HAPKIDO

Deliverable 1.2

Application of the societal risk assessment method

Team on work-package 1

Yoram Meijaard – TNO

Dayana Spagnuelo – TNO

Nitesh Bharosa – TU Delft

Contents

List of abbreviations

BIA	Business Impact Analysis
CA	Certificate Authority
CARAF	Crypto Agility Risk Assessment Framework
CIA	Confidentiality, Integrity, Availability
DH	Diffie-Hellman key exchange method
ECC	Elliptic Curve Cryptography
eIDAS	Electronic Identification And Trust Services
GRNV	Integrated Risk Analysis National Security
HAPKIDO	Hybrid Approach for Quantum-safe Public Key Infrastructure Development for Organisations
PA	Policy Authority
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
RA	Risk Assessment
RSA	Rivest–Shamir–Adleman is a public-key cryptosystem
SECRAM	Security Risk Assessment Methodology
SNDL	Store-now-decrypt-later
SRA	Societal Risk Assessment
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWOT	Strengths, Weaknesses, Opportunities, Threats
TSP	Trust Service Provider
QC	Quantum Computing
QTSP	Qualified Trust Service Provider

Summary

As the number of qubits in quantum computers increases, there is growing interest in the potential and the risks. This paper zooms in on the risks posed by quantum computers on public key infrastructures (PKI). The main objective of this study is to provide a preliminary overview of the main societal risks posed by quantum computing on PKI-based digital systems. More precisely, we look at the effects of a quantum computer's arrival before adequate measures are taken to migrate all cryptographic algorithms to a quantum-safe equivalent. In line with the scope of the HAPKIDO project, we focus on the risks for three sectors: Government, Banking and Telecom. This report builds on the Societal Risk Assessment (SRA) method developed in the first part of Work Package 1 of HAPKIDO (Deliverable 1.1). Using workshops with representatives of the respective sectors, we applied the previously developed SRA method. This approach allowed us to gain a deeper understanding of the risks posed by quantum computing to the critical business processes in Government, Banking and Telecom.

The three workshops with representatives of the three sectors reveal that the impact of the quantum computer on PKI can be devastating. The prevalence of PKI in society is such that every citizen and organisation will be impacted. From a cyber-security perspective, the impact can be measured regarding confidentiality, integrity, and availability. Two treats posed by quantum computers are: (1) real-time access to systems and data, and (2) store now, decrypt later. Real-time access yields risk for confidentiality, integrity, and availability. Store now, decrypt later mainly poses risks for confidentially, implying that while an adversary cannot access a quantum computer now, it stores encrypted secrets that can be decrypted later. This may lead to political or societal trust concerns (e.g., political, state or industry secrets out in the open can damage trust in institutions, even if they are not up to date anymore). While this scenario mainly undermines confidentiality on a technical level, there are also risks regarding the integrity of information. If an unauthorised person gains access to stored data, it could decrypt and modify it. And if that data is inserted back into source systems, the correctness, completeness, validity, and non-repudiation cannot be guaranteed.

Regarding real-time access and confidentially, service providers cannot guarantee the exclusivity and privacy of an interaction or transaction. Adversaries could easily eavesdrop on digital interactions. Regarding integrity, service providers cannot guarantee the trustworthiness of digital services. For instance, the integrity of telecom services such as voice and text will no longer be assured. Routers and TV-boxes at home may be comprised. The authenticity of news feeds cannot be assured. The identity of the persons/organisations on the other side of the phone line cannot guaranteed anymore.

When it comes to real-time access availability, the computing capacity of quantum computers could enable significant service and network disruptions. On an organisation level, the most likely action strategy – with the least damage for the organisation – is shutting down their services. On a societal level, one bank shutting down or one governmental service becoming unavailable might be manageable. However, the combined disruption of services will be devastating. Citizens will no longer be able to access governmental and financial services. The inability to use governmental services will cause social upheaval and disruption to everyday life.

Moreover, the inability to use financial services and pay for food may be much worse. The compounded effects of which will be much worse. System banks without the ability to digitally borrow or lend money internationally will collapse, causing a significant economic downturn. Consequently, the term' quantum apocalypse' is sometimes used to describe the compounded impact of quantum computers on societies relying on digital infrastructures. The anticipated

quantum apocalypse assumes that current PKI systems will not undergo upgrades with quantum-safe cryptography and have a low level of quantum readiness.

To become 'quantum ready' or 'safe', the current ubiquitous asymmetric cryptographic algorithms used in many PKI systems must be replaced by quantum-safe algorithms, also known as post-quantum cryptography (PQC) algorithms. When completing this report, some PQC algorithms are being selected and standardised by several standardisation bodies, including the NIST. However, the transition challenge from classical crypto to PQC is immense: there are billions of old and new devices that need to transition to the PQC suite of algorithms, leading to a multidecade transition process that must account for aspects such as security, hardware performance, ease of secure implementation, compliance and more (see for instance AIVD 2023).

Overall, the workshop participants that led to this report agree that the SRA developed is valuable and comprehensive. The SRA stimulates a more precise discussion on the impact of quantum computers on digital systems that rely on PKI. The participants would recommend other organisations use the method as an awareness creation and learning instrument and an instrument for mobilising actors to develop transition strategies. The latter remains an open question: what to do next? The remainder of the HAPKIDO project will focus on guiding organisations to start the migration to quantum-safe cryptography.

1 Introduction

1.1 Background

Quantum computing promises transformative simulation and modelling capabilities across various industries (WEF, 2022). Quantum computing is a relatively new combination of technologies with the potential to tackle computational problems that conventional computing cannot. If this potential is harnessed, it promises to provide great computational power, facilitating scientific breakthroughs in many fields (Gill et al., 2021; Vermaas, 2017). However, while it is expected to provide benefits in the field of cybersecurity, it is simultaneously expected to threaten the security of our digital society (Raban & Hauptman, 2018).

Today, most online communication is secured by leveraging cryptography that is hard to break. Part of the established cryptographic standards builds on the public key infrastructure (PKI) model. PKI is "a combination of software, hardware, roles, guidelines and procedures required to manage keys as digital certificates" (Bharosa et al., 2015). Essentially, it is a way to put cryptography as a technology to use and create digital trust. PKI plays a crucial role in the digital society as we know it. Many governments and businesses employ PKI for core processes that may become insecure or unavailable when quantum computers break the cryptographic algorithms foundational to PKI (Christiansen, Janssen & Bharosa, 2023). PKIs allow for various processes, including online authentication, secure communication of sensitive data between medical professionals, and signing legally binding using electronic signatures. PKI usage is interwoven in many, if not most, of our online activities, especially those requiring trust. As Amadori, Duarte & Spini (2022) discussed, several widely used data-sharing protocols use PKIs, such as TLS, SSH and S/MIME. TLS is widely used for secure communication, SSH is used to operate network services securely over an unsecured network, and S/MIME is used to encrypt and sign mail.

Today's industry-standard PKI schemes (based on X.509 certificates) can theoretically be broken, but this takes thousands of years in practice. After decades of trying, nobody has found a way to do so in a reasonable time. Nonetheless, quantum computers are expected to break modern public key cryptography using Shor's algorithm (Joseph e.a. 2022). As showed by Shor in 1994, quantum computers with sufficient stable qubits could break most currently used PKIs by efficiently solving the computational problems whose hardness is supposed to guarantee the security of the system. Since many sectors, including Government, Banking, and Telecom, depend on PKIs for digital communication, the rise of quantum computers significantly threatens the security of our digital society.

1.2 Unknown societal risks

The two most widespread public key algorithms for encrypting information today that can be broken with Shor's algorithm are Rivest–Shamir–Adleman (RSA) public-key cryptosystems and elliptic curve cryptography (ECC) (Joseph e.a., 2022). When it comes to breaking RSA and ECC, quantum computers pose two threats:

1. Store now, decrypt later.
2. Real-time access.

The first quantum threat, a store-now-decrypt-later (SNDL) attack, is already active. It corresponds to adversaries[1] capturing valuable encrypted information now, storing it and decrypting it later once quantum computers are available. For instance, organisations handling data that will remain confidential 20 years from now or organisations developing long-lived systems that will

[1] Adversaries can refer to (non)friendly state actors, private organizations or criminal organizations.

still be used decades from now (see, for instance, AIVD, 2023). The SNDL attack assumes that this information remains valuable in the future. While this scenario mainly undermines confidentiality on a technical level, it may lead to more political or societal trust concerns.

The second quantum threat is accessing systems, services or data in real-time (i.e. during digital interactions). This threat generates a *real-time access* scenario, meaning that an adversary uses a quantum-computer to do real-time decryption of asymmetric cryptography or real-time forgery of certificates. Such an attack would allow an actor to break the confidentiality of secrets, affect the integrity of documents or impersonate an authenticated entity.

We do not yet know the consequences of these two types of quantum threats for PKI systems used in various sectors (for instance, Kong e.a. 2022). The technological consequences (i.e., Public Key Cryptography standards easily being broken) are mentioned above, but how this will impact society is unclear. As part of the HAPKIDO project, this report focusses on the societal risks of quantum-unsafe PKI. The term risk is more suitable, as it implies, on the one hand, an element that we would like to protect and, on the other hand, uncertainty. Since digital trust is something of value that we would like to protect, there is significant uncertainty surrounding the development of a large enough quantum computer to break current PKC standards.

The societal risks are not clearly known, increasing the vagueness of the problem. A vague problem causes issues in solving it. There is a need to know more about the societal risks so (1) it becomes clear how pressing the matter of the quantum threat is and (2) where to focus future actions to avoid the worst effects.

By creating a shared picture of the societal risks in cooperation with actors involved with PKI, the problem perceptions of these actors start to align. The alignment of problem perceptions can bolster actor commitment to solving the matter in cooperation (Bruijn & Heuvelhof, 2008). This is particularly necessary in the case of the quantum threat to PKI, as PKI inherently involves many actors with differing roles in the trust chain. The other benefit of knowing the societal risks is that it can help to prepare for the transition to a solution. Ideally, stakeholders can decide where to prioritise mitigating the quantum threat by knowing what specific business processes and assets rely on PKI to face severe societal risks.

1.3 Objective of this study

There is little academic research on the societal risks of the quantum threat to digital services that rely on PKI (Klunder, 2022; Onkenhout,2023). **The main objective of this study is to provide a preliminary overview of the main societal risks posed by quantum computing on PKI-based digital systems.** In line with the HAPKIDO project, we focus on the risks for three sectors: Government, Banking and Telecom. This study builds on the Societal Risk Assessment method developed in the first part of Work Package 1 of HAPKIDO (deliverable 1.1).

1.4 Scope

We made several scoping choices for practical reasons. First, we focus on PKIs and systems that rely on PKIs (to distribute and validate their keys) in three sectors in the Netherlands: Government, Banking and Telecom. These sectors are in the scope of HAPKIDO, given their high dependence on secure digital information sharing. Even though this research focusses on the Netherlands, we expect that findings can be transferred to other EU and non-EU countries since most countries use the same PKC standards.

Secondly, this work-package focusses on PKI as opposed to PKC in general. More specifically, this research limits itself to PKIs with a hierarchical trust model. PKI is the applied form of PKC, generating trust necessary for societal applications. The hierarchical trust model is a widely adopted paradigm (Amadori et al., 2022). These two arguments justify the scope choice, as the societal risks of the quantum threat will be most significant when considering PKIs with a hierarchical trust model.

Thirdly, and in line with the previous scope choice, the scope excludes self-signed CAs used for applications within an organisation. Finally, the scope of this research is set to asymmetric cryptography. Symmetric cryptography is less vulnerable to the quantum threat, and applications can be relatively easily adapted compared to asymmetric cryptography. Research question

With the objective and the scope of the research set, the following research question was defined: ***'What are the expected societal risks of the quantum threats to PKI systems in Government, banking and the telecom sector in the Netherlands?'*** Answering this question is the focus of this report (HAPKIDO deliverable 1.2).

Here, we define risk as 'likelihood X impact'. Considering the uncertainty regarding when a quantum computer is strong enough to break the currently employed cryptographic algorithms, we focus more on impact than estimating the likelihood.

The second deliverable for work package 1 (deliverable 1.1) focuses on developing the method used in this deliverable. Accordingly, deliverable 1.1 focuses on the question: *What are the components of a method for assessing the potential societal risks of the quantum threats to PKI systems?*

1.5 Way of Working

To answer the main research question for all three sectors, the work package 1 team performed the same research activities for each sector in scope. The research activities include:

1. The work package team prepares a workshop based on initial contacts with stakeholders in a specific sector (i.e. Government, Banking or Telecom).
2. A 90-minute workshop with sector stakeholders is conducted. Workshop participants are asked to help fill in the SRA tables as much as possible. If needed, a second workshop is conducted.
3. The workshop results are analysed and interpreted by the team.
4. The team writes a draft report with the preliminary workshop results.
5. The preliminary results are shared with the sector experts for review.
6. The team processes the reviews in the final draft of the complete deliverable.
7. The draft deliverable is subject to a review by other HAPKIDO researchers.
8. The team processes the reviews in the final complete report.

At least three experts with deep knowledge on the PKI systems in a specific sector were present for each workshop.

Note that this research relies on workshops with (industry) experts and that the scope of the research is limited. This research cannot and does not cover all aspects of the three sectors in scope at the lowest level of detail. As there is variety across organisations in all three sectors, the risks we formulated with the organisations may not be the same for other organisations in that sector. Instead, this research aims to provide a high-level overview of the principal risks of quantum computers on the PKI in these sectors.

1.6 Reading guide

This document proceeds as follows. Section 2 provides a brief overview of the SRA method. A more detailed description of the method can be found in HAPKIDO Deliverable 1.1. Section 3 presents the expected societal risks of the quantum threat to PKI systems used by the Government. Section 4 presents the expected societal risks of the quantum threat to PKI systems in Banking. Section 5 presents the expected societal risks of the quantum threat to PKI systems in Telecom. Finally, section 6 presents this study's conclusions and some recommendations for stakeholders in the various sectors. Some avenues for further research are also presented in the final section.

2 Brief overview of the SRA method

The primary purpose of the SRA method developed in HAPKIDO is to capture the most critical risks to society that arise from the availability of quantum computing. The developed method should allow an organisation – as a critical player in a sector - to assess the societal impact of quantum computing breaking the public key cryptography used in the PKI of that organisation. While the method is focused on an organisation, the impact under consideration is on the sector as part of society. Therefore, the method is designed to have the assessing organisation adopt multiple viewpoints and a broad perspective on risks. This desire for a broad perspective has led to the choice to design for use by parties with differing roles in the PKI landscape. This design choice should allow a PA, CA, intermediary CA, end-user, or any other party reliant on PKI usage to use the SRA method.

In line with the goal, this method must be helpful when a party involved with PKI wishes to assess their societal risks considering quantum computing. It helps the assessing organisation to achieve a clear understanding of their societal risks, prioritise risks to be treated first, and prepare for the transition to quantum-safe PKI. Accordingly, we formulated the following requirements (R) for the SRA method:

- R1. Usability – experts across various PKI domains should be able to use this method.
- R2. Self-explanatory – domain experts should be able to use this method by themselves, without external guidance.
- R3. Relevance – the method must include organisational, national, and individual risk perspectives.
- R4. High granularity – the method must facilitate the detailed and specific description of assets and associated risks.

Table 1 provides an overview of the steps in the SRA method. In step 0, it is essential to discuss the three scopes of the SRA: technological, organisational, and societal influence. All three scopes are relevant and will be highlighted throughout the SRA. The technological scope is used to delineate steps 1 and 2, and the organisational and societal influence scopes are used to delineate steps 2 and 3.

In step 1, the technological scope informs which threats and vulnerabilities are relevant in the SRA. The threats and vulnerabilities are based on combining quantum computing and PKI knowledge. We use two scenarios to guide this step. Both scenarios start with the availability of a quantum computer capable of running Shor's Algorithm and breaking public key cryptography, which becomes public knowledge through a press release. After which, two different effects are considered:

i. In the real-time access scenario, a threat-actor has access to a quantum-computer to do real-time decryption of asymmetric cryptography or real-time forgery of certificates. This allows the actor to break the confidentiality of secrets, affect the integrity of documents or impersonate an authenticated entity.
ii. In the store now, decrypt later scenario, while the actor cannot access a quantum computer, the threat actor has stored encrypted secrets. When the actor gains access to a quantum computer, the actor can decrypt the secrets. Note that this scenario only concerns the confidentiality of the secrets.

In step 2, the technological scope is used again to inform which business processes, applications, and services are relevant. These are the three different types of assets used in the SRA. The organisational scope is applied to find the relevant business processes and, depending on the

assessing organisation, the relevant software applications and business services. The software applications, as do the services provided, may also fall within the societal influence scope. Then, in step 3, the three types of assets are used to find how their compromise could impact the assessing organisation and society. Both the organisational and societal influence scopes are used in this regard. The assets and the impacts are assessed by processing a business impact analysis, other previously completed risk assessments, and expert PKI knowledge.

Table 1: Overview of SRA steps

Step	**Activity**	**Purpose**
0: Determine scope	To determine the technological, organisational, and societal influence scope.	To ensure a focussed and highly relevant assessment of risks and avoid scope creep.
1: Identify threats	To identify what quantum threats are in scope and what vulnerabilities these threats exploit.	To get an idea of what to defend against so that we may find what to defend.
2: Identify assets	To list the relevant business processes, related PKI applications, and their dependent services.	To have an overview of what is to be defended so that we may find what is at stake.
3: Assess impact	To assess the potential impacts of the threats on the assets from an organisational and a societal perspective.	To give an idea of what is at stake when threats materialise.
4: Assess urgency	To review available expert judgement of the urgency of the threat.	To provide an understanding of the timescale in which specific impacts are to occur.
5: Synthesise	Combine the risk components from the previous steps and rank threat scenarios according to their need to be mitigated.	To generate an overview of the societal risks that the quantum threat brings from the point of view of a single organisation.

The societal impact analysis is based on the categories of national security defined by the Analistennetwerk Nationale Veiligheid (ANV)[2]. National security is considered at stake when safety is seriously threatened for one or more of the following categories of national safety concerns:

1. Territorial/physical,
2. Economical,
3. Ecological,
4. Social,
5. Political stability,
6. International rule of law.

These are further divided into 17 impact areas, from which seven are selected for this work (see previous report D1.1. for more details). Step 4 takes each threat and estimates the corresponding time to act. This estimation is based on expert knowledge of quantum computing and PKI. Now that the organisational and societal impacts and the estimated time per threat are known, they can be combined in step 5 to create an overview of the risks.

[2] Nationale Veiligheid | RIVM

3 Case study 1: PKI in Government

3.1 Case description

This section describes the results of applying the SRA to the case of PKI Government in the Netherlands (PKIoverheid). PKIoverheid is the nationwide Dutch trust framework that provides security for communication between Government and Government, Government and business, business and business, and Government and citizen. Logius manage it on behalf of the Ministry of Interior and Kingdom Relations. It was set up to accommodate the need for digital trust, which came with the shift towards electronic transactions.

PKIoverheid is built in such a way that the central level and the operating level are separated. The operating level is where the Trust Service Providers (TSPs) interact with the end-users directly. The central level is split into domains based on roles. PKIoverheid ensures the secure and reliable issuance of PKIo certificates by TSPs connected to the PKIoverheid system. PKIo certificates are issued under strict conditions of the PKIoverheid Policy Authority realised by Logius. The following figure provides an overview of actors in the PKIoverheid Landscape.

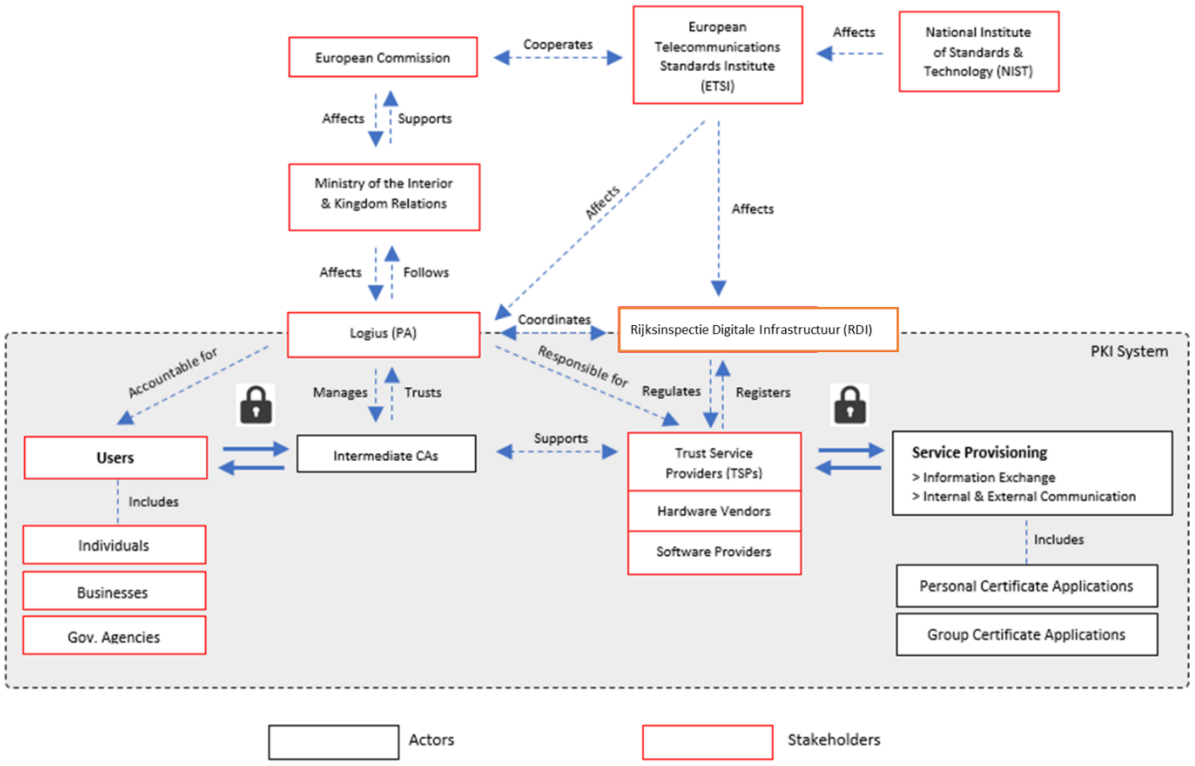

Figure 1: Overview of the PKIoverheid Landscape (Source: PhD proposal Ini Kong)

The generation and signing of certificates follow a PKI hierarchy (Bharosa e.a. 2015). Figure 2 illustrates the PKIoverheid hierarchy. For the publicly trusted root, these domains are Organisation Person, Organisation Services, Citizen, and Autonomous Devices. A private root also issues certificates that are not publicly trusted. The private root has the domains Private Services and Private Persons. Each domain has its own CA certificate, signed by the corresponding root CA. This division of domains provides transparency about the certificate user's role in the digital transaction.

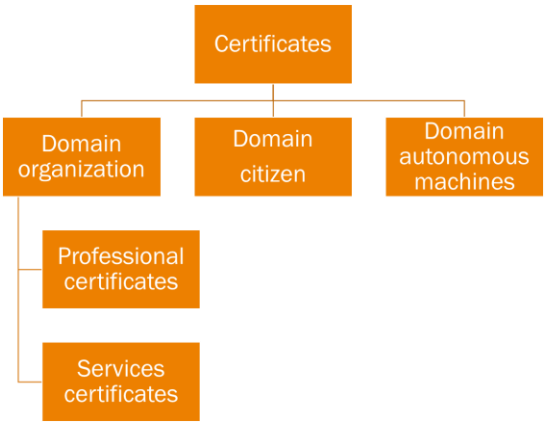

Figure 2: PKIoverheid hierarchy (Bharosa e.a. 2015)

PKIo certificates have various applications: authentication of persons, websites and systems, secure encrypted message exchange between and with the Government, qualified electronic signatures, and digital authentication. Additionally, by splitting the certificates based on roles, different security criteria can be used in supplying the certificates. Each domain CA certificate is used to sign domain-specific issuing CA certificates that TSPs manage. The TSPs use their issuing CA certificates to issue certificates to end-users. Table 2 describes all PKIoverheid TSPs, the domains in which they are active, and whether they are commercially active. The non-commercial TSPs provide certificates for specific applications. Most commercial TSPs offer a wide selection of certificates for many use-cases. Hence, the large number of domains in which they are active. Cleverbase is the exception, as it issues certificates for a specific application: identification and signing by citizens.

Table 2: Overview of PKIoverheid TSPs (is dynamic and subject to change)

Public TSPs	**Commercial TSPs**
Ministery of Defense	Cleverbase
CIBG	Digidentity
IL&T	KPN
	Quovadis/Digicert

Logius' services can be divided into four domains: Access, Interaction, Data Exchange, and Infrastructure. In addition, Logius is the manager of several systems and standards, including the Policy Authority (PA) of PKIo. As the PA, Logius has the following tasks listed in their Certificate Practise Statement (CPS):

1. Contributing towards developing and maintaining the framework of standards that underlie the PKI for the Government, The Programme of Requirements (PoR).
2. Leading the process of admittance by Trust Service Providers (TSPs) to the PKI for the Government and preparing the administration.
3. Regulating and monitoring the activities of TSPs that issue certificates under the root of the PKI for the Government.

Essentially, Logius is tasked with regulating the use of PKIoverheid through the PoR; regulating and executing the admittance of new TSPs, and checking compliance of participating TSPs with the PoR. This means that while TSPs execute the issuing of leaf certificates and take liability for this, Logius is responsible for the functioning and trustworthiness of PKIoverheid as a whole. The controls Logius employs to fulfil this responsibility are described in Logius' CPS. Logius' controls are somehow stricter than the highest level of security defined in eIDAS.

Regarding eIDAS, the Rijksinspectie voor Digitale Infrastructuur (RDI), which falls under the Ministry of Economic Affairs, oversees eIDAS trust services. Because of the split in the central part and the operating part of PKIoverheid, Logius does not have complete oversight of leaf certificates and their use. Logius is not responsible for managing this; the TSPs are. This means that Logius' view on societal impact is obscured. Therefore, it is even more attractive to apply the SRA to this case and see how well it assesses societal risks.

Another limitation in this case study is that Logius' Business Impact Analysis (BIA) is classified and can thus not be used in this research. (Internal) Access to this BIA and other previously completed risk assessments could further improve the accuracy of the results.

3.2 Workshop results

Logius is strongly invested in the HAPKIDO project and has already played a significant role in deliverable 1.1. (Development of the SRA method). Accordingly, there were multiple sessions, next to a SRA workshop, that have provided input for this section. Since PKIoverheid serves many processes, we reduced the scope of this analysis to what we consider several (expected) high-impact business processes that rely on PKIoverheid to function.

3.2.1 Access control for (semi) government personnel

PKIoverheid is essential to the functioning of the access passes to governmental institutions. These passes fall within the domain of *trustworthiness assurance for organisational persons*. Two highlighted examples of these access control passes are the Defensiepas, used by the Ministry of Defence and the UZI-pass, used by various healthcare organisations and hospitals. Figure 4 provides an overview of the access control passes based on PKIoverheid.

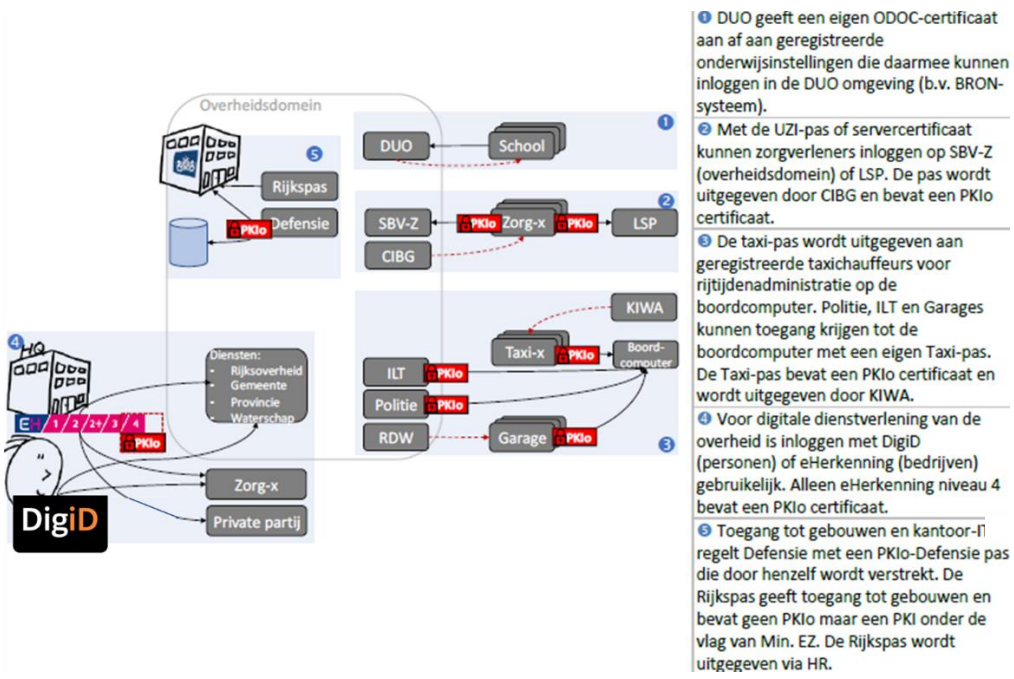

Figure 3: Overview of access control passes using PKIoverheid certificates[3]

[3] https://kennisopenbaarbestuur.nl/media/256209/onderzoek_stimulering-pkioverheid-innovalor_19-4-2019.pdf

Aside from access to restricted locations or buildings, these passes are unique identifiers used for authentication and authenticated encryption. As such, they are used to send confidential information with either stately secrets (Ministry of Defence) or patient medical records (healthcare). There is a legal requirement for up to 30 years of guaranteed secrecy for this kind of information.

Consequences

1) In the *real-time access* scenario, the pass's authenticity and integrity guarantees are voided. As such, this leads to the inability to use these passes for authentication (at buildings and information systems). This causes a significant breakdown of communications until an alternative system is created.
2) In the *store now, decrypt later* scenario, the consequence is that the encryption of medical data using the UZI-pass will be vulnerable to be decrypted. This can lead to potentially leaking sensitive health data of many patients, as the collection of medical records may already be ongoing. Potentially, this may lead to reduced communications between medical professionals and less efficient healthcare.

Organisational impact

It can be estimated that the impact of the quantum computer on the current access control passes will be significant. A complete replacement of these passes may be required, a costly but precedented procedure.

3.2.2 Communication and interaction using DigID

All Dutch citizens need DigID to interact with (semi) public agencies digitally. Setting up secure connections between citizens (web portal or APP) and (semi)-public agencies requires PKIoverheid certificates on the server side of the agencies. With 2-sided TLS (also known as 2-sided SSL), the client (the web portal/APP) and server verify each other to ensure that both parties have trusted communication. This is done when setting up the HTTP connection through a certificate exchange. If the certificates are correct, the HTTP connection is secured; thus, the connection is an HTTPS connection. In the DigiD connections (all types of interfaces), 2-sided TLS connects with the DigiD application servers that can be reached at was.digid.nl. Therefore, depending on the design of the interface, 2-sided TLS must be used when setting up the HTTP connection to the server. PKIoverheid is essential to DigiD as it provides the root of trust, which enables authentication.

It is estimated that more than 1800 government web pages require citizens to log in using DigiD. This goes beyond government services (e.g. Tax Office, municipality services, Social Security agency) and includes health service providers, health insurance providers and pension service providers. In 2022, DigiD was used 514 million times to view data or interact with public service providers [4]. On top of that, DigiD Machtigen was used 14.9 million times in 2022 to interact with public service providers on behalf of someone else (e.g. elderly and non-digital literate people).

Consequences

1. In the *real-time access* scenario, the consequences are high, as the websites and services relying on DigID cannot be trusted anymore. Accordingly, citizens will be deprived of a wide range of (semi)public services, including e-health and e-government services.
2. In the *store now, decrypt later* scenario, the consequence will be high since citizens who interact with public agencies must provide sensitive information, including personal identifiers and sometimes even income data.

[4] https://www.logius.nl/onze-organisatie/logius-rapporteert/jaarverslag-2022/jaaroverzicht-2022/het-complete-jaaroverzicht

Organisational impact
It can be estimated that the impact of the quantum computer on public service delivery is significant. When a capable quantum computer becomes available, public service providers must authenticate service users using other means than DigiD. This would be essential to avoid identity theft, as virtually all adult citizens use DigiD. In particular, the discontinuation of access for citizens to government services requires attention. The impact of 'store now, decrypt later' would cause a significant loss of confidentiality for sensitive data that is currently encrypted.

3.2.3 Business-to-government interactions (using professional certificates)

PKIoverheid provides professional (occupational) certificates for various professions (i.e. taxi drivers, accountants, tax consultants, etc.). In one example, taxi-drivers receive a professional certificate to identify them as a legal entity/person. This application of PKIoverheid exists to combat fraud and monitor these professionals' working hours to limit road-accidents.

In the eHerkenning trust framework, PKIoverheid is used by professionals, such as accountants, bailiffs and notaries, to sign *legally binding* documents. These documents are proved with an official digital signature, and legal rights can be derived from these. For example, ownership of a house can be determined by a digital signature from a notary. Figure 3 provides an overview of the use of SBR, including eHerkenning professional certificates in the Netherlands.

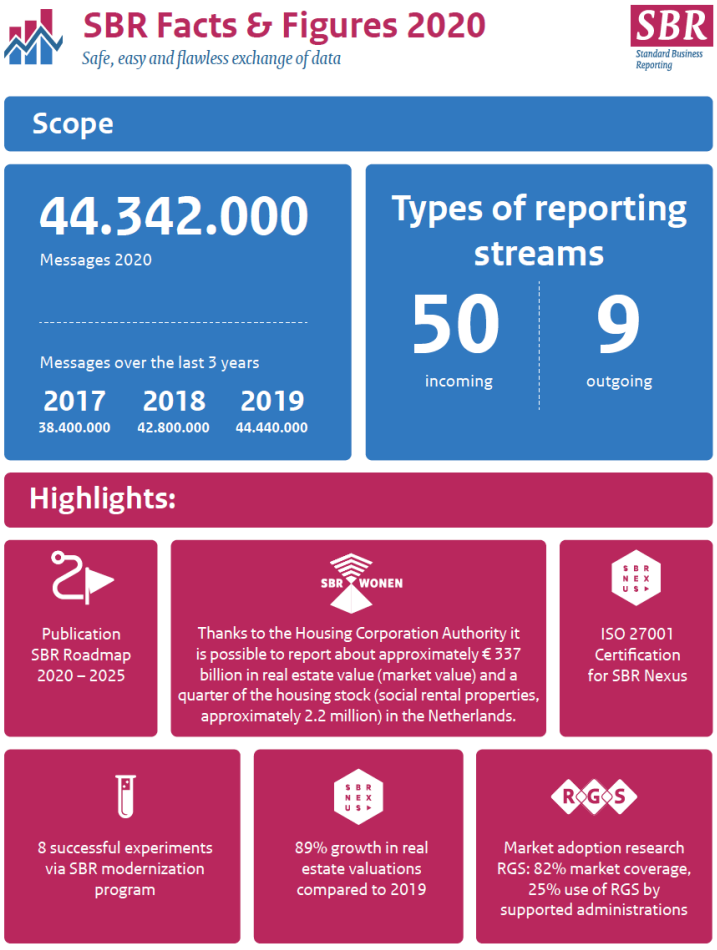

Figure 4: Overview of the use of PKIOverheid professional certificates5

[5] https://www.sbr-nl.nl/over-sbr/sbr-organisatie/publicaties/facts-figures/2020

The professional certificates and services certificates are also used for Standard Business Reporting (SBR). SBR is the national standard for the digital exchange of business reports. SBR allows Dutch businesses and their intermediaries to reduce reporting and administration work in the exchange of business information to local authorities and banks. SBR enables information in company records to be captured once only in a standard way. This means the information can easily be reused for various reports to government agencies and banks. The digital infrastructure used to exchange SBR messages is called Digipoort. Digipoort provides a safe and reliable connection for various reporting obligations and processes the messaging data between organisations and authorities like the Dutch Tax Office, Chambre of Commerce, and Office of Statistics. SBR and Digipoort are essential building blocks for several economically important transactions, including VAT (Value Added Tax), Income Tax, Corporate Tax, Annual reports and many more (Bharosa e.a. 2018).

Messages sent to Digipoort are often privacy-sensitive and confidential: after all, they contain personal and financial business data. A secure connection is set up to exchange messages. For this, you use a PKIoverheid services certificate. A PKIoverheid services certificate is tied to an organisation. All information shared is encrypted; only the requesting party has the key to read your message. This ensures identification and authentication. PKIoverheid services certificates, therefore, have a high level of reliability.

Consequences

3. In the *real-time access* scenario, the consequences are high, as the integrity of the signatures by accountants and notaries is directly coupled with legally binding documents. The quantum computer can lead to the forgery of these documents, enabling extensive scale fraud and embezzlement of property. The services provided by the accountants and notaries will no longer be trusted and will devaluate.
4. In the *store now, decrypt later* scenario, the consequence might be limited, as the certificates for professionals provide no confidentiality of data. However, it is unknown to which capacity the certificates for accountants and notaries are used for confidentiality.

Organisational impact

The impact of the quantum computer on the integrity of documents signed by professionals is very high. Accountants, bailiffs, and notaries will be significantly hindered in performing their functions. The potential for embezzlement and fraud will cause the public to distrust digital signatures. As such, their industry might need to revert to, or keep using, paper signatures as an alternative to digital signatures. This kind of rollback will be costly.

3.3 Societal impact

Governments play a crucial and unique role in society. (Semi) public agencies provide unique services, many of them online. The societal impact analysis reveals three impact areas for PKIoverheid.

Table 3: National security concerns and impact area affected by disrupted PKIoverheid.

National security concern	Impact area	Effect	Relevant business processes
1. Territorial security	1.3 Violation of the integrity of cyberspace	Disruption of governmental services, in particular of DigiD and SBR.	Communication between organisations, citizens and Government. Professional certificates. Access control passes for (semi) government.
3. Economic security	3.1 Costs	The unavailability of SBR and Digipoort will economically impact Dutch society. Substantial material damage is a consequence of potential fraud and embezzlement due to corrupted professional signatures.	Professional certificates Digipoort data exchange services
5. Social and political stability	5.1 Disruption of day-to-day life	A consequence of the unavailability of DigiD will be reduced access to government services for the entire population. If this lasts for a long time, the impact on day-to-day life will be severe.	Communication organisations, citizens and Government
	5.2 Degradation of the democratic rule of law	A consequence of the unavailability of military access control causes reduced functioning of critical governmental services. This can have a severe impact.	Access control passes for (semi) government.
	5.3 Societal unrest	A consequence of the unavailability of governmental services through DigiD and SBR might result in limited social unrest. However, if prolonged causes more substantial societal upheaval.	Communication organisations, citizens and Government

Table 3 reveals that governments' public service delivery capacity and economic capacity (e.g., filling taxes) are prone to quantum computing threats.

3.4 Conclusions for PKI Government

Overall, it becomes clear that the societal risks of the quantum threat from a PKIoverheid perspective are high. The risks are the worst from a user (citizen and business) side (no access to services), but also from an organisational point of view, especially considering store now, decrypt later attacks. These attacks may lead to loss of confidentiality for very sensitive data, and there is little time to respond.

Table 4: Impact on critical business processes relying on PKIo

Business process	Threat	Impact	Argumentation
Access control for (semi) government personnel	Real-time access (CIA)	High	Risks of forgery of military and medical personnel identity and loss of communication.
	Store now, decrypt later (C)	**Extreme**	Sensitive data can lose confidentiality. From a PA's perspective, it's hard to say if SNDL is an issue regarding the data encrypted using the UZI pass.
Business - to government interactions (using professional certificates)	Real-time access (CIA)	**Extreme**	The integrity and non-repudiation of message exchange using eHerkenning and Digipoort cannot be assured. Risks of forgery of legally binding signatures.
	Store now, decrypt later (C)	Low	Limited loss of confidentiality, but unknown impact for accountants and notaries.
Communication between organisations, citizens and Government (using DigiD)	Real-time access (CIA)	**Extreme**	Government websites cannot be trusted anymore. Public services (including social services and eHealth) become digitally unavailable.
	Store now, decrypt later (C)	High	Sensitive citizen information shared using DigiD may lose confidentiality.

The risks for Logius are so high because of the broad impact of breaches in the trustworthiness assurance of PKIoverheid. PKIoverheid is used in many applications throughout Dutch society and is the primary support of communication with the Dutch Government by citizens and organisations. The assessment shows how widespread in society this dependency is.

The shelf life of highly sensitive information such as medical history, political preference, and religion is assumed to be twenty years. One could argue that this information should stay confidential if the data subject is alive or even after. Without this assumption of personal data shelf life, Logius is already too late to prevent the loss of confidentiality of sensitive data.

There are many ways in which society may be impacted if Logius cannot secure PKIverheid. Examples include interference with information exchange for medical professionals; leaking of company secrets of many companies operating in the Netherlands; potential loss of any application that uses DigiD to facilitate communication between the Dutch Government and citizens; large-scale fraud because accountants, bailiffs, and notaries cannot securely sign documents; and leaking of military intelligence, as secure communications are challenging to set up.

The workshop with PKIoverheid representatives agreed that the SRA developed is valuable and comprehensive. The SRA stimulates a more precise discussion on the impact of quantum computers on digital systems that rely on PKI. The participants would recommend other organisations in the Government sector to use the method as a learning instrument and an instrument for mobilising actors to develop transition strategies.

The workshop also revealed that the SRA analysis for PKIoverheid is by no means complete. The workshops mainly revealed risks regarding DigiD and data exchange between business and public agencies. PKIoverheid also plays a vital role in securing government-to-government data exchange (e.g., using Diginetwork).

4 Case study 2: PKI in Banking

4.1 Case description

This section describes the results of applying the SRA to the case of Banking. A well-functioning financial system is fundamental to a modern economy, and banks perform essential functions for society. These functions include (1) facilitating transactions, (2) mobilising and allocating financial resources, (3) facilitating risk management, and (4) generating and sharing information (WRR, 2016). They must, therefore be secure and trustworthy, offline and online.

The Netherlands has a banking system consisting of national and international banks, including large system banks and smaller banks. De Nederlandse Bank (DNB) is the country's national central bank, supporting and regulating Dutch banking services alongside the Dutch Authority for Financial Markets (AFM). While the DNB is responsible for prudential supervision and is committed to ensuring sound and ethical financial institutions that meet their obligations, the AFM is responsible for market conduct supervision and ensuring fair and transparent financial markets. Apart from these, banks must also consider the procedures the European Central Bank (ECB) prescribes.

Dutch banks also operate on an EU- and intercontinental-level. The fact that SWIFT facilitates international interbank exchange is not the only relationship outside of the Netherlands that should be considered. Furthermore, the European Banking Authority handles instant payments between (European) banks. However, this research does not address the implications of the PQC transition in the international environment. Hence, these players are out of scope.

There are other out-of-scope players in the banking world. Worldline is one of the major vendors for Point of Sales terminals[6] used in shops. These terminals can be used with a debit card to pay for a transaction. The terminals of Worldline are out of scope for this research. For this study, we zoom in on the categories of key business processes of banks. Based on the findings from the first workshop with three banking experts, these business processes are captured in four main categories:

1. online banking (e.g. using your banking app, or bank webportal);
2. debit and credit card-enabled transactions (e.g., using Adyen, Paypal, Visa and Mastercard);
3. international transactions (facilitated via SWIFT); and
4. inter-bank uniform payment services (according to directive PSD2[7]).

Figure 5 provides an overview of these processes.

[6] Point of sale terminals refer to hardware and software that enables merchants to process payments to complete a customer purchase. Cash registers are the main example. We also know more terminals varying from smartphones with plugged-in card readers to countertop terminals that print receipts, scan bar codes and more.

[7] EUR-Lex - 02015L2366-20151223 - EN - EUR-Lex (europa.eu)

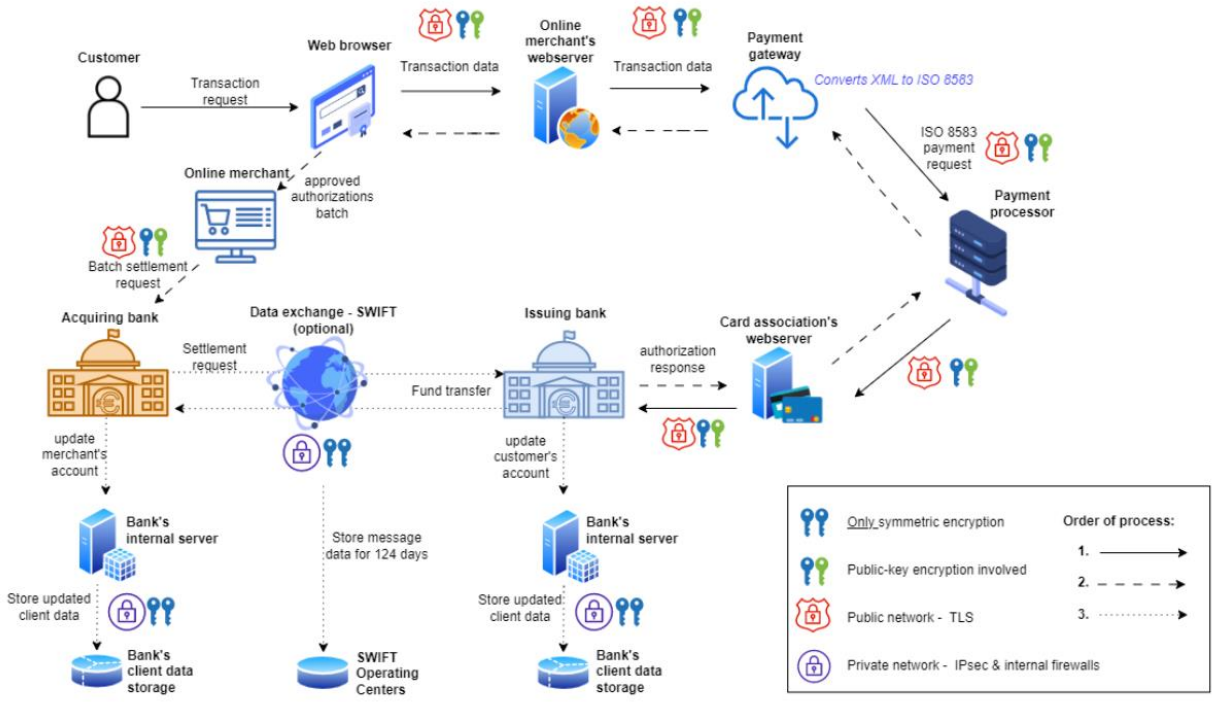

Figure 5 – Overview of banking processes (Onkenhout, 2023)

Next, the results of the analysis are described for each category.

4.2 Workshop results

4.2.1 Online banking

The first category of key business processes of banks that emerged in the workshop is online banking. This process represents a large portion of the current activities of banks, as perceived by clients. A big part is about executing payments online. Payments for goods and services should be processed swiftly, safely and cheaply. The consequences of failure to perform these tasks expand well beyond a single bank, impacting the entire economy that could quickly expose banking systems to large shocks. It is, therefore, essential that banks can absorb losses and meet their current payment obligations.

Threat scenario

The threat scenario relevant to online banking is that a Quantum Computer becomes a reality, which becomes public knowledge from a press release. Banks can react either by shutting it down as PKI will be compromised or by keeping it up and investing in more robust monitoring of transactions.

Consequences

1. Banks might decide to shut down their PKI. Consequently, users (consumers and corporations) will no longer be able to log in and be deprived of online banking. At the same time, physical contact with the banks will be limited, as few bank branches are still active.
2. If banks do not shut down their PKI but attempt to monitor suspicious behaviour, this will ensure that users can access their money. However, there can be no more guarantees of correct logins, as the quantum computer will allow for the forgery of valid certificates. Criminals and other actors are expected to start targeted attacks on individuals and organisations with significant financial assets. The effect of this is broken *non-reputation*, which for these individuals can lead to financial ruin and loss of assets.

3. The quantum computer will allow for the impersonation of trusted employees. Attackers exploiting this vulnerability will have the same (far-fetching) rights as the impersonated employee and can act like a bank employee.

Organisational impact
It is estimated to be quite likely that banks will undergo a loss of customers. Unaware that the threat is ubiquitous to all systems relying on asymmetric cryptography, customers might move to other banks or financial services. Additionally, upon discovering the threat and as attacks concretise, banks will suffer from public distrust.

4.2.2 Card-enabled transactions

The second category of crucial business processes highlighted is card-enabled transactions. Debit and Credit cards play a role in allowing for rapid payment of goods and services. However, if narrowed down to transactions with physical cards (as online transactions with credit cards fall under the business process of *online banking*), these happen in a more controlled manner, following the EMV standard[8]: with the need for physical contact or near field communication with dedicated Point of Sale devices, such as payment terminals, or ATMs.

The effects of disruptions in card transactions will cause similar distress to customers, but it will yield fewer extreme consequences than the economic collapse caused by disruptions of online banking.

Threat scenario
Since cards can work solely with symmetric encryption, the impact of a Quantum Computing threat is reduced for this category. Attacks on card-enabled transactions will rely on brute force due to the nature of symmetric encryption and the fact that keys remain inside the isolated and controlled environment of the cards. Attacks will also be less systematic than processes that rely on PKI (and consequently, asymmetric encryption), for which a quantum computer can re-calculate private keys from their corresponding public keys.

Nevertheless, symmetric encryption algorithms are still vulnerable to the quantum computer.

Consequences

1. As symmetric encryption becomes vulnerable, banks might decide to shut down the support for the bank cards. Note that Point-of-Sale systems are often outsourced to third-party service providers.
2. If bank cards keep functioning, but online banking does not, there will be a bank run on physical cash. ATMs will empty quickly, and physical cash will be scarce. Note that the provision of ATMs is outsourced to third-party service providers.
3. Bank cards depend on a chain of symmetric keys mandated in the EMV standard. While pulling this off is complex, an insider threat would be possible. In this case, an insider who breaks the master key can transfer money using any bank card.

Organisational impact
Similarly to the organisational impact of discontinuing *online banking* (see 4.2.1), it is expected that disruptions in card-enabled transactions might also lead to loss of customers and public distrust.

[8]EMV stands for Europay, Mastercard, and Visa, the three parties that established the EMV standard. EMV is a payment method based on a technical standard for smart payment cards and for payment terminals and automated teller machines which can accept them.

4.2.3 International transactions

The third category of key business processes of banks is international transactions. International banking involves transactions related to accepting deposits and loans anywhere in a currency different from the country in which the bank is located. These banking processes are used to:

- Facilitate international wire transfers.
- Facilitate cross-border payments after trade purchases.
- Facilitate digital payments by connecting payment gateways to the bank.

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) network facilitates most international money and security transfers. SWIFT is a significant messaging network banks and other financial institutions use to send and receive information, such as money transfer instructions, quickly, accurately, and securely. This payment network allows individuals and businesses to take electronic or card payments even if the customer or vendor uses a different bank than the payee. More than 11,000 global SWIFT member institutions sent an average of 42 million daily messages through the network in 2021. It is essential to state that international banking has a lot of variety. Some banks have quite some back-up authentication or encryption systems based on symmetric cryptography (with people carrying USB sticks with keys going from bank to bank to distributed keys). This category is hard to gauge and is left out of scope.

Threat scenario

The threat scenario relevant to international transactions is similar to the one presented for the category of *online banking* (see 4.2.1). Quantum computing will compromise PKI systems, and banks will react by shutting down systems or investing in more robust monitoring.

Consequences

1. Banks might decide to shut down their systems, as quantum computers render the PKI systems required for international trade unreliable.
2. Banks might also decide to keep the systems running but attempt to control transactions using challenge-response protocols based on bank cards, which will be less vulnerable to the quantum computer threat. This will ensure that customers have access to international trade, but the process to do so becomes cumbersome. As there can be no guarantee of *integrity* and *non-repudiation* of communications encrypted asymmetrically, the authenticity of requests must be guaranteed by a sequence of challenge-response steps, generating several short-living single-use tokens, reducing the window for attacks. This option will likely be unfriendly for users and offered only to enable essential transactions, as it will generate significant communication overhead in the banking systems.

Organisational impact

The immediate impact of such a threat is depriving users of international transactions. Significant economic damage to system banks can be expected, either due to loss of customers or assets, which has direct financial damages. Banks are also expected to be impacted as international loans (such as European bank, International Monetary Fund, and others) become unavailable. Banks might run out of funds, which likely leads to a collapse not only of banks but the entire European economy.

4.2.4 PSD2 services

Banks' fourth category of crucial business processes encompasses The Payment Service Directive 2 (PSD2). This is an EU (European Union) directive. PSD2 outlines a set of rules to simplify and secure online payment services. An effect of PSD2 is that customers of multiple banks can manage their

bank accounts from third-party applications. In general, PSD2 allows third parties to offer novel financial services to consumers. As such, banks offer (a part of) their services as PSD2 services to be interfaced with by third-party applications.

While it heavily depends on the backend of the PSD2 services, the primary technology that secures these services is TLS. TLS derives its secure signatures from the bank's PKI or a public TSP. Although it depends on the configuration, TLS uses classical public key encryption algorithms, such as RSA and ECC. As such, TLS is also vulnerable to a quantum computer.

Scenario
Like online banking, the scenario is that a Quantum Computer is developed and becomes public knowledge from a press release. As the trust provided by their PKI will be compromised, the banks react either by shutting down their PSD2 services or by keeping them running and investing in more robust monitoring of transactions.

Consequences

1. If the banks decide that, in reaction to the quantum computer, they shut down their PSD2 services, then the third-party applications can no longer interface with the banks. As such, these applications can no longer provide their services. If this situation continues, these third-party applications will go bankrupt. Consumers relying on these third-party applications might be able to use their original bank's services if these are still available.
2. If banks do not shut down their PSD2 services but instead increase their monitoring, then these PSD2 services might remain available to their users. However, while outside the banks' scope, the customer's authentication to the third-party application can no longer be guaranteed. Therefore, the PSD2 service might still shut down due to the third party reacting to the quantum computer.
3. Moreover, if PSD2 services can still interface with the bank, this uses classical certificates. The availability of a quantum computer might enable an attacker to forge the certificate of the PSD2 service itself, thereby interfacing with the bank on behalf of the service. This might not be detectable and breaks the non-repudiation of the service.

Organisational impact
It can safely be estimated that most PDS2 services will not survive the consequences listed above. These services depend on the now insecure interface with the banks. With no option to offer their services, the company offering these services will go bankrupt shortly after. Additionally, upon discovering this threat and its concrete attacks, the PSD2 services might suffer from public distrust for a long while.

4.3 Societal impact

Similar to the previous case study, the societal impact analysis is based on select categories of national security as defined by the ANV. Table 5 demonstrates which national security concerns are affected by the disruption of business processes in banking.

Table 5: National security concerns and impact area affected by disrupted banking services.

National security concern	Impact area	Effect	Relevant business processes
1. Territorial safety	1.3 Violation of the integrity of cyberspace	Disruption of financial transaction infrastructure.	Online banking

2. Physical safety	2.3 Lack of basic needs	Lack of physical cash and unavailable bank transactions lead to the inability of people to transfer goods and services, including basic needs.	Online banking, Card-enabled transactions, PSD2 services
3. Economic safety	3.1 Costs	Significant economic damage to system banks, either in loss of customers or loss of assets, which leads to direct financial damages.	Online banking, Card-enabled transactions, International transactions, PSD2 services
	3.2 Degradation of the vitality of the Dutch economy	Damage to system banks results in the Dutch and European economies collapsing.	International transactions, PSD2 services
5. Social and political stability	5.1 Disruption of day-to-day life	Lack of physical cash and unavailable bank transactions lead to the inability of people to transfer goods and services. This has implications for day-to-day life.	Online banking, Card-enabled transactions, PSD2 services
	5.3 Societal unrest	Unavailable banking services can lead to scarcity of goods and, more importantly, financial assets. If left for too long, it will cause (physical) violence and intimidation for remaining resources.	Online banking, Card-enabled transactions, PSD2 services
6. International rule of law	6.3 Degradation of a rule-based international financial-economic order	On a larger scale, international banking will be disrupted and might cause the global collapse of the financial order.	International transactions, PSD2 services

4.4 Conclusion for Banking

In conclusion, the impact of a future quantum computer on PKI used in banking could lead to the collapse of the global banking system, taking the economy of the Netherlands and Europe at large with it. In Table 6 an overview is given about the impact of the two main threats of per business process.

Table 6: Analysis of impact of quantum computing on banking business processes dependent on PKI.

Business process	Threat	Impact	Argumentation
Online banking	Real-time access	**Extreme**	The impact of real-time attacks on certificates of online banking could lead to the collapse of system banks (and thus the economy). This is an extreme effect.
	Store now, decrypt later	Low	The impact of 'store now, decrypt later' on online banking could lead to the loss of confidentiality of bank accounts. This could cause some, but comparatively minor, social upheaval. This is a non-zero yet low effect.
Debit/credit cards	Real-time access	High	Real-time attacks on debit/credit cards significantly impact daily life, eliminating people's ability to pay for available goods or services. This has a high impact but less than the extreme economic collapse caused by the discontinuation of system banks.
	Store now, decrypt later	Low	The impact of 'store now, decrypt later' on debit/credit cards could lead to losing pin-transactions' confidentiality. While a loss of privacy, the effect is comparatively minor.
International transactions	Real-time access	**Extreme**	The impact of real-time attacks on certificates used in international transactions could lead to the collapse of system banks, which is such an extreme effect to warrants high urgency.
	Store now, decrypt later	Low	The impact of 'store now, decrypt later' on debit/credit cards could lead to a loss of confidentiality of what countries are borrowing or spending internationally. This is a comparatively minor effect.

PSD2 services	Real-time access	Low	While the effect of real-time attacks on PSD2 services might cause the service's bankruptcy, the isolation effect is only minor (as the bank might still offer its own services).
	Store now, decrypt later	Low	The impact of store now, decrypt later on PSD2 services could lead to the loss of confidentiality of back accounts. This could cause some, but comparatively minor, social upheaval. This is a non-zero, yet low effect.

We see the most extreme impact coming from the real-time access threat due to the enormous consequences for society. In this scenario, any bank can expect a loss of trust from customers and other banks.

The workshop with representatives from the banking sector agreed that the SRA developed is valuable and comprehensive. The SRA stimulates a more precise discussion on the impact of quantum computers on digital systems that rely on PKI. The participants would recommend other organisations in the banking sector to use the method as a learning instrument and an instrument for mobilising actors to develop transition strategies.

5 Case study 3: PKI in Telecom

5.1 Case description

This section describes the results of applying the SRA to the case of Telecom, short for Telecommunication. Telecom refers to facilitating information transmission and is a critical process for many modern nations. Traditionally, the telecom-operators build and maintain a nation-spanning infrastructure consisting of cables used for voice-communication. Nowadays, the telecom-operators use a highly diverse infrastructure consisting of (glass fibre) cables, radio and electromagnetic communication systems and sensors. Moreover, these companies typically offer additional services, which have become a significant part of the companies' operations. PKI plays a role in at least seven critical services offered by telecom-operators. Based on the findings from the workshop with three experts from the telecom-sector, these services include:

1. network services;
2. secure web services;
3. customer premise equipment management service;
4. certificate services;
5. TV-services;
6. (consumer) applications; and
7. operational access and maintenance.

While all these services are essential to the organisation, only the first three services will be discussed in detail. These services are unique to the telecom-sector and are estimated to be highly impacted. To give some context, we first briefly cover the remaining four services.

Certificate services provide organisations with trusted certificates. In this case, the telecom-operator acts as a trusted service provider to the organisation. This service is similar to the role of PKIoverheid, for which we refer to Section 3.2. The impact of the quantum computer on these services is estimated to be similar.

TV-services offer television channels to clients. PKI is used to provide digital rights management for the commercial channels. Depending on the telecom operator's action, the quantum computer's impact is either limited to the (temporary) discontinuation of the commercial channels to protect digital copyright or potential infringement upon these rights. In either case, the public channels will continue to be available. The impact on these services is therefore considered to be very limited.

Applications for consumers or organisations are the apps offered by the telecom-operator for smartphones, televisions, smartwatches, etc. These apps are all offered with a certificate of the telecom-operator in the respective application marketplaces. While the quantum computer will void these certificates, the effect is not limited to the telecom operators but to all applications in these marketplaces. Therefore, the effect cannot be estimated from a purely telecom perspective.

Finally, *operational access and maintenance* refers to the steppingstone connections required for telecom operator engineers to access the telecom infrastructure for maintenance remotely. This concerns the network management systems with which the customer manages thousands of network elements. This functionality depends heavily on identity and access management for which PKI is required. This service cannot be trusted when the quantum computer arrives. In response, all maintenance needs to be done on premise. While the significant cost to the telecom operator is challenging to sustain in the long run, the impact on customers will be limited. For the remainder of this study, we will focus on the *network*, *secure web*, and *customer premise equipment management* services.

5.2 Workshop Results

5.2.1 Network services

The first type of service offered by the telecom-operators is the network services. This includes the (glass fibre) wired connection and the electromagnetic connection, e.g. 2G, 4G and 5G (most operators have already phased out 3G in the Netherlands). These services are predominantly used by customers such as consumers and businesses. There is some variety here. Some telephone infrastructures (especially phone calls and SMS) rely on symmetric encryption via keys installed in SIM cards upon manufacturing. Telecom operators also maintain high-availability networks for public (emergency) services, such as the police, fire brigade and ambulances. These are typically similar but separate infrastructures.

PKI is used for network services for two primary purposes: to establish (and verify) identities and to encrypt the network traffic. This is done for both the 'public' network and the 'emergency' network.

Scenario

The scenario is that a quantum computer is developed and becomes publicly available. Telecom operators will react if the trust provided by their PKI will be compromised. Telecom operators consider *availability* a higher priority than the service's integrity, authenticity or confidentiality. As such, the network services will remain available, but with the caveat that nothing communicated over the network can be trusted. The operator will have to publish a statement explaining to customers the consequences.

Consequences

1. Customers are still able to make phone calls. While the network cannot make the usual guarantees, customers could still use the service under some provisions. For example, when calling, customers should not disclose anything that should remain secret. Authentication with a stranger will be impossible, but users could use their familiarity with each other's voice, speech pattern or some shared secret to authenticate among family, friends, or familiars. To account for potential eavesdropping, those shared secrets must be timely and single use. It is not unthinkable that a stream of 'leaks' will occur as phone lines are intercepted or identities impersonated.
2. The lack of secrecy and authenticity will severely impact businesses. Call centres and helpdesks can have difficulties providing their services. An exceptional case is the 112-call centre, which would be an obvious target for malicious attacks.
3. The public services network, while still available, has the problem that communicated information about potential disasters might leak, which might cause the press or disaster tourists to be onsite very quickly.
4. If 'trusted' certificates can be forged entirely, then a DoS is possible where the attacker continuously sets the expiration date of the forged, now trusted, certificate to expire immediately.

Organisational impact

It can be safely estimated that the telecom network will suffer a tremendous decrease in quality of service. The operator might be held liable for this decrease in service-level. Additionally, network-operator might suffer from public distrust for a long while.

5.2.2 Secure web services

The telecom operators' second type of services are secure web services, such as hosting, email and web shops. These services are predominantly used by customers such as consumers and businesses. PKI provides certificates for these web services to be used for authenticity, integrity and TLS encryption.

Scenario

The scenario is that a quantum computer is developed and becomes publicly available. The telecom operators react as the trust provided by their PKI will be compromised. In the case of secure web services, these will be treated on a case-by-case basis based on a runbook. However, the *integrity* and *confidentiality* of these services are of higher priority than *availability*, causing several services to be shut down (temporarily).

Consequences

1. All public-facing services are impacted and potentially shut down. In particular, the web shops and self-help desks will be turned off. Customers will have to be reverted to physical stores and facilities.
2. Internal-facing services like email could remain available with additional mitigations.

Organisational impact

It can be safely estimated that most secure web services will become unavailable. Businesses that depend on these services will be impacted majorly and might go bankrupt. The operator might be held liable for this decrease in service-level. Additionally, network-operator might suffer from public distrust for a long while.

5.2.3 Customer premise equipment management service

The telecom operators' third type of service is managing *customer premise equipment*. Customer premise equipment (CPE) is the plethora of peripheral equipment required to provide networking services to customers (consumers and organisations). Examples of CPE are modems, routers, wifi-repeaters, IoT-devices, gateways etc. These CPEs are in the customer's network but maintained by the telecom-operator.

PKI is used to provide trusted access by the telecom-operator for maintenance. Interestingly, these CPEs can and typically do use vendor-specific certificate authorities rather than the certificates provided by the telecom operator. These certificates can be self-signed and maintained by the vendors.

Scenario

The scenario is that a quantum computer is developed and becomes publicly available. The telecom operators react as the trust provided by their PKI will be compromised. There are two options for CPEs: either the CPEs will receive unsecured maintenance, or the CPEs will be put in an unmanaged state. The latter can be done by deleting the list of trusted certificates from the CPE.

Consequences

1. If the CPE continues to be managed, the CPEs form an ideal target for attackers. The CPEs typically direct all consumer traffic so a takeover can be particularly devastating. CPE takeover is possible trough forging certificates, establishing a maintenance connection, and uploading malicious firmware.

2. If the CPE is put in an unmanaged state, then the CPEs would still work. However, there are two drawbacks. First, maintenance cannot be performed, so over time, vulnerabilities will not be patched, causing issues in the long term. Secondly, by no longer accepting certificates, there is no opportunity for the CPEs to be remotely brought back into maintenance. Replacing the CPE or physically uploading new trusted certificates will be costly.

Organisational impact

It can be safely estimated that CPE management will be affected by the quantum computer. The operator stands before a choice: either continue the maintenance cycle with risks of exploitation or pull the CPEs out of maintenance, which can incur significant costs later. Either way, the organisation will be economically damaged (millions of euros).

5.3 Societal impact

Similar to the previous case study, the societal impact analysis is based on select categories of national security as defined by the ANV. Table 7 demonstrates which national security concerns are affected by Telecom's disruption of business processes.

Table 7 National security concerns and impact area affected by disrupted telecom services.

National security concern	**Impact area**	**Effect**	**Relevant business processes**
1. Territorial security	1.3 Violation of the integrity of cyberspace	Disruption of web services, and violation of confidentiality and integrity in communications.	Network services, Secure web services, Customer premise equipment management service
2. Physical security	2.3 Lack of basic needs	A consequence of the lack of integrity in communications (although available) may cause disruptions in some basic needs services offered by phone, such as medical care, and national emergency services, such as police, defence, ambulance care, and fire brigade.	Network services
3. Economic Security	3.1 Costs	Economic damage to telecommunication businesses due to shutdown of offered services that cannot be trusted anymore.	Secure web services, Customer premise equipment management service
	3.2 Degradation of the vitality of the Dutch economy	---	---

5. Social and political stability	5.1 Disruption of day-to-day life	Disruption of web services and violation of confidentiality and integrity in communications will require extra authentication steps, such as personal questions, which are known only to the party being authenticated. These will have to be single-use to account for eavesdropping attacks.	Network services, Secure web services, Customer premise equipment management service
	5.3 Societal unrest	A consequence of unreliability in communications will cause misuse of infrastructures crucial for society. If left for too long, this will lead to attempts of scams, extortion, and coercion, among others.	Network services, Secure web services, Customer premise equipment management service
6. International rule of law	6.3 Degradation of a rule-based international financial-economic order	---	---

5.4 Conclusion for Telecom

The impact of a future quantum computer on PKI used in Telecom could lead to upheaval in society and a generalised lack of trust in telecommunication infrastructures. However, given Telecom's importance to society, operators would most likely opt to keep services available, leading to a moderate impact on the Netherlands and Europe. Table 8 gives an overview of the impact of the two main threats per business process. The impact is more significant in the real-time access threat due to PKI mainly being used to verify identities and authenticate actors. In general, the operators can expect a loss of trust from customers.

Table 8 Analysis of impact of quantum computing on telecom business processes dependent on PKI.

Business process	Threat	Impact	Argumentation
Network services	Real-time access	Medium	Real-time access to network services will lead to a lack of trust in the network. Authentication of parties and content encryption in the communication protocol will be broken, but services can remain available.
	Store now, decrypt later	Low	The store now, decrypt later threat that could lead to a leak of confidential conversations. It is unlikely that national security matters are communicated using such a network, so the threat's impact on society is considered low.
Secure web services	Real-time access	Medium	The threat of real-time access will primarily impact customer-facing web services. The impact is likely to be perceived but contained since alternatives (such as reverting clients to physical facilities) can be provided.
	Store now, decrypt later	Low	The impact of 'store now, decrypt later' on web services could lead to loss of confidentiality. This could cause some (relatively minor) social upheaval. This is a non-zero, but low effect.
Customer premise equipment (CPE) management	Real-time access	High	The real-time access threat to the management of CPEs can be devastating. If telecom operators opt to continue with unsecured maintenance, this will open the door for creating botnets and tampering with all internet-based customer communications. If left without maintenance, it will be costly to recover once the threat is mitigated.
	Store now, decrypt later	Low	As PKI is mainly used for authentication in CPE management, the impact of store now, decrypt later threat can be considered minimal.

Although quantum computing will compromise several business critical cryptographic algorithms, substantial additional information and technology are still required to access a telecom network to cause harm effectively. The deliverable concentrates mainly on three primary telecom services out of seven briefly explained. Although not all services are described in more detail about the stated objective, these three services can cover the most critical impact areas from quantum computing on telecom business processes dependent on PKI. The workshop with representatives from the Telecom sector agreed that the SRA developed is valuable and comprehensive. The SRA stimulates a more precise discussion on the impact of quantum computers on digital systems that rely on PKI. The participants would recommend other organisations in the Telecom sector to use the method as a learning instrument and an instrument for mobilising actors to develop transition strategies.

6 Conclusions and recommendations

6.1 Conclusions

This report studies the risks of the quantum computer on three PKI systems. More precisely, the effect of a quantum computer's arrival before adequate measures are taken to migrate all cryptographic algorithms to a quantum-safe equivalent. The workshops with representatives from the Government, Banking and Telecom sectors reveal that the impact of the quantum computer on PKI will be devastating.

Two threats posed by quantum computers are: (1) real-time access and (2) store now, decrypt later. Real-time access yields risk for confidentiality, integrity and availability. The prevalence of PKI in society is such that every citizen and institution will be impacted. Citizens will no longer be able to access governmental and financial services. The inability to use governmental services will cause social upheaval and disruption to everyday life. The inability to use financial services may be much worse, as the ability of citizens to conduct *any* transaction will cause a significant disruption to every citizen.

Moreover, the inability to conduct financial transactions extends to national banks and the Government. The overall effect of which will be much worse. System banks without the ability to borrow money internationally will collapse, causing a significant economic downturn. This scenario, one interviewee dubbed the quantum apocalypse, is a noteworthy find of this research.

Additionally, it should be noted that the effects of these sectors (Government, banking and Telecom) will compound since citizens and companies operate in all three domains. On an organisation level, the most likely action strategy – with the least damage – is shutting down their services. For society, one bank shutting down or one governmental service becoming unavailable might be manageable. However, the combined disruption of services will be devastating. It should be noted that the impact of the quantum computer on confidentiality provided by PKI is primarily relevant for the Government and Banking sector due to the sensitivity of the secured data.

Store now, decrypt later yields risks for confidentially, implying that while an adversary cannot access a quantum computer now, it stores encrypted secrets that can be decrypted later. While this scenario mainly undermines confidentiality on a technical level, it may lead to more political or societal trust concerns (e.g., political, state or industry secrets out in the open can damage trust in institutions, even if they are not timely anymore).

To conclude, the anticipated quantum apocalypse is based on the assumption that PKI systems will not undergo upgrades with quantum-safe cryptography. More precisely, the studied PKI is firmly based upon current asymmetric cryptography, and this research assumes that this will remain so. The remainder of the HAPKIDO project will research migrating PKI to use quantum-safe cryptography. This will be a fundamental update to PKIs, a major undertaking and aims to prevent the quantum apocalypse.

6.2 Recommendations

Generally, the workshop participants acknowledge that we are still in the awareness phase. Nonetheless, the organisations participating in HAPKIDO are keen on starting the next phase, focused on experimentation with the remaining four NIST post-quantum cryptography (PQC) algorithms. PKI systems should be replaced by quantum-safe algorithms, also known as PQC algorithms, to become quantum-safe. The PQC research field has flourished over the past two decades, creating a large variety of algorithms expected to resist quantum attacks. Some PQC algorithms are being selected and standardised by several standardisation bodies, including the NIST. However, even with the guidance from these essential efforts, the danger is not gone: there are billions of old and new devices that need to transition to the PQC suite of algorithms, leading to a multidecade transition process that has to account for aspects such as security, algorithm performance, ease of secure implementation, compliance and more.

Overall, the workshop participants that led to this report agree that the SRA developed is valuable and comprehensive. The SRA stimulates a more precise discussion on the impact of quantum computers on digital systems that rely on PKI. The participants would recommend other organisations to use the method as a learning instrument and an instrument for mobilising actors to develop transition strategies. The latter remains an open question: what to do next? The remainder of the HAPKIDO project will focus on guiding organisations to start the migration to quantum-safe cryptography.

7 References

AIVD (2023) The PQC Migration Handbook. Guidelines for migrating to Post Quantum Cryptography. Algemene Inlichtingen- en Veiligheidsdienst. https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook

AIVD (2021). Bereid je voor op de dreiging van quantum computers. Algemene Inlichtingen- en Veiligheidsdienst. www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers/Brochure+Dreiging+Quantumcomputers%2C+webversie+september+2021.pdf

Amadori, A., Duarte, J. D., & Spini, G. (2022). Literature Overview of Public-Key Infrastructures, with Focus on Quantum-Safe Variants Deliverable 4.1, HAPKIDO Project. TNO.

Analistennetwerk Nationale Veiligheid. (2019). Leidraad risicobeoordeling Geïntegreerde risicoanalyse Nationale Veiligheid. https://www.rivm.nl/sites/default/files/2019-10/Leidraad%20Risicobeoordeling%202019.pdf

Aven, T. (2018). An Emerging New Risk Analysis Science: Foundations and Implications. Risk Analysis, 38(5), 876–888. https://doi.org/10.1111/risa.12899

Aven, T., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., McComas, K., Renn, O., Thompson, K. M., & Zio, E. (2018). Core Subjects of Risk Analysis (p. 7). Society for Risk Analysis.

Bharosa, N., Wijk, R. van, Winne, N. de, Janssen, Marijn, Luitjens, S., & Veld, P. (2015). Challenging the chain: Governing the automated exchange and processing of business information.

Bharosa, N., Hietbrink, F., Mosterd, L., & van Oosterhout, R. (2018). Steering the adoption of standard business reporting for cross domain information exchange. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (dg.o '18). Association for Computing Machinery, New York, NY, USA, Article 16, 1–10. https://doi.org/10.1145/3209281.3209325

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

Christiansen, L.V., Bharosa, N. and Janssen, M. (2023). Policy guidelines to facilitate collective action towards quantum-safety: Recommended policy guidelines to aid and facilitate collective action in migration towards quantum-safe public key infrastructure systems. In Proceedings of the 24th Annual International Conference on Digital Government Research (DGO' 23). Association for Computing Machinery, New York, NY, USA, 108–114. https://doi.org/10.1145/3598469.3598480

Davenport, T. H., & Short, J. E. (1990). The New Industrial Engineering: Information Technology and Business Process Redesign. MIT Sloan Management Review. https://sloanreview.mit.edu/article/the-new-industrial-engineering-information-technology-and-business-process-redesign/

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

Esteves, A. M., Franks, D., & Vanclay, F. (2012). Social impact assessment: The state of the art. Impact Assessment and Project Appraisal, 30(1), 34–42. https://doi.org/10.1080/14615517.2012.660356

International Organization for Standardization [ISO]. (2018). Information technology—Security techniques—Information security management systems—Overview and vocabulary (ISO/IEC 27000:2018). https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Joosten, R., & Smulders, A. (2014). How to successfully manage risks in hyperconnected value networks (p. 44). TNO.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organisations to post-quantum cryptography. Nature, 605(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kong, I. (2023). Transitioning towards Quantum-Safe Public Key Infrastructures. PhD Proposal. TU Delft.

Kong, I., Janssen, M and Bharosa, N. (2022) Challenges in the transition towards a QS government. DG.O 2022: The 23rd Annual International Conference on Digital Government Research Pages 282–292 https://doi.org/10.1145/3543434.3543644

Klunder, T. (2022). Designing a method for assessing the societal risks posed by quantum computing on public key infrastructures. Master Thesis, TU Delft.

Le Fevre, M., Gölz, B., Flohr, R., Stelkens-Kobsch, T., & Verhoogt, T. (2017). SecRAM 2.0: Security Risk Assessment Methodology for SESAR 2020. SESAR. https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Security%20Reference%20Material%20Guidance.pdf

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

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

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 (Ijacsa), 9(3), Article 3. https://doi.org/10.14569/IJACSA.2018.090354

Mosca, D. M., & Piani, D. M. (2021). Quantum Threat Timeline Report 2020 (p. 52). Global Risk Institute. https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

Mosca, M., & Mulholland, J. (2017). A Methodology for Quantum Risk Assessment (p. 6) [Whitepaper]. Global Risk Institute.

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

Onkenhout, J. (2023). Secure Payments in the Quantum Era. A Technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector. Master Thesis, TU Delft.

Presley, A., & Liles, D. (1998). The Use of IDEF0 for the Design and Specification of Methodologies.

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. Foresight, 20(4), 353–363.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). Journal of Information Security and Applications, 18(1), 45–52.

Smart, N. P. (2016). Cryptography made simple. Springer.

Stake, R. (2003). Case Studies. In N. K. Denzin & Y. S. Lincoln (Eds.), Strategies of qualitative inquiry (2nd ed). Sage.

TNO. (n.d.). Analistennetwerk Nationale Veiligheid (ANV). TNO. Retrieved 16 March 2022, from https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/crisisbeheersing-nieuwe-uitdagingen-nieuwe-kansen/analistennetwerk-nationale-veiligheid/

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). https://doi.org/10.1007/s10676-017-9429-1

Wadhwa, K., Barnard-Wills, D., & Wright, D. (2015). The state of the art in societal impact assessment for security research. Science and Public Policy, 42(3), 339–354. https://doi.org/10.1093/scipol/scu046

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0

WEF (2022). Transitioning to a Quantum-Secure Economy. World Economic Forum Whitepaper. https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., 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), 1–19. https://doi.org/10.1140/epjqt/s40507-021-00104-z

WRR (2016). Samenleving en financiële sector in evenwicht. https://www.wrr.nl/binaries/wrr/documenten/rapporten/2016/10/12/samenleving-en-financiele-sector-in-evenwicht/R096-Samenleving-financiele-sector-evenwicht.pdf