliability and robustness. Thus, new cryptography may still result in vulnerabilities. Even if the standardization is complete, the newly introduced algorithms will need to be fully deployed into security systems and be accepted in organizations.

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. 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. 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.

Complex PKI system & Interoperability

QS cryptographic algorithm cannot be replaced with a simple 'drop-in' method. 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. To enable secure and correct communication, changes in cryptographic algorithms must be the same or compatible. The devices need to be upgraded accordingly. Otherwise, they cannot guarantee the security of newly adopted cryptography.

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. 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. Moreover, in the absence of established QS alternatives, the solution may be to deploy hybrid solutions, and using hybrid certificate schemes could double the cost on the server infrastructure, as it requires management of two systems and two certificates or more.

Table 6. Challenges in the Technological Context

Challenges	References
Incompatible Legacy System	(AccentureLabs, 2018), (CCC, 2019), (Galbraith et al., 2021), (ISARA, 2018), (Lindsay, 2020b), (Mashatan & Heintzman, 2021), (The Hague Security Delta, 2019), (Vermeer & Peet, 2020), (Wiesmaier et al., 2021)
Not-yet achieved standards from NIST	(AccentureLabs, 2018), (Barker et al., 2021b), (CCC, 2019), (ENISA, 2021), (Menezes & Stebila, 2021), (Niederhagen & Waidner, 2017), (Menezes & Stebila, 2021)
No universal QS algorithm	(Barker et al., 2021b), (CCC, 2019), (L. Chen et al., 2016), (L. Chen & Moody, 2020), (ENISA, 2021), (Vermeer & Peet, 2020)
Implementation flaws & side-channel attacks	(Macaulay, & Henderson, 2019), (Menezes & Stebila, 2021), (Niederhagen & Waidner, 2017), (Wiesmaier et al., 2021)
Lack of reliability in QS cryptography	(CCC, 2019), (ETSI, 2015), (ISARA, 2018), (Macaulay, & Henderson, 2019), (Tibbetts, 2019), (Vermeer & Peet, 2020)
Vulnerable Root CA	(ETSI, 2020), (ISARA, 2018), (Macaulay, & Henderson, 2019), (Menezes & Stebila, 2021), (Sjöberg, 2017), (Thales, 2019)
Complex PKI system & interoperability	(AccentureLabs, 2018), (Barker et al., 2021b), (CCC, 2019), (ENISA, 2021), (Galbraith et al., 2021), (Grote et al., 2019), (ISARA, 2018), (Macaulay, & Henderson, 2019), (Vermeer & Peet, 2020)
Cost of Transition	(ETSI, 2015), (ISARA, 2018), (Ma et al., 2021), (Leech et al., 2018), (Petrenko et al., 2019), (Thales, 2019), (TNO, 2020), (Vermeer & Peet, 2020)

Note. Adapted from "Challenges in the Transition toward a Quantum-safe Government," by Kong, Janssen & Bharosa (2022, p.286).

5.3.2 Organization

Organizational Category: The list of transition challenges towards a QS PKI system from the literature is shown in Table 7.

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. 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 *SNDL*. In addition, there is uncertainty in organizations to fully commit to the selection of QS cryptographic algorithms when standards are still being developed. Without a collective sense of urgency, it is difficult to achieve inter-agency coordination and collaboration for a QS PKI system.

Knowledge Gaps in Quantum Computing

Poorly understood quantum computing may delay organizations from transitioning to a QS PKI system. 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. When organizations do not have prior knowledge, they risk not taking timely action and resulting in fragmented solutions with unforeseen vulnerabilities.

No One-Size-Fits-All Transition Process

The cryptographic assets and areas that will potentially be vulnerable to quantum computers need to be identified. The time and strategy needed to transit from the current PKI system would vary across organizations. 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. Also, different QS cryptographic algorithms will have different trade-offs in the performance outcomes. 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.

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. 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. It is essential to build crypto-agility so that a system becomes more flexible and scalable. Lack of crypto-agility hinders organizations from responding and updating their systems 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. 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. 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.

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. Due to a limited use case of the QS cryptographic algorithm, organizations find it challenging to develop a business case to enter a long-term QS transition commitment. The activities related to QS transition may remain in the areas of R&D programs, and their practical application will still be delayed.

No Technical Skills & Qualified Personnel

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. 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 multinational corporations. If organizations do not 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, as these will need to be translated into a real-world environment outside the research labs. However, there is no inventory in organizations to facilitate updates in infrastructure and related protocols to QS solutions. Organizations often do not know their entire cryptographic assets and vulnerabilities. Thus, it is difficult to assess where and with what priority the QS alternatives should be implemented. This calls for a high degree of decision-making, coordination, and leadership efforts.

Table 7. Challenges in the Organizational Context

Challenges	References
Lack of Urgency	(ETSI, 2015), (Lindsay, 2020b), (Lovic, 2020), (TNO, 2020), (Vermeer & Peet, 2020)
Knowledge Gaps in quantum computing	(CCC, 2019), (Ma et al., 2021), (Macaulay, & Henderson, 2019),(Mulholland et al., 2017), (Niederhagen & Waidner, 2017), (TNO, 2020), (Vermaas, 2017)
No one-size-fits-all transition process	(Barker et al., 2021b), (CCC, 2019), (L. Chen et al., 2016), (ENISA, 2021), (ETSI, 2017), (ETSI, 2020), (Galbraith et al., 2021), (Ma et al., 2021), (TNO, 2020)
Lack of Crypto-Agility	(Barker et al., 2021b), (ETSI, 2015), (ETSI, 2020), (Grote et al., 2019), (Ma et al., 2021), (Macaulay, & Henderson, 2019), (Mehrez & El Omri, 2018), (Wiesmaier et al., 2021)
Lack of In-house management support	(Buchholz et al., 2020),(CCC, 2019), (Leech et al., 2018), (Mosca, 2015), (The Hague Security Delta, 2019)
Unclear QS transition benefits & business case	(Galbraith et al., 2021), (Ménard et al., 2020), (Mosca, 2015), (The Hague Security Delta, 2019), (Vermeer & Peet, 2020)
No technical skills & qualified personnel	(Galbraith et al., 2021), (Leech et al., 2018), (Peterssen, 2020), (TNO, 2020)
Unclear QS governance	(Barker et al., 2021b), (Galbraith et al., 2021), (Mashatan & Heintzman, 2021), (Mulholland et al., 2017), (Niederhagen & Waidner, 2017), (The Hague Security Delta, 2019), (Wiesmaier et al., 2021)

Note. Adapted from "Challenges in the Transition toward a Quantum-safe Government," by Kong, Janssen & Bharosa (2022, p.287).

5.3.3 Environment

Environmental Category: The list of transition challenges towards a QS PKI system from the literature is shown in Table 8.

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. 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. The EU-based companies are not patenting enough and are lagging behind the global trend in capital investments in quantum technology. 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.

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. In public, the risks surrounding quantum computing are largely ignored and mostly focused on its unique opportunities for scaling industry advantages. 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.

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. Under a complex system integration, any alterations in technological infrastructure would require actors to negotiate and coordinate problems. 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 their boundaries blur the extent to which organizations should initiate and take responsibility for facilitating the QS transition from the current PKI system.

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. The current framing of quantum theory is yet to be presented with a straightforward meaning and interpretation. 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 QS create too much noise when trying to find fit-for-purpose QS architectures necessary for organizations.

Lack of Policy Guidance

The topic of quantum computing is not yet among the popular topics of discussion in the European Parliament. The low awareness and magnitude of risks require an updated framework to account for quantum-computer-based threats and proactive policymaker leadership. The right incentives through procurement policy or early adoption programs can help stimulate business cases, encourage QS transition and user engagement. 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.

Need for Collaboration: Various Stakeholders

Designing a cryptographic algorithm is complex and requires knowledge in multiple sciences and engineering fields in applied cryptography and system security. Moreover, transitioning to a QS PKI system requires collaboration on many levels. There are varying interests and needs in government standards bodies, software solution providers, hardware vendors, service providers, international consortia, and PKI users. Thus, collaboration among various stakeholders is needed to establish well-coordinated contingency planning in the QS transition.

Legal Issues

The facilitation of the PKI system requires several legal issues, including privacy legislation, regulations on qualified digital signatures, and the NIS directive that ensures the security of network and information systems. The entities that process private data or offer qualified signatures are required by law to protect against state-of-the-art attacks. 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. Thus, legal issues need to be updated and comply with a QS PKI system and its new QS cryptographic algorithms.

Bureaucratic Process

In the EU, governments play a greater role in the elaboration of PKI standards and regulations when compared to the U.S. 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. The bureaucratic process in adopting QS standards and their regulations adds an extra timeline to the transition. Any uncertainty in QS solutions would raise additional regulatory problems and delay the process.

Table 8. Challenges in the Environmental Context

Challenges	References
Low level of Investment in EU	(CCC, 2019), (Ménard et al., 2020), (Lewis et al., 2018), (Lewis & Travagnin, 2018), (Räsänen et al., 2021)
Lack of awareness	(ETSI, 2015), (Lovic, 2020), (Macaulay, & Henderson, 2019), (Mulholland et al., 2017), (TNO, 2020), (Vermeer & Peet, 2020)
No clear ownership & operating institution	(Barker et al., 2021b), (Lindsay, 2020a), (Lindsay, 2020b), (Ma et al., 2021), (Mulholland et al., 2017)
Different interpretation of QS scenarios	(Barker et al., 2021b), (ENISA, 2021), (ETSI, 2017), (Smith, 2020), (Vermaas, 2017)
Lack of policy guidance	(TheHagueSecurityDelta, 2019), (Lovic, 2020), (Tibbetts, 2019), (Lewis & Travagnin, 2018), (Lewis et al., 2018), (Lindsay, 2020a), (Lewis, 2017)
Need for various stakeholders	(CCC, 2019), (L. Chen & Moody, 2020), (Mulholland et al., 2017), (Räsänen et al., 2021), (The Hague Security Delta, 2019), (Vermeer & Peet, 2020)
Legal Issues	(ETSI, 2017), (Lewis, 2017), (Ma et al., 2021), (Niederhagen & Waidner, 2017)
Bureaucratic process	(Lewis & Travagnin, 2018), (Lindsay, 2020a), (Macaulay, & Henderson, 2019)

Note. Adapted from "Challenges in the Transition toward a Quantum-safe Government," by Kong, Janssen & Bharosa (2022, p.288).

5.4 QS Transition Challenges in Practice

This section provides an overview of QS transition challenges for PKIs in practice, as discussed with experts in the context of PKI. To refine the list of QS transition challenges previously identified in the literature, semi-structured interviews were conducted with experts from government and industry to narrow the focus to the case of PKI systems in the Dutch public sector. The details of the interviewees can be found in Table 1 in Chapter 3. Section 5.4.1 discusses the four main QS transition challenges in practice, which are 1) complex PKI interdependencies, 2) lack of urgency, 3) lack of certified hardware and software, and 4) unclear QS direction and governance. The refined list of challenges can be found in Table 10.

The findings and discussion presented in this section draw upon and are adapted from the previous work, Kong, I., Janssen, M & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. Government Information Quarterly. 41, 1, 101884. https ://doi.org/10.1016/j.giq.2023.101884.

5.4.1 QS Transition Challenges in Practice

Complex PKI interdependencies

The issued digital signatures and certificates from PKIs are checked and validated by software implemented by market parties. The external experts providing products and services for PKIs also monitor communities of all the browser companies to discuss changes in PKIs (Respondent 1). The services they deliver need to be accepted by these parties and various standard bodies such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), European Telecommunication Standards Institute (ETSI), and NIST (Respondent 6). While external experts provide software to govern and manage certificates (abiding by European laws), the facilitation of PKIs must consider the whole certificate chain, which involves the Root CA and all the intermediate CAs (Respondent 6). If the encryption level of the Root changes, all underlying certificates in the same stack would need to be revoked and reissued since they do not automatically inherit the new specification (Respondent 5). One of the external experts stated that,

> "If PKI systems use different encryption levels like classical cryptographic algorithms and PQC, the Root CA, intermediate CAs, user certificates, and a whole ecosystem behind may be affected, causing complex integration issues." (Respondent 12)

Due to the interdependencies in PKIs, organizations with outdated encryption levels and those with new encryption levels may not be interoperable. Since PKIs allow different organizations and entities to communicate securely, maintaining technical interoperability allows users to share information and use digital transactions over networks. The linkages facilitating PKI systems create inherently complex interoperability challenges (Respondent 8). Any changes in the current PKI systems for QS transition also need to consider the technical interdependencies that PKIs inherently have.

Moreover, PKI systems are heavily regulated (e.g., eIDAS regulations) and must comply with international standards (e.g., NIST, ETSI, X.509 standards, etc.).

Since PKI in the Netherlands is ruled by laws and regulations, changes in the technical foundation of digital certificates cannot occur in isolation.

> "Organizations are not completely free to choose what they want and change the PKI systems." (Respondent 8)

Parties that provide PKI-related products and services for the Dutch government must follow international standards and EU regulations and meet the Programme of Requirement (PoR) to be recognized as service providers in the Netherlands (Respondent 9). The activities of these service providers are monitored, and audit communities also check the quality of PKI-related products and services (Respondent 9). Since new standards and regulations for QS solutions are not yet available for QS transitions, organizations find it challenging to modify the current PKI systems that are already compliant with existing standards and regulations.

Lack of Urgency

Although the topic of QS transition has emerged in the public domain, the respondents indicated that the level of urgency remains low. While regulatory organizations indicated a growing awareness, PKI users, such as government agencies and banks, do not have the same level of urgency (Respondent 1). One of the respondents pointed out that,

> "We expect only to come in 10 or 15 years. And that's far away. So, the time horizon of an average bank for calculating security issues is about three years." (Respondent 2)

In the case of quantum threats, the respondent states that it is unlikely for such threats to occur tomorrow. The risk appetite was different for PKI users. Some think that a time horizon of 10–15 years can be considered not urgent, but there is disagreement about the time horizon. Likewise, government agencies using PKI systems did not see the urgency in their organizations. In their views, the high urgency would only mean that PKI systems would no longer work tomorrow (Respondent 7).

Moreover, there is a lack of understanding of what a QS transition means for organizations. While it may be impossible for organizations to opt for QS transition decisions to be single-handled by one organization, respondents stated that knowledge of quantum threats and PKIs is mainly missing in non-experts, and organizations are not aware of the technical complexity that PKIs inherently have.

"If you don't understand, there will be no urgency
because you don't understand the threat, what it does, or what impact it has.
First, you need to understand." (Respondent 4)

The respondent from the regulatory organization also indicated that the QS transition topic is difficult for policymakers to grasp. Even though the facilitation of PKIs is essential in securing businesses and public services in society, the level of fuzziness in quantum threats does not provide a clear view for policymakers to recognize the risks associated with PKIs (Respondent 9). The respondent added that it does not help when experts disagree because it would only make regulatory organizations not proceed with QS transition, simply because experts do not agree. Nothing has yet been decided for QS transition (Respondent 9).

In addition, the urgency among different organizations is considered a challenge when the level of urgency varies in the PKI systems. While the level of urgency remains low in the PKI ecosystem, many organizations have varying levels of risk appetite and do not see the consequences of not transitioning to QS (Respondent 12). While there is a lack of understanding and knowledge on the topics of QS transition, the respondents also stated that the level of urgency might also differ for small government agencies and SMEs since they do not have enough resources to recognize quantum threats and the need for QS transition (Respondent 5).

Lack of Certified Hardware and Software

Suppose there are new updates in hardware and software. In that case, PKI service providers and PKI users in critical information infrastructures need to adopt new solutions to maintain interoperability and backward compatibility. In the case of QS transition, a hybrid structure that works with both classical cryptographic algorithms and QS solutions (e.g., PQC) is under discussion.

"We could also look for a hybrid approach where we deliver
both the old and new format or come up with a mixed format." (Respondent 6)

Having a hybrid structure would also mean that certified hardware and software may need to recognize two different encryption levels in the X.509 scheme (Respondent 5). Since the current PKI systems only recognize classical cryptographic algorithms, there is a need for hardware and software that can replace the existing systems. The

current PKI systems for regulatory organizations require an HSM (Hardware Security Module) and a hybrid data model to issue certificates recognizing two different encryption levels, including classical cryptographic algorithms and QS solutions (Respondent 1).

"For us, it's quite simple. We just need two things. We need to have like an HSM, We need to have a hybrid data model to create these new keys." (Respondent 1)

While the respondent emphasized that QS transitions for regulatory organizations are relatively easy, it may be difficult for PKI users such as banks, the tax office and other government agencies to change their systems (Respondent 1). This is because no currently certified hardware and/or software can run QS solutions yet. The respondents from external experts agreed that the development of certified products that implement QS solutions has not yet happened, and this would be a big challenge for organizations that need to change their systems.

"QS transition is often compared to the transition from SHA-1 to SHA-2, but the difference would be that QS transition does not have hardware and software ready." (Respondent 6)

"For the transition, we are very dependent on our suppliers. We cannot transition without them." (Respondent 11)

Moreover, another respondent from PKI users also indicated a lack of technical expertise and qualified personnel with the knowledge and experience to work with the hardware and software for QS transition (Respondent 7). Getting to certified products that support QS solutions, there may need to be some judgment that it is safe enough to rely on these new products in practice. This also requires a certification process that can be pretty intensive and time-consuming (Respondent 6). However, the standards for new QS solutions are not yet agreed upon. Commercial software providers also need to leverage those new specific algorithms to ensure that their software can generate certificates using the new QS encryption scheme. This is because service providers' existing commercial software only uses classical encryption levels. This would not support the post-quantum encryption level (Respondent 12). There is a lack of technical expertise and qualified personnel who understand how the process of a QS transition works (Respondent 5). For PKI users who need to sign their emails and contracts, users of notary services, and organizations that use custom software to perform specific types of work, new

certified hardware and software that can run QS algorithms are not yet available (Respondent 12).

Unclear QS Direction and Governance

The respondents stated that organizations currently do not have directions for QS transition. The respondents from the PKI users category stated that organizations are all monitoring the development of QS solutions (which have not yet been finalized) and remain conservative towards the QS transition because security issues in the current PKI systems have not yet occurred.

> "Organizations are keeping their eyes on the development. They do not have an actual QS transition strategy or other actions that they have planned." (Respondent 7)

Within organizations, modifying PKI systems is considered as "under the hood" _changes by the IT department, which often go unnoticed in user functionality (Respondent 7). Another respondent also emphasized that it would be more challenging for SMEs with insufficient resources to transition to QS PKI systems without recognizing the impact of quantum threats (Respondent 2). As long as the security remains status quo, no issues have emerged in the current PKI systems for organizations. Thus, without recognizing the impact of quantum threats in organizations, it is challenging to realize the scope of QS transition and organize what changes may be needed. The respondents also agreed that it might be easier for homogenous organizations, such as banks, to plan for a QS transition with the ECB as a regulator and DNB (Dutch National Bank) in the Netherlands. However, the respondent also emphasized that the direction for a QS transition is not yet available in the sector (Respondent 2).

For regulatory organizations, IT and government in the Netherlands are very decentralized, and every ministry has responsibility for certain executive agencies falling under that ministry (e.g., energy, water management, education, national security, etc.) (Respondent 9). Mobilizing the governance of PKI systems to proceed with a QS transition may take a lot of time and requires convincing non-technical people (Respondent 9). The respondents agreed that the changes in the current PKI systems may extend to other critical infrastructures. However, there is no clear path to where and what to do with which technology.

"It's very difficult on our operational level to organize change
because we are waiting for the instructions on what to do." (Respondent 3)

Although PKIs have evolved immensely over the past decades, previous experience has shown that modifications in the PKIs are complex. Without clear governance, it would be difficult for organizations to proceed with changes in the current PKI systems. For external experts, having organizational-level governance was not an issue. Since PKI-related changes are part of their core business, they stated that a governance structure is in place to address changes. However, they saw the most significant risk in cross-organization-level governance. Although Logius acts as a Policy Authority (PA) and manages the PKI system for the PKIoverheid certificates, the coordination and accountability for the QS transition remain unclear, and organizations were unsure of their roles and responsibilities. (Respondent 4).

"It is not yet clear enough who is doing what,
and the main risks are cross-organizational." (Respondent 6)

"Someone has to make costs to facilitate. Who is taking the burden?
What will it do to the whole ecosystem?" (Respondent 10)

Since the facilitation of PKI systems requires multiple actors to secure information sharing and digital transactions, cross-organizational governance is crucial for the QS transition. However, no specific document provides guidelines, and no national roadmap to move along the QS transitions.

"The organizations do not know
who is making the decisions for QS transition and who are collaborating,
who to include paying for the cost of transition." (Respondent 5)

The existing PKI governance indicates a set of roles, security policies, encryption mechanisms, and procedures with diverse actors. This is not suitable for a QS transition since it requires clear responsibilities to follow and priority setting given scarce resources. With varying levels of urgency, interest, and expectations for QS transition, organizations are waiting for each other, and it is unclear who should make the first moves (Respondent 8).

Table 9. Description of QS Transition Challenges in Practice

Main Challenges	Description of QS Transition Challenges
Complex PKI Interdependencies	-PKI systems are heavily regulated (e.g., eIDAS regulations) and must comply with international standards (e.g., NIST, ETSI, X.509 standards, etc.) -Various standard bodies need to be considered, such as IETF, WWW, W3C, ETSI, NIST -Changes in PKIs cannot occur in isolation & need to consider the whole certificate chain -Interoperability issues may arise between organizations with old encryption levels and organizations with new encryption levels -New standards and regulations for QS solutions are not yet available for QS transition
Lack of Urgency	-Quantum threats are viewed as unlikely to occur tomorrow -Level of urgency varies with different risk appetite -A lack of understanding of what QS transition means -No clear view for policymakers to recognize the risks associated with PKIs -Level of urgency remains low in the PKI ecosystem as a whole
Lack of Certified Hardware & Software	-Updates & new solutions need to consider interoperability & backward compatibility -Certified hardware and/or software may need to recognize two different encryption levels in the X.509 scheme -A lack of technical expertise and qualified personnel with knowledge and experience -Agreements are needed for new QS solutions before software providers generate certificates using new QS encryption scheme.
Unclear QS Direction & Governance	-Organizations currently do not have directions for QS transition -Changes in the current PKI systems may extend to other critical infrastructures -External experts saw the biggest risk in cross-organization governance -IT & government are very decentralized, unsure of the roles & responsibilities -Organizations are waiting for each other, and it is not clear who makes the first moves

Note. Adapted from "Realizing Quantum-safe Information Sharing," by Kong, Janssen & Bharosa (2024, p. 8).

Table 9 presents various challenges that organizations may encounter in the QS transition. The four main categories of QS transition challenges and description of these challenges show that institutional, organizational, and policy aspects of QS transition are interconnected, and many dependencies among actors exist within the ecosystem, and it would be crucial to recognize these when preparing for QS transition. After the interviews with experts, the list of QS transition challenges has been refined with relevant transition challenges in practice.

Table 10. Refined List of QS Transition Challenges

QS Transition Challenges	Code	Description
Legacy System Constraints	C1	The existing system is rigid and only supports a handful of algorithms. The existing system may need changes in the hardware and/ or software depending on the compatibility of new QS solutions.
No Availability of QS Standardization	C2	NIST is currently selecting practical standards and guidelines for QS solutions. Thus, standards for QS cryptographic algorithms are not yet available.
No QS Standards & Selection	C3	Organization has not yet selected which QS solutions will be used and whether to have a full substitution of QS solution or a hybrid solution. The selection criteria for QS solutions are not clear.
No Reliable & Secure QS Solutions	C4	The QS solutions have not been tested and currently, there is no testing is available to prove the security of QS solutions.
No Availability of Certified QS Hardware & Software	C5	The suppliers of the current technology are not yet ready to provide the certified technology compartments for the replacement technology. e.g. HSM and certificate issuance software for QS solutions.
Knowledge Needs within Organizations	C6	There is a lack of knowledge on quantum computing-based threats, and risks associated with the technology in organizational assets e.g. cryptographic assets, and vulnerabilities etc.
Lack of Urgency within Organizations	C7	The arrival of a large-scale quantum computer is perceived to be decades away, and there is a lack of urgency for QS transition in organizations.
No Business Case for Organizations	C8	Organization finds it difficult to enter long-term QS transition commitments without clear business benefits and opportunities.
Lack of Technical Skills & Qualified Personnel	C9	There is a lack of qualified personnel who can understand QS solutions and make decisions on the implementation process.
Unclear QS Governance within Organizations	C10	Organization does not have transition plans, and they do not know what to prioritize for QS transition.
Lack of Urgency in the Ecosystem	C11	There is a lack of collective sense of urgency, and it is difficult to achieve inter-agency coordination and collaborations with multiple stakeholders.
Unclear QS Governance in the Ecosystem	C12	Organization does not know which organizations are in the lead and who takes responsibility for what.
Lack of Collaboration in the Ecosystem	C13	The varying levels of interests, needs and expectations contribute to duplication of efforts, limited knowledge sharing and fragmented decision making within the ecosystem.
Lack of Policy & Regulations for QS Solutions	C14	There is a lack of policy and legal implications for the QS transition, and compliances for QS solutions need to be updated.
Complex Technological Interdependency in the Ecosystem	C15	Changes in the existing system cannot occur in isolation due to its chain of interdependencies including governing bodies, standards bodies, hardware providers, third-party software providers etc.

Note. Adapted from "Analyzing Dependencies among Challenges for Quantum-safe Transition," by Kong, Janssen & Bharosa (2023, p.12).

Table 10 shows the refined list of QS transition challenges. The QS Transition Challenges are clustered into three different categories: Technological, Organizational, and Ecosystem. Although the Technology-Organization-Environment (TOE) framework was initially used to organize the results from the literature, the term "*environment"* has been revised to "*ecosystem"* to better address challenges that may arise in the context of QS transition.

5.5 Chapter Conclusion

The chapter provided an overview of stakeholders in the PKI systems for the government and shows the complexity of PKI systems. This includes stakeholders such as users (individuals, businesses, and government agencies), external expertise (QTSPs, hardware vendors, and software providers), governing bodies (Logius, AT, and Ministry of Interior and Kingdom Relations), and standardization bodies (NIST, ETSI). With multiple stakeholders in the PKI, the process of identity authentication, authorization, and digital certification is maintained to ensure secure communication and information exchange. Yet, all those stakeholders have different systems and are organized in various ways, which complicates the realization of QS in the PKI. Some are already preparing, whereas others are not at the early stages. Thus, QS transition needs to be carefully planned, and a coordinated approach is needed to prepare organizations for transitioning their existing infrastructures.

The chapter set out to answer sub-question 1, "*What are the challenges that hinder organizations in transitioning toward QS PKI systems?"* The list of 24 socio-technical transition challenges for QS transition in the literature was identified using a systematic literature review. Then, the transition challenges previously identified in the literature were refined through semi-structured interviews with experts from government and industry. This allowed the researcher to focus on the case of PKI systems in the Dutch public sector. The TOE framework was used to cluster the challenges and provide a multi-perspective view with a diverse set of challenges (technical or non-technical). The factors, such as technological, organizational, and ecosystem categories, bring an advantage when understanding a diverse set of transition challenges (technical or non-technical) that can emerge within and outside organizations.

The chapter concludes with a list of QS transition challenges for PKI systems. The transition challenges include Availability of QS Standardization, No QS standards & selection, No Reliable & Secure QS solution, Non-PQC systems (e.g., Certificate Authorities & Users), and No Availability of QS Hardware & Software, Lack of Urgency within Organization, No Business case for QS Transition,

Knowledge Needs within Organizations, Lack of Technical skills & Qualified Personnel, and No QS Governance within Organization, Complex Technical Interdependencies, Lack of Collaboration, Lack of Urgency in the Ecosystem, No QS Governance in the Ecosystem, and Lack of Policy & Regulations for QS Solutions. Thus, the list of transition challenges for QS transition shows that a wide variety of challenges that are socio-technical need to be addressed, and transitioning existing infrastructure to QS remains complex.

Chapter 6 Stages of Growth Model

6.1 Introduction

This chapter introduces the stages of a growth model for QS transition, and answers sub-question 2 and sub-question 3. Section 6.2 explains the development of the growth model by outlining how different stages in the model were derived using the ISM-MICMAC approach. Section 6.3 provides details on the five stages of the growth model, and a list of discontinuities that act as necessary conditions that must be met in the ecosystem for organizations to move from one stage to the next. Section 6.4 discusses actions needed across organizations and introduces QS transition capabilities that organizations may need to execute during QS transition. The chapter concludes in Section 6.5.

Parts of this chapter are based on the following publications:
Kong, I., Janssen, M., & Bharosa, N. (2024). Navigating through the Unknowns-Readiness Assessment Model for Quantum-safe Transition. Electronic Government: 23rd IFIP WG 8.5 International Conference, EGOV 2024, Ghent-Leuven, Belgium, September 3–5, 2024, Proceedings. p. 438 – 453. https://dx.doi.org/10.1007/978-3-031-70274-7_27

Kong, I., Janssen, M., & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition. In: CEUR Workshop Proceedings. 3449.

Kong, I. (2022). Transitioning towards quantum-safe government: Examining stages of growth models for Quantum-safe public key infrastructure systems. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022. https://doi.org/10.1145/3560107.3560182

6.2 Development Process of the Stages of Growth Model

This section outlines the development process of the Stages of Growth Model for QS transition. Although there exist many methods, they are often based on intuition or on historical data. The latter is not available for becoming QS yet. In contrast, we opted for a systematic approach in which we take the challenges as a starting point and employ the expertise of those working in this domain. Section 6.2.1 elaborates on the steps in applying the ISM-MICMAC approach to examine the contextual relationship between QS transition challenges and identify challenges that

organizations may need to prioritize. Section 6.2.3 presents the results from MICMAC analysis using the dependence and driving power diagrams across different organizations in the Dutch government PKIs. Section 6.2.3 discusses the results from ISM analysis using the structural hierarchical models across different organizations in the Dutch government PKIs.

6.2.1 Steps in Applying the ISM-MICMAC Approach

The literature review of the growth model revealed that the majority of the growth models do not have a systematic approach in deriving different stages of the models. The current methods often involve developing stages based on interviews, and stages would emerge from them. The list of QS transition challenges (shown in Table 10) was used as the starting point to develop the stages of the growth model. An integrated Interpretive Structural Modeling (ISM)- Matrice d'Impacts Croisés Multiplication Appliquée à un Classement (MICMAC) approach was used to provide a systematic, structured process for prioritizing the identified challenges based on their driving and dependence power. The results highlight which challenges need to be addressed with priorities in hierarchical levels.

The ISM-MICMAC approach was selected to examine the interrelationship between QS transition challenges. Other approaches, such as Structural Equation Modeling (SEM), which requires larger quantitative datasets, or Analytic Hierarchy Process (AHP), which examines the relative importance and preference of factors, were not suited for the research. With the expert-based qualitative data, ISM-MICMAC can examine how these different challenges influence one another to provide in-depth insights into system dynamics and strategic priorities for organizations looking to address these challenges. The ISM-MICMAC provides a systematic method for arranging the dependencies between the steps required to transition to a QS situation.

The ISM is a methodology of systemic structuring modelling introduced by Warfield (1974), which can be applied when identifying relationships among factors. A set of factors in complex issues is structured into a comprehensive, systemic, hierarchical model (Attri et al., 2013; Janssen et al., 2019; Warfield, 1974). The MICMAC analysis validates the results obtained from ISM and was introduced by Godet (1973) to illustrate the relationship between the factors according to their driving power and dependence power using four categories: autonomous, dependent, linkage, and independent (Godet, 2000; Gorane & Kant, 2015; Janssen et al., 2019). While ISM can analyze the interrelationships between the factors that influence the system, the MICMAC classifies factors based on driving power and dependence

power. The steps in applying the ISM-MICMAC approach (shown in Appendix B) for QS transition challenges are described below with an example of the results obtained from government PKIs among ministries. The findings and discussion presented in this section draw upon and are adapted from the previous work, Kong, I., Janssen, M & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition. In: CEUR Workshop Proceedings. 3449.

Step 1: Identify and finalize the list of factors that will be used as input for the ISM-MICMAC approach. The list of QS transition challenges used as an input is shown in Table 10.

Step 2: Develop a Structural Self-Interaction Matrix (SSIM) to collect data on contextual relationships between the list of QS transition challenges.

Step 3: Examine the contextual relationship between any two factors (i and j) and fill out the SSIM. Start from a yellow box (C1, C2) and indicate one of the four symbols below to represent the relationship between factors.

V: Challenge i will influence Challenge j
A: Challenge j will influence Challenge i
X: Challenge i and Challenge j will influence each other
O: Challenge i and Challenge j are not related

Step 4: Establish Initial Reachability Matrix (IRM) from the SSIM matrix. IRM is a binary matrix with 0's and 1's that is derived in accordance to four symbols following the rules for the substitution.

If the (i,j) is V, then (i,j) in the reachability matrix becomes 1 and the (j,i) becomes 0
If the (i,j) is A, then (i,j) in the reachability matrix becomes 0 and the (j,i) becomes 1
If the (i,j) is X, then (i,j) in the reachability matrix becomes 1 and the (j,i) becomes 1
If the (i,j) is O, then (i,j) in the reachability matrix becomes 0 and the (j,i) becomes 0

Step 5: Test the IRM for transitivity and derive the Final Reachability Matrix (FRM). The transitivity is incorporated to fill the gap and 1* entries are indicated to show the changed relationships for the final reachability matrix. Table 11 shows the FRM that is revised from the IRM in accordance with the transitivity. The changes are highlighted in grey boxes and are indicated with 1* entries.

Concept of Transitivity: If factor A influences factor B, and factor B influences factor C, then factor A also influences factor C. If there was no initial relationship between factor A and factor C in IRM, then the concept of transitivity is achieved between factor A and factor C, and 1* entry is indicated in the FRM.

The concept of transitivity shows the links that are not immediately visible between factors and shows the hidden chain of influence. After obtaining the results in Step 5 from ISM transitivity, factors that influence and are influenced can be further identified in Step 6 with a reachability matrix consisting of a reachability set and an antecedent set. The results from Step 5 can be further used for the MICMAC categorization using four quadrants (e.g., autonomous, dependent, linkage, and driver) in Step 11. Different factors can be categorized based on their driving power and dependence power.

Table 11. Final Reachability Matrix

Structural Self-Interactive Matrix (SSIM)			j													
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
i	Legacy System Constraints	C1	1	1*	1*	1*	1*	0	1	1	1*	1*	1*	0	1	1*	1*
	No Availability of QS Standardization	C2	1*	1	1*	1	1	1*	1*	1	1*	1*	1	1*	1*	1	1
	No QS Standards & Selection	C3	1	1	1	1	1	1*	1*	1	1*	1	1*	1*	1	1	1
	No Reliable & Secure QS Solutions	C4	1	1	1	1	1	1*	1*	1	1	1*	1*	1*	1*	1	1
	No Availability of QS Hardware & Software	C5	1	1	1*	1	1	1	1*	1	1*	1*	1*	1	1*	1*	1
	Knowledge Needs within Organizations	C6	1	1	1	1	1	1	1	1	1	1	1*	1*	0	1*	1*
	Lack of Urgency within Organizations	C7	1*	1	1	1	1	1*	1	1*	1	1	1*	1*	0	1*	1*
	No Business Case for Organizations	C8	1*	1	1*	1*	1*	1*	1	1	1	1	1	1*	1*	1*	1
	Lack of Technical Skills & Qualified Personnel	C9	1*	1	1	1	1	1*	0	1*	1	1	1*	1	1*	1*	1
	Unclear QS Governance within Organizations	C10	1*	1	1*	1	1	1*	0	1*	1	1	1*	1*	0	1*	1*
	Lack of Urgency in the Ecosystem	C11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Unclear QS Governance in the Ecosystem	C12	1	1	1	1	1	1*	1*	1*	1*	1	1	1	1	1	1
	Lack of Collaboration in the Ecosystem	C13	1	1	1	1	1	1*	1	1	1*	1	1	1	1	1	1
	Lack of Policy & Regulations for QS Solutions	C14	1	1	1	1	1	1	1	1	1	1	1	1	1*	1	1
	Complex Technological Interdependency in the Ecosystem	C15	1	1	1	1	1	1*	1*	1	1*	1	1*	1	1	1	1

Note. Adapted from "Analyzing Dependencies among Challenges for Quantum-safe Transition," by Kong, Janssen & Bharosa (2023, p. 5).

Step 7: Obtain a reachability matrix with the reachability set and antecedent set from the entries in rows and columns in FRM. e.g., In the reachability set, factors in the row that are affected by factor C1 are identified. In the antecedent set, factors in the column that are affecting factor C1 are identified. After the reachability set and

antecedent set are determined, the intersection set is derived from the list of factors from the intersection of these sets.

Step 8: Once the reachability matrix is determined in Step 7, Step 8 is taken to determine the level of each QS transition challenge. Partition the reachability matrix and classify the FRM into various levels. The top-level factors (L1) include those factors that will be led by other factors in the lower level (L2, L3, etc.). Once the top-level factor is identified, it is removed from consideration. Then, the same process is repeated to find out the factors in the next level. This process continues until the level of each factor is found. Table 12 shows different levels for QS transition challenges. The concept of transitivity applied to the ISM-MICMAC approach structures the interrelationships among the identified challenges and enables the derivation of hierarchical levels.

Table. 12 Overview of the Levels for QS Transition Challenges

Level	Challenge	Code
1	Legacy System Constraints	C1
	Unclear QS Governance within Organizations	C10
2	Lack of Technical Skills & Qualified Personnel	C9
	Knowledge Needs within Organizations	C6
	Lack of Urgency within Organizations	C7
3	No Availability of QS standardization	C2
	No QS Standards & Selection	C3
	No Reliable & Secure QS Solutions	C4
	No Availability of QS Hardware & Software	C5
	No Business Case for Organizations	C8
	Lack of Urgency in the Ecosystem	C11
	Lack of Policy & Regulations for QS Solutions	C14
	Complex Technological Interdependency in the Ecosystem	C15
4	Unclear QS Governance in the Ecosystem	C12
	Lack of Collaboration in the Ecosystem	C13

Note. Adapted from "Analyzing Dependencies among Challenges for Quantum-safe Transition" by Kong, Janssen & Bharosa (2023, p. 5).

The levels identified in Step 8 represent different stages where factors influence and are influenced by one another. By identifying factors across different levels, the ISM-MIACMAC approach also reveals challenges that may need to be addressed at different stages, with varying priorities. The indication of factors at different levels suggests that factors cannot be addressed all at once. Thus, the levels of different factors reflect a sequential logic for addressing these factors at different stages.

Step 9: Organize the ISM-based hierarchy factors using different levels of a partition obtained in Step 7. Develop a visual representation of the ISM-based hierarchy model. Section 6.2.3 further discusses the results obtained from the ISM-based hierarchy models.

Step 10: Analyze the FRM obtained in Step 5 and calculate the summation of rows and columns based on their driving and dependence power. Table 13 shows the summation of driving power and dependence power of QS transition challenges.

Table 13. Example of the Summation of Driving Power & Dependence Power

Structural Self-Interactive Matrix (SSIM)			j														Driving Power
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	
i	Legacy System Constraints	C1	1	1*	1*	1*	1*	0	1	1	1*	1*	1*	0	1	1*	1*	13
	No Availability of QS Standardization	C2	1*	1	1*	1	1	1*	1*	1	1*	1*	1	1*	1*	1	1	15
	No QS Standards & Selection	C3	1	1	1	1	1	1*	1*	1	1*	1	1*	1*	1	1	1	15
	No Reliable & Secure QS Solutions	C4	1	1	1	1	1	1*	1*	1	1	1*	1*	1*	1*	1	1	15
	No Availability of QS Hardware & Software	C5	1	1	1*	1	1	1	1*	1	1*	1*	1*	1	1*	1*	1	15
	Knowledge Needs within Organizations	C6	1	1	1	1	1	1	1	1	1	1	1*	1*	0	1*	1*	14
	Lack of Urgency within Organizations	C7	1*	1	1	1	1	1*	1	1*	1	1	1*	1*	0	1*	1*	14
	No Business Case for Organizations	C8	1*	1	1*	1*	1*	1*	1	1	1	1	1	1*	1*	1*	1	15
	Lack of Technical Skills & Qualified Personnel	C9	1*	1	1	1	1	1*	0	1*	1	1	1*	1	1*	1*	1	14
	Unclear QS Governance within Organizations	C10	1*	1	1*	1	1	1*	0	1*	1	1	1*	1*	0	1*	1*	13
	Lack of Urgency in the *Ecosystem*	C11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
	Unclear QS Governance in the *Ecosystem*	C12	1	1	1	1	1	1*	1*	1*	1*	1	1	1	1	1	1	15
	Lack of Collaboration in the *Ecosystem*	C13	1	1	1	1	1	1*	1	1	1*	1	1	1	1	1	1	15
	Lack of Policy & Regulations for QS solutions	C14	1	1	1	1	1	1	1	1	1	1	1	1	1*	1	1	15
	Complex Technological Interdependency in the *Ecosystem*	C15	1	1	1	1	1	1*	1*	1	1*	1	1*	1	1	1	1	15
Dependence Power			15	15	15	15	15	14	13	15	15	15	15	14	12	15	15	

Note. Adapted from "Analyzing Dependencies among Challenges for Quantum-safe Transition" by Kong, Janssen & Bharosa (2023, p. 6).

Step 11: Classify the factors in a driving and dependence power diagram in accordance with the summation of driving power and dependence power obtained in Step 9. Find out which of the four quadrants each factor belongs to. There are four quadrants in the driving and dependence power diagram:

Autonomous: Factors that have weak drive power and weak dependence power.
Dependent: Factors that have weak drive power but strong dependence power.
Linkage: Factors that have strong drive power as well as strong dependence power.
Drivers/Independent: Factors that have strong drive power but weak dependence power.

6.2.2 Results from the MICMAC analysis: Driving power & Dependence power

The driving power and dependence power of each QS transition challenge is placed in one of the four quadrants in the power diagram (autonomous, dependent, linkage, and independent). The results of MICMAC analysis across different organizations that are part of the Dutch government PKIs, e.g., Ministries, Certificate Authorities (CAs), and PKI users, are shown below.

Ministries

The categorization of QS transition challenges in four quadrants (e.g., autonomous, dependent, linkage, and independent) with the perspectives of the ministries in the Dutch government PKIs is shown in Figure 14.

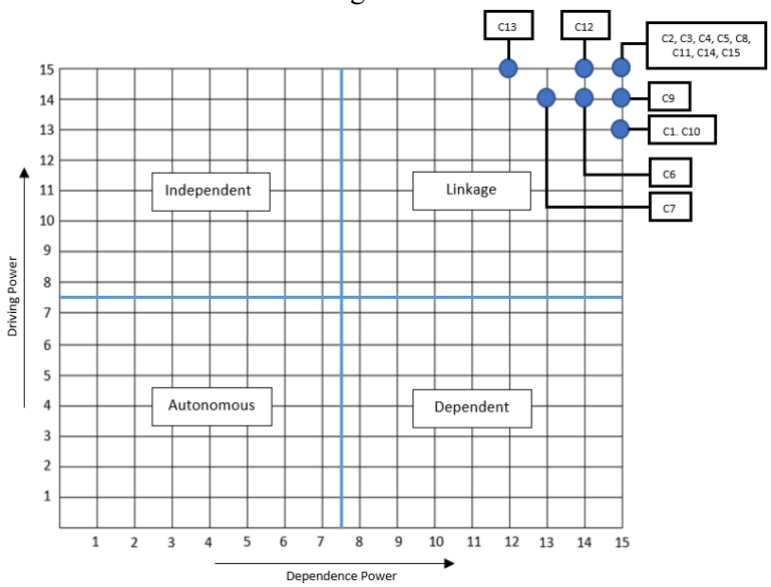


Figure 14. Driving Power & Dependence Power Diagram Among Ministries

Note. Adapted from "Analyzing Dependencies among Challenges for Quantum-safe Transition" by Kong, Janssen & Bharosa (2023, p. 7).

Autonomous: A set of challenges in this quadrant has weak driving power and weak dependence power, which signals that the challenges are relatively disconnected from the context. From the perspectives of the ministries, no QS transition challenges were placed in an autonomous quadrant. Having no challenges placed in the autonomous quadrant indicates that all 15 QS transition challenges have a significant influence on QS transition.

Dependent: A set of challenges in this quadrant that have strong dependence power would require all other QS transition challenges to address the QS transition. From the perspectives of the ministries, no QS transition challenges were placed in a dependent quadrant. This indicates that no QS transition challenges have weak driving power and strong dependence power.

Linkage: A set of challenges in this quadrant has strong driving power and strong dependence power. Having both strong driving power and dependence power signals that addressing change regarding the challenge will impact other challenges and have an impact on itself. From the perspectives of the ministries, all 15 QS transition challenges were placed in the linkage quadrant. This indicates that all the QS transition challenges are interrelated, and they impact each other.

Drivers/Independent: A set of challenges in this quadrant has strong driving power and weak dependence power. These factors are also known as key factors falling into the quadrant of independent or linkage. The challenges with strong driving power can impact other challenges, which should be given priority. From the perspectives of the ministries, no QS transition challenges were placed in an independent quadrant, and this indicates that key factors for QS may still need to be identified.

Certificate Authorities (CAs)

The categorization of QS transition challenges in four quadrants (e.g., autonomous, dependent, linkage, and independent) with the perspectives of the Certificate Authorities (CAs) in the Dutch government PKIs is shown in Figure 15.

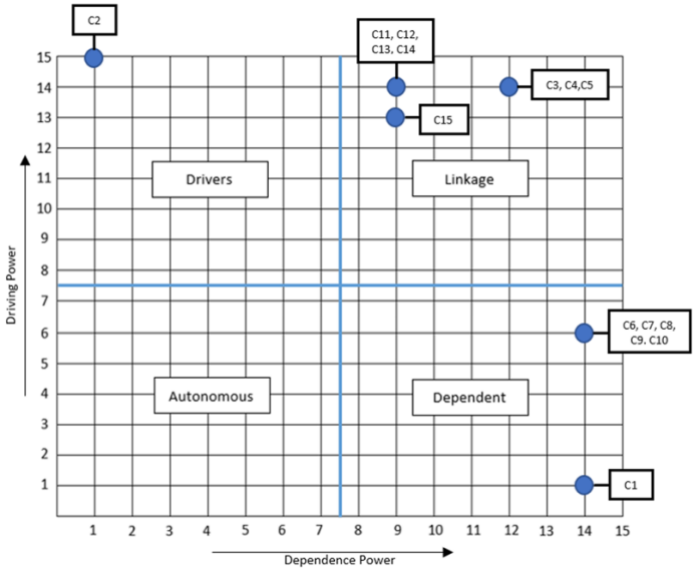


Figure 15. Driving Power & Dependence Power Diagram of CAs

Autonomous: From the perspectives of the CAs, no QS transition challenges were placed in an autonomous quadrant. This indicates that all 15 challenges are relatively connected to the context of QS transition without having weak driving power and weak dependence power.

Dependent: A set of challenges in this quadrant has weak driving power and strong dependence power. The challenges placed in this quadrant have strong dependence power, which indicates that they are heavily influenced by other challenges that have high driving power. From the perspectives of the CAs, challenges placed in dependent quadrant are Legacy System Constraints (C1), Knowledge Needs within Organizations (C6), Lack of Urgency within Organizations (C7), No Business Case for Organizations (C8), Lack of Technical Skills & Qualified Personnel (C9), and Unclear QS Governance within Organizations (C10) have weak driving power and strong dependence power.

Linkage: A set of challenges in this quadrant has strong driving power and strong dependence power. From the perspectives of the CAs, challenges placed in linkage quadrant are No QS Standards & Selection (C3), No Reliable & Secure QS Solutions (C4), No Availability of QS Hardware & Software (C5), Lack of Urgency in the Ecosystem (C11), Unclear QS Governance in the Ecosystem (C12), Lack of Collaboration in the Ecosystem (C13) Lack of Policy & Regulations for QS Solutions (C14) and Complex Technological Interdependency in the Ecosystem (C15). These challenges have strong driving power and dependence power, which also means that these challenges impact other challenges and have an impact on themselves.

Drivers/Independent: A set of challenges in this quadrant has strong driving power and weak dependence power. From the perspectives of the CAs, challenge No Availability of QS Standardization (C2) is placed in the driver's quadrant. This indicates that the following challenge has strong driving power and can impact other challenges.

PKI Users

The categorization of QS transition challenges in four quadrants (e.g., autonomous, dependent, linkage, and independent) with the perspectives of PKI users in the Dutch government PKIs is shown in Figure 16.

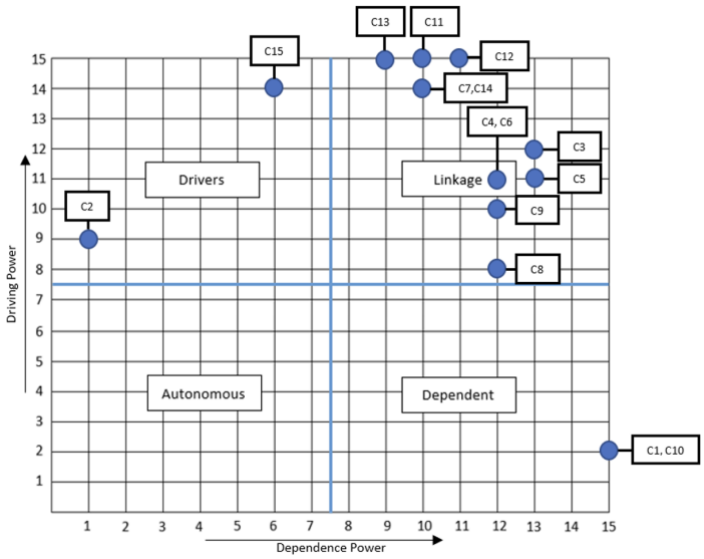


Figure 16. Driving Power & Dependence Power Diagram of PKI Users

Autonomous: A set of challenges in this quadrant has weak driving power and weak dependence power, which signals that the challenges are relatively disconnected from the context. From the perspectives of the PKI users, no QS transition challenges are placed in an autonomous quadrant.

Dependent: A set of challenges in this quadrant has weak driving power and strong dependence power. From the perspectives of the PKI users, challenges placed in this quadrant are Legacy System Constraints (C1) and Unclear QS Governance within Organizations (C10). These challenges have strong dependence power and are influenced by other QS transition challenges.

Linkage: A set of challenges in this quadrant has strong driving power and strong dependence power. From the perspectives of the PKI users, challenges placed in the linkage quadrant are No QS Standards & Selection (C3), No Reliable & Secure QS Solutions (C4), No Availability of QS Hardware & Software (C5), Knowledge Needs within Organizations (C6), Lack of Urgency within Organizations (C7), No Business Case for Organizations (C8), Lack of Technical Skills & Qualified Personnel (C9), Lack of Urgency in the Ecosystem (C11), Unclear QS Governance in the Ecosystem (C12), Lack of Collaboration in the Ecosystem (C13) and Lack of Policy & Regulations for QS Solutions (C14). These challenges in the linkage quadrant are interrelated, and they impact each other.

Drivers/Independent: A set of challenges in this quadrant has strong driving power and weak dependence power. From the perspectives of the PKI users, challenges placed in this quadrant are No Availability of QS Standardization (C2) and Complex Technological Interdependency in the Ecosystem (C15). These challenges have a strong driving power and impact other challenges.

In summary, the results from MICMAC analysis across different organizations indicate QS transition challenges are largely intertwined and they influence each other. There were similarities and differences regarding challenges placed with the perspectives among ministries, CAs, and PKI users. On the one hand, all three perspectives showed that many uncertainties are lingering for QS transition and challenges are interrelated. On the other hand, CAs and PKI users saw that organizational challenges were dependent on and influenced by the technology and

ecosystem challenges. This differed from the perspectives of the ministries, as all the challenges were placed in the linkage quadrant.

As ministries operate across sectors within and beyond national borders, they not only need to remain compliant with global regulations and national implementations, but their decisions also affect other critical infrastructures across different sectors, such as finance, telecom, energy, and water. For CAs, the majority of QS transition challenges were placed in the linkage quadrant and the dependent quadrant, with one transition challenge in the driver's quadrant. Since CAs need to achieve interoperability, compliance, and strict oversight to facilitate the digital infrastructures, decisions regarding global regulations, national laws, and technical standards need to be considered for CAs, as these are relevant to their business processes.

Moreover, QS transition challenges from the end-user perspective showed that the majority of QS transition challenges are interdependent. Since end-user organizations need to stay compatible with their internal systems and external systems in the ecosystem, the development of QS standards and complex technological interdependencies in the ecosystem were driving other challenges. Although the decisions of PKI users may not affect the broader digital ecosystem in the same way as ministries and CAs, PKI users need to make sure that their legacy systems support QS cryptographic solutions when available and follow compliance if mandated.

6.2.3 Results from the ISM analysis: A Structural Hierarchical Model of QS transition challenges

The ISM-based hierarchy shows the interrelationship between QS transition challenges and how these challenges influence each other. The results provide the ISM-based hierarchy of QS transition challenges with examples of various organizations within the Dutch government PKI system, including ministries, Certificate Authorities (CAs), and PKI users.

Ministries

The results of the ISM-based hierarchy with the perspectives among ministries show that there are four levels of hierarchy for QS transition challenges. Figure 17 shows an example of the ISM-based hierarchical model using QS transition challenges.

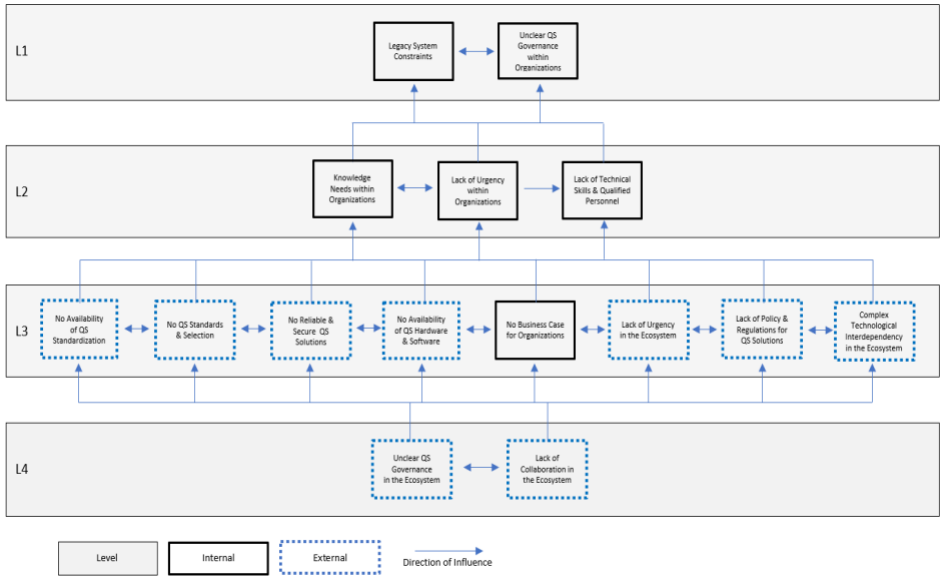


Figure 17. Structural Hierarchical Model developed by the Ministries
Note. Adapted from "Analyzing Dependencies among Challenges for Quantum-safe Transition" by Kong, Janssen & Bharosa (2023, p. 7).

In Level 4, there are two challenges with strong driving power, which include: Unclear QS Governance in the Ecosystem (C12) and a Lack of Collaboration in the Ecosystem (C13). In Level 3, there are eight challenges which include: No Availability of QS Standardization (C2), No QS Standards & Selection (C3), No Reliable & Secure QS Solutions (C4), No Availability of QS Hardware & Software

(C5), No Business Case for Organizations (C8), Lack of Urgency in the Ecosystem (C11), Lack of Policy & Regulations for QS Solutions (C14) and Complex Technological Interdependency in the Ecosystem (C15). The list of challenges in Level 4 and Level 3 included mostly external challenges in the ecosystem, except for No Business Case for Organizations (C8).

The list of challenges in Level 2 and Level 1 largely focuses on the internal challenges that relate to the organizational aspects. In Level 2, there are three challenges, which include: Knowledge Needs within Organizations (C6), Lack of Urgency within Organizations (C7), and Lack of Technical Skills & Qualified Personnel (C9). In Level 1, there are two challenges, which include: Legacy System Constraints (C1) and Unclear QS Governance within Organizations (C10). These challenges show the weak driving power and are influenced by a whole range of other challenges related to technology and ecosystem that have higher driving power in the lower hierarchy.

Certificate Authorities (CAs)

The results of the ISM-based hierarchy with the perspectives of CAs show that there are four levels of hierarchy for QS transition challenges. Figure 18 shows an example of the ISM-based hierarchical model using QS transition challenges.

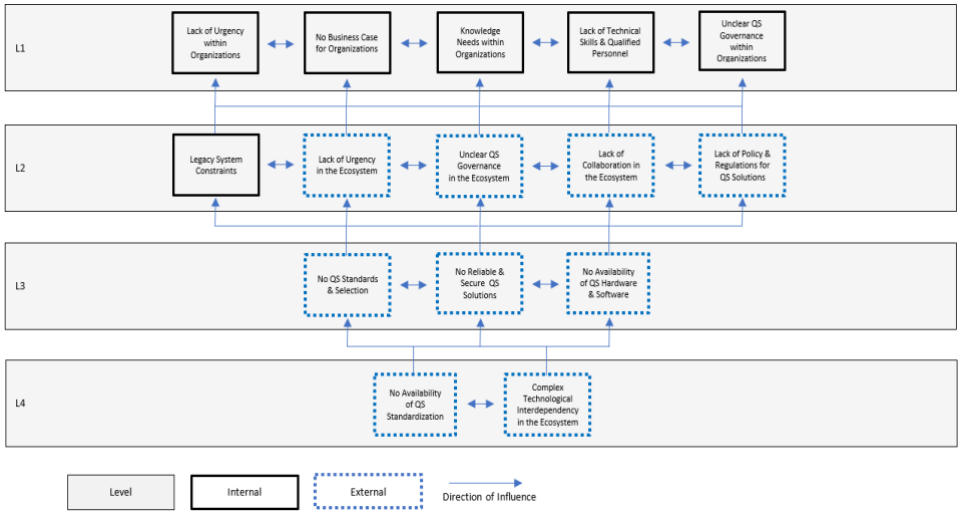


Figure 18. Structural Hierarchical Model of CAs

In Level 4, there are two challenges that have strong driving power, which include: No Availability of QS Standardization (C2) and Complex Technological

Interdependency in the Ecosystem (C15). In Level 3, No QS Standards & Selection (C3), No Reliable & Secure QS Solutions (C4), No Availability of QS Hardware & Software (C5). The challenges in Level 4 and Level 3 mainly focused on external challenges related to technology.

In Level 2, there are five challenges, which include: Legacy System Constraints (C1), Lack of Urgency in the Ecosystem (C11), Unclear QS Governance in the Ecosystem (C12), Lack of Collaboration in the Ecosystem (C13), and Lack of Policy & Regulations for QS Solutions (C14). The results show that the addressing legacy system of CAs needed to be prioritized as soon as the list of external challenges in the ecosystem was addressed. From the perspectives of CAs, they may need to maintain interoperability, compliance, and strict oversight to continue facilitating the secure digital communication and information exchange. In Level 1, there are five challenges that have weak driving power, which include: Lack of Urgency within Organizations (C7), No Business Case for Organizations (C8), Knowledge Needs within Organizations (C6), Lack of Technical Skills & Qualified Personnel (C9), and Unclear QS Governance within Organizations (C10).

PKI Users

The results of the ISM-based hierarchy with the perspectives of PKI users show that there are four levels of hierarchy for QS transition challenges. Figure 19 shows an example of the ISM-based hierarchical model using QS transition challenges.

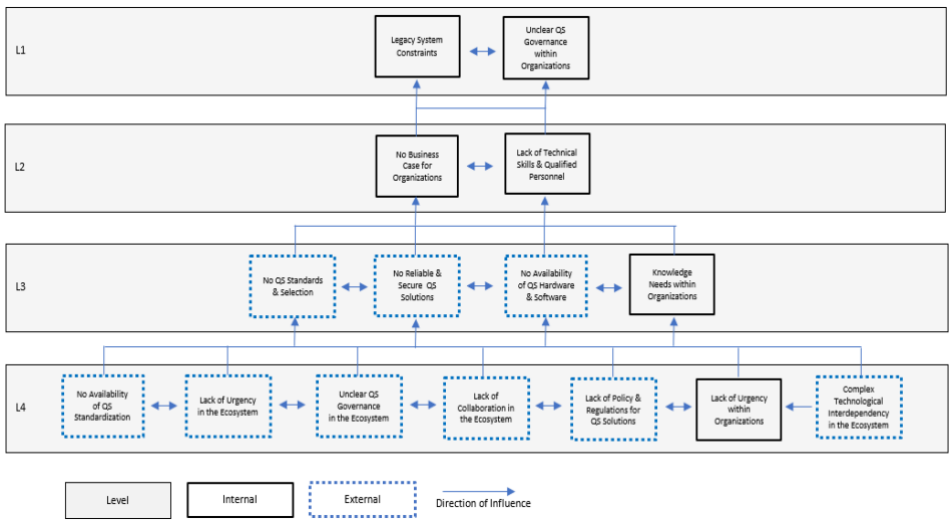


Figure 19. Structural Hierarchical Model of PKI Users

The lowest level of the hierarchy (level 4) consists of challenges that have stronger driving power. There are seven challenges in Level 4 which include: No Availability of QS Standardization (C2), Lack of Urgency in the Ecosystem (C11), Unclear QS Governance in the Ecosystem (C12), Lack of Collaboration in the Ecosystem (C13), Lack of Policy & Regulations for QS Solutions (C14), Lack of Urgency within Organizations (C7) and Complex Technological Interdependency in the Ecosystem (C15). Although the majority of the challenges in Level 4 include external challenges in the ecosystem, the end-user organizations saw that it was crucial to address Lack of Urgency within Organizations (C7) as one of the priorities.

In Level 3, there are four challenges, which include: No QS Standards & Selection (C3), No Reliable & Secure QS Solutions (C4), No Availability of QS Hardware & Software (C5), and Knowledge Needs within Organizations (C6). The internal challenges related to QS transition in organizations need to be addressed as early as possible for organizations to recognize the complexity of QS transition. In Level 2, there are two challenges, which include: No Business Case for Organizations (C8) and Lack of Technical Skills & Qualified Personnel (C9). In Level 1, there are two challenges with weak driving power, which include: Legacy System Constraints (C1) and Unclear QS Governance within Organizations (C10). These challenges are influenced by other challenges related to technology and the ecosystem that have higher driving power in a lower hierarchy.

A Synthesized Structural Hierarchical Model of QS Transition Challenges

With the results obtained from ISM-MICMAC analysis, a structural hierarchical model of QS transition challenges has been synthesized. By taking perspectives across different organizations that are part of the Dutch government PKIs, Ministries, Certificate Authorities (CAs), and PKI users, all levels identified in different models have been integrated. The synthesized model includes five levels of hierarchy. Figure 20 shows the synthesized structural hierarchical model of QS transition challenges. By combining the results of a structural hierarchical model from the ministries, CAs, and PKI users, the structural hierarchical model with four levels has been extended to five levels.

While the challenges at the bottom level act as drivers and influence others, challenges at the top level are influenced and depend on the challenges at the bottom level. Likewise, the results showed that inter-organizational dynamics exist in the wider ecosystem, including ministries, CAs, and PKI users. The institutional constraints and interdependencies that exist across organizations indicated bottom-up and top-down patterns across different levels of transition challenges. The lowest

level of hierarchy starts with Level 5, which has the most driving power and includes challenges such as No Availability of QS Standardization (C2) and Complex Technological Interdependency in the Ecosystem (C15). The results across different organizations saw that the external challenges in the ecosystem start with recognizing the need for QS standards and the interdependencies that exist between organizations when facilitating digital communication and information exchange.

In Level 4, other external challenges include Lack of Collaboration in the Ecosystem (C13), Lack of Urgency in the Ecosystem (C11), Unclear QS Governance in the Ecosystem (C12), No QS Standards & Selection (C3), and No Reliable & Secure QS Solutions (C4). These challenges in the ecosystem need to be addressed with priority as QS standards become available and organizations recognize technological interdependencies in their existing infrastructures. Since organizations cannot work in silos, there is a need to collaborate and raise urgency while navigating the development of QS technology.

In Level 3, challenges that are influenced by lower hierarchy that are in Level 4 and Level 5 are Lack of Policy & Regulations for QS Solutions (C14), Knowledge Needs within Organizations (C6), Lack of Urgency within Organizations (C7), and No Availability of QS Hardware & Software (C5). For QS transition, internal challenges related to Knowledge Needs within Organizations (C6), Lack of Urgency within Organizations (C7) were considered important. By addressing these challenges with priority, organizations may further prepare for their QS transition processes.

The challenges, such as No QS Standards & Selection (C3), and No Reliable & Secure QS Solutions (C4) and No Availability of QS Hardware & Software (C5) were initially identified at the same level across ministries, CAs and PKI users. This reflects the complexity of interdependencies in the ecosystem and assumes that QS hardware and software is developed in parallel with QS solutions. However, this does not fully account for the fact that key decisions made need to be made by 1. the hardware and software vendors, whose decisions shape the availability and deployment of QS products, and 2. organizations, whose adoption decisions determine the implementation of QS products.

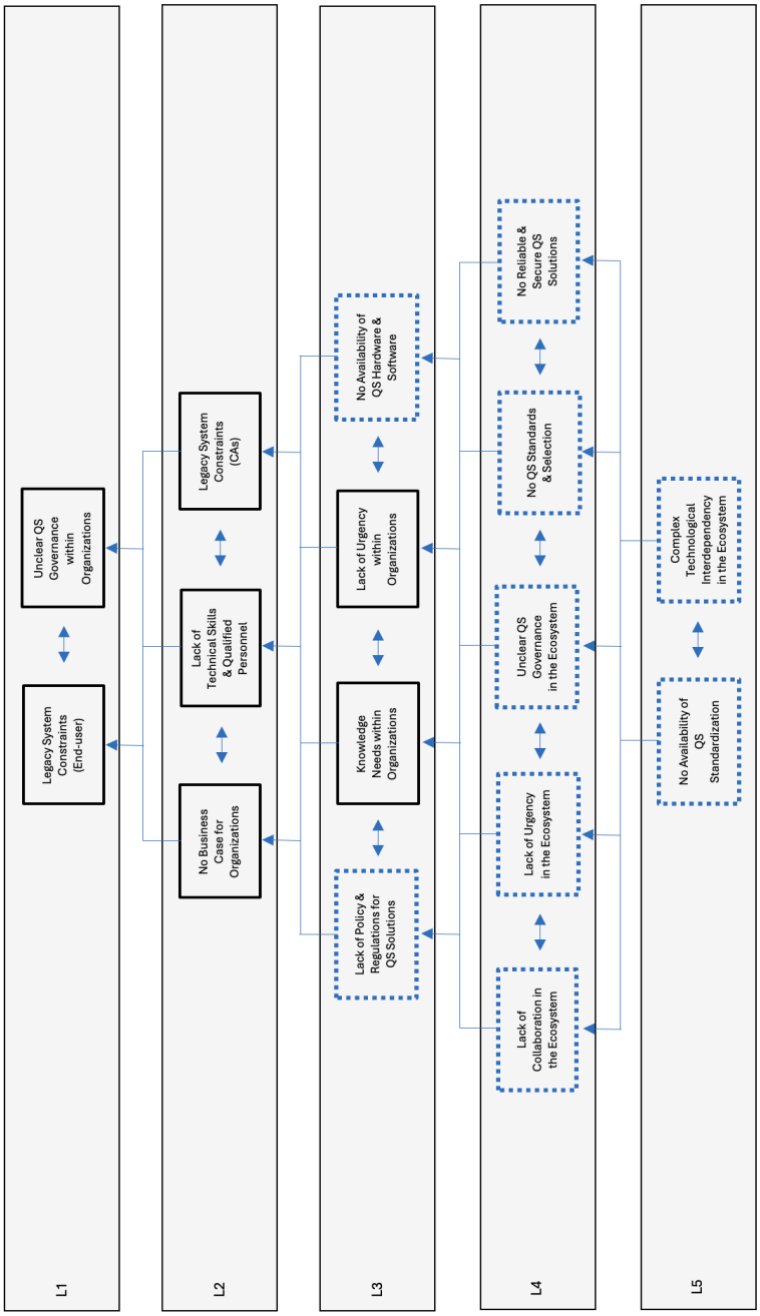


Figure 20. Synthesized Hierarchical Model of QS Transition Challenges

Thus, the synthesis further elaborates the complex ecosystem dependencies by indicating that the establishment of QS standards, validation and institutional alignment may be required prior to No Availability of QS Hardware & Software (C5). This results in positioning No Availability of QS Hardware & Software (C5) after No QS Standards & Selection (C3), and No Reliable & Secure QS Solutions (C4) into a separate level, more accurately capturing the conditions under which QS Hardware & Software become available to organizations.

In Level 2, challenges include No Business Case for Organizations (C8), Lack of Technical Skills & Qualified Personnel (C9), and Legacy System Constraints (C1). As challenges related to policies and regulations for QS solutions and the QS technology are addressed in the previous level, internal challenges regarding organizational aspects are addressed. In this level, the challenge, legacy system constraints (C1), is mentioned as part of CAs to tackle their existing infrastructure prior to addressing legacy systems of end-user organizations.

In Level 1, internal challenges are addressed within organizations, which include Unclear QS Governance within Organizations (C10) and Legacy System Constraints (C1). While Level 2 indicates that CAs may start preparing earlier than PKI users, such preparation may only be possible once necessary policies, regulations, and QS technology are available in Level 3. As CAs modify their infrastructures, PKI users may coordinate the process to begin their transitions to address constraints in their legacy systems.

In summary, transition challenges among the ministries are highly interdependent due to the international and national context. This implies that even large organizations like ministries need to monitor changes in the ecosystem regarding QS transition. The international and national context can influence and is influenced by other regulatory organizations and standard organizations in the EU, and other parts around the world. For ministries, having business cases for organizations was considered important. However, this was influenced by changes in the technology and ecosystem context. Many uncertainties needed to be addressed in the beginning to start their preparation for QS transition.

Likewise, CAs also heavily emphasized the need to address transition challenges in the ecosystem that are external to the organizations. While ministries, CAs, and PKI users share that both transition challenges related to technology and ecosystem aspects are crucial in influencing transition challenges related to organizational aspects, CAs put more emphasis on the transition challenges related to technology at the beginning of the QS transition. For CAs, it was crucial to maintain the facilitation of infrastructures, and their businesses would be heavily

influenced by collaboration, governance, and policies related to QS transition in the ecosystem. Thus, addressing legacy system constraints needs to be addressed first when making changes for QS transition.

Although the PKI users showed a similar need to address transition challenges in the ecosystem, it was crucial to address the lack of urgency within their organizations, which was given priority while recognizing the changes that occur in the ecosystem. This also shows that PKI users need more drivers to start preparing for QS transition when compared to CAs. This implies that PKI users are influenced by other actors in the ecosystem and cannot make decisions on their own. For PKI users, there needs to be some level of certainty to start their preparation for QS transition. While similarities across three perspectives across ministries, CAs, and PKI users show that there are challenges in the ecosystem that organizations need to navigate, differences also show that the timeline for QS transition may vary across organizations.

6.3 Stages of Growth Model for QS Transition

This section presents a stages of growth model for QS transition. The 15 QS transition challenges in Section 6.2 serve as an empirical foundation for the ISM-MICMAC approach. The hierarchical set of interrelated challenges provided an initial basis for structuring the stages of the growth model for QS transition. The iterations of the growth model can be found in Appendix D. Section 6.3.1 presents a five-stage growth model for QS Transitions, which includes QS awareness, QS assessment, QS preparation, QS implementation, and QS adaptation. At each stage of the growth model, discontinuities are presented as the necessary conditions in the ecosystem that must be met for organizations to move from one stage to the next.

6.3.1 Five Stages of Growth Model for QS Transitions

There are five stages in the model, which include QS awareness phase (Stage 1), QS assessment phase (Stage 2), QS preparation phase (Stage 3), QS implementation phase (Stage 4), and QS adaptation phase (Stage 5). The five stages of the growth model for QS transition are shown in Figure 21.

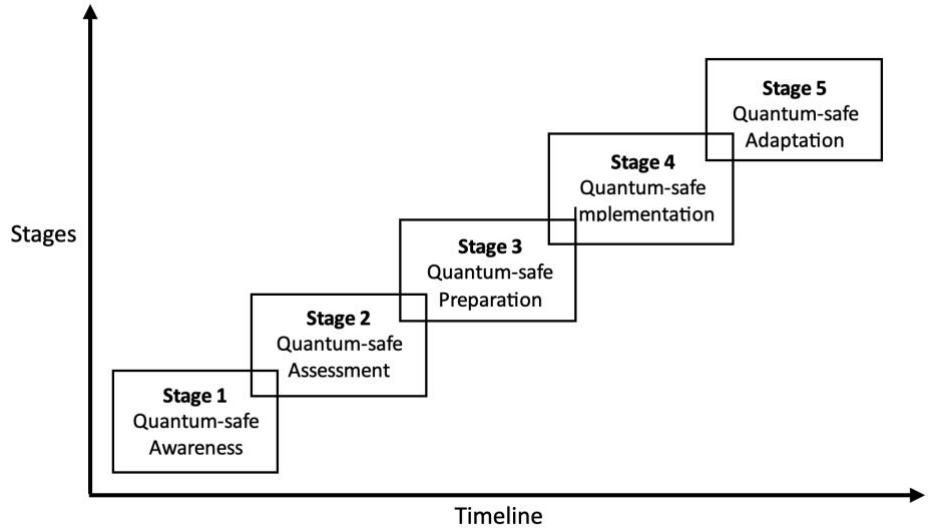


Figure 21. Stages of Growth Model for QS Transition

Due to complex interdependencies that existing infrastructures rely on, the results show that organizations cannot achieve QS transition in isolation, and collective actions are needed across organizations to achieve quantum safety. Thus, the growth model takes an ecosystem perspective and recognizes different organizations that facilitate digital communication and information exchange to take part in QS transition. With the idea that growth follows in stages, discontinuities act as necessary conditions that must be met in the ecosystem to move from one stage to the next. By prioritizing the list of challenges that need to be addressed in the ecosystem, different stages of QS transition and discontinuities are identified. The list of discontinuities is listed in Table 14.

To explain the five stages of the growth model, an example of Dutch government PKIs is used. When describing different stages of the growth model, organizations are mentioned in three different levels: ecosystem level, inter-organizational level, and intra-organizational level. Figure 22 shows interdependencies across organizations at different levels (e.g., ecosystem level, inter-organizational level & intra-organizational level). The arrow indicates the scope of influence across organizations at different levels. More details can be found in Section 6.4.

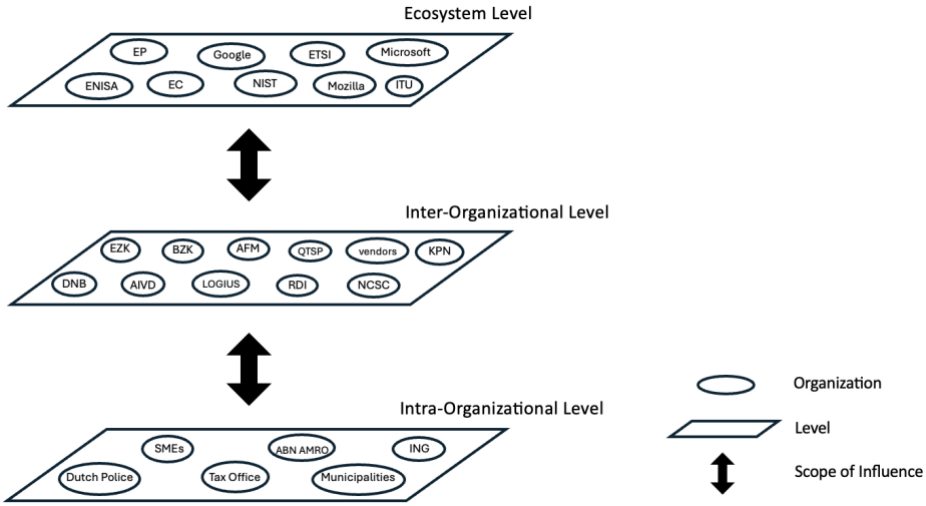


Figure 22. Interdependencies Across Organizations

Organizations at the inter-organizational level include government agencies that apply national regulations and/ standards (e.g., ministries, Logius, National Cyber Security Centre (NCSC)), organizations that manage and operate critical infrastructures across and within sectors in a national context (e.g., the Central Bank of the Netherlands, De Autoriteit Financiële Markten (AFM), KPN, vendors, etc.). Organizations at the intra-organizational level include public and private entities that do not necessarily operate or manage critical infrastructures but rather rely on the services provided by these infrastructures (e.g., government agencies, banks, tax offices, hospitals, service providers, and other small and medium enterprises (SMEs)).

Table 14. Discontinuities that Need to be Met at Different Stages

Stage	Discontinuities
1	-Acknowledgement of systematic risks & vulnerabilities of quantum threats -Finalized list of PQC Standardization
2	-Establishment of a steering committee and international working groups for QS transition -Establishment of a testing environment for QS cryptographic solution
3	-Availability of selected QS cryptographic solutions validated through testing -Development of policies & regulations that support QS transition
4	-Availability of QS cryptographic solutions in HSM & Certificate Issuance software (CAs)
5	-Availability of lessons learned and best practices from the implementation of QS cryptographic solutions -Establishment of a cross-organizational coordination mechanism for QS cryptographic solutions

Stage 1: QS Awareness

Stage 1 of the growth model for QS transition is known as *QS awareness stage*. At this stage, organizations may start recognizing the potential security issues posed by quantum computing technology. However, there are many uncertainties, and limited knowledge is available for organizations since QS transition is at its early stage. One of the discontinuities for stage 1 is *the acknowledgement of systematic risks and vulnerabilities of quantum threats*. Through documented reports, briefings, and knowledge-sharing sessions, the topic of quantum computing threats may be discussed at the ecosystem level. In Europe, regulatory organizations such as the European Commission have recognized the need to achieve quantum safety and have drafted a recommendation on a coordinated implementation roadmap for QS transition (European Commission, 2024a). Due to complex technical interdependencies that existing infrastructures rely on, organizations at the inter-organizational level and the intra-organizational level may influence and be influenced by organizations at the ecosystem level. Another discontinuity for Stage 1 is *the finalized list of PQC standardization.* Since 2016, NIST, as a standardization body, has been working on providing standards and guidelines for QS cryptographic algorithms. The announcement from the NIST in August 2024 showed the ongoing list of standards for QS cryptographic algorithms that are PQC-based (Alagic et al., 2025).

Stage 2: QS Assessment

Stage 2 of the growth model for QS transition is known as *QS assessment stage.* At stage 2, the finalized list of PQC standardization announced by the NIST signals other standardization organizations, such as ETSI, ENISA, IETF, and IEEE. With the growing awareness of QS transition, organizations that are frontrunners may start assessing the impact and risk in their business processes. At this stage, organizations may recognize the need for QS governance to define common standards, provide certification schemes, and enable stakeholder collaborations. One of the discontinuities for Stage 2 is *the establishment of a steering committee and international working groups for QS transition.* Organizations at the ecosystem level may actively seek inter(national) expertise for advisory input and subject matter experts for QS cryptographic solutions. Organizations may establish a formal structure with governing bodies, steering committees, and international working groups to address the governance vacuum for the QS transition. Moreover, organizations may recognize the need to test different QS cryptographic algorithms.

Without the testing process, it would be difficult to integrate QS cryptographic solutions into hardware and software products. Another discontinuity for Stage 2 is *the establishment of a testing environment for QS cryptographic solutions.* At this stage, organizations with resources and knowledge may take part in joint testbeds and provide performance benchmarks of QS cryptographic solutions. Some organizations may also be involved in making external decisions and setting up a testing environment. Others may decide to stay informed and wait for those decisions to crystallize. Hardware vendors and software companies that provide the products and services of the existing infrastructures may start thinking ahead to build products to meet the demands of their customers.

Stage 3: QS Preparation

Stage 3 of the growth model is known as *QS preparation stage*. At Stage 3, knowledge sharing and collaboration across organizations may actively occur to prepare for QS transition. Organizations may or may not start their preparations depending on their organization's risk appetite. Some organizations that are part of a steering committee and working groups for QS transition may participate in the testing environment. Other organizations may continue to follow up on the progress of the testing results. The first discontinuity for Stage 3 is *the availability of selected QS cryptographic solutions validated through testing*. By assessing the suitability, functionality, and resilience of potential QS cryptographic solutions, organizations that rely on vendors and third-party providers for hardware and software may gain a clearer understanding of their requirements for future applications and use cases**.** However, it is crucial that organizations finalize their assessments of their existing infrastructures to understand the risk, readiness, and impact of QS transition. Without having the knowledge of their vulnerabilities, it would be difficult for organizations to identify which of their business processes need to be prioritized. Another discontinuity is *the development of policies and regulations that support QS transition.* During this stage, organizations at the ecosystem level may develop policies and regulations to provide legal mandates and additional compliance related to PQC standards. While policy and regulations may be non-sector specific, some clarifications may be provided to align regulatory requirements and what is expected in organizations to avoid last-minute transitions.

Stage 4: QS Implementation

Stage 4 of the growth model is known as *QS implementation stage.* At Stage 4, organizations may actively start taking transition initiatives and execute the

transitions that they have carefully planned. Organizations that were waiting for guidance on transitions from the inter-organizational level and the available QS technologies may implement QS cryptographic solutions to protect their most important assets. During this stage, organizations that have not already done so should actively identify the functional and non-functional requirements in their existing infrastructures for QS cryptographic solutions. Organizations may further seek resources, training & expertise to coordinate their transitions with various stakeholders. From the selected list of QS cryptographic solutions validated through testing, it is crucial that the hardware and software that can run these cryptographic solutions are ready and available at this stage. The discontinuity for Stage 4 is *the availability of selected QS cryptographic solutions in Hardware Security Module (HSM) & Certificate Issuance software.* Without the availability of QS hardware and software, organizations cannot implement QS cryptographic solutions in their existing infrastructures. As QS technology evolves, more products and services may be available for organizations to implement QS cryptographic solutions in their existing infrastructures. To avoid fragmentation and issues related to interoperability and backward compatibility, organizations may start their implementation on a small scale and coordinate their transition timing with their service providers (e.g., CAs).

Stage 5: QS Adaptation

Stage 5 of the growth model is known as *QS adaptation stage*. Once implementing QS cryptographic solutions on a small scale has taken place successfully, the organization may continue with a full-scale transition to implement QS cryptographic solutions across systems, services, and products. One discontinuity for Stage 5 is *the lessons learned and best practices from the implementation of QS cryptographic solutions.* During this stage, the shared knowledge from transitions is needed to support organizations as they integrate QS cryptographic solutions into a wide variety of applications and complete a full-scale transition in the existing infrastructure. Another discontinuity for Stage 5 is *the establishment of cross-organizational coordination mechanisms for QS cryptographic solutions.* By establishing cross-organizational coordination mechanisms, early pilots and implementation efforts in organizations at the previous stages do not remain isolated and can be followed through consistent adoption. Since QS transition requires cross-organizational efforts, organizations need to align stakeholders and resources, maintain interoperability, and monitor changes in the QS cryptographic solutions. For organizations at the inter-organizational and intra-organizational levels, this allows organizations to work towards a seamless transition with coordinated efforts

and avoid starting from scratch with no carryover. It is during this stage that organizations adopt QS cryptographic solutions in a scaled environment across all systems. Due to the nature of evolving security threats and challenges, it is crucial for organizations to stay up-to-date with changes that occur in the ecosystem and further develop highly adaptive security strategies in their systems.

6.4 Quantum-safe Transition Capabilities

Section 6.4 introduces QS transition capabilities across organizations. By navigating the discontinuities in the ecosystem and taking actionable steps, uncertainties may be reduced for the QS transition. Section 6.4.1 discusses actions needed across organizations to move from one stage to the next. The sector further introduces the term QS transition capabilities to highlight dynamic capabilities that organizations may need in order to execute actions and achieve long-term growth towards quantum-safety. Section 6.4.2 discusses the scope of influence across organizations at different levels (e.g., ecosystem level, inter-organizational level, and intra-organizational level) and discusses the process of *growth by learning* and *learning by growth* that are recursive and multi-level, where organizations across different levels co-evolve to collectively achieve quantum-safety.

6.4.1 Actions Needed Across Organizations

This section discusses actions needed across organizations at each stage of the growth model for QS transition.

Through the iterative process and synthesizing the results of workshops, the list of key actions that can address QS transition challenges has been identified. While organizations have different levels of resources, risk appetite, and timelines for QS transition, an overview of different actions needed at the inter-organizational level and intra-organization level shows that QS transition remains complex, and organizations cannot grow towards QS in silos. By understanding the scope of QS transition and what different organizations can do, organizations may need to take action and carefully prepare for QS transition while navigating the changes in the ecosystem. Table 15 shows an overview of discontinuities in 5 stages and actions at the inter-organizational level and intra-organizational level. Actions needed across organizations per stage for QS transition are described below.

Stage 1

As organizations stay up-to-date with the finalized list of PQC standardization, several actions are needed across organizations. For organizations at the inter-organizational levels, it may be crucial to participate in discussions on QS cryptographic solutions with industry, academia, and government. From joining working groups and collaborating in public-private partnerships to discussing guidelines and industry-wide standards and supporting research projects and labs through funding, organizations can be directly and indirectly involved in research on QS cryptographic solutions. For organizations at the intra-organizational levels, the announcement from the NIST not only signals organizations to start considering PQC as an option to implement in the existing infrastructures, but also to raise awareness on the topic of QS transition. At stage 1, organizations need to raise awareness on the importance of implementing QS cryptographic solutions. While recognizing the challenges posed by quantum threats, organizations also need to focus on the opportunities that QS transition may bring to safeguard the existing infrastructures. For organizations, communicating the importance of QS transition across departments and the management level is seen as the crucial first step in ensuring timely preparation for the QS transition.

Stage 2

There are several actions needed across organizations. Organizations at the inter-organizational level, as well as organizations that operate and manage critical infrastructures at a national level, need to actively take the initiative to address QS governance. By defining clear roles, responsibilities, and decision-making structures, organizations may need to participate in a steering committee and working groups at a national level to discuss the direction and the need for QS transition. These may also lead to organizations joining forces across and within sectors to share knowledge and insights on implementing and adopting QS cryptographic solutions. In order to address the technical uncertainties for QS transition, organizations may need to establish a testing environment to validate the list of potential QS cryptographic solutions. On the one hand, organizations that have enough resources and knowledge may test and select the potential QS cryptographic algorithms in their own internal labs. On the other hand, organizations may come together and form public-private partnerships to establish a testing environment with multiple stakeholders. For organizations at the intra-organizational level, they may stay up-to-date with the testing process. While doing so, these organizations also need to conduct an assessment of their existing infrastructures to identify the level of risk,

readiness, and impact for QS transition. Without the knowledge of their cryptographic assets and potential vulnerabilities, organizations cannot identify which of their business processes need to implement QS cryptographic solutions with priority.

Stage 3

There are several actions needed across organizations at Stage 3. Organizations at the inter-organizational level need to develop or buy in certified hardware and software that are suitable for the QS cryptographic solutions that are validated through testing. This may depend on whether organizations develop on their own or rely on third parties for QS hardware and/or software. Although it may not be necessary for all hardware and software to be certified, certifications such as FIPS 140-2/3 (Federal Information Processing Standards), Common criteria (ISO/IEC 15409), ISO 27001, and eIDAS ensure that products and services used for the facilitation of the critical infrastructures comply with industry and national security standards. While frontrunner organizations may follow recommendations at the ecosystem level to voluntarily prepare for QS transition, some organizations may be more hesitant as the management level of the organizations does not see the business opportunity. For these organizations, the development of relevant sector-specific guidelines may ease the discussions in allocating the budget and setting the direction for QS transition. As organizations start their preparation for QS transition, it is crucial to communicate tendering requirements for QS hardware and software that they need in their existing infrastructures. In doing so, organizations not only prepare their infrastructures for long-term resilience but also include their vendors and third-party companies in their transition timeline.

Stage 4

As QS hardware and software become available in the ecosystems at Stage 4, several actions are needed across organizations. For organizations at the inter-organizational level, the facilitation of the expertise center may be needed to share knowledge and skills across organizations. Although the majority of organizations should already be executing their QS transitions at this stage, there may be organizations that are lagging in their transition preparations. For these organizations, it is crucial that the expertise center is available and provides support for the transitions. In addition, CAs that are service providers in facilitating the existing infrastructures need to migrate their non-PQC systems to selected QS cryptographic solutions. It is crucial that CAs migrate their infrastructures before the PKI users to ensure interoperability

and backward compatibility. This allows both CAs and end-user organizations to maintain their business continuity and coordinate QS transition to avoid potential delays and unforeseen disruptions. Organizations at the intra-organizational level need to start migrating their non-PQC part of the systems on a smaller scale with a defined scope. With the available external knowledge and skills from the expertise center, organizations can further address knowledge needs and training to manage QS transition. While the implementation of QS cryptographic solutions is monitored and assessed for their usability and effectiveness, the sector-wide industry best practices and guidelines can support organizations throughout the transition process.

Stage 5

There are several actions needed across organizations. For organizations at the inter-organizational level, collaboration across sectors is needed to coordinate adaptive responses and address evolving security threats and challenges. Organizations may build on lessons learned, foster innovation and development via joint projects and initiatives, and align policies and standards to reflect best practices. Organizations may further share knowledge and experience within and across sectors. For organizations at the intra-organizational level, organizations need to finalize the adoption of QS cryptographic solutions in a scaled environment across all systems. The implementation and adoption process in the existing infrastructures is expected to be iterative and time-consuming. At Stage 5, it would be inevitable for organizations to monitor, adapt, and adjust security practices based on new insights, regulatory changes, and technological changes. By monitoring uncertainties and potential threats, organizations may adjust strategies and ensure that responses remain relevant and timely. With the lessons learned and best practices available, organizations can maintain a continuous dialogue with their stakeholders and enable rapid adaptation to change. In doing so, organizations may continue to improve their security strategies and stay up-to-date with new cryptographic algorithms, protocols, and technologies.

Table 15. Actions Needed in Organizations for QS Transition

Stage	Level	Actions Needed Across Organizations
1	Inter-org.	-Participate in discussions on QS cryptographic solutions across industry, academia and government
	Intra-org.	-Raise awareness on the importance of QS transition & the complexities in implementing QS cryptographic solutions

2	Inter-org.	-Define clear roles, responsibilities and decision-making structure for QS governance via. a steering committee & working groups -Establish a testing environment to test & select suitable QS standards
	Intra-org.	-Conduct assessments to identify the level of risk, readiness, & impact for QS transition
3	Inter-org.	-Develop hardware and software that are suitable with QS cryptographic solutions -Develop relevant sector-wide guidelines that support QS transition
	Intra-org.	-Communicate tendering requirements for QS products and services (e.g., hardware and software using QS cryptographic solutions)
4	Inter-org.	-Migrate non-PQC systems of CAs to selected QS cryptographic solutions -Facilitate expertise center for QS transition to share knowledge and skills needed for QS transition
	Intra-org.	-Modify non-PQC part of the existing systems in a smaller scale with QS cryptographic solutions -Provide training and support to ensure that QS transition is managed with necessary skills and expertise
5	Inter-org.	-Foster collaboration across sectors on future research, development and standard setting to address evolving security threats and challenges
	Intra-org.	-Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems -Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technological changes

QS Transition Capabilities

The stages of growth model are useful in navigating the development and guiding organizations to navigate discontinuities as a set of necessary conditions that must be met at each stage. While the list of discontinuities signals changes occurring in the ecosystem, organizations may need to prepare and execute actions to move with the ecosystem. Thus, an organization may need to develop dynamic capabilities to evolve and ensure long-term growth in a rapidly changing environment. The dynamic capabilities refer to the ability to build upon existing capabilities and develop new capabilities (Teece, 2007, 2014, 2018). In doing so, dynamic capabilities provide a competitive advantage in addressing the actions to do the right things.

With capabilities of sensing, seizing, and transforming, the strategy of the organization as a whole becomes reinforced, and organizational structures and resources sustain long-term advantage (Teece, 2007, 2018). First, sensing capabilities allow an organization to identify opportunities and threats in its external environment. Second, seizing capabilities provides the organization with the ability to capture value from identified opportunities and threats so that insights can be put into action. Third, transforming capabilities reconfigure assets to renew and enhance

its resources, structures, and processes to ensure that over time the organization adapts to the changes in the external environment. Thus, it is crucial for organizations to sustain themselves and achieve growth to continuously evolve with the uncertainties that occur outside of organizations.

For QS transition, organizations may gradually change at each stage to implement QS cryptographic solutions in their existing infrastructures. Since organizations cannot achieve quantum safety in silos, organizations need to not only navigate the changes in the ecosystem but also develop new capabilities that may enable organizations to execute the actions needed. As capabilities at the previous stage are further improved and substituted with new capabilities for the next stage, dynamic capabilities may allow organizations to move from one stage to the next. With a layered view of the growth model, the dynamic capabilities required at different stages are identified at both the inter-organizational level and intra-organizational level, as organizations across different levels may need to take part in QS transition.

In this research, dynamic capabilities are further termed as QS transition capabilities to better indicate capabilities that organizations may develop in order to execute actions needed to grow towards QS. Throughout the five stages, QS transition capabilities allow different organizations to execute actions for QS transition. While organizations at the inter-organizational level may need a set of capabilities as they operate and provide products and services within the ecosystem, organizations at the intra-organizational level may focus on the set of capabilities that correspond to the actions they may need to execute internally and further take part in transition efforts. Table 16 shows the list of QS transition capabilities across different organizations, which are categorized into three capabilities: sensing, seizing, and transforming.

QS Transition Capabilities: Sensing

By detecting opportunities and assessing threats, organizations with sensing capabilities can recognize the need for QS transition. The list of QS transition capabilities needed at Stage 1 is an ability to engage and discuss the development of QS cryptographic solutions across industry, academia, and government, and at the inter-organizational level, and an ability to raise awareness and align stakeholders to implement QS cryptographic solutions at the intra-organizational level. At Stage 2, organizations at the inter-organizational level need to develop an ability to establish a national QS governance framework and an ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms. For an

organization at the intra-organization level, the ability to assess evolving risks, readiness, and the impact of quantum threats on the organization's business processes needs to be developed.

QS Transition Capabilities: Seizing

Organizations with seizing capabilities can mobilize resources to capture value from identified opportunities and respond to threats. By making decisions and selecting strategies, organizations can convert insights into actions towards addressing security needs to implement QS cryptographic solutions. At the inter-organizational level, the list of QS transition capabilities that need to be developed at Stage 3 includes an ability to integrate QS cryptographic solutions validated through testing into certified hardware and software, and an ability to create and update sectoral guidelines to support QS transition. At the intra-organizational level, organizations need to develop an ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition.

At Stage 4, organizations at the inter-organization level need to develop an ability to modify existing systems with QS cryptographic solutions and an ability to facilitate cross-organizational knowledge sharing & skill development for QS transition. For organizations at the intra-organizational level, QS transition capabilities, such as the ability to implement QS cryptographic solutions in a small-scale environment before deployment, and the ability to upskill employees and share knowledge across departments to manage the implementation of QS cryptographic solutions, need to be developed. In doing so, organizations can make decisions to allocate their resources and plan out their strategies as uncertainties regarding QS transition may require organizations to take action in rapidly changing external environments.

QS Transition Capabilities: Transforming

As organizations strive to maintain competitiveness through protecting and reconfiguring their intangible and tangible assets, transforming capabilities allow organizations to sustain growth and support under continuous renewal of structures and resources. Organizations across the ecosystem need to stay aligned and evolve together to collectively achieve quantum safety. At Stage 5, organizations at the inter-organizational level need to develop an ability to coordinate cross-sectoral adaptive responses to address evolving security threats and challenges. For an organization at the intra-organizational level, the ability to integrate QS cryptographic solutions in a scaled environment across all systems, and the ability

to monitor, adapt, and adjust security practices to changes in the external environment are needed as QS transition capabilities.

Since critical infrastructures such as PKI are facilitated with multiple organizations, the list of QS transition capabilities from Stage 1 to Stage 5 of the growth model, which are categorized into sensing, seizing, and transforming, shows what capabilities may be needed across organizations at the inter-organizational level and intra-organization level. By scanning the environment they are in, assessing the threats posed by quantum computing technology, organizations may need to take actions that can translate into strategies and respond to the need to stay secure and compliant. This not only addresses security challenges in the quantum era but also improves security postures to maintain their strategic fit over time.

Table 16. Categorized List of QS Transition Capabilities

Category	Stage	Level	QS Transition Capabilities
Sensing	1	Inter-org.	-The ability to engage and discuss the development of QS cryptographic solutions across industry, academia and government
		Intra-org.	-The ability to raise awareness and align stakeholders to implement QS cryptographic solutions
	2	Inter-org.	-The ability to establish a national QS governance framework -The ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms
		Intra-org.	-The ability to assess evolving risks & impact of quantum threats on the organization's business processes
Seizing	3	Inter-org.	-The ability to integrate QS cryptographic solutions validated through testing into certified hardware and software -The ability to create and update sectoral guidelines to support QS transition
		Intra-org.	-The ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition.
	4	Inter-org.	-The ability to modify existing systems with QS cryptographic solutions -The ability to facilitate cross-organizational knowledge sharing & skill development for QS transition
		Intra-org.	-The ability to implement QS cryptographic solutions in a small-scale environment before deployment -The ability to upskill employees and share knowledge across departments to manage the implementation of QS cryptographic solutions
Transforming	5	Inter-org.	-The ability to coordinate cross-sectoral adaptive responses to address evolving security threats and challenges

		Intra-org.	-The ability to integrate QS cryptographic solutions in a scaled environment across all systems -The ability to monitor, adapt, and adjust security practices to changes in the external environment

6.4.2 Scope of Influence: Interdependencies Across Organizations

The stages of growth model for QS transition shows the scope of influences that may occur between organizations at the ecosystem, inter-organizational, and intra-organizational levels. Various organizations may influence, coordinate, and interact in such a way that organizations at different levels can work towards implementing QS cryptographic solutions. Organizations that are at the inter-organizational levels and the national governments can influence and be influenced by regulatory bodies that govern across the EU (e.g., Regulations on GDPR, eIDAS, NIS 2 directives, and Cyber Resilience Act etc.). As multiple initiatives unfold in the national context, the European Commission has recently published a recommendation on a coordinated implementation roadmap for the PQC transition (European Commission, 2024). The document aims to facilitate the PQC transition of EU Member States, encouraging them to take appropriate measures to secure digital infrastructure and other critical infrastructures. This recommendation calls for the establishment of the NIS Cooperation Group, including representatives of national security agencies and cybersecurity experts, national cybersecurity authorities, and ENISA (European Commission, 2024). This may signal organizations at different levels that appropriate measures are needed in defining and coordinating QS transition and roadmap for PQC implementation.

As one of the EU Member States, the Netherlands may also introduce changes and decisions in the policies and Dutch laws that may help organizations at the inter-organizational and intra-organizational level to start their preparation for QS transition. The current national laws, such as the Dutch Implementation Act, Digital Government Act, Financial Supervision Act, and Telecommunication Act, show how organizations across different sectors in the Netherlands follow policies and regulations to maintain the integrity of critical infrastructures and prevent potential security risks. The regulatory authorities from the ecosystem level, such as ICTU and ENISA, may take part in setting the requirements and regulating the preparatory process for the secure transition of the existing infrastructures. At a national level, regulatory organizations that govern across sectors such as RDI and AFM may also play a role in preparing organizations to follow the industry-wide standards and best practices. In the context of the Dutch national public sector, decisions made at the ecosystem level can influence organizations at the inter-

organizational level, such as ministries that operate across sectors and facilitate critical infrastructures. Across Dutch ministries (e.g., BZK, DEF, EZK, FIN, JenV, lenW, and VWS), each ministry has its own internal process and may need to discuss the proposed changes within its scope, as well as coordinate with relevant suppliers and service providers (e.g., hardware vendors and software companies) it relies on.

Since implementing and adopting PQC-based QS solutions in existing infrastructures requires the availability of QS solutions, organizations may need to monitor the development of QS solutions and verify whether they have been tested. While the list of PQC standards from NIST may influence ETSI and other standardization bodies at the ecosystem level, it may also influence frontrunner organizations at both the inter-organizational level and the organizational level that are looking to start preparing for QS transition. Likewise, the development of QS technology in both the ecosystem level (e.g., big tech companies such as Google, IBM, Microsoft, Mozilla, etc.), startups, and knowledge institutions may influence or be influenced by hardware vendors and software companies that provide the services and products to secure the facilitation of the existing infrastructures. These organizations may also engage in building testing beds for QS solutions and may take part in knowledge sharing across sectors. Organizations that are end-users may be dependent on changes that have been made across sectors and within sectors at the inter-organizational levels due to the possibilities of interoperability and backward compatibility issues. Thus, it may be crucial for organizations that depend on other organizations to navigate the availability of QS technology and follow up with their stakeholders at the inter-organizational level.

Process of Growth by Learning & Learning by Growth

The stages of growth model further discuss the importance of the process of *Growth by Learning* and *Learning by Growth.* In the context of QS transition, applying a big-bang approach may not be possible for QS transition due to multiple interdependencies that organizations rely on. From the list of standardization based on Post-Quantum Cryptography (PQC), the NIST IR 8547 initial public draft to the EU-wide proposal on QS transition, organizations may need to monitor and navigate changes in both technology and governance with multiple stakeholders. As previously described in Section 6.3, there are discontinuities at different stages in the growth model, and various organizations between the ecosystem level, inter-organizational level, and intra-organization level may need to be involved in QS transition. As a result, moving from one stage to the next may require organizations to continuously learn and grow. Through recursive and multi-level learning and

growing processes, organizations across different levels are not at odds but co-evolve to collectively achieve quantum-safety. The process of *Growth by Learning* and *Learning by Growth* is illustrated in Figure 23 and further explained below.

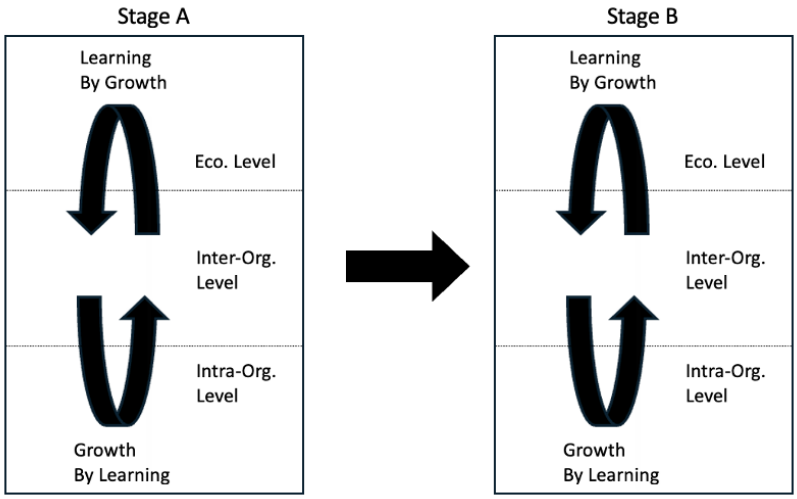


Figure 23. Process of Learning by Growth & Growth by Learning

On the one hand, the process of *Growth by Learning* emphasizes that organizations adapt to the changing environment by gaining knowledge and strategies. While maintaining technical interoperability & backward compatibility remain important, uncertainties may hinder organizations from planning and executing QS transition. Without the knowledge and understanding of the changing environment, organizations may face risks in meeting the appropriate compliance, strategy, and operational aspects of the existing infrastructures. The learning process allows organizations to better navigate and manage themselves in their transition processes. While the discontinuities for QS transition enable organizations to take further actions, organizations may learn from the process and grow to the next stage. As the selected QS solutions are validated through testing, QS technology in hardware and software may become available for organizations to implement in their existing infrastructure. However, it is crucial that organizations assess their infrastructures and learn which areas are critical. Without this knowledge, organizations may not know which critical areas need to be changed or what kind of QS solutions may be suitable in their existing infrastructures. It would be difficult for organizations to carefully plan and move their existing infrastructures swiftly, even if the

discontinuities occur, for the organization to move to the next stage in the QS transition.

On the other hand, the process of *Learning by Growth* emphasizes that organizations gain knowledge and refined strategies by growing. The changing environment is inevitable for QS transition, and organizations may encounter challenges, opportunities, and experiences as they grow from one stage to the next. In order to move their existing infrastructures, organizations may find that growth in this stage acts as a catalyst for further learning. Since multiple organizations need to be part of QS transition, the acquired knowledge and experience from the growth may help organizations involved to better navigate the changing environment. As discontinuities enable the necessary conditions to transition between stages and challenges that were initially hindered organizations are addressed, organizations may navigate their transition processes and respond to the changing market, technology, and regulations. The lessons learned from the growth provide practical insights and may provide internal knowledge for organizations to further prepare for the next stages. In doing so, the growth contributes to continuous learning and fosters innovation in organizations and further learning activities such as training programs and workshops. Organizations may continue to improve their future decision-making and strategic planning to grow to the next stage towards achieving quantum-safety.

In each stage, the process of *Growth by Learning* and *Learning by Growth* may need to occur simultaneously across organizations at different levels. Although the process may vary from one organization to another, such a process is necessary for organizations to carefully prepare and plan to collectively achieve quantum-safety. For public organizations, the existing infrastructures not only depend on other organizations, but also provide products and services to large numbers of different users, including individuals, businesses, and other government agencies. Thus, the existing infrastructures need to safeguard the public interest and remain flexible, secure, scalable, and reliable (Janssen et al., 2009). Due to the multiple uncertainties, the process allows organizations to act in accordance with the changing environment. In doing so, organizations may minimize their risks of being too slow or too fast in their transition process. With the process of *Growth by Learning* and Learning by Growth, organizations may not only navigate the changing market, technology, and regulation for QS transition but also carefully prepare for actionable steps from one stage to the next in accordance with the changes in the ecosystem.

6.5 Chapter Conclusion

The first part of the chapter explains the development of the growth model and introduces five stages of growth model for QS transition, answering sub-question 2 *"What are the different stages in the growth model and discontinuities for QS PKI systems?"*. By using the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach, different stages of the model were derived to systematically prioritize transition challenges in a hierarchical structural model. The results showed that organizations cannot achieve QS transition alone and that it is crucial to navigate changes in the ecosystem in order to collectively move to QS. As organizations grow in stages, the discontinuities represent necessary conditions that must be met in the ecosystem. They represent boundary markers and set the stage for the next phase of growth, enabling organizations to transition from one stage to the next.

The growth model for QS transition has five stages, including Stage 1 QS awareness, Stage 2 QS assessment, Stage 3 QS preparation, Stage 4 QS implementation, and Stage 5 QS adaptation. The discontinuities per stage are as follows: In Stage 1, *the acknowledgement of systematic risks and vulnerabilities of quantum threat,* and *a finalized list of PQC standards*. In Stage 2, *the establishment of a steering committee and (international) working groups for QS transition,* and *the establishment of a testing environment for QS cryptographic solutions.* In Stage 3, *the development of policies & regulations that support QS transition*, and *the availability of selected QS cryptographic solutions validated through testing*. In Stage 4, *the availability of QS cryptographic solutions in HSM & Certificate Issuance software (CAs)*. In Stage 5, *the availability of lessons learned and best practices from the Implementation of QS cryptographic solutions,* and *the development of a cross-organizational coordination mechanism for QS cryptographic solutions.*

The second part of the chapter answers sub-question 3, *"What transition capabilities are needed across organizations for QS PKI systems?"*. The transition capabilities are identified through actions needed in organizations at the inter-organizational and intra-organizational levels. For organizations at the inter-organization level, QS transition capabilities are as follows: At Stage 1, an ability to engage and discuss the development of QS cryptographic solutions across industry, academia, and government. At Stage 2, an ability to establish a national QS governance framework and an ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms. At Stage 3, an ability to integrate QS cryptographic solutions validated through testing into certified hardware and

software, and an ability to create and update sectoral guidelines to support QS transition. At stage 4, an ability to modify existing systems with QS cryptographic solutions and an ability to facilitate cross-organizational knowledge sharing & skill development for QS transition. At Stage 5, an ability to coordinate cross-sectoral adaptive responses to address evolving security threats.

For organizations at the intra-organization level, QS transition capabilities are as follows: At Stage 1, an ability to raise awareness and align stakeholders to implement QS cryptographic solution. At Stage 2, an ability to assess evolving risks & impact of quantum threats on the organization's business processes needs to be developed. At Stage 3, an ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition. At Stage 4, an ability to implement QS cryptographic solutions in a small-scale environment before deployment, and an ability to upskill employees and share knowledge across departments to manage the implementation of QS cryptographic solutions. At Stage 5, the ability to integrate QS cryptographic solutions at scale, and the ability to monitor, adapt, and adjust to changes in the external environment.

Based on Teece (2016), the list of transition capabilities in different stages uses the categorization of *sensing, seizing, and transforming*. This is because organizations not only need to navigate discontinuities in the ecosystem but also develop these transition capabilities to move with the ecosystem. Without these transition capabilities, it may be difficult for organizations to maintain a competitive advantage in the evolving security landscape and ensure long-term growth. The transition capabilities at Stage 1 and Stage 2 are categorized as *Sensing* capabilities that detect opportunities and assess threats. The transition capabilities at Stage 3 and Stage 4 are categorized as *Seizing* capabilities that mobilize resources to capture value from identified opportunities and respond to threats. The transition capabilities at Stage 5 are categorized as *Transforming* capabilities that maintain competitiveness through protecting and reconfiguring their intangible and tangible assets.

The chapter also emphasizes the importance of the process of *Growth by Learning* and *Learning by Growth.* In each stage, the process of *Growth by Learning* and *Learning by Growth* may need to occur simultaneously across organizations at different levels. Although the process may vary from one organization to another, the results show that such a process of growth and learning is necessary for organizations to carefully prepare for actionable steps in accordance with the changes in the ecosystem. The learning process allows organizations to better navigate and manage themselves in their transition processes. Through recursive and

multi-level learning and growth processes, organizations across different levels are not at odds but co-evolve to collectively achieve quantum safety. In doing so, organizations may minimize their risks of being too slow or too fast in their transition process.

Chapter 7 Evaluation

7.1 Introduction

This chapter evaluates the stages of growth model for QS transition and answers Research Question 4: "*To what extent is the growth model for QS transition relevant and useful for organizations?* The developed stages of the growth model do not aim to describe what is known but rather serve as a forward-looking tool that can guide organizations through periods of uncertainty and transformation. Thus, relevance and usefulness are two dimensions that are focused on in this chapter to evaluate the stages of the growth model. The relevance of the growth model was assessed to determine whether the model captures the relevant key socio-technical challenges of the current situation and provides actionable guidance for QS transition. The usefulness of the growth model is assessed to determine whether the growth model aligns with the needs of experts and practitioners and can serve as a useful tool for organizations to transition towards QS. Section 7.2 outlines the evaluation approach used to assess the relevance and usefulness of the growth model for organizations. Section 7.3 synthesizes the results obtained from evaluating the growth model and highlights the findings for the QS transition moving forward. The chapter concludes in Section 7.4 and provides a passage leading to the final chapter, where the conclusions and further research directions of the research are drawn.

7.2 Evaluation Approach

This section outlines the evaluation approach used to assess the relevance and usefulness of the growth model for QS transition. Section 7.2.1 discusses the purpose of evaluating the relevance and usefulness of the model. Section 7.2.2 describes how the evaluation of the relevance and usefulness of the growth model was conducted and analyzed.

7.2.1 Evaluation of Stages of Growth Model: Relevance & Usefulness

With the insights gathered from both literature and practice, the stages of growth model serve as a forward-looking tool. Since there is no ready-to-use growth model for organizations looking to transition to a QS future, the developed growth model in the context of QS transition is intended to extend knowledge on how critical infrastructures that depend on PKI can become QS. The focus of the growth model is on the use by organizations that have limited knowledge of the technical infrastructures and complexities in becoming QS. By simplifying the process of QS transition into a series of stages, the growth model takes an *ecosystem perspective,*

recognizing complex interdependencies that exist between different organizations, and provides actionable guidance for organizations looking to transition their PKI systems.

Moreover, the stages of growth models are inherently prescriptive and are oriented toward shaping direction for the future with yet-to-be-realized conditions. It is developed not to describe what is known, but to guide organizations through periods of uncertainty and transformation. Since QS transition that the model aims to support has not yet been crystallized, outcome-based validation is neither possible nor appropriate at this stage. The evaluation does not attempt to validate future outcomes but instead seeks to assess the relevance of the model from the details presented and assess the potential for the practical usefulness of the model. The first part of the evaluation assessed whether the model captures the relevant key socio-technical challenges and actionable guidance needed for QS transition. The second part of the evaluation assesses whether the growth model aligns with the needs of experts and practitioners and can serve as a useful tool for organizations.

By evaluating the *relevance*, experts and intended users can assess whether the growth model reflects the context of QS transition and resonates with real-world challenges that it is intended to serve. According to Saracevic (2007), relevance is multi-dimensional, user-dependent, and requires evaluating different attributes such as cognitive, situational, and affective. What is relevant or not can be subjective, since for one stakeholder it may be relevant while for others it may not be. Likewise, Schamber et al (1990) and Barry & Schamber (1998) state that there are multiple and situational criteria where user needs, tasks, and situational context need to be assessed. Mizzaro (1998) and Cosjin & Ingwersen (2000) discuss different dimensions, such as topical, cognitive, and situational components. Since the topic of relevance varies depending on the context, user needs, and goals of the model, a tailored evaluation with multiple criteria seemed useful when assessing the relevance. In doing so, the evaluation provides a fuller picture of the growth model and room for target improvements. Table 17 shows four key dimensions of relevance applied to the evaluation of a growth model.

Table 17. Four Key Dimensions Used to Evaluate Relevance

Dimension	Description	Applied to the Evaluation	Literature
Contextual Relevance	Is the content appropriate for the specific situation?	To what extent is the action essential at the following stage?	Saracevic (2007), Cosjin & Ingwersen (2000), Schamber et al (1990)

Topical Relevance	Does the content address the specific need expressed?	How well does this action address your organization's needs?	Saraceviv (2007), Mizzaro (1998)
Cognitive Relevance	Does the content support the intended users?	To what extent do you believe this action contributes to the growth in becoming a QS?	Saracevic (2007), Cosjin & Ingwersen (2000), Barry & Schamber (1998), Mizzaro (1998)
Actionability	Is the content timely and practical for the intended user?	How actionable is this action at this stage?"	Cosjin & Ingwersen (2000), Barry & Schamber (1998), Mizzaro (1998)

On the other hand, *usefulness* is assessed to provide insights on how to further facilitate the acceptance of the model (Taherdoost, 2017). By evaluating usefulness, experts and intended users can assess whether the growth model can be accepted and integrated to be used by practitioners. With a framework such as the Technology Acceptance Model (TAM), more insights can be gathered with a systematic approach, and it can be checked whether the growth model is assessed accordingly (Davis, 1989; Marangunić & Granić, 2015; O'Dea, 2025). Key constructs of the *Technology Acceptance Model (TAM*) have been used to evaluate the growth model in a structured and systematic way. Table 18 shows key dimensions used to evaluate usefulness using TAM. By understanding the perceived usefulness, perceived ease of use, attitude towards use, and behavioral intention to use, the evaluation can clarify whether the growth model could be accepted in practice. Since the growth model is at its early stage, evaluating the usefulness is ideal for the model that is intended to provide long-term support as QS transition evolves.

Table 18. Four Key Dimensions Used to Evaluate Usefulness Using TAM

Dimension	Description	Applied to the Evaluation
Perceived Usefulness	Does the model help improve decision-making / strategic planning of the context?	How well does the model align with the current needs of your organization?
Perceived Ease of Use	Is the model easy to understand and usable by those intended to use it?	How easy do you think it will be to use the model within your organization?
Attitude Toward Use	Do users see value in integrating it into their practices?	How useful do you consider this model for addressing your organization's current challenges?
Behavioral Intention to Use	Do users have intention to use the model?	How likely are you to incorporate this model in your work?

7.2.2 Evaluation Process of the Stages of Growth Model

The purpose of the evaluation ensures that the developed stage model is not only informed by research but also shaped by the needs and experiences of practitioners, where feedback is representative of the intended user base. Given the early stage of the growth model and the trajectories of QS transition, it was crucial to gather experts and practitioners who could provide multiple perspectives and insights to assess the relevance and usefulness of the growth model. We opted for using a workshop and interviews to evaluate the relevance and usefulness of the stages of growth models. In this research, only one workshop was organized due to the lack of experts and practitioners in the field of QS transition who are affiliated with the public sector. The list of 12 participants in the workshop is shown in Table 19.

Table 19. List of Participants in the Workshop

#	Role	Organization	Perspective
1	Program Manager	Government Agencies	Regulatory Organization & PKI user
2	Change Manager	Government Agencies	Regulatory Organization & PKI user
3	CISO	Government Agencies	Regulatory Organization & PKI user
4	Cybersecurity Advisor	Government Agencies	Regulatory Organization & PKI user
5	Policy Advisor	Government Agencies	Regulatory Organization & PKI user
6	Policy Advisor	Government Agencies	Regulatory Organization & PKI user
7	Innovation Manager	Government Agencies	Regulatory Organization & PKI user
8	Policy Advisor	Government Agencies	PKI user
9	Quantum Security Specialist	Government Agencies	PKI user
10	Cybersecurity Advisor	Government Agencies	PKI user
11	Researcher	Research Institutes	External Expert
12	Researcher	Research Institutes	External Expert

In addition to the workshops, interviews were conducted which enabled the inclusion of all perspectives. Table 20 shows the evaluation workshop and interviews conducted**.** While the workshop provided opportunities for multiple participants to share their diverse perspectives and capture insights into the ecosystem aspects of the growth model and QS transition, interviews allowed for deeper insights into the QS transition in the PKI systems. Based on participants' availabilities and relevant knowledge and experience with PKIs in the Netherlands, we used purposive sampling to invite the participants to the workshop and interviews. Various experts and practitioners affiliated with the public sector were invited from government agencies, service providers, and research institutes.

Table 20. List of Evaluation Workshop & Interviews

#	Methods	Organization	Perspective	Date Conducted
1	Workshop	Government Agencies/Research Institutes	Regulatory Organization & PKI user	12/03/2025
2	Interview	Government Agencies/ Service Providers	CAs	19/03/2025
3	Interview	Government Agencies	PKI user	28/03/2025
4	Interview	Government Agencies	Regulatory Organization	03/04/2025

The workshop lasted 120 minutes, and the interviews lasted 90 minutes. While the evaluation Workshop was held in person, semi-structured interviews were held online using Teams and Webex due to the availability of the participants. Both the workshop and interviews began with a 15-minute presentation about the stages of growth model, the theoretical foundation, the intended purpose, and the details of each stage. The participants of the workshop and interviews were guided through different stages of growth model for QS transition. As per the stage, the discontinuities and actions needed across organizations were discussed. To minimize the response bias, another researcher was present at the workshop, and additional interviews were held to triangulate data obtained from the workshop. The insights gathered on the relevance and usefulness of the stages of growth model for QS transition were gathered. The evaluation process included expert feedback to assess relevance and used the Technology Acceptance Model (TAM) framework to assess the potential usefulness of the growth model in practice. While the expert feedback provided deeper insights on the topic of QS transition and the TAM framework, it allowed practitioners to assess the perceived practical implications of the model. To assess the relevance and usefulness of the growth model, an evaluation was conducted with experts and intended users using Mentimeter during the workshop.

After the presentation of the stages of growth model, participants were asked to provide their feedback using the questions on Mentimeter. For the first part of the evaluation, questions assessing the relevance of the growth model were asked. These included questions in Table 16, e.g., “To what extent is the action essential at the following stage?”, “How well does this action address your organization’s needs?”, “To what extent do you believe this action contributes to the growth in becoming QS?” and “How actionable is this action at this stage?” For the second part of the evaluation, questions assessing the usefulness of the growth model were asked. These included questions in Table 17, such as, “How useful is the model in addressing QS transition challenges?”, “How easy do you think it will be to use the

model within your organization?" "How well does the model align with the current needs of your organization?" and "How likely are you to incorporate this model in your work?". For researchers, the evaluation provides a way to refine the model based on the expert insights and its perceived utility before its integration for use.

Moreover, the primary strengths and primary weaknesses of the growth model were discussed. The participants could select a maximum of two from the multiple choices, which have been derived from the literature based on the stages of growth model theories (explained in Section 4.2). The primary strengths of the growth model included "enhances understanding of complex topics", "practical relevance to real-world situations", "flexibility to adapt to different scenarios", "facilitates collaboration and communication", "encourages multidisciplinary approaches", and "others". The primary weaknesses of the growth model included "an oversimplification of complex issues", "limited applicability to specific contexts", "possibilities in misinterpretation", "difficulties in measuring effectiveness", "difficulty in integrating with existing practices", and "others". Based on the theory of the growth model, the multiple-choice questions have been prepared. By asking about the strengths and weaknesses of the growth model, the questions allow researchers to reflect on the theories used and better understand whether the perceived strengths and weaknesses of the growth model align with the strengths and weaknesses of the growth model presented in the literature.

After the results have been gathered from the evaluation workshops, these have been synthesized to assess the relevance and usefulness of the growth model. The results from the Mentimeter and notes taken during the workshops were used to provide insights from the feedback from the experts and opinions of the intended users. By assessing relevance and usefulness as part of the evaluation, the evaluation may identify not only the model's potential strengths but also the adjustments needed to improve its real-world applicability. The relevance of the growth model was analyzed using four dimensions (e.g., topical relevance, contextual relevance, cognitive relevance, and actionability), and recurring insights have been drawn. The usefulness of the growth model was analyzed using TAM-based questions across four dimensions (e.g., perceived usefulness, perceived ease of use, attitude toward use, and behavioral intention to use). The results have been collected and analyzed to summarize the key insights. The results have been synthesized and cross-validated with researchers to enhance reliability.

7.3 Evaluation Results

This section highlights the results of the evaluation conducted to assess the relevance and usefulness of the growth model for QS transition. Section 7.3.1 presents the results of the evaluation on the relevance of the growth model and shows how well the growth model meets the intended purpose and the context of QS transition. Section 7.3.2 focuses on the results of the evaluation on the usefulness of the growth model and presents how users perceive the growth model using the TAM framework. The results of a five-point scale have been grouped into five categories, indicating low, low-moderate, moderate, moderate-high, and high. By aligning the five points with the five categories of the score, variation of the score is highlighted without the loss of detail. This allows the interpretation of the results to be clearly discussed.

7.3.1 Relevance

Contextual Relevance

For the first part of the evaluation on the relevance of the growth model, contextual relevance has been assessed with the question, "To what extent is the action essential at the following stage?" Table 21 shows the contextual relevance of actions across organizations in different stages.

Table 21. Context Relevance of Actions Across Organizations in Stages

Stage	Code	Actions Needed Across Organizations	Essentiality
1	A1	-Participate in discussion on QS cryptographic solutions with industry, academia and government	Moderate
	A2	-Raise awareness on the importance of implementing QS cryptographic solutions	High
2	A3	-Define clear roles, responsibilities and decision-making structure for QS governance via. a steering committee & working groups	High
	A4	-Facilitate testing environment to test & select suitable QS standards	Moderate-High
	A5	-Conduct assessments to identify the level of risk, readiness, & impact for QS transition	High
3	A6	-Develop certified hardware and software that are suitable with QS cryptographic solutions	High
	A7	-Develop relevant sector-wide guidelines that support QS transition	High
	A8	-Communicate tendering requirements for QS products and services (e.g., hardware and software using QS cryptographic solutions)	Moderate-High
4	A9	-Migrate non-PQC systems of CAs to selected QS cryptographic solutions	High

	A10	-Facilitate an expertise center for QS transition to share knowledge and skills needed for QS transition	Moderate
	A11	-Modify non-PQC part of the existing systems in a smaller scale with QS cryptographic solutions	High
	A12	-Provide training and support to ensure that QS transition is managed with necessary skills and expertise	Moderate-High
5	A13	-Foster collaboration across sectors on future research, development and standard setting to address evolving security threats and challenges	Moderate
	A14	-Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems	High
	A15	-Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes	High

The contextual relevance was evaluated based on the level of essentiality of actions at their respective stage. The results showed that nine actions were considered highly essential which are A2 Raise awareness on the importance of implementing QS cryptographic solutions, A3 Define clear roles, responsibilities and decision-making structure for QS governance, A5 Conduct assessments to identify the level of risk, readiness, & impact for QS transition, A6 Develop certified hardware and software that are suitable with QS cryptographic solutions, A7 Develop relevant sector-wide guidelines that support QS transition, A9 Migrate non-PQC systems of CAs to selected QS cryptographic solutions, A11 Modify non-PQC part of the existing systems in a smaller scale with QS cryptographic solutions, A14 Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems and A15 Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes.

Moreover, three actions demonstrated moderate levels of essentiality. These include actions such as A1 Participate in discussion on QS cryptographic solutions with industry, academia, and government, A10 Facilitate expertise center for QS transition to share knowledge and skills needed for QS transition, and A13 Foster collaboration across sectors on future research, development, and standard setting to address evolving security threats and challenges. Participants saw that not all actions were essential for organizations at the following stage. For PKI users, these actions depended on their risk appetite, business cases, and whether they had the budget to execute these actions. Without any roadmap or timeline for QS transition, it was uncertain for PKI users to determine whether these actions were essential for them to invest in. One of the participants also stated that, “Participating in discussion for QS cryptographic solutions means various things.” This can refer to attending

conferences, workshops, or even joining the working groups for PQC initiatives. While this was important for some (e.g., Regulatory government and CAs), as it ties closely to their businesses and maintaining security of the public and the entire PKIoverheid, others (e.g., PKI users) saw that such actions would depend on the decisions made by the central level of the government and whether these initiatives closely link to their priorities.

Topical Relevance

For the second part of the evaluation on the relevance of the growth model, topical relevance has been assessed with the question, "How well does this action address your organization's needs?" Table 22 shows the topical relevance of actions across organizations in different stages.

Table 22. Topical Relevance of Actions Across Organizations in Stages

Stage	Code	Actions Needed Across Organizations	Needs
1	A1	-Participate in discussion on QS cryptographic solutions with industry, academia and government	Moderate
	A2	-Raise awareness on the importance of implementing QS cryptographic solutions	Moderate-High
2	A3	-Define clear roles, responsibilities and decision-making structure for QS governance via. a steering committee & working groups	Moderate-High
	A4	-Establish a testing environment to test & select suitable QS standards	Moderate
	A5	-Conduct assessments to identify the level of risk, readiness, & impact for QS transition	High
3	A6	-Develop certified hardware and software that are suitable with QS cryptographic solutions	Moderate
	A7	-Develop relevant sector-wide guidelines that support QS transition	High
	A8	-Communicate tendering requirements for QS products and services (e.g., hardware and software using QS cryptographic solutions)	Moderate-High
4	A9	-Migrate non-PQC systems of CAs to selected QS cryptographic solutions	High
	A10	-Facilitate an expertise center for QS transition to share knowledge and skills needed for QS transition	High
	A11	-Modify non-PQC part of the existing systems in a smaller scale with QS cryptographic solutions	Moderate-High
	A12	-Provide training and support to ensure that QS transition is managed with necessary skills and expertise	Moderate-High
5	A13	-Foster collaboration across sectors on future research, development and standard setting to address evolving security threats and challenges	Moderate-High

	A14	-Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems	High
	A15	-Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes	High

The topical relevance was evaluated based on how well the list of actions aligns with the level of needs within organizations. The results showed six actions that align with a high level of organizational needs. These include A5 Conduct assessments to identify the level of risk, readiness, & impact for QS transition. A7 Develop relevant sector-wide guidelines that support QS transition, A9 Migrate non-PQC systems of CAs to selected QS cryptographic solutions, A10 Facilitate an expertise center for QS transition to share knowledge and skills needed for QS transition A14 Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems and A15 Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes. While CAs and PKI users both saw actions such as A5, A7, A9, and A10 to be directly aligned with current needs that need to be addressed for QS transition, actions such as A14 and A15 were aligned more with long-term organizational needs that organizations should strive towards.

In addition, three actions were aligned with a moderate level of organizational needs. These include A1 Participate in discussion on QS cryptographic solutions with industry, academia, and government, A4 Establish a testing environment to test & select suitable QS standards, and A6 Develop certified hardware and software that are suitable with QS cryptographic solutions. These actions depended on the roles and responsibilities of organizations in the ecosystem. For regulatory organizations and CAs, these actions were a much higher priority than PKI users. For example, one of the participants from the regulatory organization stated that, “Participating in discussion is very crucial, because we need to collaborate and share knowledge. You can’t sit alone on the island”. The participant also commented that, “the availability of hardware and software may not always have to be certified. However, it is important to consider this when your business processes involve highly sensitive information and require high-level resilience.” Other participants who are PKI users shared that, “these actions were not the main responsibility of government agencies, and this is something that need to be discussed at the central level.” Others also added that, “These actions are something that need to be addressed at the EU level as it is highly relevant for fostering the EU market.”

Cognitive Relevance

The third part of the evaluation on the relevance of the growth model assessed cognitive relevance with the question, "To what extent do you believe this action contributes to the growth in becoming a QS? From the list of actions, all actions were considered to have a high level of contribution to the growth towards becoming a QS. The results indicate that there is a high level of cognitive relevance for the list of actions across organizations for QS transition. In addition to the results, some remarks have been made by the participants of the workshops. As the participants unanimously agreed that the list of actions in the growth model contributes to the growth towards becoming QS, three key insights have been shared moving forward with the preparation for QS transition.

Focus on Organizational Aspects of QS transition

Regarding the action, such as A2 Raise awareness on the importance of implementing QS cryptographic solutions, there is a lot of emphasis on the importance of raising awareness right now. However, much of the discussion taking place is purely technical. Recognizing the broader implications of implementing and adopting PQC standards in the existing infrastructures, the participants stated that having perspectives with a focus on the organizational aspects of QS transition is important. With the current security strategies and compliance with NIS 2 directives, organizations may need to raise awareness on the importance of looking into Governance, Risk, and Compliance (GRC) strategies and including topics such as quantum threats and QS transition in their discussion. One of the participants stated that, "A clear explanation is needed at the internal level of the organizations to commit our resources. There is a lot of convincing to do."

Uncertainties Regarding Testing Environment

With a new technology on the horizon that is based on PQC standards, discussion regarding the facilitation of the testing environment still needs to occur. Thus, the action, A4 Establish a testing environment to test and select suitable QS standards, contributes to the growth towards becoming QS. Although the list of standards based on PQC from the NIST has been announced, there are still several clarifications needed. First, what is the testing scope? Is the testing focused on IT scenarios or different use cases? Second, debates on whether testing should be managed centrally or decentralized are not yet clear. Third, there is importance in validating third-party products from the vendors and establishing criteria for vendor testing compliance.

What are the third-party risks involved in QS transition? How can organizations address this? Also, the testing environment comes with chicken and egg discussions as one participant raised a question, “Do we need to secure buy-in before setting up the testing environment? Or can it be obtained afterwards?” These questions revealed uncertainties regarding QS technology and that there are dependencies still existing in the process (e.g., communication, approval, budgeting, and resource allocation). The list of questions showed organizations’ concerns regarding the potential risks involved in QS transition.

Integrate Knowledge Across Organizations on QS transition
Multiple organizations need to be involved, and a coordinated approach is needed to prepare for QS transition. However, the current ecosystem remains fragmented. Thus, actions such as A1 Participate in discussion on QS cryptographic solutions with industry, academia, and government, and A13 Foster collaboration across sectors on future research, development, and standard setting to address evolving security threats and challenges have a significant impact on the growth towards becoming QS. For organizations looking to transition their infrastructures, there are various ways in which they can participate. One of the participants stated that, “Organizations would benefit from streamlining the knowledge. More experience needs to be shared from the lessons learned and best practices from the industry”. Since organizations need to coordinate collective efforts, it would be crucial to create a shared repository or library of knowledge for QS transition. For SMEs, knowledge integration may be needed to further prepare for QS transition due to a lack of resources and knowledge available. For regulatory organizations, collaboration may also extend to the EU level, where member states can share knowledge and the process towards their transitions to PQC. However, differences in efforts and decisions on transition may also be witnessed across the jurisdictions, as different national rules and policies may apply.

Actionability
For the last part of the evaluation on the relevance of the growth model, actionability has been assessed with the question, “How actionable is this action at this stage?” When the question was asked, the results showed that the majority of actions at Stage 1 of the growth model for QS transition scored high on actionability. However, the rest of the actions at later stages of the model, such as Stage 2, Stage 3, Stage 4, and Stage 5, scored low on actionability. The participants highlighted that these actions at the later stages are seen as actionable with a long-term view. Without a clear

timeline for QS transition, it is difficult to indicate high actionability for these actions, as many uncertainties and interdependencies may play a role in preparing these actions for QS transition.

Moreover, participants expressed that some of the actions should already be done at an earlier stage of the growth model. These actions include A5 Conduct assessments to identify the level of risk, readiness, & impact for QS transition, A8 Communicate tendering requirements for QS products and services, and A12 Provide training and support to ensure that QS transition is managed with the necessary skills and expertise. However, these actions also scored low on actionability, indicating that current capabilities in executing these actions may be lacking in organizations. Several key challenges that may hinder executing these actions at earlier stages are discussed, and what organizations may need to do to further prepare for QS transition are further highlighted.

No Regret Moves

In the decision-making literature, the term 'no regret moves' aligns with selecting an option that the decision maker will have the lowest projected regret (Chorus, 2010). Likewise, 'doing nothing' may lead to greater regret in the context of QS transition, as every other option may serve as a reminder of what was missed. Although actions such as *A5 conduct assessment to identify the level of risk, readiness, and impact for QS transition* should already be done at an earlier stage, the maturity level of QS cryptographic solutions is not yet high. Thus, organizations may not be able to grasp the clear scope of the changes needed for QS transition due to low technology readiness. This is even more difficult for organizations that are large and have multiple critical business processes. Without a finalized list of QS cryptographic solutions available from the testing, organizations may decide to just wait for solutions to be ready before taking the necessary actions to prepare for QS transition.

The Dutch PQC Migration Handbook Part II (2024) introduces no-regrets moves for organizations to start their preparation for QS transition. The list of no-regrets moves includes assessing supply chain dependencies, establishing cryptographic asset management, reviewing cryptographic policies, conducting risk assessment, estimating the costs of migration, staying informed on regulatory requirements, providing a backup plan, and collaborating with organizations. The list of no-regret moves indicates that organizations need to fully understand their own systems and what 'crown jewels' they need to protect. There needs to be a discussion on the prioritization of risks. By gaining full knowledge of their

infrastructures, organizations can identify their critical processes and understand the scope of QS transition. In doing so, organizations can better identify and communicate where internal and external collaboration is needed.

(Certified) QS Hardware & Software

For action such as *A8 communicate tendering requirements for QS products and services,* organizations can already discuss requirements for tendering and include the supply chain in the discussion. However, there are a lot of uncertainties regarding whether available hardware and software are suitable for QS cryptographic solutions and whether these products should be certified. At the EU level, Common Criteria (CC) is available as the standard for certifying products related to security (e.g., ISO/IEC 15408), and with a mutual recognition agreement, EU member states can recognize products of each other (e.g., EU-SOG-IS-MRA) and regulate the market. In the Netherlands, AIVD is responsible for approving products for use in government-classified environments (International Organization for Standardization, 2022; SOG-IS Management Committee, 2010).

In the case of PKIoverheid, strict requirements are defined in Trust Service Provider Requirement Assessments for products and providers. The approval from NBV under NCSC is needed for security-related products. Although certification acts as a quality signal and ensures a baseline level of security and interoperability, CC evaluations are time-consuming, and any changes in the products after certification would require re-certification. To move forward, expectations for QS products and services need to be communicated to vendors. For security-critical products in governments and regulated industries, pre-tender negotiations may be needed, and provincial acceptance with conditions may further take place. The supply chain for meeting the demands of QS hardware and software is not yet clear. Participants raised the need for a timeline. While organizations can already start communicating tendering requirements for QS products and services, it was important for industries to provide these products and services.

Training & Supporting Needs

In order to prepare for QS transition in a timely manner, actions such as *A12 provide training and support to ensure that QS transition is managed with the necessary skills and expertise,* which should already be done in the earlier stage of the model. However, the current level of training and support does not provide much guidance on why organizations should commit their resources to QS transition. The lack of awareness of the risks associated with quantum threats also hinders transition efforts

that are much needed in organizations. For example, earlier-mentioned preparation for no-regret moves and communicating with vendors would all require a basic understanding of what to look for, what is missing, and how to go about making decisions. One of the participants stated, “Training should also be done early.” Others stated that, “Support may also vary across organizations, and this would depend on where they are in the process of preparation for QS transition.”

With the ecosystem remaining a strong and a weak link for organizations, the secure facilitation of PKI with QS cryptographic solutions depends on organizations collectively becoming QS. If this is not the case, the infrastructure will not become fully secure, with potential backward compatibility and interoperability issues. Organizations are currently facing a lack of training and support to discuss strategies related to PQC-based QS cryptographic solutions. Some questions were raised, such as, “How do you involve your management and other departments in the process?”, “How do we know which QS cryptographic solutions to choose from?” For many organizations, these gaps in training and knowledge cannot be addressed alone. Thus, it is crucial to stay informed about updates on the development of QS technology and connect with the available expertise center. Organization-wide awareness sessions and easy-to-understand guides are needed to bring together cross-functional departments.

7.3.2 Usefulness (TAM-Based Assessment)

In addition to assessing the relevance of the growth model, participants evaluated the usefulness based on four dimensions from the Technology Acceptance Model (TAM): perceived usefulness, perceived ease of use, attitude toward use, and behavioral intention to use. This section synthesizes those findings to understand how the model is received as a practical tool for decision-making and coordination. For researchers, the evaluation provides a way to refine the model based on the expert insights and its perceived utility before its integration for use. Table 23 shows the results from the evaluation regarding the usefulness of the growth model for QS transition based on TAM.

Table 23. Usefulness of the Growth Model for QS Transition Based on TAM

Dimension	Actions Needed Across Organizations	Usefulness
Perceived Usefulness	How useful is the model in addressing QS transition challenges?	Moderate-High
Perceived Ease of Use	How easy do you think it will be to use the model within your organization?”	Moderate

Attitude Toward Use	How well does the model align with the current needs of your organization?	Moderate
Behavioral Intention to Use	How likely are you to incorporate this model in your work?	Moderate-High

Perceived Usefulness

The perceived usefulness of the growth model has been assessed with the question, "How useful is the model in addressing QS transition challenges?" The results indicate that the growth model is moderate-high level of usefulness in addressing QS transition challenges. The insights from the participants shared that the model provides a high-level overview of discontinuities and actions, which are often fuzzy processes. It may be possible that not all actions need to be followed in the model, and not all conditions are easy to detect. However, the usefulness lies in addressing socio-technical transition challenges and providing the system-level complexity of QS transition. The different stages of the growth model show the discontinuities that organizations need to navigate in the ecosystem and the current stage of the organization. The overview of QS transition allows organizations to think about stages ahead and what preparation may be needed within and across organizations for QS transition. Participants also shared that it would be useful to have examples for each of the actions mentioned in the model.

Perceived Ease of Use

The perceived ease of use of the growth model has been assessed with the question, "How easy do you think it will be to use the model within your organization?" The results show that the growth model is moderately easy to use within the organizations. The comments from both CAs and PKI users stated that the model is flexible to use and can be tailored to different intentions of use. This would depend on the roles of the practitioners using the model. One participant pointed out that "It is important not to confuse the growth model with an implementation plan." Another participant expressed that, "Providing a high-level overview of QS transition has added value for policy officers when thinking ahead about what organizations may need to grow towards being QS." Additionally, the PKI users indicated that expected years for QS transition would help in preparing for QS transition in the coming years. However, it is important to note that, at the time of evaluation, no timeline was made aware in the ecosystem regarding the expected completion date for QS transition.

Attitude Towards Use

The attitude towards the use of the growth model has been assessed with the question, "How well does the model align with the current needs of your organization?" The results indicate that the model moderately aligns with the current needs of organizations. For CAs, the model was highly aligned to the current needs because CAs need to navigate changes in QS technology, regulations, and other business needs. The growth model allows a broader view of different risks and priorities that need to be considered with various stakeholders involved. One of the participants expressed that, "the growth model may be too high level for project managers". For PKI users, many of the decisions for QS transition cannot be made in siloes. However, the model aligns with the needs of organizations to monitor the changes in the ecosystem. For PKI users in the public sector, many decisions need to be made at the central level to clarify directions, and many will follow the lead. Additionally, the participants agreed that the model can be useful for relevant roles within and around organizations dealing with QS transition planning and strategy, including but not limited to practitioners involved in awareness, business continuity, transition planning, and change management.

Behavioral Intention to Use

The behavioral intention to use the growth model has been assessed with the question, "How likely are you to incorporate this model in your work?" The results show a moderately high intention from organizations to incorporate the model in their work. The insights shared indicated that the focus on the ecosystem discussion is important for CAs. This is because many of the critical business processes need conversation with multiple stakeholders. By incorporating the model, organizations can start delegating the responsibility and communicating which stakeholders may need to be involved. With such a wicked problem, having a high-level overview provides the complexity that organizations may face and creates room for discussions. One of the participants stated, "I can use the model for dialogue, communication, and awareness about the huge amount of work that needs to be done". This way, organizations may start thinking about how to prepare for QS transition. The growth model can also be relevant to designing the multi-year transition roadmap that aligns with regulatory frameworks such as NIS 2 directive and the EU Cyber Resilience Act.

Additional questions on the perceived strengths and weaknesses of the growth model reflect the strengths and weaknesses of the growth model presented in the literature. The primary strengths of the growth model selected are "enhances

understanding of complex topics", "facilitates collaboration and communication", and "encourages multidisciplinary approaches". The growth model was assessed as an important tool in creating urgency and awareness. By providing a good overview of transition, the growth model can be used to communicate and coordinate QS transition process within organizations and across organizations. With a broad overview of QS transition, the growth model was considered as a well-rounded model for experts and non-experts to grasp the complexity of achieving quantum safety while recognizing both socio-technical predicaments that organizations need to be mindful of. The growth model allows organizations to identify the current stage they are in and helps them think of next steps when making changes in the dynamic environment of the security landscape.

Moreover, primary weaknesses of the growth model selected are "provides an oversimplification of complex issues", "difficult to integrate with existing practice", and "provides limited applicability to a specific context". The weaknesses that have been addressed from the evaluation of the growth model were inherent in the growth model. While the growth model offers a tailored approach for developing strategies and creating a roadmap for QS transition, the model may not suffice those looking for step-by-step implementation instructions. Organizations that are looking for the next steps in preparing implementation within organizations may gain further insights from other external sources, such as the recently published PQC migration handbook. The details on how to go about the transition planning may differ across organizations. Since the growth model provides a high-level view of QS transition in different stages and transition capabilities needed across organizations, further research may examine step-by-step guidance that organizations can follow for practical implementation.

7.4 Chapter Conclusion

The chapter provided an evaluation process and the evaluation of the stages of growth model for QS transition. With the insights gathered from both literature and practice, the growth model serves as a forward-looking tool that can guide organizations through periods of uncertainty and transformation. Since outcome-based validation is neither possible nor appropriate due to the early stage of QS transition, the evaluation assessed the relevance and usefulness of the model. As part of the evaluation, various experts and practitioners affiliated with the public sector were invited from Dutch ministries, government agencies, and research institutes. Due to the decentralized nature of PKI systems in the Dutch public sector, it was crucial to gather multiple perspectives and insights from experts and practitioners.

In doing so, the evaluation workshops ensured that the growth model is not only informed by research but also shaped by the needs and experiences of practitioners, who are the intended user base. The results from the evaluation of the relevance and usefulness of the growth model answer sub-question 4 *"To what extent is the growth model for QS transition relevant and useful for organizations?"*.

The relevance of the model was assessed using multiple criteria, including contextual relevance, topical relevance, cognitive relevance, and actionability. The results for contextual relevance showed that all actions were essential for organizations that saw QS transition as an important business case. For PKI users, the essentiality of actions differed depending on their risk appetite, business case, and available budget. The results for topical relevance showed that actions addressed the organization's needs. While some actions were of higher priority to regulatory organizations and CA, PKI users didn't see it as their main responsibility and stated that decisions must be made at the central level of the government, where they will follow the lead. The results indicated that actions depended on the roles and responsibilities of organizations in the ecosystem. For cognitive relevance, the results showed that all actions contribute to the growth of becoming QS. For actionability, the actions at the beginning of the growth model scored high on actionability. Since at the time of evaluation, no timeline was available for QS transition, experts and practitioners saw low actionability in actions at later stages.

The usefulness of the growth model was assessed based on four dimensions from the Technology Acceptance Model (TAM) framework, including perceived usefulness, perceived ease of use, attitude toward use, and behavioral intention to use. The results for perceived usefulness indicated that the usefulness of the model lies in recognizing QS transition challenges and providing a system-level overview of QS transition. The results for perceived ease of use showed that the growth model is easy to use and can be tailored to different intentions of use. For the attitude towards use, the results showed that the model meets the current needs of organizations. The model would be useful for multiple relevant roles within and around organizations dealing with QS transition planning and strategy, including but not limited to practitioners involved in awareness, business continuity, transition planning, and change management. The results for behavioral intention to use indicated that CAs have a high intention to incorporate the model since they need to align with multiple stakeholders for their critical business processes. For PKI users, they will follow the lead once decisions are made at the central level and comply with statutory requirements.

The chapter further highlighted the perceived strengths and weaknesses of the growth model. The growth model was assessed as an important tool in creating urgency and awareness. By taking an *ecosystem perspective,* the growth model provides a good overview of QS transition and can be used to communicate and coordinate QS transition process within organizations and across organizations. The simplified process of QS transition with a series of stages allows experts and non-experts to grasp the complexity of achieving quantum safety while recognizing both socio-technical transition challenges organizations may need to consider. Organizations may use the growth model to identify the current stage they are in and prepare for their next steps when making changes in the dynamic environment of the security landscape. It is essential to note that while the growth model provides a tailored approach for developing strategies and creating a roadmap for QS transition, it may not be sufficient for those seeking step-by-step implementation instructions. Organizations can gain additional insights from other external sources, such as the recently published PQC migration handbook II.

Chapter 8 Conclusions

This chapter presents the key findings, contributions, and discusses the limitations of the research and offers recommendations for future research. In Section 8.1, the research questions of this study are revisited, and a summary of key findings for each research question is presented. In Section 8.2, the scientific and societal contributions of the study are highlighted. In Section 8.3**,** limitations of the research are discussed, and in Section 8.4, potential areas for future research are identified.

8.1 Research Findings

This section provides the key findings from this research. To answer the main research question, "*What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems*?" four sub-questions have been formulated in *Chapter* 1. The following section highlights the key findings for each research question and discusses the results obtained through this research in *Chapters 5, 6,* and *7.*

Sub-question 1: QS Transition Challenges in the Context of PKI Systems

This research provides the first investigation of socio-technical transition challenges in the context of PKI systems. By taking the whole ecosystem into account, the research examines different QS transition challenges in both literature and practice. Chapter 5 answers sub-question 1: "*What are the challenges that hinder organizations in transitioning toward QS PKI systems?*" Chapter 5 begins with the introduction to the scope of the case study in the context of PKI in the Dutch public sector as part of the case study. The research provides an overview of the whole ecosystem that multiple organizations may need to be part of. From governing bodies such as the Ministry of Central Government, Logius, Rijksinspectie Digitale Infrastructuur (RDI), standardization bodies such as NIST and ETSI, Qualified Trust Service Providers (QTSPs), relevant external expertise such as Qualified Trust Service Providers (QTSPs), hardware vendors, software providers, and users including individuals, businesses and government agencies, there are diverse organizations involved in maintaining services in the complex PKI landscapes and ensuring secure communication and information exchange.

The list of transition challenges from SLR has been refined using a series of semi-structured interviews with experts and practitioners. The 15 QS transition challenges have been categorized into three different categories using the TOE framework: Technological, Organizational, and Ecosystem Categories. In this research, transition challenges are extended beyond technological aspects and

include organizational and ecosystem aspects that many organizations are still not aware of. In the technological category, the identified transition challenges are Availability of QS Standardization, No QS standards & selection, No Reliable & Secure QS solution, Non-PQC systems (e.g., CAs & PKI users), and No Availability of QS Hardware & Software. In the organizational category, the identified transition challenges are Lack of Urgency within Organization, No Business case for QS Transition, Knowledge Needs within Organizations, Lack of Technical skills & Qualified Personnel, and No QS Governance within Organization. In the Ecosystem category, the identified transition challenges are Complex Technical Interdependencies, Lack of Collaboration, Lack of Urgency in the Ecosystem, No QS Governance in the Ecosystem, and Lack of Policy & Regulations for QS Solutions. QS transition challenges are socio-technical and remain complex as a multi-disciplinary approach is needed for understanding QS transition.

Sub-question 2: Stages of Growth Model & Discontinuities for QS Transition
This research is the first to develop a stages of growth model for QS transition that is grounded in QS transition challenges and presents how organizations can collectively become QS. The first part of Chapter 6 answers sub-question 2: "*What are the different stages in the growth model and discontinuities for QS PKI systems?"* This research uses a structured and systematic method called Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach. The ISM-MICMAC approach provides a systematic way to structure and prioritize the identified transition challenges based on their driving and dependence power. The results highlight which challenges need to be addressed with priorities in hierarchical levels. Building on this empirical foundation, discontinuities are derived from the challenges in the ecosystem, representing boundary markers to move between stages in the growth model. These discontinuities act as necessary conditions that must be met in the ecosystem to move from one stage to the next.

There are diverse organizations across different levels in the ecosystem, at the inter-organizational and intra-organizational levels. At the ecosystem level, there are regulatory organizations (e.g., European Commission (EC), European Parliament (EP)), international standardization organizations (e.g., NIST, ETSI), and organizations that are responsible for network and information security (e.g., ENISA) and other multinational companies (e.g., Microsoft, Mozilla, etc.). At the inter-organizational level, there are government agencies (e.g., ministries, Logius, National Cyber Security Centre (NCSC)), and organizations within sectors at a national context that manage and operate critical infrastructures across (e.g., the

Central Bank of the Netherlands, *De Autoriteit Financiële Markten (AFM),* KPN, vendors, etc.). At the intra-organizational level, there are public and private entities such as government agencies, banks, tax offices, hospitals, service providers, and other small and medium enterprises (SMEs) that rely on critical infrastructure managed and operated at the inter-organizational level.

The results have been synthesized to develop a growth model for QS transition. The Five stages of Growth Model for QS Transition are Stage 1 QS awareness, Stage 2 QS assessment, Stage 3 QS preparation, Stage 4 QS implementation, and Stage 5 QS adaptation. For each stage of the model, the identified list of discontinuities acts as a set of necessary conditions that must be met in the ecosystem for QS transition.

At Stage 1, also known as QS awareness stage, discontinuities include 1) acknowledgement of risks & vulnerabilities of quantum threats, and 2) a finalized list of PQC standardization must occur in the ecosystem. During Stage 1, the security issues related to quantum computing technology may be discussed. However, there are many uncertainties and limited knowledge available in the ecosystem. The announcement from the standardization bodies on standards and guidance for QS cryptographic algorithms may raise awareness and allow organizations to recognize the need for QS transition.

At Stage 2, also known as QS assessment stage, discontinuities include 1) establishment of a steering committee and working groups, and 2) establishment of a testing environment for QS cryptographic solutions. During Stage 2, organizations may start assessing their existing infrastructures (e.g., risk, readiness, and impact) to prepare for QS transition. In the ecosystem, organizations recognize the need for QS transition and seek expertise to coordinate transition efforts. Some organizations may be involved in setting up testing environments for QS cryptographic solutions.

At Stage 3, also known as QS preparation stage, discontinuities include 1) availability of selected QS cryptographic solutions validated through testing and 2) development of policies & regulations that support QS transition. During Stage 3, there are various transition efforts depending on the organization's risk appetite. The majority of the organizations that are not participating in the testing environment may wait for the development of QS cryptographic solutions. While organizations finalize their assessments for existing infrastructures, mandatory policies and regulations may be available in the ecosystem to provide legal mandates and additional compliance related to PQC standards.

In Stage 4, also known as QS implementation stage, discontinuity includes 1) availability of QS cryptographic solutions in HSM & Certificate Issuance

software (CAs). Without the availability of QS hardware and software, organizations cannot implement QS cryptographic solutions in their existing infrastructures. During Stage 4, organizations may further seek resources, training & expertise to coordinate their transitions with various stakeholders such as CAs. To avoid interoperability and backward compatibility issues, organizations may start their implementation on a small scale.

In Stage 5, also known as QS adaptation stage, discontinuity includes 1) availability of lessons learned and best practices from the implementation of QS cryptographic solutions and 2) development of a cross-organizational coordination mechanism. During Stage 5, a full-scale transition may take place to implement QS cryptographic solutions across systems, services, and products. With the record of lessons learned and best practices from the prior stages of QS transition, organizations may further have a good overview and achieve the agility needed for a seamless transition that can be collectively achieved in the quantum era.

Sub-question 3: List of Transition Capabilities for QS Transition

The second part of Chapter 6 answers sub-question 3: "*What capabilities are needed across organizations for QS PKI systems*?" By following Teece's definition of dynamic capabilities, the research is the first to apply the term *Transition Capability* in the context of QS transition to refer to the ability to build upon existing capabilities and develop new capabilities for QS transition. The list of QS transition capabilities is identified at both the inter-organizational level and the intra-organizational level. Due to diverse organizations that are interdependent across different levels in the ecosystem, organizations may need to collectively take part and execute actions to carefully prepare for QS transition. The list of QS transition capabilities is categorized into Sensing, Seizing, and Transforming. QS transition capabilities in Stage 1 and Stage 2 are categorized as Sensing capabilities that detect opportunities and assess threats. QS transition capabilities in Stage 3 and Stage 4 are categorized as seizing capabilities that mobilize resources to capture value from identified opportunities and respond to threats. QS transition capabilities in Stage 5 are categorized as transforming capabilities, which maintain competitiveness through protecting and reconfiguring their intangible and tangible assets.

For organizations at the inter-organization level, QS transition capabilities are as follows: At Stage 1, an ability to engage and discuss the development of QS cryptographic solutions across industry, academia, and government. At Stage 2, an ability to establish a national QS governance framework and an ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms.

At Stage 3, an ability to integrate QS cryptographic solutions validated through testing into certified hardware and software, and an ability to create and update sectoral guidelines to support QS transition. At stage 4, an ability to modify existing systems with QS cryptographic solutions and an ability to facilitate cross-organizational knowledge sharing & skill development for QS transition. At Stage 5, an ability to coordinate cross-sectoral adaptive responses to address evolving security threats and challenges.

For organizations at the intra-organization level, QS transition capabilities are as follows: At Stage 1, an ability to raise awareness and align stakeholders to implement QS cryptographic solutions. At Stage 2, an ability to assess evolving risks & impact of quantum threats on the organization's business processes to determine which of the assets need to be protected. At Stage 3, an ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition. At Stage 4, an ability to implement QS cryptographic solutions in a small-scale environment before deployment, and an ability to upskill employees and share knowledge across departments to manage the implementation of QS cryptographic solutions. At Stage 5, the ability to integrate QS cryptographic solutions in a scaled environment across all systems, and the ability to monitor, adapt, and adjust security practices to changes in the external environment.

From Stage 1 to Stage 5, the list of QS transition capabilities shows capabilities that may be needed across different organizations at the inter-organizational level and intra-organizational level. In doing so, the research extends the study on capabilities needed in the context of QS transition. While the developed stages of the growth model can act as a guidance tool and communication instrument within organizations and across organizations, organizations may need to navigate the ecosystem they are in and may need to take actions that can translate into strategies for QS transition. By recognizing the transition capabilities needed for QS transition, organizations can not only start their preparation to move to the quantum era but also maintain their strategic fit over time with the evolving challenges in the security landscape to stay secure and compliant.

Sub-question 4: Relevance & Usefulness of the Growth Model

The growth model for QS transition is evaluated in Chapter 7, which also answers sub-question 4: "*To what extent is the growth model for QS transition relevant and useful for organizations?*" The research provides knowledge on QS transition challenges and identifies actionable guidance for organizations looking to transition their PKI systems. By taking an ecosystem perspective, the stages of growth model

show a system-level view of QS transition with diverse organizations at the intra-organizational level and inter-organizational level. For practitioners, the growth model may provide a communication tool within and across organizations to navigate QS transition. Due to interdependencies that exist in PKI systems, organizations may need to navigate changes that occur in the ecosystem and examine the transition capabilities needed per stage to grow towards QS.

Since QS transition is still at its early stage and experiences of moving through different phases do not exist, the evaluation focuses on assessing the relevance and usefulness of the growth model. The first part of the evaluation focuses on the relevance and assesses whether the model captures the relevant key socio-technical challenges and actionable guidance needed for QS transition. Since the topic of relevance varies depending on the context, user needs, and goals of the model, a tailored evaluation with multiple criteria was selected, which includes contextual relevance, topical relevance, cognitive relevance, and actionability. The contextual relevance examines the level of essentiality of actions across organizations for QS transition, and the topical relevance looks at how well the actions for QS transition address the organization's needs. The cognitive relevance assesses the extent to which the list of actions contributes to the growth of becoming a QS. The actionability examines how feasible actions are at this stage.

For contextual relevance, nine actions were considered highly essential. These include A2 Raise awareness on the importance of implementing QS cryptographic solutions, A3 Define clear roles, responsibilities and decision-making structure for QS governance, A5 Conduct assessments to identify the level of risk, readiness, & impact for QS transition, A6 Develop certified hardware and software that are suitable with QS cryptographic solutions, A7 Develop relevant sector-wide guidelines that support QS transition, A9 Migrate non-PQC systems of CAs to selected QS cryptographic solutions, A11 Modify non-PQC part of the existing systems in a smaller scale with QS cryptographic solutions, A14 Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems and A15 Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes. The results showed that most actions were essential for organizations that saw QS transition as an important business case. For PKI users, the essentiality of actions differed depending on their risk appetite, business case, and available budget.

For topical relevance, six actions were aligned with a high level of organizational needs. These include A5 Conduct assessments to identify the level of risk, readiness, & impact for QS transition. A7 Develop relevant sector-wide

guidelines that support QS transition, A9 Migrate non-PQC systems of CAs to selected QS cryptographic solutions, A10 Facilitate an expertise center for QS transition to share knowledge and skills needed for QS transition A14 Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems and A15 Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory & technology changes. While actions such as A5, A7, A9, and A10 to be directly aligned with current needs that need to be addressed for QS transition, actions such as A14 and A15 were aligned more with long-term organizational needs that organizations should strive towards.

For cognitive relevance, the results showed that all actions contribute to the growth of becoming QS. Three key insights have been shared to prepare for QS transition. First, the organizational aspects of QS transition need to be focused. Although there is a high emphasis on raising awareness for QS transition, much of the discussion taking place is purely technical. Organizations may need to raise awareness on Governance, Risk, and Compliance (GRC) strategies. Second, there are still uncertainties regarding the testing environment. The list of standards from NIST still needs to be tested, and clarification may be needed on the testing scope, testing scenarios or use cases, and whether testing should be centralized or decentralized. Also, validating third-party products from the vendors and establishing criteria for vendor testing compliance are needed. Third, knowledge integration across organizations is needed due to the current fragmented ecosystem. It would be crucial to streamline the knowledge and create a shared repository or library of knowledge for QS transition.

For actionability, the results indicated that the majority of actions at Stage 1 of the growth model for QS transition scored high on actionability. However, actions at later stages scored low on actionability. At the time of evaluation, the lack of a clear timeline made it difficult to indicate the high actionability of these actions. For actions that cannot be done at an earlier stage, three insights were highlighted to further prepare for QS transition. First, no regret moves can still be taken by organizations to gain full knowledge of their infrastructure to prepare for QS transition. Second, expectations for QS products and services need to be communicated to vendors. This may involve pre-tender negotiations and providing provincial acceptance with conditions. Third, training and support are needed to collectively become QS. In doing so, organizations may need to address strategies and discuss risks and prioritization for QS transition.

The second part of the evaluation focuses on the usefulness of the growth model and assesses how intended users perceive it, based on the TAM framework.

Since the growth model is at its early stage, evaluating the usefulness is ideal for the model that is intended to provide long-term support as QS transition evolves. The evaluation can clarify whether the growth model could be adopted in practice. Based on four dimensions from the TAM framework, the evaluation assessed perceived usefulness, perceived ease of use, attitude toward use, and behavioral intention to use. The perceived usefulness assesses how useful the model is in addressing QS transition challenges. The perceived ease of use assesses how easy it would be to use the model. The attitude towards use assesses how well the model aligns with the current needs. The behavioral intention to use assesses how likely one is to incorporate the model in work.

For the perceived usefulness, the results indicate that the growth model is useful in addressing QS transition challenges. While recognizing that not all actions and the details in the model have to be followed, a high-level overview of discontinuities and actions needed across organizations shows that the usefulness of the growth model lies in addressing QS transition challenges and providing a system-level view of the transition complexity. The overview of QS transition allows organizations to think about the stages ahead and what preparation may be needed within and across organizations for QS transition.

For the perceived ease of use, the results show that the growth model is easy to use and flexible, which can be tailored to different intentions of use. While the growth model provides the list of actions needed across organizations, it is important to recognize that the growth model does not offer detailed step-by-step instructions on how to transition the existing infrastructures to QS. Since, at the time of evaluation, no timeline for QS transition was made available in the ecosystem, the indication of expected years for QS transition was considered important to determine the expected date of completion for implementing QS cryptographic algorithms based on PQC.

For the attitude towards the use of the growth model, the results show that the model meets the current needs of organizations for CAs and a moderate level of alignment for PKI users. Since changes in QS transition are closely tied to the QS technology, regulations, and other business needs, a broader view of the model provided CAs with QS transition challenges and different actions that need to be prioritized. While the growth model would be useful for roles involving awareness, business continuity, transition planning, and change management, the model was considered to be too high-level for project managers.

For the behavioral intention to use, organizations showed intentions to incorporate the model in their work. The model can allow organizations to create

rooms for discussion. Since much work needs to be done for QS transition, the model can be used for building dialogue, communication, and awareness across and within organizations. In doing so, organizations can start delegating the responsibility and communicating with their stakeholders. For CAs, it is important to discuss the topic of QS transition in the ecosystem, as multiple stakeholders are needed to facilitate their critical business processes. While this was also true for PKI users in the public sector, many decisions still need to be made at the central level, so they will follow the lead.

Main RQ: Key Challenges & Stages of Growth for Organizations to Follow

By synthesizing the answers to sub-questions 1 to 4, this research answers the main research question, "*What are the key challenges and what stages of growth can organizations follow to transition to Quantum-safe (QS) PKI systems*?" The first part of the main research question, which asks about the key challenges, has been answered in sub-question 1. The results show that the list of QS transition challenges is socio-technical, and organizations need to go beyond technical aspects and address challenges in the organizational and ecosystem aspects. The 15 QS transition challenges have been clustered into the Technological, Organizational, and Ecosystem Categories using the TOE framework. The identified QS transition challenges in the technological category include the Availability of QS Standardization, No QS standards & selection, No Reliable & Secure QS solution, Non-PQC systems (e.g., CAs & End-users), and No Availability of QS Hardware & Software. The identified QS transition challenges in the organizational category include Lack of Urgency within Organization, No Business case for QS Transition, Knowledge Needs within Organizations, Lack of Technical skills & Qualified Personnel, and No QS Governance within Organization. The identified QS transition challenges in the Ecosystem category include Complex Technical Interdependencies, Lack of Collaboration, Lack of Urgency in the Ecosystem, No QS Governance in the Ecosystem, and Lack of Policy & Regulations for QS Solutions. QS transition challenges are socio-technical and remain complex as a multi-disciplinary approach is needed for understanding QS transition.

The second part of the main research question, which asks about the stages of growth that organizations can follow to transition to QS PKI systems, has been answered in sub-questions 2 and 3. The growth model serves as a forward-looking tool that provides long-term guidance as organizations search for insights through periods of uncertainty and transformation. The five stages of the growth model include Stage 1 QS awareness, Stage 2 QS assessment, Stage 3 QS preparation,

Stage 4 QS implementation, and Stage 5 QS adaptation. For each stage in the model, the list of discontinuities acts as a necessary condition that must be met in the ecosystem for organizations to move from one stage to the next. In Stage 1, discontinuities include *the acknowledgement of systematic risks and vulnerabilities of quantum threat* and *a finalized list of PQC standards*. In Stage 2, discontinuities include *the establishment of a steering committee and (international) working groups for QS transition,* and *the establishment of a testing environment for QS cryptographic solutions.* In Stage 3, discontinuities include *the development of policies & regulations that support QS transition*, and *the availability of selected QS cryptographic solutions validated through testing*. In Stage 4, discontinuity includes *the availability of QS cryptographic solutions in HSM & Certificate Issuance software (CAs)*. In Stage 5, discontinuities include *the availability of lessons learned and best practices from the Implementation of QS cryptographic solutions* and *the establishment of a cross-organizational coordination mechanism for QS cryptographic solutions.*

Moreover, organizations not only need to monitor the list of discontinuities but also develop transition capabilities so that they are prepared to move with the ecosystem. For organizations at the inter-organization level, QS transition capabilities are as follows: At Stage 1, an ability to engage and discuss the development of QS cryptographic solutions across industry, academia, and government. At Stage 2, an ability to establish a national QS governance framework and an ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms. At Stage 3, an ability to integrate QS cryptographic solutions validated through testing into certified hardware and software, and an ability to create and update sectoral guidelines to support QS transition. At stage 4, an ability to modify existing systems with QS cryptographic solutions and an ability to facilitate cross-organizational knowledge sharing & skill development for QS transition. At Stage 5, an ability to coordinate cross-sectoral adaptive responses (across sectors) to address evolving security threats and challenges. Organizational at the inter-organizational level include government agencies that apply national regulations and/ standards (e.g., ministries, Logius, National Cyber Security Centre (NCSC)), organizations that manage and operate critical infrastructures across and within sectors in a national context (e.g., the Central Bank of the Netherlands*, De Autoriteit Financiële Markten (AFM),* KPN, vendors, etc.).

For organizations at the intra-organization level, QS transition capabilities are as follows: At Stage 1, an ability to raise awareness and align stakeholders to implement QS cryptographic solutions. At Stage 2, an ability to assess evolving risks

& impact of quantum threats on the organization's business processes to determine which of the assets need to be protected. At Stage 3, an ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition. At Stage 4, an ability to implement QS cryptographic solutions in a small-scale environment before deployment, and an ability to upskill employees and share knowledge across departments to manage the implementation of QS cryptographic solutions. At Stage 5, the ability to integrate QS cryptographic solutions at scale, and the ability to monitor, adapt, and adjust to changes in the external environment. Organizations at the intra-organizational level include public and private entities that do not necessarily operate or manage critical infrastructures but rather rely on the services provided by these infrastructures (e.g., government agencies, banks, tax offices, hospitals, service providers, and other small and medium enterprises (SMEs)).

The results show that QS transition cannot be achieved in silos, and organizations need to navigate changes in the ecosystem to collectively move toward QS. The changes in the ecosystem for QS transition show that the discontinuities in Stage 1 and Stage 2, which are necessary conditions in the ecosystem, have been met. Such discontinuities include acknowledgement of risks & vulnerabilities of quantum threats, a finalized list of PQC standardization must occur in the ecosystem, establishment of a steering committee and working groups, and establishment of a testing environment for QS cryptographic solutions. For organizations, this also implies that transition capabilities for Stage 1 and Stage 2 need to be developed to move with the ecosystem. At the inter-organization level, the list of transition capabilities includes: an ability to engage and discuss the development of QS cryptographic solutions across industry, academia, and government, an ability to establish a national QS governance framework, and an ability to build a testing environment to evaluate and select appropriate QS cryptographic algorithms. At the intra-organizational level, the list of transition capabilities includes: an ability to raise awareness and align stakeholders to implement QS cryptographic solutions, an ability to assess evolving risks, readiness, and impact of quantum threats on the organization's business processes to determine which of the assets need to be protected.

As organizations at the inter-organizational level take initiative to engage and discuss the development of QS cryptographic solutions across industry, academia, and government, the steering committee and working at a national level actively discuss the direction and the need for QS transition. The existing technical uncertainties need to be addressed by validating the list of potential QS

cryptographic solutions. This may also lead organizations to come together and form public-private partnerships to establish a testing environment with multiple stakeholders. Further knowledge and insights need to be shared as organizations at the intra-organizational level stay up-to-date with the testing process for QS cryptographic solutions. The current stage for QS transition remains at Stage 2. During this stage, some organizations may or may not have started their preparation for QS transition, depending on their organization's risk appetite. The frontrunner organizations may voluntarily prepare for QS transition, and others may be more hesitant as the management-level of the organizations does not see the business opportunity. However, it is crucial for organizations to start assessing their existing infrastructures to move with the ecosystem. Without the knowledge of their cryptographic assets and potential vulnerabilities, organizations cannot identify which of their business processes need to implement QS cryptographic solutions with priority.

For organizations to further move to the next stage, discontinuities in Stage 3 also need to be met. These include *the development of policies & regulations that support QS transition*, *the availability of selected QS cryptographic solutions validated through testing.* Although there are no separate policies and regulations related to the topic of QS transition, some areas in the existing policy and regulations remain highly relevant. For example, future threats such as quantum computing technology can be interpreted in CRA, which provides a legal incentive to adopt robust cybersecurity measures, and in the NIS 2 directive, to focus on risk management and incident reporting on critical infrastructures and essential services. Going forward, it remains crucial to validate the suitability, functionality, and resilience of QS cryptographic solutions. The results of testing may affect the supply chain and timeline for QS transition, as organizations depend on vendors and third-party companies for their hardware and software. For organizations, transition capabilities at Stage 3 need to be developed to move with the ecosystem. For organizations at the inter-organizational level, these include an ability to integrate QS cryptographic solutions validated through testing into certified hardware and software, and an ability to create and update sectoral guidelines to support QS transition. For organizations at the intra-organizational level, this includes an ability to define and initiate tendering processes for products and services to meet the evolving business needs for QS transition.

8.2 Scientific & Societal Contribution

This section highlights the contributions of the research in both theory and practice. Section 8.2.1 discusses the scientific contribution of the research. Section 8.2.2 discusses the societal contribution of the research.

8.2.1 Scientific Contribution

First, this research contributes to a new body of knowledge on how organizations can achieve ecosystem-wide quantum safety in digital infrastructures. The research gathered insights on socio-technical aspects of PKI systems and further discusses 'what should be done' in the context of the research. By exploring QS transition for PKI systems, the research identified transition challenges and a list of factors that are relevant for organizations when transitioning to QS PKI systems. While previous studies have largely focused on the technical challenges of QS transition on QS cryptographic algorithms, this is the first study to capture various socio-technical challenges and extend knowledge on the complexity of QS transition by exploring institutional, organizational, and policy aspects of transition that organizations may need to be aware of. The integration of Stages of Growth with Dynamic Capabilities (Sensing, Seizing, Transforming) provides a robust lens for understanding how to move between stages.

Second, this research is the first to develop a stages of growth model for QS transition that is grounded in QS transition challenges. By using Theory for Design and Action, the research builds on the empirical findings of the PKI systems and further examines what may be needed to prepare for QS transition. The research is the first to apply the theories, such as the Stages of Growth Model and Dynamic Capabilities, in the context of QS transition. Using the stages of growth model, QS transition is dissected into a series of stages, and organizations may recognize the changes that occur in the ecosystem. The growth model for QS transition may be used to shape the future trajectories of QS transition for critical infrastructures that depend on PKI systems. According to Gregor (2006), creating something new that shapes future phenomena is considered to be the scientific contribution to Theory for Design and Action.

Third, this research strengthens knowledge on QS transition in the case of PKI systems in the public sector. The existing infrastructures need to implement QS cryptographic solutions in order to provide digital products and services that are reliable. However, there is a gap in the literature on how the existing PKI systems can transition to QS PKI systems. By using Theory for design and action as a theoretical framework, this study contributes to both the descriptive level and

prescriptive level of QS transition. By analyzing the topic of QS transition in PKI systems, the research gives guidance on how different organizations in the ecosystem can collectively transition to QS PKI systems.

Fourth, the research extends the stages of growth model theory by using Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC). The ISM-MICMAC approach helps in breaking down a complex topic into a clear, structured visual representation of a structural hierarchical model, even with a limited empirical data set. As existing research on the stages of growth models does not provide a systematic way for deriving different stages of growth models, this research provides a novel approach in applying ISM-MICMAC approach to develop a stage-based growth model for QS transition. The research introduces stages of the growth model and discontinuities that represent boundary markers between stages and act as necessary conditions that must be met in the ecosystem to move from one stage to the next.

8.2.2 Societal Contribution

Next to the scientific contributions, the research has several societal contributions. First, this research provides organizations with an overview of QS transition stages and capabilities. This fills the gap in what organizations can move forward for QS transition in their PKI systems. The list of transition capabilities further provides a lens for examining what capabilities organizations may need to develop to move from one stage to the next. In doing so, transition capabilities allow organizations to take appropriate actions and maintain their competitive advantage by staying ahead of potential security threats in the quantum era. While there are many uncertainties in the direction of QS transition, decisions cannot be made in silos due to possible interoperability and backward compatibility issues in PKI systems. This study allows organizations to understand the complex trajectories of QS transition and start the discussions within and across organizations to coordinate transition efforts.

Second, this research contributes to laying the groundwork for moving to QS PKI systems in the public sector. The use of PKI systems provides strong credentials for electronic identity management for individuals, businesses, and government agencies. For the public sector, many critical infrastructures depend on PKIs for secure digital transactions and information exchange. As organizations become increasingly dependent on the digital environment, the knowledge of the security framework of PKI must remain strong and protected against quantum computing-based threats in the quantum era. By providing knowledge on QS transition, this study raises awareness and urgency that transitioning PKI systems

cannot be done in silos, and quantum safety must be collectively achieved in the ecosystem.

Third, this research introduces a stages of growth model grounded in QS transition challenges that organizations find relevant and useful. Due to underlying technical components and multiple actors involved in facilitating PKI systems, transitioning PKI systems remains complex. Since QS transition currently lacks guidance, the stages of growth model can be used as a benchmark to understand where an organization stands now while taking the whole ecosystem into account, and to suggest what organizations may need to grow further. The growth model is context-specific and can be tailored to fit its own objective. The growth model shows that organizations may need to navigate what happens in the ecosystem and follow up with the development of QS cryptographic solutions.

Fourth, this research contributes to securing the PKI systems in the Netherlands as part of a larger project called HAPKIDO, which stands for *Hybrid Approach to Quantum-safe Public Key Infrastructure Development for Organization.* Together with consortium partners, including CWI, Logius, KPN, Microsoft, and Zynyo, the HAPKIDO project collectively provides guidance for organizations transitioning towards QS PKI systems, along with the growth model developed in this study.

In addition, research outputs from HAPKIDO have been shared with the international PKI consortium in 2023 and 2024. Likewise, the Dutch PQC Migration Handbook Part II (2024) includes the research outputs of the growth model for QS transition. By recognizing socio-technical transition challenges, organizations may need to develop QS transition capabilities and take coherent actions to stay secure and compliant. For practitioners, the findings of the research imply that quantum safety in PKI systems that critical infrastructures depend on must be collectively achieved. Likewise, the findings of this research not only prepare organizations to move to the quantum era but also maintain their strategic fit over time with the evolving challenges in the security landscape.

8.3 Limitations

Section 8.3 provides an overview of limitations in the research. The three sets of limitations stem from the research scope, methods used, and bias in the research. Section 8.3.1 discusses limitations regarding the research scope. Section 8.3.2 addresses limitations on methods used in the research and constraints on the sample size. Section 8.3.3 discusses limitations from bias, which include researcher bias, selection bias, and response bias.

8.3.1 Limitation on Research Scope

The research on the topic of QS transition in the case of PKI systems in the Dutch public sector provides a context-specific exploration. Yet, the focus on the Dutch context in the research provides a context-specific limitation, as a detailed overview of the single case of PKI systems restricts external validity. While there is an underlying assumption that most PKI systems follow similar structures with key technical components (explained in Section 2.2.2), it is possible to have different actors involved, policies, and regulatory environments. As a result, the findings from a single case of PKI systems may differ in organizational aspects when applied to other national contexts.

Moreover, multiple embedded units of analysis in the case serve as an important part of maintaining the focus of a case study. In doing so, the research uses multiple QS transition processes as units of analysis, which are based on diverse organizations in the ecosystem, and builds a deeper understanding of the case. These organizations, including PKI users, organizations that manage and operate PKI systems, and organizations that provide external expertise, have been categorized into three levels: ecosystem level, inter-organizational level, and intra-organizational level (explained in Section 6.3.2). Although the research tried to include diverse organizations at different levels involved in QS transition, the topic of QS transition is an emerging topic, and the development of QS technology is ongoing. Thus, additional organizations may be involved and need to work together to collectively achieve quantum safety as the QS transition evolves.

In addition, the growth model does not explicitly account for broader geopolitical dynamics beyond the defined stakeholder network. While actors such as standardization bodies and policy-relevant organizations are included, the wider strategic environment in which they operate is not explicitly discussed. This includes, for example, shifts in economic competition between states and major geopolitical events that may influence the QS transition. These external influences may still play a significant role in shaping the timing and conditions under which transitions between growth stages occur. This indicates the importance of considering broader contextual factors when interpreting the results, as it may offer additional context for understanding developments during the transition process.

8.3.2 Limitation on Research Methods Used

The mixed-methods case study with a sequential approach presents a methodological coherence with four phases of the research (explained in 3.3.2). By

moving phase by phase, one after another, new insights were generated. The research methods, such as literature review and interviews (explained in Section 3.4.1 and Section 3.4.2), have been conducted as part of Phase 1 of the research. Also, the ISM-MICMAC approach (explained in Section 3.4.4), which took place in Phase 2 of the research, used the list of QS transition challenges from Phase 1 as an input to understand the contextual relationship between challenges. Thus, the results of each research phase depended on the outcomes of the previous phase. Although this research does not rush to finalize the list of QS transition challenges, there is an inherent limitation in taking a sequential approach. Thus, additional exploration of QS transition challenges may be suggested to ensure that details are up-to-date and changes regarding QS transition are properly incorporated.

In addition, the small sample size throughout the research poses limitations. Due to the early stage of QS transition, the research on QS Transition is a relatively new and understudied topic. Despite the efforts made to increase the sample size, the availability of eligible individuals with knowledge of QS transition was limited, which constrained the sample size. This has affected the availability of experts with sufficient knowledge and experience in the topic of QS transition. For interviews, the lack of experts resulted in a limited number of available interviewees (explained in Section 3.4.2). For the workshop to conduct the ISM-MICMAC approach, the results are highly dependent on the knowledge and experience of the experts' inputs. Although the invited experts for the ISM-MICMAC approach were carefully selected to reflect diverse perspectives on QS transition, only a small sample of experts was available and was representative of the workshops.

8.3.3 Bias

Given the nature of the research philosophy (explained in 3.2.2) and case study design (explained in Section 3.3.4), there are possible *researcher biases* that inherently exist. While efforts were made to mitigate bias through data triangulation, careful interview selection, and documentation of the analysis, it is important to acknowledge potential sources of bias to maintain transparency and credibility. The research used a series of interviews and workshops to capture different perspectives on the PKI systems in the Dutch public sector. This may have resulted in *interpretation bias,* as the analysis of data collected from relevant experts and practitioners relied heavily on the interpretation of the researcher to develop a system-level understanding of QS transition. To mitigate this, the results of interviews and workshops have been discussed with the members of the research team to gain an understanding of QS transition.

As previously mentioned, the research on QS transition is still relatively new, and only a small number of relevant experts and practitioners are available. This constraint may introduce *selection bias*, as the participant pool is necessarily restricted to individuals with relevant experience and knowledge. Although efforts were made during the selection process to include key actors in the domain, not all identified participants were available to participate. Additionally, *response bias* may have occurred when participants offered responses deemed favorable by the researcher or when they influenced one another in workshops. To mitigate this, multiple data sources from interviews and workshops were used. In addition, participants were given clear instructions, and the objectives of data collection were communicated transparently to encourage honest and independent responses.

Moreover, some participants who were involved in earlier interviews (e.g., Phase 1) may have also contributed to interviews and workshops (e.g., Phase 4). While this overlap ensured continuity and allowed participants to evaluate the model based on prior contextual understanding, it may lead to a degree of perspective concentration across research phases. To mitigate this, additional participants from relevant domains and organizations (e.g., 10 participants) were included in the evaluation workshop. The inclusion of both returning experts and new participants provided an opportunity to broaden the empirical perspective on QS transition and reduce reliance on prior contributors. The number of new participants also reflects that the initially limited size of the expert pool in QS transition domain seems to be expanding over time. As QS is an emerging field, including new participants who had not been involved in earlier phases of the research was possible, whereas initially, only a small number of individuals were available.

8.4 Future Research Directions

This section highlights several recommendations for future research directions on the topic of QS transition. Three potential research streams are identified as future research directions, which are conceptual, empirical, and practical. Section 8.3.1 discusses the first avenue of research stream that extends the conceptual development of the research. Section 8.3.2 introduces the second avenue of research stream that focuses on the empirical exploration of the research. Section 8.3.3 concludes with research directions into practical implications.

8.4.1 Conceptual Development

In this research, the term QS transition capabilities is used to highlight dynamic capabilities that organizations may need to execute actions and achieve long-term

growth towards quantum-safety. Further research can explore how QS transition capabilities can be developed within organizations, which capabilities should be given priority, and how organizations can absorb QS in their organization. Building on the concept of absorptive capacity, some scholars take a micro-foundational lens to understand how actions, interactions, and the learning process of individuals and teams generate such capabilities (Felin et al., 2015). Extending this perspective, collaborative design research may provide insights into how innovation unfolds as a temporal, emergent process rather than as a set of predefined routines (Smulders et al., 2018; Smulders & Dorst, 2007). Further research could investigate the micro-level, learning-based mechanisms, and socio-interaction dynamics that shape new technologies in the context of QS transition.

Moreover, the system-level guidance is derived from identifying discontinuities per stage of the growth model and key actions needed for organizations to move from one stage to the next. Future research can explore institutional change and risk governance in the context of QS transition, providing new insights into how institutions adapt their security strategies and governance mechanisms to protect existing infrastructures. Also, there is an emerging concept of cryptographic agility, which may provide a foundation for both deeper theoretical exploration and practice-oriented research in the quantum era. Future research can examine how organizations respond to long-term threats posed by disruptive technological triggers.

In addition, the development of QS cryptographic algorithms based on PQC is ongoing. Parallel to the research on PQC, there is research on Quantum Key Distribution (QKD) that may offer possibilities in safeguarding communication infrastructures and building a quantum internet. While QKD and PQC provide different alternatives for safeguarding digital communication and information exchange, combining or complementing both may offer intersections that are worth exploring. The list of socio-technical transition challenges and the development of a stages of growth model for QS transition based on PQC may be integrated to offer a starting point to examine transition challenges relevant to QKD and extend the stages of growth model.

8.4.2 Empirical Exploration

From the results obtained in this research, such as QS transition challenges, the stages of growth model, and actions needed across organizations, further research can be conducted by gathering additional empirical data. This research focuses on the PKI systems in the context of QS transition and identifies key QS transition

challenges and actionable guidance for organizations looking to transition their current PKI systems towards QS ones. While this research offers a useful starting point for the work in the quantum era, ongoing research is needed to keep the topic of QS transition up-to-date. Future research can further extend the list of QS transition challenges and how these challenges were addressed to prepare organizations in an ecosystem. These can be explored from multiple data sources, such as literature reviews, interviews, and workshops with experts and practitioners.

Moreover, the research did not validate outcomes regarding different stages of growth and the list of QS transition capabilities across organizations. Since the QS transition is in its early stages, the evaluation in this research was conducted to establish the conceptual relevance and practical usefulness of the growth model. Future research can track the participating organizations over 5-10 years to validate if the predicted stages hold true. Future research can focus on testing relationships in the model, such as discontinuities per stage and a list of QS transition capabilities. This may extend the theoretical framework of this research with a stronger empirical foundation, which may lead to new insights into the stages of the growth model and QS transition capabilities.

In addition, the case study focuses on PKI systems in the Dutch public sector with multiple embedded units of analysis to extend knowledge on QS transition. With QS transition processes as the embedded multiple units of analysis, this study explores different stages of the growth model and transition capabilities that organizations may need to develop across the inter- and intra-organizational levels when transitioning their PKI systems to become QS. The framework can be tested in Finance, Healthcare, or Energy sectors, which have different risk appetites and legacy constraints. Additional research can be conducted in another context and apply growth models in other sectors and other countries. In doing so, future research can offer comparative perspectives (e.g., similarities and differences on QS transition processes) and strengthen empirical investigation from multiple cases on PKI systems.

8.4.3 Practical Implementation

This research reveals that QS transition is not just technical and requires a multidisciplinary approach with various stakeholders in the field. At the time of conducting this research, no ready-to-use growth model was available for organizations in the context of QS transition. By using a series of stages, the growth model developed in this research provides a high-level overview of QS transition for both experts and non-experts. Thus, future research can improve the growth

model and translate stage-specific actions across different organizations into clear, step-by-step guidance that organizations can follow. Organizations may benefit from the resulting knowledge and resources when planning their transition for practical implementation.

Likewise, future research can be conducted to integrate new insights and knowledge gained from the growth model into existing security frameworks. How can practitioners apply the tools and approaches they already use to implement and manage security for QS transition? How can organizations streamline workflows and coordinate between cross-functional departments (e.g., security, legal, operations, etc.)? By extending the insights from this research into widely used governance models and standards, including COBIT, NIST CSF, and ISO27001, organizations can further enhance these frameworks to support more informed decision-making and better coordination across security practices as they navigate and respond to QS transition.

Furthermore, the security framework of PKI systems is no longer secure against CRQC. This implies that cryptographic components need to be safely replaced without weakening overall security, and organizations may need to invest in their cryptographic agility to survive in the quantum era. Crypto-agility can be conceptualized as a permanent capability, while QS transition is a one-time (albeit long) event. Building on Fehr's work that examines the security and modular protocol design (Don et al., 2019; Fallahpour et al., 2025; Fehr & Huang, 2023), future research can apply these insights to real-world deployment, algorithm replacement strategies, and governance of PQC. The research can further advance the topic of cryptographic agility in organizations' security strategies and examine how organizations can implement long-term cryptographic change.

In addition, research may be needed to examine how training programs and workshops can help organizations maintain a robust security posture in the quantum era. Future research can explore how organizations can continuously learn and grow to address emerging security threats. This may involve practical initiatives such as targeted training, knowledge-sharing practices, and the integration of tools that capture and apply lessons from emerging threats. The research may examine how these initiatives can be implemented through cross-functional coordination and alignment to enable organizations to continuously adapt to evolving technological and organizational changes.

Bibliography

AbuGhanem, M. (2025). IBM quantum computers: Evolution, performance, and future directions. *The Journal of Supercomputing*, *81*(5), 687. https://doi.org/10.1007/s11227-025-07047-7

AccentureLabs. (2018). *CRYPTOGRAPHY IN A POST-QUANTUM WORLD. Preparing intelligent enterprises now for a secure future.*

Adams, C. M., & Lloyd, S. (1999). *Understanding PKI: Concepts, Standards, and Deployment Considerations*. https://api.semanticscholar.org/CorpusID:56860038

AIVD. (2021). *Prepare for the threat of quantum computers*.

AIVD. (2024). *Position paper on Quantum Key Distribution. Algemene Inlichtingen- en Veiligheidsdienst.* https://www.aivd.nl/documenten/publicaties/2024/01/26/position-paper-on-quantum-key-distribution

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process* (NIST IR 8413-Upd1; p. NIST IR 8413-upd1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8413-upd1

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2024). *Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography*

standardization process (NIST IR 8528; p. NIST IR 8528). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8528

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2025). *Status report on the fourth round of the NIST post-quantum cryptography standardization process* (NIST IR 8545; p. NIST IR 8545). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8545

Albar, D., & Perdana, B. F. F. (2021). Designing Digital Certificate Issuance Information System. *IOP Conference Series: Materials Science and Engineering*, *1158*(1), 012018. https://doi.org/10.1088/1757-899X/1158/1/012018

Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems*, *17*(5), 448–469. https://doi.org/10.1057/ejis.2008.37

Andersen, K. V., & Henriksen, H. Z. (2006). E-government maturity models: Extension of the Layne and Lee model. *Government Information Quarterly*, *23*(2), 236–248. https://doi.org/10.1016/j.giq.2005.11.008

Aquina, N., Cimoli, B., Das, S., Hövelmanns, K., Weber, F. J., Okonkwo, C., Rommel, S., Škorić, B., Tafur Monroy, I., & Verschoor, S. (2025). A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. *EPJ Quantum Technology*, *12*(1), 51. https://doi.org/10.1140/epjqt/s40507-025-00350-5

Bibliography

Arend, R. J., & Bromiley, P. (2009). Assessing the dynamic capabilities view: Spare change, everyone? *Strategic Organization*, *7*(1), 75–90. https://doi.org/10.1177/1476127008100132

Attri, R., Dev, N., & Sharma, V. (2013). *Interpretive Structural Modelling (ISM) approach: An Overview*. https://api.semanticscholar.org/CorpusID:212449453

Banoth, R., & Regar, R. (2023). Asymmetric Key Cryptography. In R. Banoth & R. Regar, *Classical and Modern Cryptography for Beginners* (pp. 109–165). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-32959-3_4

Barker et al. (2021a). *MIGRATION TO POST-QUANTUM CRYPTOGRAPHY*.

Barker, W., Dakota Consulting, & Guithersburg, MD. (2021b). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04282021

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99–120.

Barry, C. L., & Schamber, L. (1998). Users' criteria for relevance evaluation: A cross-situational comparison. *Information Processing & Management*, *34*(2–3), 219–236. https://doi.org/10.1016/S0306-4573(97)00078-2

Baskerville, R., & Pries-Heje, J. (2010). Explanatory Design Theory. *Business & Information Systems Engineering*, *2*(5), 271–282. https://doi.org/10.1007/s12599-010-0118-4

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management: A Procedure Model and its Application. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Bharosa, N., van Wijk, R., de Winne, N., & Janssen, M. (2015). *Challenging the Chain—Governing the Automated Exchange and Processing of Business Information*. IOS Press.

Bindel, N., Herath, U., McKague, M., & Stebila, D. (2017). Transitioning to a Quantum-Resistant Public Key Infrastructure. In T. Lange & T. Takagi (Eds.), *Post-Quantum Cryptography* (Vol. 10346, pp. 384–405). Springer International Publishing. https://doi.org/10.1007/978-3-319-59879-6_22

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches. *Communications of the Association for Information Systems*, *34*. https://doi.org/10.17705/1CAIS.03412

Bohr, N. (1913). On the constitution of atoms and molecules. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, *26*(151), 1–25. https://doi.org/10.1080/14786441308634955

Bova, F., Goldfarb, A., & Melko, R. G. (2021). Commercial applications of quantum computing. *EPJ Quantum Technology*, *8*(1), 2. https://doi.org/10.1140/epjqt/s40507-021-00091-1

Bravyi, S., Cross, A. W., Gambetta, J. M., Maslov, D., Rall, P., & Yoder, T. J. (2024). High-threshold and low-overhead fault-tolerant quantum memory. *Nature*, *627*(8005), 778–782. https://doi.org/10.1038/s41586-024-07107-7

Broadbent, A., & Schaffner, C. (2016). Quantum Cryptography Beyond Quantum Key Distribution. *Designs, Codes and Cryptography*, *78*(1), 351–382. https://doi.org/10.1007/s10623-015-0157-4

Brookes, N., Butler, M., Dey, P., & Clark, R. (2014). The use of maturity models in improving project management performance: An empirical investigation.

International Journal of Managing Projects in Business, *7*. https://doi.org/10.1108/IJMPB-03-2013-0007

Brooks, M. (2023). Quantum computers: What are they good for? *Nature*. https://doi.org/10.1038/d41586-023-01692-9

Brooks, P., El-Gayar, O., & Sarnikar, S. (2015). A framework for developing a domain specific business intelligence maturity model: Application to healthcare. *International Journal of Information Management*, *35*(3), 337–345. https://doi.org/10.1016/j.ijinfomgt.2015.01.011

Buchholz, S., Mariani, J., Routh, A., Keyal, A., & Kishnani, P. (2020). *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.* Https://Www.Ndtahq.Com/the-Realists-Guide-to-Quantum-Technology-and-National-Security/.

Buchmann, J. A., Karatsiolis, E., & Wiesmaier, A. (2013). *Introduction to Public Key Infrastructures*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40657-7

Caralli, R. A., Knight, M., & Montgomery, A. (2012). *Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability*. Software Engineering Institute. Carnegie Mellon University.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Castelvecchi, D. (2024). ‘A truly remarkable breakthrough’: Google’s new quantum chip achieves accuracy milestone. *Nature*, *636*(8043), 527–528. https://doi.org/10.1038/d41586-024-04028-3

Cavaye, A. L. M. (1995). User participation in system development revisited. *Information & Management*, *28*(5), 311–323. https://doi.org/10.1016/0378-7206(94)00053-L

CCC. (2019). *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.1909.07353

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography* (NIST IR 8105; p. NIST IR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Chen, L., & Moody, D. (2020). *New Mission and Opportunity for Mathematics Researchers: Cryptography in the Quantum Era*.

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, *14*(3), 197–235. https://doi.org/10.1111/j.1365-2575.2004.00173.x

Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S. (2003). *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF Network Working Group.

Chorus, C. G. (2010). A New Model of Random Regret Minimization. *European Journal of Transport and Infrastructure Research*. https://doi.org/10.18757/EJTIR.2010.10.2.2881

Chrissis, M. B., Konrad, M., & Shrum, S. (2011). *CMMI for development: Guidelines for process integration and product improvement* (3rd ed). Addison-Wesley.

CISA. (2023, August 21). *CISA, NSA and NIST Publish New Resource for Migrating to Post-Quantum Cryptography*. America's Cyber Defense Agency. https://www.cisa.gov/news-events/news/cisa-nsa-and-nist-publish-new-resource-migrating-post-quantum-cryptography

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive Capacity: A New Perspective on Learning and Innovation. *Administrative Science Quarterly*, *35*(1), 128. https://doi.org/10.2307/2393553

Collis, D. J., & Anand, B. N. (2021). The Virtues and Limitations of Dynamic Capabilities. *Strategic Management Review*, *2*(1), 47–78. https://doi.org/10.1561/111.00000017

Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., & Nicholas, R. (2005). *Internet X.509 Public Key Infrastructure- Certification Path Building*. Network Working Group.

Cosijn, E., & Ingwersen, P. (2000). Dimensions of relevance. *Information Processing & Management*, *36*(4), 533–550. https://doi.org/10.1016/S0306-4573(99)00072-2

Coursey, D., & Norris, D. F. (2008). Models of E-Government: Are They Correct? An Empirical Assessment. *Public Administration Review*, *68*(3), 523–536. https://doi.org/10.1111/j.1540-6210.2008.00888.x

Covers, O., & Doeland, M. (2020). How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure. *Journal of Payments Strategy & Systems*, *14*(2), 147. https://doi.org/10.69554/ZUTP3146

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd edition). Sage.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (Fourth edition). SAGE.

Crosby, P. B. (1980). *Quality is free: The art of making quality certain*. McGraw-Hill.

Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity*, *9*(1), tyad001. https://doi.org/10.1093/cybsec/tyad001

Daley, A. J., Bloch, I., Kokail, C., Flannigan, S., Pearson, N., Troyer, M., & Zoller, P. (2022). Practical quantum advantage in quantum simulation. *Nature*, *607*(7920), 667–676. https://doi.org/10.1038/s41586-022-04940-6

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

de Bruin, T., Freeze, R., Kulkarni, U., & Rosemann, M. (2005). *Understanding the Main Phases of Developing a Maturity Assessment Model*. ACIS 2005 Proceedings. https://aisel.aisnet.org/acis2005/109

De Carvalho, J. V., Rocha, Á., & De Vasconcelos, J. B. (2016). Maturity Models for Hospital Information Systems Management: Are They Mature? In Y.-W. Chen, C. Torro, S. Tanaka, R. J. Howlett, & L. C. Jain (Eds.), *Innovation in Medicine and Healthcare 2015* (Vol. 45, pp. 541–552). Springer International Publishing. https://doi.org/10.1007/978-3-319-23024-5_49

De Toni, A., & Tonchia, S. (2003). Strategic planning and firms' competencies: Traditional approaches and new perspectives. *International Journal of Operations & Production Management*, *23*(9), 947–976. https://doi.org/10.1108/01443570310491729

De Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology*, *19*(4), 271–276. https://doi.org/10.1007/s10676-017-9439-z

Dedehayir, O., Mäkinen, S. J., & Ortt, J. R. (2022). Innovation ecosystems as structures: Actor roles, timing of their entrance, and interactions. *Technological Forecasting and Social Change*, *183*, 121875. https://doi.org/10.1016/j.techfore.2022.121875

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, *6*(2), 80–88. https://doi.org/10.1177/1558689812437186

Devi K, S., Paranitharan, K. P., & Agniveesh A, I. (2021). Interpretive framework by analysing the enablers for implementation of Industry 4.0: An ISM approach. *Total Quality Management & Business Excellence*, *32*(13–14), 1494–1514. https://doi.org/10.1080/14783363.2020.1735933

Don, J., Fehr, S., Majenz, C., & Schaffner, C. (2019). *Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model*. https://doi.org/10.48550/ARXIV.1902.07556

Dosi, G., Nelson, R., & Winter, S. (2000). The Nature And Dynamics Of Organizational Capabilities. In *Nature & Dynamics of Organizational Capabilities*. https://doi.org/10.1093/0199248540.001.0001

Dowling, J. P., & Milburn, G. J. (2003). Quantum technology: The second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, *361*(1809), 1655–1674. https://doi.org/10.1098/rsta.2003.1227

Duperrin, J.-C., & Godet, M. (1973). *Méthode de hiérarchisation des éléments d'un système: Essai de prospective du système de l'énergie nucléaire dans son contexte sociétal*.

Easterby-Smith, M., Lyles, M. A., & Peteraf, M. A. (2009). Dynamic Capabilities: Current Debates and Future Directions. *British Journal of Management*, *20*(s1). https://doi.org/10.1111/j.1467-8551.2008.00609.x

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532. https://doi.org/10.2307/258557

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities And Challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/amj.2007.24160888

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11%3C1105::AID-SMJ133%3E3.0.CO;2-E

ENISA. (2021). *Post-quantum cryptography: Current state and quantum mitigation.* Publications Office. https://data.europa.eu/doi/10.2824/92307

ENISA. (2022). *Post-Quantum Cryptography: Integration Study*. Publications Office. https://data.europa.eu/doi/10.2824/151162

ENISA. (2025). *THREAT LANDSCAPE 2025*. European Union Agency for Cybersecurity.

ETSI. (2015). *Quantum Safe Cryptography and Security—An introduction, benefits, enablers and challenges* (No. 8).

ETSI. (2017). *GR QSC 003—V1.1.1—Quantum Safe Cryptography; Case Studies and Deployment Scenarios*.

ETSI. (2020). *ETSI TR 103 619—V1.1.1—CYBER; Migration strategies and recommendations to Quantum Safe schemes*.

European Commission. (2020). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the*

Digital Decade. Oxford University Press. https://doi.org/10.1093/law-oeeul/e66.013.66

European Commission. (2024a). *COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*.

European Commission. (2024b). *Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework*.

European Parliament and Council of the European Union. (2022). *REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*.

European Union. (2014). *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

Fallahpour, P., Fehr, S., & Huang, Y.-H. (2025). *Tighter Quantum Security for Fiat-Shamir-with-Aborts and Hash-and-Sign-with-Retry Signatures*. https://eprint.iacr.org/2025/985

Favaretto, J. E. R., & Meirelles, F. de S. (2015). *NOLAN´S STAGE LEVEL MEASUREMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY IN MODERN ORGANIZATIONS*.

Fehr, S., & Huang, Y.-H. (2023). On the Quantum Security of HAWK. In T. Johansson & D. Smith-Tone (Eds.), *Post-Quantum Cryptography* (Vol. 14154, pp. 405–416). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-40003-2_15

Felin, T., Foss, N. J., & Ployhart, R. E. (2015). The Microfoundations Movement in Strategy and Organization Theory. *Academy of Management Annals*, *9*(1), 575–632. https://doi.org/10.5465/19416520.2015.1007651

Feynman, R. P. (1948). Space-Time Approach to Non-Relativistic Quantum Mechanics. *Reviews of Modern Physics*, *20*(2), 367–387. https://doi.org/10.1103/RevModPhys.20.367

Freeman, R. E. (2023). Stakeholder Management: Framework and Philosophy. In S. D. Dmytriyev & R. E. Freeman (Eds.), *R. Edward Freeman's Selected Works on Stakeholder Theory and Business Ethics* (Vol. 53, pp. 61–88). Springer International Publishing. https://doi.org/10.1007/978-3-031-04564-6_3

Galbraith, S., Liu, D., Nepal, S., Pieprzyk, J., Liu, J., Steinfeld, R., Sakzad, A., Esgin, M., Kuchta, V., Susilo, W., Plantard, T., & Dung, D. (2021). *The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography*. CSIRO.

Gibney, E. (2019). *The Quantum Gold Rush*.

Gibson, C., & Nolan, R. (1974). Managing the Four Stages of EDP Growth. *Harvard Business Review*, *52*.

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Giron, A. A. (2023). Migrating Applications to Post-Quantum Cryptography: Beyond Algorithm Replacement: *Proceedings of the 20th International Conference on Security and Cryptography*, 857–862. https://doi.org/10.5220/0012138800003555

Godet, M. (2000). The Art of Scenarios and Strategic Planning. *Technological Forecasting and Social Change*, *65*(1), 3–22. https://doi.org/10.1016/S0040-1625(99)00120-1

Godinho Filho, M., Monteiro, L., De Oliveira Mota, R., Dos Santos Leite Gonella, J., & De Souza Campos, L. M. (2022). The Relationship between Circular Economy, Industry 4.0 and Supply Chain Performance: A Combined ISM/Fuzzy MICMAC Approach. *Sustainability*, *14*(5), 2772. https://doi.org/10.3390/su14052772

Goel, P., Kumar, R., Banga, H. K., Kaur, S., Kumar, R., Pimenov, D. Y., & Giasin, K. (2022). Deployment of Interpretive Structural Modeling in Barriers to Industry 4.0: A Case of Small and Medium Enterprises. *Journal of Risk and Financial Management*, *15*(4), 171. https://doi.org/10.3390/jrfm15040171

Google Quantum AI and Collaborators, Acharya, R., Abanin, D. A., Aghababaie-Beni, L., Aleiner, I., Andersen, T. I., Ansmann, M., Arute, F., Arya, K., Asfaw, A., Astrakhantsev, N., Atalaya, J., Babbush, R., Bacon, D., Ballard, B., Bardin, J. C., Bausch, J., Bengtsson, A., Bilmes, A., … Zobrist, N. (2024). Quantum error correction below the surface code threshold. *Nature*. https://doi.org/10.1038/s41586-024-08449-y

Gorane, S. J., & Kant, R. (2015). Modelling the SCM implementation barriers: An integrated ISM-fuzzy MICMAC approach. *Journal of Modelling in Management*, *10*(2), 158–178. https://doi.org/10.1108/JM2-08-2012-0026

Gottschalk, P. (2009). *E-Government Interoperability: Frameworks for Aligned Development*.

Gottschalk, P., & Solli-Sæther, H. (2006). Maturity model for IT outsourcing relationships. *Industrial Management & Data Systems*, *106*(2), 200–212. https://doi.org/10.1108/02635570610649853

Gottschalk, P., & Solli-Sæther, H. (2008). Stages of e-government interoperability. *Electronic Government, An International Journal*, *5*(3), 310–320.

Gregor. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611. https://doi.org/10.2307/25148742

Grote, O., Ahrens, A., & Benavente-Peces, C. (2019). *Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques*. https://doi.org/10.5220/0008162800910098

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96*, 212–219. https://doi.org/10.1145/237814.237866

Guba, E., & Lincoln, Y. (1994). Competing Paradigms in Qualitative Research. In *Handbook of Qualitative Research* (Denzin, N.K. and Lincoln Y.S., pp. 105–117). Thousand Oaks.

Heisenberg, Werner. (1983). The physical content of quantum kinematics and mechanics. *Quantum Theory and Measurement*, 62–84.

Helfat, C. E., Finkelstein, S., Mitchell, W., Peteraf, M. A., Singh, H., Teece, D. J., & Winter, S. G. (Eds.). (2007). *Dynamic capabilities: Understanding strategic change in organizations*. Blackwell Pub.

Helfat, C. E., & Peteraf, M. A. (2015). Managerial cognitive capabilities and the microfoundations of dynamic capabilities. *Strategic Management Journal*, *36*(6), 831–850. https://doi.org/10.1002/smj.2247

Hiller, J., & Belanger, F. (2001). Privacy Strategies for Electronic Government. *E-Government 2001*, 162–198.

Hirschheim, R., Klein, H. K., & Newman, M. (1991). Information systems development as social action: Theoretical perspective and practice. *Management Science*. https://api.semanticscholar.org/CorpusID:152946770

Huang, J., & Nicol, D. M. (2017). An anatomy of trust in public key infrastructure. *International Journal of Critical Infrastructures*, *13*(2/3), 238. https://doi.org/10.1504/IJCIS.2017.088234

Hunt, R. (2001). Technological infrastructure for PKI and digital certification. *Computer Communications*, *24*, 1460–1471. https://doi.org/10.1016/S0140-3664(01)00293-6

IBM. (2024). *IBM Launches Its Most Advanced Quantum Computers, Fueling New Scientific Value and Progress towards Quantum Advantage*. https://newsroom.ibm.com/2024-11-13-ibm-launches-its-most-advanced-quantum-computers,-fueling-new-scientific-value-and-progress-towards-quantum-advantage

Innovalor. (2019). *PKIoverheid Onderzoek naar mogelijkheden om gebruik te vergroten bijvoorbeeld via verplichtstelling*.

International Organization for Standardization. (2022). *ISO/IEC 15408-1:2022-Information security, cybersecurity and privacy protection-Evaluation criteria for IT security.* ISO.

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

Iversen, J., Nielsen, P. A., & Norbjerg, J. (1999). Situated assessment of problems in software development. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *30*(2), 66–81. https://doi.org/10.1145/383371.383376

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Jansen, A., & Ølnes, S. (2016). The nature of public e-services and their quality dimensions. *Government Information Quarterly*, *33*(4), 647–657. https://doi.org/10.1016/j.giq.2016.08.005

Janssen, M., Chun, S. A., & Gil-Garcia, J. R. (2009). Building the next generation of digital government infrastructures. *Government Information Quarterly*, *26*(2), 233–237. https://doi.org/10.1016/j.giq.2008.12.006

Janssen, M., Luthra, S., Mangla, S., Rana, N. P., & Dwivedi, Y. K. (2019). Challenges for adopting and implementing IoT in smart cities: An integrated MICMAC-ISM approach. *Internet Research*, *29*(6), 1589–1616. https://doi.org/10.1108/INTR-06-2018-0252

Janssen, M., & van Veenstra, A. F. (2005). *Stages of Growth in e-Government: An Architectural Approach*. *3*(4).

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kalampokis, E., Tambouris, E., & Tarabanis, K. A. (2011). Open Government Data: A Stage Model. *International Conference on Electronic Government*. https://api.semanticscholar.org/CorpusID:13139441

Käppler, S. A., & Schneider, B. (2022). *Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms*. 61–49. https://doi.org/10.29007/2tpw

Kazanjian, R. K., & Drazin, R. (1990). A stage-contingent model of design and growth for technology based new ventures. *Journal of Business Venturing*, *5*(3), 137–150. https://doi.org/10.1016/0883-9026(90)90028-R

Kim, Eddins, A., Anand, S., Wei, K. X., Van Den Berg, E., Rosenblatt, S., Nayfeh, H., Wu, Y., Zaletel, M., Temme, K., & Kandala, A. (2023). Evidence for the utility of quantum computing before fault tolerance. *Nature*, *618*(7965), 500–505. https://doi.org/10.1038/s41586-023-06096-3

Kim, & Yoo, J. (2019). Platform Growth Model: The Four Stages of Growth Model. *Sustainability*, *11*(20), 5562. https://doi.org/10.3390/su11205562

King, J. L., & Kraemer, K. L. (1983). *Evolution and Organizational Information Systems: An Assessment of Nolan's Stage Model*. *12*. http://aisel.aisnet.org/icis1983/12

Klievink, B., & Janssen, M. (2009). Realizing joined-up government—Dynamic capabilities and stage models for transformation. *Government Information Quarterly*, *26*(2), 275–284. https://doi.org/10.1016/j.giq.2008.12.007

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

Kong, I., Janssen, M., & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition. In J. Ubacht, C. Csáki, L. Danneels, N. Edelmann, M. Janssen, E. Kalampokis, I. Lingren, A.-S. Novak, P. Panagiotopoulos, P. Parycek, G. V. Pereira, I. Susha, G. Schwabe, S. Virkar, E. Tambouris, & A. Zuiderwijk (Eds.), *Joint Proceedings of Ongoing Research, Practitioners, Posters, Workshops, and Projects at EGOV-CeDEM-ePart 2023 co-located with the International Conference EGOV-CeDEM-ePart (EGOV-CeDEM-ePart 2023), Corvinus University of Budapest, September 4-7, 2023* (Vol. 3449). CEUR-WS.org. https://ceur-ws.org/Vol-3449/paper5.pdf

Kong, I., Janssen, M., & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly*, *41*(1), 101884. https://doi.org/https://doi.org/10.1016/j.giq.2023.101884

Kramer, A. (2023). Quantum algorithm offers faster way to hack internet encryption. *Science*, *381*(6664). https://www.science.org/content/article/surprising-and-supercool-quantum-algorithm-offers-faster-way-hack-internet-encryption

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors*, *21*(18), 6225. https://doi.org/10.3390/s21186225

Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array*, *15*, 100242. https://doi.org/10.1016/j.array.2022.100242

Kumar, P., Bhamu, J., & Sangwan, K. S. (2021). Analysis of Barriers to Industry 4.0 adoption in Manufacturing Organizations: An ISM Approach. *Procedia CIRP*, *98*, 85–90. https://doi.org/10.1016/j.procir.2021.01.010

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly*, *18*(2), 122–136. https://doi.org/10.1016/S0740-624X(01)00066-1

Lee, A. S. (2004). Thinking about Social Theory and Philosophy for Information Systems. In *Social Theory and Philosophy for Information Systems*. John Wiley & Sons Ltd.

Lee, J. (2010). 10year retrospect on stage models of e-Government: A qualitative meta-synthesis. *Government Information Quarterly*, *27*(3), 220–230. https://doi.org/10.1016/j.giq.2009.12.009

Lee, J., Lee, D., & Kang, S. (2007). *An Overview of the Business Process Maturity Model (BPMM)*. *4537*, 395. https://doi.org/10.1007/978-3-540-72909-9_42

Leech, D. P., Ferris, S., & Scott, J. T. (2018). *The economic impacts of the advanced encryption standard, 1996-2017* (NIST GCR 18-017; p. NIST GCR 18-017). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.GCR.18-017

Lewis, A. M. (2017). *The impact of quantum technologies on the EU's future policies. Part 1, Quantum time.* European Commission. Joint Research Centre. https://data.europa.eu/doi/10.2760/832942

Lewis, A. M., Ferigato, C., Travagnin, M., & Floresu, E. (2018). *The impact of quantum technologies on the EU's future policies. Part 3, Perspectives for quantum computing.* European Commission. Joint Research Centre. https://data.europa.eu/doi/10.2760/737170

Lewis, A. M., & Travagnin, M. (2018). *The impact of quantum technologies on the EU's future policies. Part 2, Quantum communications: From science to policies*. European Commission. Joint Research Centre. https://data.europa.eu/doi/10.2760/881896

Lewis, A. M., & Travagnin, M. (2022). *A secure quantum communications infrastructure for Europe: Technical background for a policy vision*. European Commission. Joint Research Centre.

Lindgren, I., & Jansson, G. (2013). Electronic services in the public sector: A conceptual framework. *Government Information Quarterly*, *30*(2), 163–172. https://doi.org/10.1016/j.giq.2012.10.005

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

Lindsay, J. R. (2020b). Surviving the Quantum Cryptocalypse—Lindsay. *Strategic Studies Quarterly*.

Linn, J. (2000). *Trust Models and Management in Public-Key Infrastructures*.

Liu, D., Nepal, S., Abuadbba, S., Wang, J., & Chau, S. (2025). *Quantum Safe Transition: Reality, Hurdles and Pathways*. CSIRO.

Logius. (2024a). *Certification Practice Statements for the Policy Authority PKIoverheid*.

Logius. (2024b). *PKIoverheid Programme of Requirements 5.1*. https://cp.pkioverheid.nl/pkioverheid-por-v5.1.html

Logius. (2025a). *Certification Practice Statement Policy Authority PKIoverheid Unified v5.5*. https://cps.pkioverheid.nl/pkioverheid-cps-unified-v5.5.html#id__1-introduction

Logius. (2025b). *PKIoverheid*. Logius | Ministerie van Binnenlandse Zaken En Koninkrijkrelaties. https://www.logius.nl/onze-dienstverlening/toegang/pkioverheid

Lovic, V. (2020). *Quantum Key Distribution: Advantages, Challenges and Policy*. https://doi.org/10.17863/CAM.58622

Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI). *International Journal of Information Management*, *38*(1), 42–44. https://doi.org/10.1016/j.ijinfomgt.2017.08.004

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

Macaulay, T., & Henderson, R. (2019). *Cryptographic Agility in Practice: Emerging Use Cases*.

Maheshwari, D., Janssen, M., & van Veenstra, A. F. (2011). *A multi-level framework for measuring and benchmarking public service organizations: Connecting stages-of-growth models and enterprise architecture*.

Mandviwalla, A., Ohshiro, K., & Ji, B. (2018). Implementaing Grover's Algorithm on the IBM Quantum Computers. *IEEE International Conference on Big Data*.

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Martin, K. M. (2025). Applications of Cryptography. In K. M. Martin, *Everyday Cryptography* (3rd ed., pp. 355–440). Oxford University PressOxford. https://doi.org/10.1093/oso/9780198903277.003.0011

Mashatan, A., & Heintzman, D. (2021). The complex path to quantum resistance. *Communications of the ACM*, *64*(9), 46–53. https://doi.org/10.1145/3464905

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090354

Mehrez, H. A., & El Omri, O. (2018). The crypto-agility properties. *The 12th International Conference on Society, Cybernetics and Informatics*, 99–103.

Memon, Q. A., Al Ahmad, M., & Pecht, M. (2024). Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs. *Quantum Reports*, *6*(4), 627–663. https://doi.org/10.3390/quantum6040039

Ménard, A., Ostojic, I., Patel, M., & Volz, D. (2020). A game plan for quantum computing. *McKinsey Quarterly*, 1–8.

Menezes, A., & Stebila, D. (2021). Challenges in Cryptography. *IEEE Security & Privacy*, *19*(2), 70–73. https://doi.org/10.1109/MSEC.2021.3049730

Mettler, T., & Rohner, P. (2009). Supplier Relationship Management: A Case Study in the Context of Health Care. *Journal of Theoretical and Applied Electronic Commerce Research*, *4*(3). https://doi.org/10.4067/S0718-18762009000300006

Mishra, P., & Sharma, R. K. (2015). Integration of Six Sigma and ISM to improve Supply Chain Coordination – A conceptual framework. *International Journal of Production Management and Engineering*, *3*(1), 75. https://doi.org/10.4995/ijpme.2015.3150

Mizzaro, S. (1998). How many relevances in information retrieval? *Interacting with Computers*, *10*(3), 303–320. https://doi.org/10.1016/S0953-5438(98)00012-5

Moon, M. (2002). The Evolution of E-Government Among Municipalities: Rhetoric or Reality. *Public Administration Review*, *62*, 424–433. https://doi.org/10.1111/0033-3352.00196

Morse, J. M., & Niehaus, L. (2016). *Mixed method design: Principles and procedures*. Routledge, Taylor and Francis. https://doi.org/10.4324/9781315424538

Mosca, M. (2015). *Cybersecurity in an era with quantum computers: Will we be ready?* https://eprint.iacr.org/2015/1075

Mosca, M. & Piani, M. (2023). *Quantum Threat Timeline Report 2023*.

Mulholland, J., Mosca, M., & Braun, J. (2017). The Day the Cryptography Dies. *IEEE Security & Privacy*, *15*(4), 14–21. https://doi.org/10.1109/MSP.2017.3151325

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, *21*(2), 241–242. https://doi.org/10.2307/249422

Myers, M. D., & Klein, H. K. (2011). A Set of Principles for Conducting Critical Research in Information Systems. *MIS Quarterly*, *35*(1), 17–36. https://doi.org/10.2307/23043487

Nelson, R., & Winter, S. (1982). *An Evolutionary Theory of Economic Change*. Harvard University Press.

Niederhagen, R., & Waidner, M. (2017). *Practical Post-Quantum Cryptography*. Fraunhofer Institute for Secure Information Technology.

Niehaves, B., & Becker, J. (2006). *Epistemological Perspectives on Design Science in IS Research*.

Niehaves, B., Plattfaut, R., & Becker, J. (2013). Business process management capabilities in local governments: A multi-method study. *Government Information Quarterly*, *30*(3), 217–225. https://doi.org/10.1016/j.giq.2013.03.002

Bibliography

NIST. (2024a). *Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard*.

NIST. (2024b). *Module-lattice-based digital signature standard* (NIST FIPS 204; p. NIST FIPS 204). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.FIPS.204

NIST. (2024c). *Module-lattice-based key-encapsulation mechanism standard* (NIST FIPS 203; p. NIST FIPS 203). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.FIPS.203

NIST. (2024d). *Stateless hash-based digital signature standard* (NIST FIPS 205; p. NIST FIPS 205). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.FIPS.205

NIST. (2024e). *Transition to Post-Quantum Cryptography Standards* (NIST IR 8547 ipd; p. NIST IR 8547 ipd). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8547.ipd

Nolan, R. L. (1973). Managing the computer resource: A stage hypothesis. *Communications of the ACM*, *16*(7), 399–405. https://doi.org/10.1145/362280.362284

Nolan, R. L. (1979). Managing the crisis in data processing. *Harvard Business Review*, 115–126.

NSA. (2024, May 5). *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

O'Dea, M. (2025). Book Review: The Technology Acceptance Model - 30 Years of TAM by Fred D. Davis and Andrina Granic. *Journal of University Teaching and Learning Practice*, *21*(08). https://doi.org/10.53761/ffx9bd95

OECD. (2024). *Key concepts and current technical trends in cryptography for policy makers* (OECD Digital Economy Papers No. 364; OECD Digital Economy Papers, Vol. 364). https://doi.org/10.1787/29d9fbad-en

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, *3*(3), 398–427. https://doi.org/10.1287/orsc.3.3.398

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1

Ortt, J. R., & Van Der Duin, P. A. (2008). The evolution of innovation management towards contextual innovation. *European Journal of Innovation Management*, *11*(4), 522–538. https://doi.org/10.1108/14601060810911147

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-04101-3

Paar, C., Pelzl, J., & Güneysu, T. (2024). *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-69007-9

Pandza, K., & Thorpe, R. (2009). Creative Search and Strategic Sense-making: Missing Dimensions in the Concept of Dynamic Capabilities. *British Journal of Management*, *20*(s1). https://doi.org/10.1111/j.1467-8551.2008.00616.x

Paulk, M., Curtis, B., Chrissis, M., & Weber, C. (1993). Capability Maturity Model, Version 1.1. *Software, IEEE*, *10*, 18–27. https://doi.org/10.1109/52.219617

Penrose. (1959). *The Theory of the Growth of the Firm*. John Wiley & Sons.

Penrose. (1995). *The Theory of the Growth of the Firm* (3rd ed.). Oxford University PressOxford. https://doi.org/10.1093/0198289774.001.0001

Peterssen, G. (2020). Quantum technology impact: The necessary workforce for developing quantum software. *Proceedings of the 1st International Workshop on the QuANtum SoftWare Engineering & Programming (QANSWER)*, 6–22.

Petrenko, K., Mashatan, A., & Shirazi, F. (2019). 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*, *46*, 151–163. https://doi.org/10.1016/j.jisa.2019.03.007

Planck, M. (1900). On the Theory of the Energy Distribution Law of the Normal Spectrum. *Verhandlungen Der Deutschen Physikalischen Gesellschaft*, *2*, 38–45.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity Models in Information Systems Research: Literature Search and Analysis. *Communications of the Association for Information Systems*, *29*. https://doi.org/10.17705/1CAIS.02927

Poeppelbuss, J., & Roeglinger, M. (2011). *WHAT MAKES A USEFUL MATURITY MODEL? A FRAMEWORK OF GENERAL DESIGN PRINCIPLES FOR MATURITY MODELS AND ITS DEMONSTRATION IN BUSINESS PROCESS MANAGEMENT*.

Prananto, A., Mckay, J., & Marshall, P. (2003). *A Study of the Progression of E-Business Maturity in Australian SMEs*.

Putterman, H., Noh, K., Hann, C. T., MacCabe, G. S., Aghaeimeibodi, S., Patel, R. N., Lee, M., Jones, W. M., Moradinejad, H., Rodriguez, R., Mahuli, N., Rose, J., Owens, J. C., Levine, H., Rosenfeld, E., Reinhold, P., Moncelsi, L., Alcid, J. A., Alidoust, N., … Painter, O. (2024). *Hardware-efficient quantum error correction using concatenated bosonic qubits* (arXiv:2409.13025). arXiv. https://doi.org/10.48550/arXiv.2409.13025

Raber, D., Wortmann, F., & Winter, R. (2013). Situational Business Intelligence Maturity Models: An Exploratory Analysis. *2013 46th Hawaii International Conference on System Sciences*, 3797–3806. https://doi.org/10.1109/HICSS.2013.483

Ranjan, S., Sharma, V., Thakkar, J. J., & Gaddam, H. K. (2024). An Integrated ISM-MICMAC Approach for Investigating Sources of Wastes in Circular Economy: A Case of Apparel Industry. *Operations Research Forum*, *5*(2), 42. https://doi.org/10.1007/s43069-024-00320-0

Räsänen, M., Mäkynen, H., Möttönen, M., & Goetz, J. (2021). Path to European quantum unicorns. *EPJ Quantum Technology*, *8*(1), 5. https://doi.org/10.1140/epjqt/s40507-021-00095-x

Rassa, R. C., Garber, V., & Etter, D. (2002). Capability Maturity Model® Integration (CMMI℠): A view from the sponsors. *Systems Engineering*, *5*(1), 3–6. https://doi.org/10.1002/sys.10011

Richardson, G. B. (1972). The Organisation of Industry. *The Economic Journal*, *82*(327), 883. https://doi.org/10.2307/2230256

Rooks, G., Matzat, U., & Sadowski, B. (2017). An empirical test of stage models of e-government development: Evidence from Dutch municipalities. *The Information Society*, *33*(4), 215–225. https://doi.org/10.1080/01972243.2017.1318194

Sabani, M., Savvas, I., Poulakis, D., & Makris, G. (2022). Quantum Key Distribution: Basic Protocols and Threats. *Proceedings of the 26th Pan-Hellenic Conference on Informatics*, 383–388. https://doi.org/10.1145/3575879.3576022

Saracevic, T. (2007). Relevance: A review of the literature and a framework for thinking on the notion in information science. Part II: nature and manifestations of relevance. *Journal of the American Society for Information Science and Technology*, *58*(13), 1915–1933. https://doi.org/10.1002/asi.20682

Saunders, M., Thornhill, A., & Lewis, P. (2019). *Research methods for business students* (Eigth Edition). Pearson.

Schamber, L., Eisenberg, M. B., & Nilan, M. S. (1990). A re-examination of relevance: Toward a dynamic, situational definition. *Information Processing & Management*, *26*(6), 755–776. https://doi.org/10.1016/0306-4573(90)90050-C

Schrödinger, E. (1926). Quantisierung als Eigenwertproblem. *Annalen Der Physik*, *384*(4), 361–376. https://doi.org/10.1002/andp.19263840404

Shor, P. W. (1994). Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. In L. M. Adleman & M.-D. Huang (Eds.), *Algorithmic Number Theory* (Vol. 877, pp. 289–289). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-58691-1_68

Siau, K., & Long, Y. (2005). Synthesizing e-government stage models – a meta-synthesis based on meta-ethnography approach. *Industrial Management & Data Systems*, *105*(4), 443–458. https://doi.org/10.1108/02635570510592352

Singh, K., Abraham, R., Yadav, J., Agrawal, A. K., Kolar, P., Misra, M., & Yadav, A. (2023). Analysis of barriers for sustainable agro-food supply chain: An interpretive

structural modeling and MICMAC approach. *Environment, Development and Sustainability*, *26*(10), 25311–25333. https://doi.org/10.1007/s10668-023-03680-5

Sivaprakasam, R., Selladurai, V., & Sasikumar, P. (2015). Implementation of interpretive structural modelling methodology as a strategic decision making tool in a Green Supply Chain Context. *Annals of Operations Research*, *233*(1), 423–448. https://doi.org/10.1007/s10479-013-1516-z

Sjöberg, M. (2017). *Post-quantum algorithms for digital signing in Public Key Infrastructures.* KTH Royal Institute of Technology.

Smith, F. L. (2020). Quantum technology hype and national security. *Security Dialogue*, *51*(5), 499–516. https://doi.org/10.1177/0967010620904922

Smulders, F., & Dorst, K. (2007). Towards a co-evolution model of the NPD-Manufacturing interface. *In Proceedings of the 16th International Conference on Engineering Design (ICED'07)*, 1–12.

Smulders, F., Kamp, A., & Fortin, C. (2018). The CDIO framework and new perspectives on technological innovation. *The 14th International CDIO Conference: Proceedings – Full Papers*, 40–52.

SOG-IS Management Committee. (2010). *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates Version 3.0*. SOG-IS Management Committee

Solli-Sæther, H., & Gottschalk, P. (2010). The Modeling Process for Stage Models. *Journal of Organizational Computing and Electronic Commerce*, *20*(3), 279–293. https://doi.org/10.1080/10919392.2010.494535

Sood, V., & Chauhan, R. P. (2024). Archives of Quantum Computing: Research Progress and Challenges. *Archives of Computational Methods in Engineering*, *31*(1), 73–91. https://doi.org/10.1007/s11831-023-09973-2

Taherdoost, H. (2017). Understanding of e-service security dimensions and its effect on quality and intention to use. *Information & Computer Security*, *25*(5), 535–559. https://doi.org/10.1108/ICS-09-2016-0074

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

Teece, D. J. (2014). A dynamic capabilities-based entrepreneurial theory of the multinational enterprise. *Journal of International Business Studies*, *45*(1), 8–37. https://doi.org/10.1057/jibs.2013.54

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, *51*(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007

Teece, D. J., Peteraf, M. A., & Leih, S. (2016). Dynamic Capabilities and Organizational Agility: Risk, Uncertainty and Entrepreneurial Management in the Innovation Economy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2771245

Teece, D. J., & Pisano, G. (1994). The Dynamic Capabilities of Firms: An Introduction. *Industrial and Corporate Change*, *3*(3), 537–556. https://doi.org/10.1093/icc/3.3.537-a

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z

Thales. (2019). *Upgrading Existing Security Systems to Agile Quantum-Safe with SafeNet Luna HSMs and SafeNet High Speed Encryptors. 2019.* Thales.

The Hague Security Delta. (2019). *Understanding the Strategic and Technical Significance of Technology for Security. Implications of Quantum Computing within the Cybersecurity Domain.*

Thordsen, T., & Bick, M. (2023). A decade of digital maturity models: Much ado about nothing? *Information Systems and E-Business Management*, *21*(4), 947–976. https://doi.org/10.1007/s10257-023-00656-w

Tibbetts, J. (2019). *Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers* (LLNL-TR--790870, 1566798, 987895; p. LLNL-TR--790870, 1566798, 987895). https://doi.org/10.2172/1566798

TNO. (2020). *Migration to Quantum-safe Cryptography. About Making Decisions on When, What and How to Migrate to a Quantum-safe Situation*.

TNO, CWI, & AIVD. (2024). *The PQC Migration Handbook. Guidelines for Migrating to Post-Quantum Cryptography*.

Van Der Duin, P. A., & Ortt, J. R. (2020). *Organizing, Implementing, and Assessing Contextual Innovation Management* (pp. 109–122). https://doi.org/10.4324/9781315687131-7

Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*, *19*(4), 241–246. https://doi.org/10.1007/s10676-017-9429-1

Vermeer, M., & Peet, E. (2020). *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*. RAND Corporation. https://doi.org/10.7249/RR3102

Vitharana, P., & Mone, M. A. (2008). Measuring Critical Factors of Software Quality Management: Development and Validation of an Instrument. *Information Resources Management Journal*, *21*(2), 18–37. https://doi.org/10.4018/irmj.2008040102

Vogt, S., & Funke, H. (2021). How Quantum Computers threat security of PKIs and thus eIDs. *Open Identity Summit 2021*. https://dl.gi.de/handle/20.500.12116/36504,

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, *4*(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Wang, C. L., & Ahmed, P. K. (2007). Dynamic capabilities: A review and research agenda. *International Journal of Management Reviews*, *9*(1), 31–51. https://doi.org/10.1111/j.1468-2370.2007.00201.x

Warfield, J. N. (1974). Toward Interpretation of Complex Structural Models. *IEEE Transactions on Systems, Man, and Cybernetics*, *SMC-4*(5), 405–417. https://doi.org/10.1109/TSMC.1974.4309336

Weber. (2004). Editor's Comments: The Rhetoric of Positivism versus Interpretivism: A Personal View. *MIS Quarterly*, *28*(1), iii. https://doi.org/10.2307/25148621

Wiesmaier, A., Alnahawi, N., & Grasmeyer, T. (2021). *On PQC Migration and Crypto-Agility*.

Winter, S. G. (2003). Understanding dynamic capabilities. *Strategic Management Journal*, *24*(10), 991–995. https://doi.org/10.1002/smj.318

Yin, R. K. (2018). *Case study research and applications: Design and methods* (Sixth edition). SAGE.

Yunakovsky, S. E., Kot, M., Pozhar, N. O., Nabokov, D., Kudinov, M. A., Guglya, A., Kiktenko, E. O., Kolycheva, E., Borisov, A., & Fedorov, A. K. (2021). Towards

security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology*, *8*(1), 14. https://doi.org/10.1140/epjqt/s40507-021-00104-z

Zahra, S. A., & George, G. (2002). Absorptive Capacity: A Review, Reconceptualization, and Extension. *The Academy of Management Review*, *27*(2), 185. https://doi.org/10.2307/4134351

Zollo, M., & Winter, S. G. (2002). Deliberate Learning and the Evolution of Dynamic Capabilities. *Organization Science*, *13*(3), 339–351. https://doi.org/10.1287/orsc.13.3.339.2780

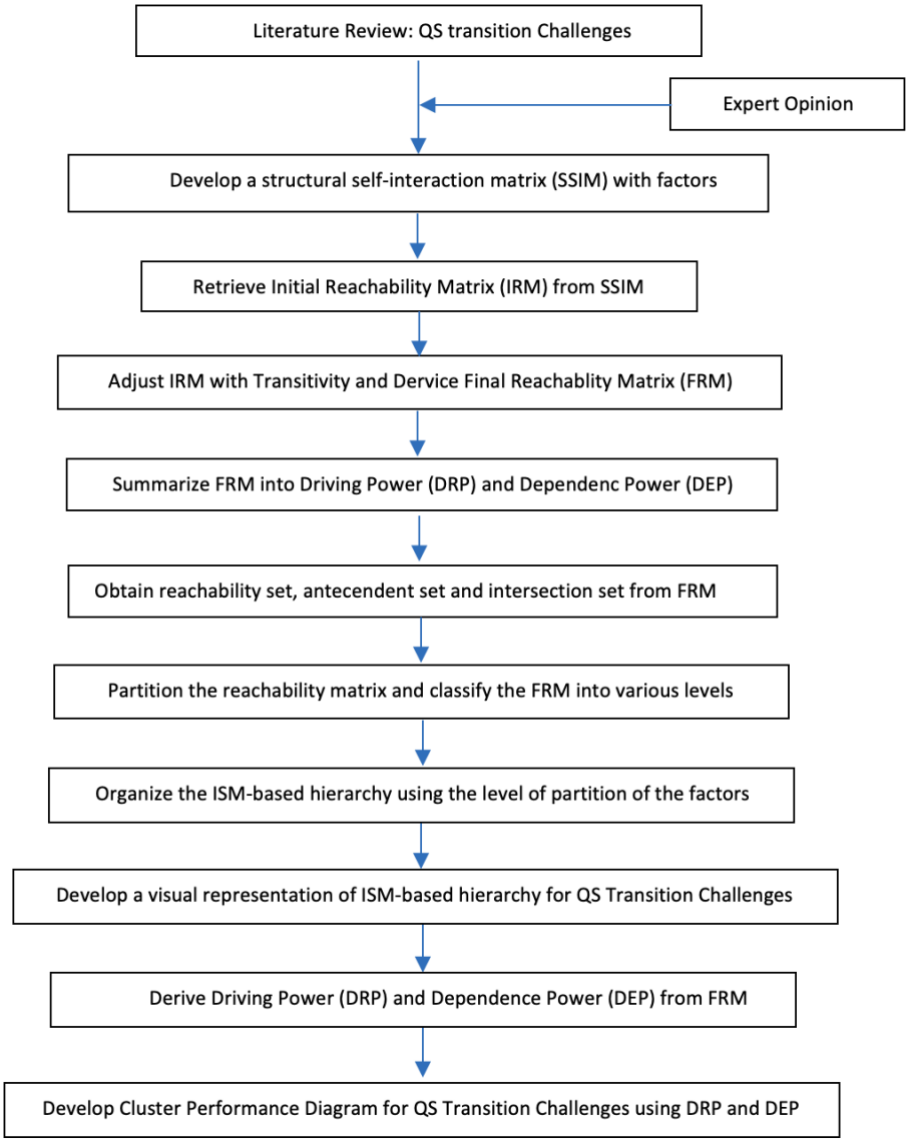
Appendices

Appendix A: List of Abbreviations

AFM	De Autoriteit Financiële Markten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AT	Agentschap Telecom
BZK	Dutch Ministry of the Interior and Kingdom Relations
CA	Certificate Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
CI	Critical Infrastructures
CII	Critical Information Infrastructure
COBIT	Control Objectives for Information and Related Technologies
CRQC	Cryptographically Relevant Quantum Computer
DC	Dynamic Capabilities
DEF	Dutch Ministry of Defense
DNB	De Nederlandsche Bank
EBA	European Bank Authority
EC	European Commission
eIDAS	electronic IDentification, Authentication, and trust Services
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EP	European Parliament
EZK	Dutch Ministry of Economic Affairs
FIN	Dutch Ministry of Finance
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
ICT	Information Communication Technology
ICTU	Information and Communications Technology Unit
IEEE	Institute of Electrical and Electronics Engineers
IenW	Dutch Ministry of Infrastructure and Water Management
IETF	Internet Engineering Task Force
IS	Information Systems
JenV	Dutch Ministry of Justice and Security
MRA	Mutual Recognition Agreement
NCSC	National Cyber Security Centre
NIS 2	Directive Network and Information Security II Directive

NIST	National Institute of Standards & Technology
NIST CSF	NIST Cybersecurity Framework
OC	Organizational Capabilities
PKI	Public Key Infrastructures
PQC	Post Quantum Cryptography
QS	Quantum-safe
QKD	Quantum Key Distribution
QTSP	Qualified Trust Service Provider
RA	Readiness Assessment
RDI	Rijksinspectie Digitale Infrastructuur
SLR	Systematic Literature Review
SME	Small-Medium Enterprise
SNDL	Store Now Decrypt Later
SOG-IS	Senior Officials Group-Information Systems Security
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TNO	Netherlands Organisation for Applied Scientific Research
VWS	Dutch Ministry of Health, Welfare and Sport

Appendix B: Flow Diagram of ISM-MICMAC



Note. Adapted from "Interpretive Structural Modelling (ISM) Approach: An Overview," by Attri et al. (2013, p.4).

Appendix C: Interview & Workshop Protocols

Phase 1: Email Sample- Interview Request

Title: Interview Request
Dear _____,

My name is Ini Kong, and I am a Ph.D. Researcher at Delft University of Technology (TU Delft) who will be conducting the research under the supervision of Prof. Dr. Ir. Marijn Janssen and Prof. Dr. Ir. Nitesh Bharosa.

The research on *Transition towards Quantum-safe (QS) Public Key Infrastructure (PKI) system* is part of a larger project called Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations (HAPKIDO). Our research aims to guide organizations transitioning towards a QS PKI system by developing growth models for QS transition.

We are currently conducting interviews with experts in practice to know more about the challenges that organizations encounter when transitioning towards a QS PKI system. We believe that your inputs are highly valuable and were hoping you would be willing to be interviewed for this study.

The interview would last about ~ 60 minutes. You and your company's name will remain strictly confidential and will not be used in any way. We would be happy to share the transcripts after the interview and follow up with our findings. If you are available for the interview, please indicate your availability in the upcoming weeks. Further information on the project and an informed consent sheet for the interview are attached in the email.

Thank you very much for your consideration in being interviewed for this study.

We look forward to hearing from you.

Kind regards,

Ini Kong
PhD candidate | Engineering Systems and Services Department
Faculty of Technology, Policy & Management
Delft University of Technology

Phase 1: Interview Protocol

About the research

The research on Transition towards Quantum-safe (QS) Public Key Infrastructure (PKI) system is part of a larger project called Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations (HAPKIDO). Our research aims to guide organizations transitioning towards a QS PKI system by developing growth models for QS transition.

About the Interview

From today's interview, we would like to hear about different challenges that organizations may encounter when transitioning towards a QS PKI system. We have gathered the list of challenges from the literature and would like to discuss these challenges in practice.

Consent regarding Data

The interview is estimated to take about ~60 minutes, and the result of the interview will be stored according to TU Delft Research Data Framework Policy (https://data.4tu.nl/). All the information is solely used for research purposes, and all the confidential data will be deleted once the project is completed. Your participation is voluntary, and you have the right to stop the interview at any time. The result will be anonymized so that it does not trace back to the individual participants.

Time Schedule (60 minutes)

Introduction (5 minutes)
Research background (5 minutes)
List of Questions (45 minutes)
a. About Interviewee
- Could you briefly introduce yourself and your organization?
- What is your title or position in the organization?
- What are your general job responsibilities?
- Who are the internal and external stakeholders?

b. Current challenges & Major concerns
-What are the current challenges and major concerns for QS transition?

c. Challenges in Practice
- Given an overview of the list of challenges found in the literature, are there any similar/different challenges in the context of QS transition? And why?
- Are there any additional challenges that you see missing on the list that are considered important and relevant in the context of the QS transition?

d. Opportunities to address challenges
- How may these challenges in the context of QS transition be addressed?

Closing (5 minutes)

Phase 4: Evaluation Interview Protocol

About the Research

The research on developing a stage model for Quantum-safe (QS) Transition is part of a larger project called Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations (HAPKIDO). The concept of stage models allows us to understand how an organization can be arranged and evolve toward its desired stage.

About the Interview

The interview ensures that the developed stage model is not only informed by research but also shaped by the needs and experiences of practitioners, where feedback is actionable and representative of the intended user base.

Key Objectives

-To share key insights on the stage model for QS Transition
-To discuss discontinuities & key actions needed across organizations
-To gather feedback on the developed growth model in practice

Consent regarding the data

The interview is estimated to take about ~90 minutes, and the result of today's interview will be stored according to TU Delft Research Data Framework Policy (https://data.4tu.nl/). To properly process the answers today, notes will be made & Mentimeter will be used to collect the data. All the information is solely used for research purposes, and all the confidential data will be deleted once the project is completed. Your participation is voluntary, and you have the right to stop the interview at any time. The result will be anonymized so that it does not trace back to the individual participants.

Time Schedule (90 minutes)

Introduction (5 minutes)
    -An overview of the objectives & agenda of the workshop
Research Background (20 minutes)
    -Share key insights from the research
    -Explain the stage model for QS Transition
Discussion Part 1: Discontinuities & Actions needed across organizations (30 minutes)
    -Discuss the details of discontinuities & actions needed
Discussion Part 2: A Stage Model for QS Transition (30 minutes)
    -Discuss the relevance & usefulness of the growth model
Next Steps & Closing (5 minutes)
    -Provide details on next steps & conclude the workshop

Phase 2: Workshop Protocol (ISM-MICMAC)

About the Research

The research on *Transition towards Quantum-safe (QS) Public Key Infrastructure (PKI) system* is part of a larger project called HAPKIDO (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations). Our research aims to guide organizations transitioning towards a QS PKI system by developing growth models for QS transition.

About the Workshop

During the workshop, we will examine the contextual relationship between QS transition challenges that were identified through the literature review and semi-structured interviews. We use an Interpretive Structural Modelling (ISM) and Cross-Impact Matrix Multiplication (MICMAC) analysis to understand the contextual interaction between these challenges and classify these challenges into driving power and dependence power. The results of the workshop will show QS transition challenges in a hierarchical structural model and identify key dominant challenges for organizations to prioritize.

Key Objectives

-To fill out the Structural Self-Interactive Matrix (SSIM) chart
-To examine the contextual relationship between QS transition challenges

Consent regarding Data

The workshop is estimated to take about ~150 minutes, and the result will be stored according to TU Delft Research Data Framework Policy (https://data.4tu.nl/). All the information is solely used for research purposes, and all the confidential data will be deleted once the project is completed. Your participation is voluntary, and you have the right to stop the workshop at any time. The result will be anonymized so that it does not trace back to the individual participants.

Time Schedule (150 minutes)

Introduction (5 minutes)
Research Background (10 minutes)
    -List of challenges from the literature review and semi-structured interviews
Instructions regarding the SSIM chart (15 minutes)
Discussion Part I: Fill out the SSIM chart (40 minutes)
Break (15 minutes)
Discussion Part II: Fill out the SSIM chart (60 minutes)
Closing (5 minutes)

Phase 3: Workshop Protocol

About the Research

The research on *Transition towards Quantum-safe (QS) Public Key Infrastructure (PKI) system* is part of a larger project called HAPKIDO (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations). Our research aims to guide organizations transitioning towards a QS PKI system by developing growth models for QS transition.

About the Workshop

From today's workshop, we would like to hear about the list of actions needed to address challenges. We have gathered the list of challenges from the literature and practice. A deeper understanding of how we can address these challenges may provide us with important insights into QS transition.

Consent regarding Data

The workshop is estimated to take about ~60 minutes, and the result will be stored according to TU Delft Research Data Framework Policy (https://data.4tu.nl/). All the information is solely used for research purposes, and all the confidential data will be deleted once the project is completed. Your participation is voluntary, and you have the right to stop the workshop at any time. The result will be anonymized so that it does not trace back to the individual participants.

Time Schedule (60 minutes)

Introduction (5 minutes)

Research Background (10 minutes)

-Share key insights from the ISM-MICMAC workshops

-Explain the stages of growth model for QS Transition

Discussion (40 minutes)

a. List of Challenges

-Is the challenge at the right level?

If not, at which level can this challenge be addressed?

-Are there any challenges that need to be added/moved/dropped/modified?

b. List of Actions

-What actions address this challenge?

-Are there any actions that need to be added/moved/dropped/modified?

Next Steps & Closing (5 minutes)

-Provide details on next steps & updates about an Organizational QS Readiness Assessment Tool

Phase 4: Email Sample- Evaluation Workshop Request

Title: Workshop Request
Dear _____,

We hope this email finds you well. We are pleased to invite you to participate in our upcoming workshop titled "A Growth Model for Quantum-Safe (QS) Transition."

The workshop will take place on:

During the workshop, we will delve into a developed growth model for QS transition based on Post-Quantum Cryptography (PQC). This is an initial exploration of a transition roadmap with a series of stages. The concept of the growth model enables organizations to assess where they stand and which actions they can take towards Quantum resilience.

Our focus is to share key insights learned from the research and discuss the overall usefulness of the growth model.

The workshop will be held at the following address:

Please let us know if you are able to attend by kindly accepting or declining this email.

We look forward to welcoming you as a participant in the workshop.

If you have any comments or questions about the workshop, please do not hesitate to contact me for further information. Thank you!

Best regards,

Ini Kong
PhD candidate | Engineering Systems and Services Department
Faculty of Technology, Policy & Management
Delft University of Technology

Phase 4: Evaluation Workshop Protocol

About the Research

The research on developing a stage model for Quantum-safe (QS) Transition is part of a larger project called (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations (HAPKIDO). The concept of stage models allows us to understand how an organization can be arranged and evolve toward its desired stage.

About the Workshop

The workshop ensures that the developed stage model is not only informed by research but also shaped by the needs and experiences of practitioners, where feedback is actionable and representative of the intended user base.

Key Objectives

-To share key insights on the stage model for QS Transition
-To discuss discontinuities & key actions needed across organizations
-To gather feedback on the developed growth model in practice

Consent regarding the data

The workshop is estimated to take about ~120hrs, and the result of today's workshop will be stored according to TU Delft Research Data Framework Policy (https://data.4tu.nl/). To properly process the answers today, notes will be made & Mentimeter will be used to collect the data. All the information is solely used for research purposes, and all the confidential data will be deleted once the project is completed. Your participation is voluntary, and you have the right to stop the workshop at any time. The result will be anonymized so that it does not trace back to the individual participants.

Time Schedule (120 minutes)

Introduction (5 minutes)
    -An overview of the objectives & agenda of the workshop
Research Background (20 minutes)
    -Share key insights from the research & explain the stage model for QS Transition
Discussion Part 1: Discontinuities & Actions needed across organizations (40 minutes)
    -Discuss the details of discontinuities & actions needed
Break (10 minutes)
Discussion Part 2: A Stage Model for QS Transition (40 minutes)
    -Discuss the relevance & usefulness of the growth model
Next Steps & Closing (5 minutes)
    -Provide details on next steps & conclude the workshop

Appendix D: Iterations of the Growth Model

Appendix D contains iterations of the growth model for QS transition discussed in Section 6.3. The synthesized hierarchical model of QS transition challenges shown in Figure 20 in Section 6.2 provided an initial basis for structuring five stages of the growth model for QS transition.

First Iteration: With a List of Challenges per Stage

	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Ecosystem	Complex Technical Interdependencies QS standards (availability)	Collaboration Urgency QS Governance QS solutions (Selection) QS solutions (Reliable & Secure)	Policy & Regulations QS hardware & Software		
Organization			Urgency Knowledge	Business Case Legacy System (CAs) Skills & Personnel	Legacy System (End Users) QS Governance

In the first Iteration, the QS transition challenges were divided into two levels in the first iteration: Ecosystem Level and Organizational Level. The growth model shows that the challenges at the ecosystem level are dominant at the earlier stages, and challenges at the organizational level are influenced by these challenges at the ecosystem level.

Second Iteration: With a List of Challenges per Stage

	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Ecosystem	Complex Technical Interdependencies QS standards (availability)	Collaboration QS standards (selection)	Policy & Regulations QS hardware & Software		
Inter-Organization	Awareness	QS Governance QS solutions (Selection) QS solutions (Reliable & Secure)	Urgency Knowledge	Legacy System (CAs)	
Intra-Organization			Awareness	Business Case Skills & Personnel	Legacy System (End Users) QS Governance

In the second iteration, the growth model was further divided into three levels: ecosystem level, inter-organizational level, and intra-organizational level. Three challenges that were

initially placed at Stage 2 at the ecosystem level in the first iteration were placed at the inter-organizational level. Two challenges at Stage 3 and one challenge at Stage 4 that were initially placed at the organizational level were reassigned to the inter-organizational level as they were considered more appropriately addressed at that level.

One challenge at Stage 2 was added at the inter-organizational level, and one challenge at Stage 3 was added at the intra-organizational level. The challenge 'Awareness' was identified as crucial, as it enables organizations to understand the relevance of QS transition, align stakeholders, and drive coordinated actions across levels. However, the findings suggest that addressing awareness at the intra-organizational level may depend on overcoming dominant challenges at earlier stages across the ecosystem and inter-organizational level.

Third Iteration: With a List of Actions Needed per Stage

	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Ecosystem (Discontinuities)	Acknowledgement of risks & vulnerabilities of quantum threats Finalized list of PQC Standardization	Establishment of a steering committee and international working groups for QS transition Establishment of a testing environment to evaluate QS cryptographic solutions	Availability of selected QS cryptographic solutions validated through testing Developed policies & regulations that support QS transition	Availability of certified hardware and software suitable with QS cryptographic solutions	Development of a cross-organizational coordination mechanism for QS cryptographic solutions
Inter-Organization	Create awareness on importance and benefits of adopting QS solutions in the existing systems	Define clear roles, responsibilities and decision-making structure for QS governance Set up a testing environment to select and adopt relevant QS cryptographic standards Select and adopt relevant QS cryptographic standards that are suitable	Develop sector-wide QS transition plans (e.g.,industry wide initiatives) Develop certifiedhardware and software that are suitable with QS cryptographic solutions	Modify legacy systems with selected QS cryptographic solutions Establishment of an expertise center to share knowledge (e.g., workshops, training, resource for QS technology, best practices)	
Intra-Organization			Create awareness on the importance of QS transition and the complexities in implementing QS cryptographic solutions Finalize risk & impact assessment (e.g., interdependencies, processes and regulations etc.) Communicate tendering requirements for QS products and services	Identify business case for QS transition, conduct cost-benefit analysis, value proposition on implementing QS cryptographic solutions Recruit/ train personnel with necessary skills and expertise on QS transition	Modify legacy systems (hardware and software) with selected QS cryptographic solutions Outline clear roles, responsibilities and decision making structure for QS governance

In the third iteration, the challenges at the ecosystem level are conceptualized as discontinuities, representing boundary markers to move between stages and act as necessary conditions that must be met in the ecosystem to move from one stage to the next. This is because dynamics at the ecosystem level are highly complex, multi-actor, and only partially observable. As such, they are more appropriately framed as 'what needs to happen' rather than as discrete actions. In contrast, the challenges at the inter-and intra-organizational levels were translated into key actions, reflecting 'what actors can do' to address them. Although complexity remains at these levels, it is more structured and situated within institutional and organizational contexts, allowing challenges to be more directly translated into actionable guidance.

Fourth Iteration: With a List of Actions Needed per Stage

	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Ecosystem (Discontinuities)	Acknowledgement of risks & vulnerabilities of quantum threats Finalized list of PQC Standardization	Establishment of a steering committee and international working groups for QS transition Establishment of a testing environment to evaluate QS cryptographic solutions	Availability of selected QS cryptographic solutions validated through testing Developed policies & regulations that support QS transition	Availability of certified hardware and software suitable with QS cryptographic solutions	Availability of lessons learned and best practices from the implementation of QS cryptographic solutions Development of a cross-organizational coordination mechanism for QS cryptographic solutions
Inter-Organization	Participate in discussions on QS cryptographic solutions with industry, academia, and government	Define clear roles, responsibilities and decision-making structure for QS governance Establish a testing environment to test & select suitable QS standards	Develop hardware and software that are suitable with QS cryptographic solutions Developed relevant sector-wide guidelines that support QS transition	Migrate non-PQC systems of CAs to selected QS cryptographic solutions Facilitate an expertise center to share knowledge and skills needed for QS transition	Foster collaboration across sectors on future research, development and standard setting to address evolving security threats challenges
Intra-Organization	Raise awareness on the importance of implementing QS cryptographic solutions	Conduct assessments to identify the level of risk, readiness & impact for QS transition	Communicate tendering requirements for products and servies (e.g., hardware and software using QS cryptographic solutions)	Modify non-PQC part of the existing systems in a smaller scale with QS cryptographic solutions Provide training and support to ensure that QS transition is managed with necessary skills and expertise	Finalize the adoption of QS cryptographic solutions in a scaled environment across all systems Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory and technological changes

In the fourth iteration, the list of discontinuities and the list of key actions have been further refined. The key actions have been identified across inter-and intra-organizational levels at each stage. The findings suggest that organizations not only need to navigate the list of discontinuities in the ecosystem but also need to be prepared to take actions needed at each stage to collectively move to QS PKIs.

List of Publications

HAPKIDO. (2026). Quantum-safe Transition Roadmap Handbook. TNO. Available at: https://project-hapkido.nl/deliverables/

Kong, I., Janssen, M. & Bharosa, N. (2026). Self-Assessment for QS Transition. TNO. https://project-hapkido.nl/deliverables/self-assessment-qs-transition/

Kong, I., Janssen, M. & Bharosa, N. (2024). Navigating through the Unknowns-Readiness Assessment Model for Quantum-safe Transition. Electronic Government: 23rd IFIP WG 8.5 International Conference, EGOV 2024, Ghent-Leuven, Belgium, September 3–5, 2024, Proceedings. p. 438 – 453. https://dx.doi.org/10.1007/978-3-031-70274-7_27

Kong, I., Janssen, M. & Bharosa, N. (2024). Deriving Government Roles for directing and supporting Quantum-safe Transitions. DGO 2024: Proceedings of the 25th Annual International Conference on Digital Government Research, p.507 – 514. https://doi.org/10.1145/3657054.3657114

Kong, I., Janssen, M. & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. [**Best ESS PhD Paper Award].** Government Information Quarterly. 41, 1, 101884. https ://doi.org/10.1016/j.giq.2023.101884

Kong, I., Janssen, M. & Bharosa, N. (2024). Organizational Readiness Model for Quantum-safe Transition. TNO. https://project-hapkido.nl/deliverables/organizational-readiness-model-quantum/

Christiansen, L., Kong, I., & Bharosa, N. (2023). Governing the transition to quantum-safe PKIs in the Netherlands: Paving the way for our quantum-safe future. TNO. https://project-hapkido.nl/deliverables/governing-transition-quantum-safe-pkis/

Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition. In: CEUR Workshop Proceedings. 3449. https://resolver.tudelft.nl/uuid:40471115-106c-4cd7-8e0b-917155dc1008

Kong, I. (2022). Transitioning towards quantum-safe government: Examining stages of growth models for Quantum-safe public key infrastructure systems. Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022. https://doi.org/10.1145/3560107.3560182

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). **[Best Management Paper Award].** https://doi.org/10.1145/3543434.3543644

Curriculum Vitae

Ini Kong is a PhD candidate at the Department of Engineering Systems and Services, Faculty of Technology, Policy and Management, Delft University of Technology, The Netherlands. Her PhD research is the first to address the socio-technical aspects of QS transition, presenting a novel approach in identifying different stages of growth model that investigates how organizations can achieve ecosystem-wide quantum safety. Her research is part of a larger project called Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations (HAPKIDO) funded by Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

In 2022, she received the Best Management Paper Award at the 23rd Annual International Conference on Digital Government Research for her work on addressing threats of quantum computing technology on Public Key Infrastructure (PKI) systems and identifying socio-technical transition challenges for a quantum-safe government. For providing original insights on a topic of high scientific importance and utmost practical importance, Ini received the Best ESS PhD Paper Award at the Faculty of Technology, Policy and Management with her paper "*Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions."*

Ini is actively involved in raising awareness and communicating with diverse stakeholders on the topic of PQC Transition. She participated as an invited speaker to present her research work at Rijksoverheid, the ISACA Risk event, and the Dutch Central Bank, among others. She has provided external subject-matter expertise and feedback to European-level post-quantum cryptography coordination activities and at the meeting of the Centre for European Policy Studies (CEPS) task force on *Strengthening the EU transition to a Quantum-safe World.* Her research work has been cited by The World Bank Group on Public Key Infrastructure.

During her research, she also participated in the International Cyber Security Summer School, organized by Hague Security Delta. She collaborated with a project team to tackle a challenge from De Nederlandsche Bank (DNB) that focused on analyzing quantum computing threats in the banking sector. She learned about the complexities of information security infrastructures during a visit to NATO Communication Information Agency (NCIA) and gained insights into transnational cybercrime during a visit to Europol.

Ini holds a Master of Science in Environment and Society studies from Radboud University. During her graduate studies, Ini completed her internship at Provincie Gelderland in the Energy Transition department. Ini also holds a Double Major in Bachelor of Arts with Honors in Political Science and Sociology from the University of Toronto, Canada.

Beyond her research, Ini is a volunteer at the Skilling and Education team at Women4Cyber Netherlands. Based in the Hague, Women4Cyber Netherlands is the Dutch chapter of the Women4Cyber initiative that is aimed at promoting, encouraging, and supporting the participation of women in cybersecurity.