Anna van Buerenplein 1
2595 DA Den Haag
P.O. Box 96800
2509 JE The Hague
The Netherlands

www.tno.nl

T +31 88 866 00 00

TNO report TNO 2022 R11823

HAPKIDO

D2.1 Requirements Analysis

Date	4 October 2022
Author	A. Smulders (TNO)
Co-autors	A. Amadori (TNO) G. Spini (TNO) L. Spit (Microsoft) N. Bharosa (TU Delft) R. van de Hesseweg (KPN) S. Fehr (CWI) J. Hament (Zynyo) M. Geerdink (Zynyo) P. van den Berg (Logius) J. van den Berge (Logius) S. Konings (Zynyo)
Number of pages	33
Number of appendices	1
Customer	NWO (NWA.1215.18.002)
Project name	HAPKIDO
Project number	060.43667

Contents

1 Introduction

This report is a result of the HAPKIDO project and was produced in joint effort by the partners within work package 2 in the HAPKIDO project; Zynyo, Microsoft, KPN, TU Delft, CWI and Logius. The main objective of the HAPKIDO project is to answer the research question; how can a transition towards quantum-safe Public-key Infrastructure (PKI) systems be realized? For a complete overview of the project, its objectives, breakdown in work packages and activities, we refer to the project plan. The purpose of this document is to show how the HAPKIDO project derives requirements for future quantum-safe (PKI) systems.

PKI systems play an important role in societal processes, as is shown in the results from HAPKIDO work package 1 “societal impact assessment”. While PKI systems rely on public-key cryptography, it is known that the emergence of quantum computers threaten the properties of the PKI systems and since there is a dependency on PKI, pose a direct threat on the societal processes. Therefore, there is a need to migrate from current PKI systems to quantum-safe PKI.

The target audience for this report are primarily the partners in the project providing input to further guide the activities and developments in the HAPKIDO project. In addition this report is of interest for those stakeholders confronted with questions and challenges related to migration of current PKI systems to quantum-safe PKI systems.

In order to address this migration from a requirements perspective, we need to understand the current requirements that PKI systems have on the underlying cryptography and the system as a whole and how these requirements might change over time. In this deliverable we focus on how to identify those changes in requirements that are likely to have the most impact on future quantum-safe PKI systems.

As a means to assess these requirements, two use case where selected by the partners in the project. A use case in scope of the HAPKIDO project is a PKI-enabled function relevant for one or more societal critical process. In this report we focus on the use cases eDelivery for the societal critical process “Internet and data services” and eSeal for the societal critical process “Electronic messaging and information disclosure to citizens”. The societal critical processes are defined by the NCTV and a given for the HAPKIDO project. The PKI-enabled functions where selected by the project partners based relevance to the critical processes and potential to identify transition related challenges.

These use cases used to validate the way of selecting and use case analyses. The result is an overview of requirements that are relevant for those application domains, based on use case analyses. This also includes an assessment of which requirements are potentially conflicting or require a distinct approach for migration from a classical PKI to a quantum-safe PKI.

1.1 Terminology

Public-key Infrastructure (PKI[1]) (NIST SP 800-53 Rev. 4): The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public-key certificates. The purpose of a PKI is the administering of certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public-key certificates.

PKI core processes: key management (including generation), key distribution (private and public-key), public-key validation.

Quantum-safe cryptography: cryptographic schemes that are resistant to attacks by both classical and quantum computers.[2]

Quantum-safe PKI: a PKI where the underlying cryptographic components are quantum-safe.

Hybrid PKI: Three different definitions exist. In all three cases, the name denotes a PKI where the underlying cryptographic components consist of a combination of both classical and quantum-safe cryptographic primitives; the three different definitions describe which properties are expected from this combination:

- (Definition I): the quantum-safe part can be switched off, or anyway ignored, in such a way that parties that are unable to process quantum-safe cryptographic primitives can still make use of the PKI functionality (possibly with some minor modifications to the PKI functions, e.g. to verify a signature).
- (Definition II): when both classical and quantum-safe primitives are used, the PKI core processes are secure (from a cryptographic perspective) as long as one of the two components is secure.
- (Definition III): both the properties of Definition I and of Definition II are met when both pre-quantum and post-quantum cryptographic schemes are employed.

In all three cases, it is generally implied that the classical cryptographic components are the ones used in current PKIs.

Cryptographic primitives: basic cryptographic algorithms and schemes that are often used as building blocks in more complex cryptographic constructions. Examples: hash functions and encryption schemes.

Public-key cryptography: cryptographic primitives that involve two keys, a “public” and a “secret” (or “private”) key, where the former is meant to be disseminated among several users, or even made entirely public, while the latter must remain secret and only accessible by one party, the “owner”, in order for the primitive to provide security. Examples: public-key encryption and digital signature schemes.

PKI-enabled functionality: functionality using public and private keys managed by a PKI, such as eSeal, authentication and eDelivery.

Application domain: an application domain (e.g. ICT/Telecom, Banking, Energy) is used to cluster critical infrastructure processes that, if disrupted, lead to societal

[1] Adapted from: public key infrastructure (PKI) - Glossary | CSRC (nist.gov) which has more variants and sources

[2] Adapted from: https://www.etsi.org/technologies/quantum-safe-cryptography

disruption and form a threat to the national security. The critical infrastructure processes, and the related application domains, are defined by the NCTV[3].

Certificate: public-key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it[4]. Whitin this report the term certificate is used for public-key certificate.

Certificate Authority (CA): authority trusted by one or more users to create and assign certificates.

Trust Service: electronic service which enhances trust and confidence in electronic transaction.

Trust Service Provider (TSP): is a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider. Examples of TSPs are Logius, Zynyo and KPN.

Use case: within the scope of this document, a use case is the basis for a more in depth analysis to identify new or changing requirements. A use case is a combination of a process related to one of the application domains and a PKI-enabled functionality with a potential impact on migration of the PKI core processes.

1.2 Scope

The scope for this deliverable is set by a combination of the following demarcations.

The first demarcation is formed by a subset of application domains and their related critical infrastructure processes. For the application domains we follow the scope set by the HAPKIDO project (ICT/Telecom, Financial and Digital Government). In this deliverable these application domains and the related processes form the starting point for our analysis.

The second demarcation is set by the PKI core processes. Focussing on PKI core processes puts the emphasis on potential migration challenges for these PKI core processes.

The third demarcation is formed by a subset of PKI-enabled functionalities. This subset is used to scope the work for analysis per application domain. The PKI-enabled functionality forms the basis to validate relevant migration options for the PKI core processes.

[3] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
[4] ETSI EN 319 411-1 V1.3.1 (2021-05)

2 Approach

The objective of the work package[5], of which this deliverable is the first result, is to collect, structure, and deconflict requirements. The collection of requirements is done based on the application domains and stakeholders identified in WP1 as a starting point. This enables the identification of potential gaps and changes needed in the requirements. For the current situation, our starting point are these sources (ETSI EN 319 411-1 v1.2.2 [1], ETSI EN 319 411-2 v2.2.2 [2], CA/Browser Forum [3], eIDAS [4], and Logius.

In order to achieve this objective, the work package focuses on the changes in requirements related to these documents and on identifying new or changed requirements. For this, results from other work packages in the HAPKIDO project are used as input.

2.1 Document structure

This document reflects the different activities and their results within work package 2 of the HAPKIDO project. Section 3 is a result of a brainstorm with Subject Matter Experts (SMEs). A number of documents where selected as relevant input for this work package by the partners in this project from the large body of available documentation [5]. These documents were selected based on the assessment by the SMEs to contain the most relevant information to support an analysis which would highlight the relevant differences from current classical PKI in relation to quantum-safe PKI. Additionally, these documents provided input to draft a reference model for PKI which formed the basis for further analysis and scoping of our work.

The application domains within the scope of this work package are described in section 4. Thereby these application domains are in line with the work done in work package 1, in which a societal impact analysis was done for the same application domains. With representatives from these application domains, a selection of use cases was made based on the information from the input documents and the reference model.

In section 5, a summary of the analysis of the provided documents is given. The objective was to identify any options that could result in variations in migration from the current situation to a quantum-safe PKI. These options were assessed with the SMEs in the project, resulting in potential issues for migration and use of a quantum-safe PKI. These options were used as input for the selection and analysis of use cases. Initial requirements for the PKI core processes are part of the results and conclusions of this document.

[5] Work package 2, within the HAPKIDO Project

3 PKI reference model

Although PKI has been around for decades, what is and what is not PKI is not always clear. This clarity is required in order to identify areas of interest and to relate the requirements resulting from our use cases analysis to specific PKI core process requirements. In this section, we present a reference model for PKI systems.

This reference model supports reasoning why elements are deemed in or out scope of this research and will further help focussing on requirement areas not yet or insufficiently addressed. The reference model is based on information presented in CYBER; Migration strategies and recommendations to quantum-safe schemes [6] with additions from quantum-safe Cryptography; quantum-safe threat assessment [7]. The PKI reference model was then validated by the SMEs involved in the project.

The following describes the steps taken to construct this reference model. Since the project's focus is on PKI and its related public-key based cryptographic functions, we need to be able to distinguish these specific cryptographic functions from other cryptographic functions. Our starting point is that public-key based cryptographic functions are a subset of the overall set of cryptographic functions.

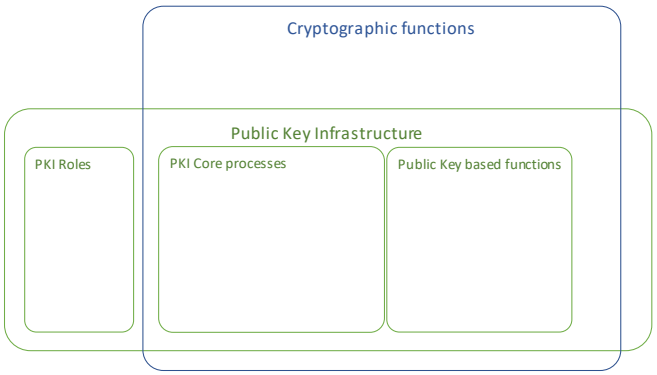

Figure 1: Public-key Infrastructure as a partially overlapping subset of cryptographic functions

Within a PKI distinct roles can be identified. These roles are related to the PKI core processes. Figure 2 shows the generic structure as shown in Figure 1, populated with examples for each of its subsections. Note that this is not an exhaustive list.

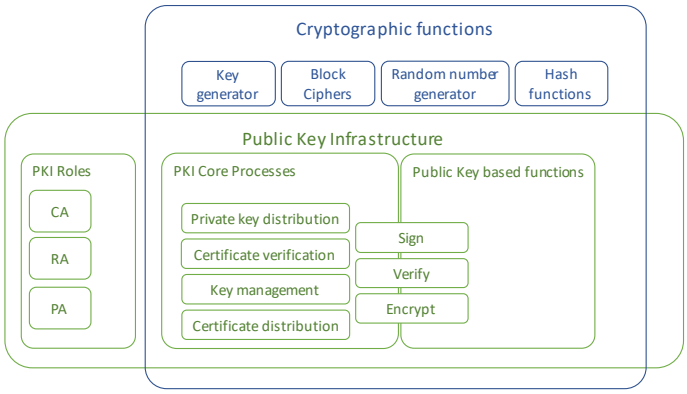

Figure 2: Populated reference model

The elements shown in Figure 2 are given to illustrate the different focus areas. The elements are not exhaustive, their purpose is to provide guidance (reference) to distinguish what the scope of the project. In the next step we extend the reference model with a section containing possible applications of PKI-enabled functionality. These are also mentioned in the references but are not strictly part of the PKI itself. This addition was included since it provides a basis to identify use cases and link these to the core aspects of PKI. It further helps to determine the scope and focus of our work in this work package.

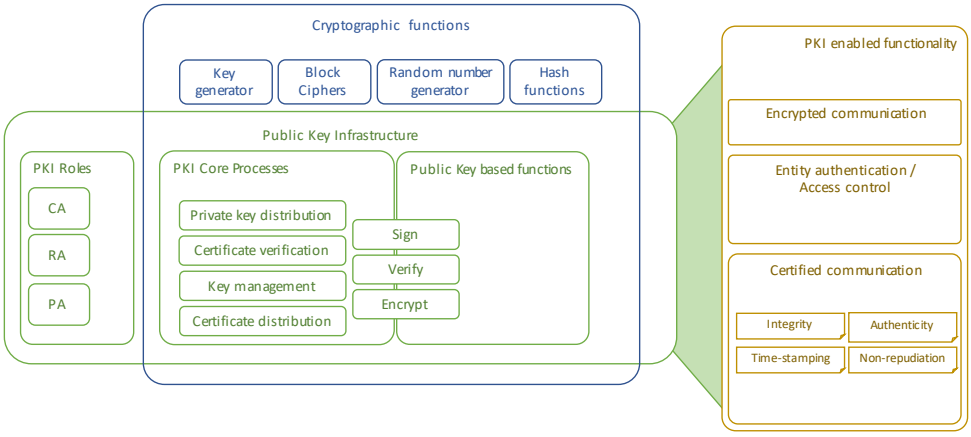

Figure 3: PKI reference model extended with application of PKI-enabled functionality

3.1 Core PKI Processes

At the core of a PKI are the processes to manage and distribute key material [1]. Our research focusses primarily on this area of the reference model. Which does not mean that the other elements in this reference model are not addressed. These elements are considered when relevant for making choices concerning these core PKI processes. In the next section these core processes are further described.

At every PKI there are a number of core processes. Depending on how keys are generated and by whom, there are some variations in the implementation of the core

PKI processes. In this section we describe these core processes and highlight where the general variations are.

With a document describing the PKI processes [2] as a starting point an SME workshop was held to outline the core PKI processes and the main functions in those processes were identified. The main purpose of this exercise was to identify potential issues for migration, focussing on both potential changes in the process as well as changes in the main functions in these processes. The result from the workshop is given in Figure 4, below, showing the high-level core processes:

- Key Management
- Key Distribution
  - Private key Distribution
  - Public-key Distribution (user certificates)
  - Public-key Distribution (root certificates)
- Public-key Verification

For each high-level core process, the main functions are identified. In the figure below, the high-level core processes are shown as horizontal blocks. Within each of these blocks, the main functions are given. These core processes and their functions are used in the analysis of the use cases in order to identify changes in requirements and where these changes are applicable. In the figure below, both the CA and TSP are included. The figure is based on a root structure where the CA handles key material and certificates for the TSPs[6] within its root structure. The end user key material and certificates are handled by the TSP.

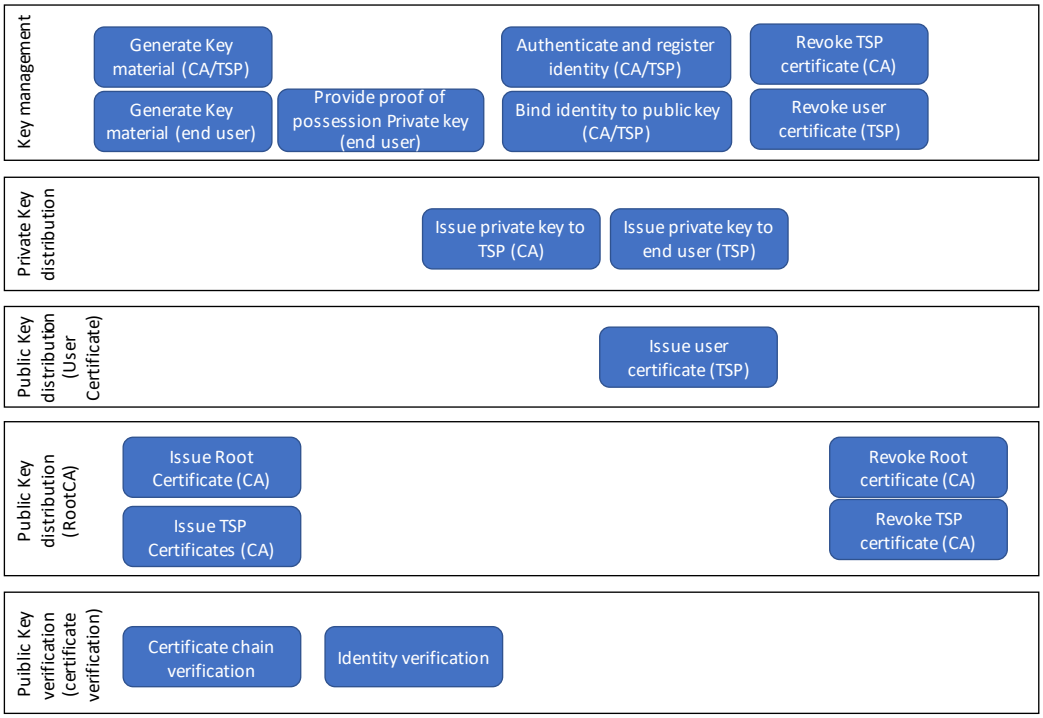

Figure 4: High-level overview of core PKI processes

[6] The figure represents generic buildingblocks, for our analysis we are focussing on the requirements related to Qualified TSPs.

Usually the public-private key pair is generated by the CA or TSP. In general the CA generates public-private key pairs for a TSP, and a TSP generates a public-private key pairs for the end users.

For a public-private key pair generated at the CA or TSP there are basically two variations to provide the end user with the private key. One is where the keypair is generated in a Hardware Security Module (HSM) or a Signature Creation Device (SCD), where the HSM/SCD is physically handed to the end user.

Another variation is where the private key needs to be communicated to the end user via a digital infrastructure. In this variation, it is essential to use a quantum-safe medium to communicate the private key to the end user.
There are cases where the public-private key pair is generated by the end user. Such a case is when an end user running a web server, generates the public-private key pair to be used for secure communication with that webserver.

4 Application domains

The critical societal processes as defined by the NCTV [8] are a subset of all societal processes. From this overall set only a subset is within scope of this project. This scope is visualised in Figure 5. These critical processes are further divided into category A and category B processes (see Appendix 1: Critical Processes). Category A contains the processes with potentially the highest economical, physical or societal impact. Within the HAPKIDO project only the category B processes (see Table 1) are in scope. For completeness we assume that there is another group of processes that are non-critical. The purpose of this figure is to focus our work and provide a rationale for choices made in this project for scoping. This results in the following graphical representation of application domains.

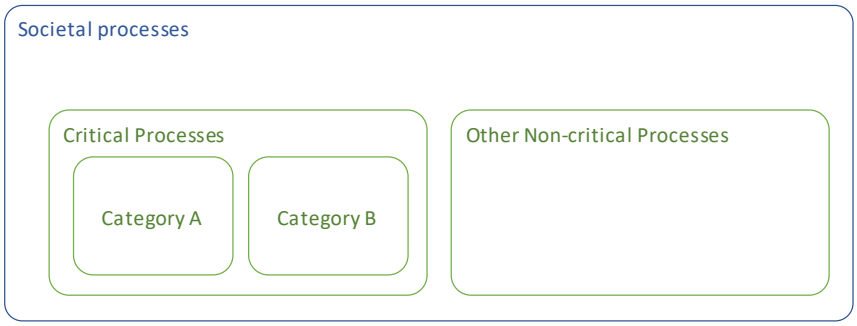

Figure 5: Societal processes and the sub-set of critical processes

In the table below, a summary is given of the critical processes in scope of the HAPKIDO project. The complete list of critical processes as indicated by the NLD government is also provided in Appendix 1: Critical Processes. In the next sections, we illustrate the connection between these application domains and PKI-enabled functions. These steps are further detailed in the next sections.

Table 1: overview of critical processes in scope of this project.

Application domain	Critical processes
ICT/Telecom	Internet and data services
	Internet access and data traffic
	Voice services and text messaging
Financial	Retail transactions
	Consumer financial transactions
	High-value transactions between banks
	Securities trading
Digital government	Personal and organisational record databases
	Interconnectivity between record databases
	Electronic messaging and information disclosure to citizens
	Identification of citizens and organisations

In addition to these application domains, the healthcare domain is also in scope of HAPKIDO. Please note that the healthcare domain is not on the NLD list of critical processes. There are indications that in the future these processes may added to the list of critical processes [9]. Since these processes are not included yet in that list, we haven't included them in this deliverable. In the planned iteration of this deliverable they may be included when available.

5 Identified options for migration

At the start of the project, an analysis was made on the available documents identified at the initiation of the project. These documents are “CYBER Migration strategies and recommendations to Quantum Safe schemes” [6] and “Quantum-Safe threat assessment” [7]. The objective was to identify requirements that may influence migration to quantum-safe PKI and for which different options are given. The assumption behind this is that which option is preferred depends on specific aspects related to a use case.
The first step is to see if options that impact migration could be derived from the identified input documents. As described in section 3 the reference model is used to focus on the options related to key management. For this we started with assessing those documents that would contain options related to the key management aspect.

Table 2: Migration options related to quantum-safe PKI

Concept requirement	Migration Options
Ensuring Backwards compatibility	- Using parallel classical and quantum-safe Certificate chains - Using hybrid certificate chains (supported by X.509)
Ensuring cryptographic agility	- Providing support to switch between multiple quantum-safe algorithms - Restricting modes - Revising the strength of individual parameters
Ensuring confidentiality of encrypted data during migration	No options given. “Statement on page 13: “Where the base state is that all data is encrypted and also subjected to cryptographically assured file integrity the non-quantum-safe cryptography encryption should not be removed (i.e. go clear) prior to imposing the quantum-safe cryptography-based encryption mode”
Allowing a stepwise migration	- Isolate sub-systems as far as possible to discrete security domains (DSD) - Interconnection between DSDs via quantum-safe pathways
Ensuring a secured state for assets over multiple generation of cryptography (given a QC threat)	- Encrypted - Cryptographically enabled access restriction

The options given above are directly related to the PKI core processes except one, which seems mainly to apply to the application of PKI based cryptographic functions in our reference model.

If the option “Ensuring confidentiality of encrypted data during migration” needs to be supported by the PKI core processes. And access to encrypted information is dependent on the PKI, this may impact the PKI core processes. Since it requires both the classical key pairs as well as the quantum-safe key pairs to be supported as long as the information itself needs to be encrypted. Since this requirement depends on the handling of the private keys after these have be distributed to end users, it seems to have little impact on the PKI core processes. It may have impact on the mechanisms used to distribute the private keys to end users.

In the figure below, a high-level visual representation of the PKI core processes migration is given of the options described above. In the figure the orange parts represent the quantum-safe PKI (future state) and the green the classical PKI (current state). The blue area indicates where both the classical as well as the quantum-safe PKI co-exist (Hybrid state). In section 6 and 7 we describe functionality and use cases in order to establish which type of applications of PKI-enabled functionality have the most impact on the duration needed to migrate from the current to the desired future state.

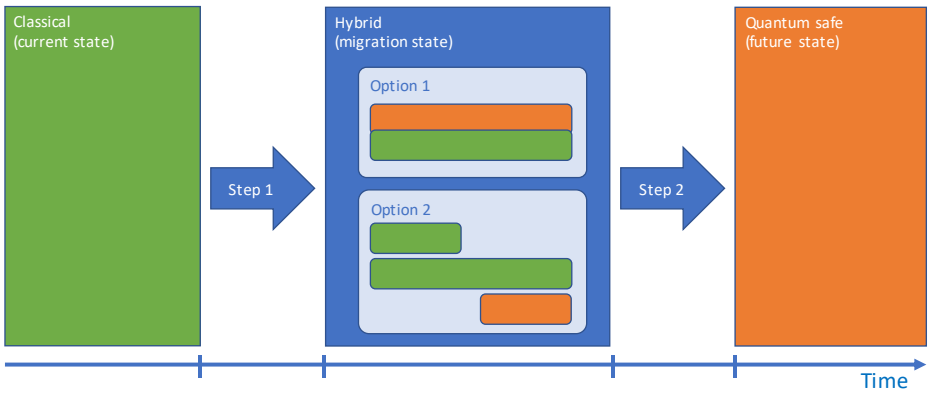

Figure 6: graphical representation of PKI core processes migration options

Focus of our work is on the identification of PKI-enabled functionality in relation to application domains (use cases). More specific, focus is on those use cases that aid the assessment of migration related requirements and options as outlined in section 3. This assessment should provide sufficient background to establish if there are distinct migration requirements and preferred options for the PKI core processes.

5.1 Timeline considerations for use case analysis

The reference model in Figure 3 and the migration options in Table 3, were used to identify relevant PKI-enabled functionality for PKI migration. The migration options presented in table 3 all relate to the retention of either confidentiality or integrity after classical PKI-based functionality becomes broken by large-scale quantum computers.

This observation allows us to identify PKI-enabled functionalities that are most and least affected by migration to a quantum-safe PKI. For example, one of the lesser affected functionalities is authentication, because handing out new quantum-safe based credentials and invalidating classical cryptography based credential access can be done in a relatively short period of time, and mainly depend on the agility of PKI-enabled applications (in the far right of the reference model). In a worst case scenario PKI based access can be denied, keeping access to information secure from Quantum-capable adversaries who target the PKI system. For other functionalities, the required retention time with respect to confidentiality and integrity is less clear and seems to be highly dependent on the for other are less clear and the assumption is that it depends on the use case. In the next section, we investigate this dependency on the use case further.

5.2 Considerations depending on Hybrid PKI definition

There is no universal definition of a hybrid PKI. There are three common definitions, which were presented in the introduction. These different definitions have implications on the implementations of the core processes of the hybrid PKI.
Recall that the first definition dictates that the quantum-safe part can be switched off, or anyway ignored, in such a way that parties that are unable to process quantum-safe cryptographic primitives can still make use of the PKI functionality (possibly with some minor modifications to the PKI functions, e.g., to verify a signature). This definition 'allows' the core PKI to have relatively independent core processes for both the classic as well as the quantum-safe PKI. As long as users have a fall back option to the classical PKI.

The second definition states that the PKI core processes remain secure when both classical and quantum-safe components are used, as long as one of the two components is secure. For backward compatibility this would require that users should use both classical and quantum-safe building blocks. And are able to select the correct building block needed for a provable secure PKI while either the classical PKI or the quantum-safe components may be broken.

The third definition states that both the properties of Definition I and of Definition II must be met. This third definition requires the most complex implementations for the core processes and is therefore likely to have the most impact. Currently the standardisation efforts seem to be in line with definitions I and II while in the academic world the third definition is also used for designing a hybrid PKI.

6 PKI-enabled functionality as input to use cases

During the identification of PKI-enabled functionality, the project team focussed on the functionalities that have potential for a case that would highlight issues that would impact the migration phase, in relation to the PKI core processes (see section 3).

With the subject matter experts (SMEs) within the project, a brainstorm was held to identify PKI-enabled functionality that would require attention when considering the key management migration options. One of the aspects, are options that would extend a migration scenario over time. We first focused on PKI-enabled functionality identified on the eIDAS website [4]. Based on this initial assessment two PKI-enabled functionalities were identified. One PKI-enabled functionality is electronic seals and another is e-delivery. These PKI-enabled functionalities are described in the following sections.

6.1 Functionality: Electronic Seals

The functional description of electronic seals (eSeals) in this section is based on the requirements for electronic seals on the eIDAS website [4]:

> ‘An electronic seal’ refers to any data in an electronic form, which is attached to or logically associated with other data in electronic form, to ensure the latter’s origin and integrity.

Technically an eSeal has many similarities with an (qualified) electronic signature. The main difference is that where signatures are meant to be used by individuals, eSeals are meant to be used by a legal entity (i.e., organisations)

There are a number of aspects to an electronic seal. It provides to the creator of an electronic seal a high-level of confidence that data needed when creating a seal, under his control is used for electronic seal creation. The eSeal is linked to this data in such a way that any subsequent change in the data is detectable. Electronic seals are uniquely linked to the creator of the seal and are capable of identifying the creator of the seal.

Further distinctions are made between advanced electronic seals and advanced electronic seals based on a qualified certificate for electronic seals. Where relevant we will highlight the differences in our analysis for these two distinct variants of electronic seals. As mentioned in the introduction of this section, in our use case analysis, we will focus on potential effects for a prolonged migration (see section 5).

One of the issues with eSeals is that the validity of an eSeal may be shorter than the requirements to ensure the origin and integrity of the document it is attached to. Extending the trustworthiness of the qualified electronic signature beyond the technological validity period is possible using a preservation service. Especially this service is of interest in the context of this section, since it refers to a service aimed at extending the validity of an eSeal beyond its technological validity period. This is especially relevant in cases when classical cryptographic algorithms, used to apply an eSeal, are no longer deemed safe and a migration to a quantum-safe cryptography based eSeal is needed. Revoking the validity of an eSeal once it can be forged by quantum-capable adversaries, shouldn’t revoke the legal validity of the document it

was applied to. Focussing on this specific service should provide background information when assessing the migration options from section 5.

6.1.1 *Migration options when considering preservation of electronic seals*

Our use case will focus on the relationship between the presented migration options in section 5 and the requirements for a validation and preservation service during the migration period. In this migration period both PKI-enabled functionality based on classical cryptography as well as PKI-enabled functionality based on quantum safe cryptography are assumed to be available.

In our use case we assume the existence of a document with a qualified electronic seal based on classical cryptography. This seal needs to be preserved while observing the requirements set out in the EU regulation. The starting point is a document which has a qualified electronic seal linked to it which was created within a PKI system using classical cryptographic algorithms.

In the following figure four options derived from the options outlined in section 5 are graphically represented. The yellow icon represents an eSeal based on classical cryptography and orange icon represents an eSeal based on quantum-safe cryptography.
In the first hybrid eSeal solution, the quantum-safe eSeal is based on the entire document *including the classical eSeal*. In the second hybrid eSeal solution, the quantum-safe eSeal is only based on the original document. There are therefore two eSeals that link to the same document and are independently valid, but one is classical and one is quantum-safe. The third option is where the original document (with an eSeal based on classical cryptography) can be re-issued by an authorised organisation with a new eSeal based on quantum-safe cryptography. The fourth option combines option one and three.

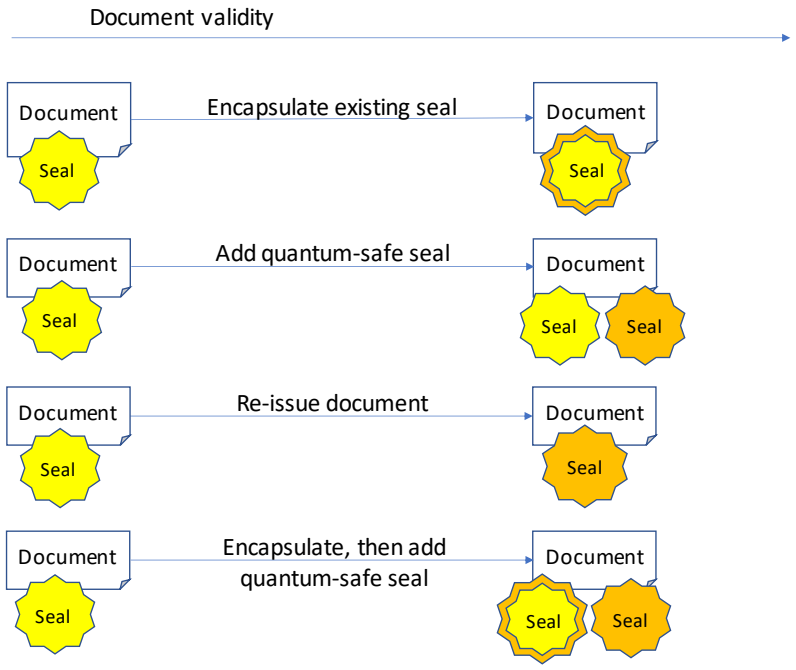

Figure 7: possible migration options related to seals

From our use case we derive that a preservation service must be able to handle seals (including the source document) based on classical cryptography and seals based on quantum-safe cryptography as output. In The figure above we assume that the document validity (preservation goal) extends the validity of the initial eSeal attached to that document [11]. The preservation goal is a point in time up to where it must be possible to assess the validity of a document, in this case using an eSeal attached to a document. The impact on the migration time for a PKI depends on which of these hybrid eSeal solutions is chosen. This could be the case in which there needs to be a historic link between eSeals created using classical cryptography and eSeals created using quantum-safe cryptography. In the use case we have analysed only the third option seemed relevant. Since it requires no historic relation between the classical and quantum safe situation, it wouldn't additionally prolong the migration from a classical to a quantum-safe PKI.

When applying the three definitions of a hybrid PKI to the different options shown in Figure 7, we encounter some caveats in relation to the third definition of hybrid. Encapsulating an existing seal created using classical crypto, within a quantum-safe seal is compliant with the first definition of a hybrid PKI. Adding a quantum-safe seal follows the second definition of a Hybrid PKI. If we then take the encapsulated existing seal and add the quantum-safe seal it creates a base for alignment with the third definition of hybrid. Compliance to the definition fully depends on the implementation at the user. For the third definition this seems more complex due to the interdependency of both the classical as well as quantum-safe cryptographic components. This means that even if the PKI core processes are fully compliant with the third definition, that is not a guarantee that the depending PKI-enabled functionality is compliant to the definition as well.

6.2 Functionality: Timestamp

This functionality is closely related to the seal functionality, at its core it uses similar PKI-enabled functions. The main difference is that a seal 'signs' the content of the document in order to preserve the integrity of the document itself. A timestamp also 'signs' the proof of a document's existence at a certain point in time. This makes that a timestamp is a specific type of signature providing a proof of existence and integrity of the document at a certain point in time. In relation to time, for timestamps two levels are defined, PAdES-DTS-BET and PAdES-DTS-A [12]. The PAdES-DTS-BET level defines requirements for the generation of a basic PAdES-DTS signature providing a proof of existence and integrity of the document. The PAdES-DTS-A level defines requirements for the incorporation of electronic timestamps that allow validation of the PAdES-DTS signature beyond the lifespan of PAdES-DTS-BET timestamps. This level aims to tackle the long term availability and integrity of the validation material.

Although the timestamp functionality is slightly different from the eSeal functionality they are often used in combination for instance for archiving purposes. For these combinations PAdES baseline profiles are available [14] distinguishing the profiles, B, T, LT and LTA. Thereby B covers requirements for short term electronic signature; Profile T covers the requirements for electronic signature with timestamp. The LT profile covers electronic signature with timestamp and VRI (verification related information) that allows verifying the signature even if the signing CA is not available

anymore. And the profile LTA (long term archiving) is very similar to the former LTV profile, covering electronic signature with qualified timestamp and VRI. For our scope both the LT and LTA profiles seem of interest to analyse via a use case.

Looking at both eSeals and timestamps, it seems that at their core these share the same issue with respect to migration. How to maintain the functionality when a timestamp was applied using classical crypto, and the classical crypto is compromised. Time stamping is also used as functionality in the functionality eDelivery of documents which is described in the next section.

6.3 Functionality: eDelivery of documents

This description of the eDelivery functionality is based on the overview given on the website of the EU [4] and more specifically for eDelivery [14] and the eIDAS regulation for eDelivery [10]. When looking more in depth at eDelivery, we can identify different functionalities. eDelivery provides functionality to exchange information between two parties. The eDelivery functionality ensures that the sending party cannot deny sending information and the receiving party cannot deny receiving the information.

The following steps (see Figure 8 for a schematical representation) describe how an eDelivery service works in terms of other PKI functionalities:

- A sender is authenticated by the eDelivery service.
- The sender sends a signed document to the eDelivery service.
- The signature's validity is verified by the eDelivery service[7]
- The sender provides the identity of the addressee of the document to the eDelivery service.
- The eDelivery service provides a time-stamped receipt to the sender.
- The eDelivery service provider notifies the addressee that a document is available. If an e-mail service is used as a medium, the notification e-mail is signed first[8].
- The addressee is authenticated by the eDelivery service.
- The eDelivery service provides the document to the addressee
- The eDelivery service provides a timestamped notification of delivery to both sender and addressee.

Various sub-functionalities of eDelivery, such as access control, identification and authentication, can be realised using PKI-enabled functionalities. These sub-functions can also be implemented using alternatives that do not require PKI-enabled functions. However, since the focus is on PKIs, the assumption is that PKI-enabled functionality is used where applicable. Date and time of sending, receiving and any change of data are indicated by a qualified electronic timestamp.

[7] Note that in this description we assume the sender is also the signer of the document.
[8] Requiring S/MIME

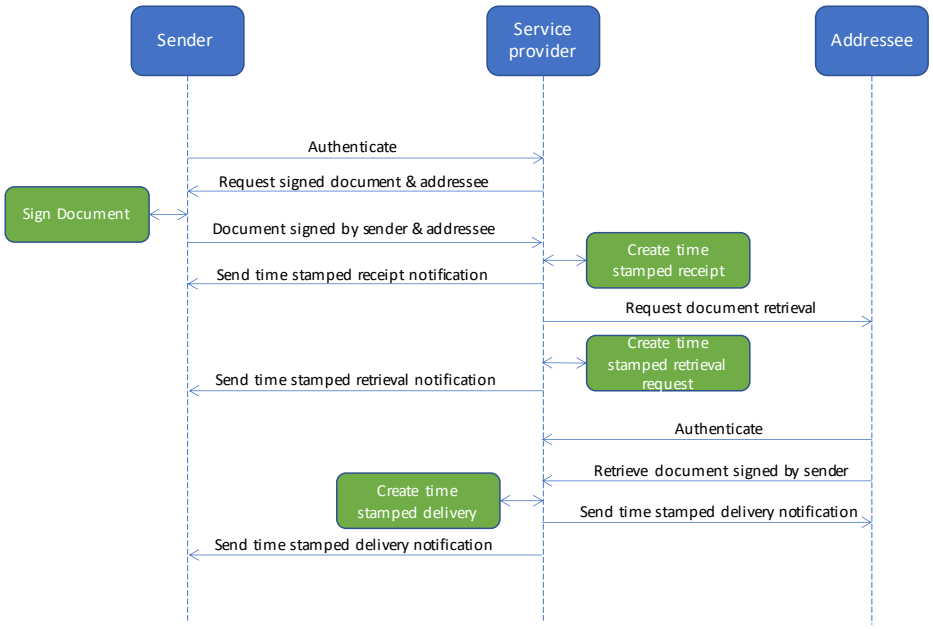

Figure 8: eDelivery schematic overview of functionality

What is not included in the description above, are cases with more than one service provider. Even with multiple service providers the same PKI-enabled functionalities as described above would be used.

7 Use case analysis

For each application domain the processes identified in section 4 are used as a reference for the use case analysis. Based on the reference model and identified options for migration, an assessment is made to elicit specific requirements per application domain. These requirements per application domain form the starting point for the next step, identifying potential overlapping, conflicting and/ or application domain specific requirements. Note that this analysis uses a high-level approach where the identified processes in section 3 are used as a starting point.

The description of the application domains and critical processes cover a broad range of specific applications and required functionality. This means that a selection mechanism is needed to select a use case. In this work package the selection was made by doing a high-level scoring of the relevance of a specific function for a specific critical process in an application domain. In the next iteration of this deliverable this selection method will be evaluated and if possible refined.

7.1 Use case functionality: Electronic seals

Due to time and capacity constraints in the project, it is necessary to limit the number of use cases to assess. In order to prioritise and select a use case, an expert opinion was given for the relevance of eSeals related to each of the critical processes. The result is shown in Table 3.

Table 3: relevance assessment of use case functionality electronic seals in relation to critical processes

Application domain	Critical processes	Relevance
ICT/Telecom	Internet and data services	-
	Internet access and data traffic	-
	Voice services and text messaging	-
Financial	Retail transactions	-
	Consumer financial transactions	-
	High-value transactions between banks	-
	Securities trading	-
Digital government	Personal and organisational record databases	-
	Interconnectivity between record databases	-/+
	Electronic messaging and information disclosure to citizens	+
	Identification of citizens and organisations	-

Based on the relevance assessment as a result of the expert opinion shown in Table 4, we have decided to focus on the critical process called “Electronic messaging and information disclosure to citizens” within the Digital Government application domain.

7.1.1 Use case description

For the use case PKI-enabled functionality *eSeals* for the critical process *Electronic messaging and information disclosure to citizens* we took the application of an eSeal on a formal document as a starting point. A user requests a formal document from a governmental agency. That agency provides that document with an eSeal, do the user can prove authenticity of the document to a third party if needed. The assumption is, that as long as the eSeal on a document is valid the document is valid (and authentic). This use case assumes that at some point in time the validity of the eSeal can no longer be established. This could be the case when a quantum-capable adversary becomes a real threat and classical cryptography is used. Another case is when an efficient attack is found in general. Any eSeal which is created using such cryptography should then be considered invalid. This may impact the validity of the document to which the eSeal was attached to. What we are trying to extract is the potential impact (if any) on the core PKI processes as outlined in section 3.1.

In order to make this functionality more tangible in relation to the application domain, we looked for a case where the provided information to a user should per definition have a long validity. For this case we settled on the case related to a (university) degree. Once obtained the degree is valid for a lifetime. This means that once issued it remains valid. During the analysis we learned that in in the Netherlands a central authority exists, which keeps records of university degrees (DUO). DUO is assigned as a basic registration, amongst others responsible for recording and maintaining information on who has which degree. In the cases where an eSeal is broken or no longer valid, DUO can re-issue the original document with a new eSeal. In such a case a preservation service may not be needed.

7.1.2 Use case analysis

The assumption is that at a point in time any classical cryptography used to apply an eSeal is ‘broken’. The existence of a central authority that can reissue degrees solves the problem to preserve an existing eSeal. If no such organisation exists there is still no issue if the original issuing organisation (in this case the university itself) still exists. A third variant is where the original organisation is no longer in existence and there is no central organisation that has the securely stored original data. Summarised these variants are:

1. the original issuing organisation still exists that has securely stored the originals. This organisation can re-issue same document with a new eSeal.
2. An organisation is assigned to securely store original documents issued by others and is authorised to issue these with a new eSeal.
3. The original organisation is no longer in existence or there are no securely stored originals. A preservation function may be needed.

When evaluating these variations, we observed the following. For variants one and two, there seems to be no impact on the core PKI. An authorised organisation, which has access to a security stored original document can reissue the document with a new quantum-safe valid eSeal.

For variant three we did not find a specific example that fits this variant. Since we are looking at a limited set of use cases our advice to the governance work package is to address this in their work package as a potential variant. If such an example is found, it can be addressed in the next iteration of this deliverable. Based on the variants one

and two there doesn't seem to be an impact on the migration timeline for the PKI core processes.

7.1.3 *Observations, recommended to address in the work package governance*

Although some observations are out of scope for this work package, they will be shared with the work package related to governance in the HAPKIDO project. Especially since some of these issues need to be addressed from a governance perspective.

While discussing this use case with the SMEs some questions that may be relevant for the Governance work package popped up. Such as: Is a qualified TSP allowed to reissue any existing document with a new eSeal? This is also relevant for the question, what is the added value of including (or encapsulating) the original eSeal? Assuming that the underlying algorithm will be broken. Please note that this only seems relevant under the assumption that the validity of the document itself outlives the validity of the eSeal.

Other questions are related to expected changes in the lifespan of root certificates. Once the life span of root certificates falls below the lifespan of the documents issued under this root, an assessment is needed on what to do with the documents, for which the validity is solely dependent on the eSeal attached to it.

A suggested alternative to use a qualified timestamp to address the issue of long term document validity, seems to have the same problem. A timestamp uses the same cryptographic building blocks as an eSeal. Meaning that the timestamp itself can no longer be assumed correct, when the underlying cryptography is deemed broken. This implies that a similar set of governance questions are related to timestamps as to eSeals.

7.2 Use case functionality: eDelivery

In order to prioritise and select a use case, an expert opinion was given for the relevance of eDelivery related to each of the critical processes. The result is shown in Table 4.

Table 4: relevance assessment of use case functionality eDelivery in relation to critical processes

Application domain	Critical processes	Relevance
ICT/Telecom	Internet and data services	+
	Internet access and data traffic	-
	Voice services and text messaging	-
Financial	Retail transactions	-
	Consumer financial transactions	-
	High-value transactions between banks	-
	Securities trading	-
Digital government	Personal and organisational record databases	-

	Interconnectivity between record databases	-
	Electronic messaging and information disclosure to citizens	+
	Identification of citizens and organisations	-

Based on the assessment result shown in the table above the most likely application domain for this functionality is ICT/Telecom and the critical process Internet and data services.

7.2.1 Use case description

For the use case PKI-enabled functionality *eDelivery* for the critical process *Internet and data services* we look at the communication between lawyers and law courts. Since May 2022, law firms are allowed to send case filings (documents and proof) in the context of litigation procedures using eDelivery to the law courts. The assumption is, that if the eDelivery is technically correct it can be used as a legally valid replacement of the telefax.

The use case is quite straightforward. The law firm is able to send by way of an eDelivery court documents (including supporting documents that serve as proof (bewijsstukken)). The receiving law court will receive and file the incoming eDelivery and add it to the legal case file.

eDelivery is a valid way to send a message in a registered form. Once the eDelivery has been sent and its attachments have been opened, the audit trail will provide legal proof on the data (both of e-mail and attachments) as well as the addressee(s). According to Dutch private law, it is sufficient for a sender to be able to prove that the addressee was able to open the message (either by way of a letter or an -email) that was addressed and sent to him/her. It is up to the addressee to open and read the message. If the addressee doesn't open or read, that does not mean (legally) that the message has not been received. By sending the message in a registered way the sender is able to prove that the message has been delivered. Jurisprudence confirms that, besides the registered mail, a (correct) eDelivery also constitutes a legal proof of reception.

7.2.2 Use case analysis

Some PKI-enabled functionalities used for eDelivery have no impact on the PKI core processes. This includes the PKI-enabled functionality authentication. Apart from this, the use case has a lot of similarities with the eSeal use case. Especially where it is related to the required lifespan of the documents in the eDelivery use case. To be more precise the lifespan relates to:

- the lifespan of the document signed by the sender
- the lifespan of the receipts signed by the eDelivery service
- the lifespan of the timestamp(s) provided by the eDelivery service on these receipts.

The impact on the authentication functionality enabled by (PKI) that requires a valid personal certificate seems limited. These certificates are valid for a certain period of time (often 1 to 3 years). They can be renewed by the certificate authority and can be reissued with a different seal for migration purposes.

A requirement of the eDelivery service is to keep an audit log. This functionality uses both eSeal and timestamp functionality, noting that not all information is necessarily kept by the eDelivery provider. This is due to GDPR data retention requirement to store privacy sensitive data for the shortest time possible. This means the audit log cannot be renewed, which could impact migration. For documents that have a long legal lifetime, it is necessary to archive these audit logs for a longer period of time, since they are part of evidence in case there is a legal dispute.

Additionally if the eDelivery service uses email for communication, these can be signed using PKI. If these emails contain important decisions/information that may be part of the evidence that might be needed in a legal dispute, then these too need to be archived. This is outside the scope of this analysis though as for eDelivery this is not the case since the emails are only part of the notification / communication but are not the basis for proof of delivery.

7.2.3 Observations, recommended to address in the work package governance

Based on the use case analysis, a topic to address in the projects governance work package may be the question related to legal implications of archiving signed emails containing important decisions/information. This specifically applies to the archiving of signed emails with certificates with a certificate lifespan shorter than the archiving requirements.

8 Overview of initial requirements

Within the first analysis we focussed on finding those requirements directly related to different options to migrate the PKI core processes from classical to quantum-safe crypto.

Starting with the analysis of the PKI core processes (see section 3.1), a potential issue arises depending on how a private key is provided to the user. This is true for cases where the key needs transmitted over a communication line, opposed to delivery to the user stored within a HSM or SCD.

> The requirement is that in those cases the communication channel used to provide the private key to the user needs to be quantum-safe.

Previous work as presented in section 5 yields the following high-level requirements:

- Ensuring Backwards compatibility
- Ensuring cryptographic agility
- Allowing a stepwise migration
- Ensuring a secured state for assets over multiple generations of cryptography (given a QC threat)
- Ensuring confidentiality of encrypted data during migration

For each of these requirements different options are given in order to achieve that requirement. Which option is preferred depends on the use case and its specific requirements some of which may impact the PKI core processes. In our analysis we focussed on identifying options that would lead to potential issues and additional requirements to the PKI core processes.

One such issue is related to the additional description for the requirement ensuring confidentiality of encrypted data during migration. This requirement dictates that classical encryption should not be removed during migration to quantum-safe encryption. Based on results from in WP5, there doesn't seem to be requirements for cryptographic functions in the scope of that work package that are able to implement this requirement. Currently our assessment is that this requirement doesn't depend on how the PKI core processes are implemented.

> The implication is that this requires end-users to implement additional measures in order to fulfil this requirement. Since these measures are not depending on the PKI core processes, and no PKI-enabled functionality to support this is in development, these required measures are outside the scope of this work package.

Migration implies a defined timespan, where starting from a situation with only classical cryptography to a state where only quantum-safe cryptography exists. The intermediate state is where a hybrid solution may be required. Based on a high-level glance at the different implementation options (see section 5.1), the major challenges seem to reside in the area where end users need to keep information confidential beyond the point where classical PKI based functionality may become broken. For instance when the cryptographic primitives on which the functionality depends is broken. This would undermine the whole trust structure which a PKI should provide.

The second problem may be in the area where information integrity needs to be preserved beyond the time where functionality based on classical cryptography may be broken. In this work package we focused on the potential issues related to information integrity.

Since hybrid PKI has 3 distinct definitions and each definition results in different requirements, it is important to assess a use cases in relation to these definitions. Especially the third definition of Hybrid may have additional implications for the core PKI processes, since all processes should be implemented such that the requirements related to the third definition are met. Currently, the standardisation efforts seem to be in line with definitions I and II, while in the academic world the third definition is also used for designing a hybrid PKI.

> Although in this work package we did not identify such a use case, it may be that there will be use cases which are based on the third definition. If such use cases will be identified, an assessment is needed to determine if current standardisation efforts related to the PKI core processes will support these cases.

An assessment of PKI-enabled functionalities is described in section 6.1. Starting with the eSeal functionality we see that an eSeal is linked to data in such a way that any subsequent change in the data is detectable. Electronic seals are uniquely linked to the creator of the seal and are capable of identifying the creator of the seal. The eIDAS regulation amongst others describes how a qualified preservation service provides extension to the trustworthiness of the qualified electronic signature beyond the technological validity period.

The use case analysis shows that this may be a requirement relevant for eSeals related to documents that don't have an authentic source. In our search for use cases we weren't able to identify such a use case.

Based on the use case analysis starting with the eSeal use case it seems that there are three variants of this use case:

1. the original issuing organisation still exists that has securely stored the originals. This organisation can re-issue same document with new seal.
2. An organisation is assigned to securely store original documents and is authorised to issue these with a new eSeal.
3. The original organisation is no longer in existence or there are no securely stored originals. A preservation function may be needed.

When evaluating these variations, we observed the following. For variants one and two, there seems to be no impact on the core PKI. An authorised organisation, which has access to a security stored original document can reissue the document with a new valid eSeal.

> For variant three we didn't find a specific example that fits this variant. Since we are looking at a limited set of use cases our advice to the governance work package is to address this in their work package as a potential variant.

If such an example is found, it can be addressed in the next iteration of this deliverable. Based on the variants one and two there doesn't seem to be an impact on the migration timeline for the PKI core processes. The approach in this deliverable

can be used to support such assessments and possible identification of relevant cases.

The high-level requirement for the eDelivery functionality is that neither the sender cannot deny sending the document and the addressee cannot deny receiving the document. Depending on the life time requirements per use case this may mean that additional measures are needed to achieve this requirement which are out of scope of the PKI itself. This is either the case when the life span of the issued certificates is shorter (1-3 years) than the timespan requirement from an eDelivery use case. Or in cases where an algorithm is deemed no longer secure.

Looking into the timestamp functionality (see section 6.2) it seems that eSeals and timestamps at their core share the same issue. How to maintain the functionality when a timestamp was applied with a classical crypto, and the classical crypto is compromised.

A requirement of the eDelivery service is to keep an audit log. This functionality uses both eSeal and timestamp functionality, noting that not all information is necessarily kept by the eDelivery provider. This is due to GDPR data retention requirement to store privacy sensitive data for the shortest time possible. This means that an audit log might not be renewed or reissued.

For documents that have a long legal lifetime, it is necessary to archive these audit logs for a longer period of time, since they are part of evidence in case there is a legal dispute. Since the legal lifetime may outlive the technical lifespan related to certificates and keys (and subsequentially) PKI-enabled functionality, additional measures need to be taken by end-users which are outside the scope of this work package.

9 Conclusions and next steps

The approach described in this documents supports the identification of requirements (changing and new) enabling the identification of challenges and solutions to migrate to future quantum-safe PKI systems.

It also provides input to the work package focussing on governance, by providing questions related to potential issues identified in the use cases. The focus is on those issues that would have implications for a use case but are not directly related to the PKI core processes themselves.

In this work package we focussed on use cases where potentially a big impact can be expected related to the PKI-core processes by selecting those use cases that have long term integrity requirements. Although we expected to find such use cases, it seems that to achieve this requirement the role of PKI seems limited, at least not for the use cases analysed in this document. Depending on the PKI-enabled functionality applied in a use-case, this requirement could be achieved without imposing additional requirements on the migration period for the PKI core processes.

For now the analysed use cases for eSeals did not yield specific issues that would result in additional requirements for migration options of the PKI core processes. Mainly because the use case doesn’t require a hybrid PKI.

There is a caveat thought, when assessing the use cases, we found that depending on the definition of hybrid was considered, the conclusion of the analysis would differ. Intermediate results from work package 5 support this assessment, where it seems different forms of hybrid result in different technological solutions that may impact the Core PKI processes. The results of this assessment will be discussed within the program.

Using the core process description and insights from the use cases, functional building blocks in the core processes will be identified in collaboration with the relevant work packages. The detailing of these building blocks and including further detailing of requirements is expected to be handled in the work package focusing on the migration architecture.

For this work package the next step is to extend the use cases to identify further challenges for other application domains that may have impact on the migration of the PKI core processes.

10 References

[1] ETSI, “EN 319 411-1 v1.2.2; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements,” 2018.

[2] ETSI, “EN 319 411-2 v2.2.2; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates,” 2018.

[3] The CA/Browser Forum, “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,” 2022.

[4] European Commision, “Digital Europe: eIDAS enablers,” [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Homepage. [Accessed 6 March 2022].

[5] P. v. d. Berg, *Overzicht vigerend PKIoverheid normenkaders,* Logius Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2020.

[6] ETSI, “TR 103 619 - V1.1.1 - CYBER Migration strategies and recommendations to Quantum-safe schemes,” ETSI, 2020.

[7] ETSI, “GR quantum-safeC 004: Quantum-Safe Cryptography; Quantum-Safe threat assessment,” ETSI, 2017.

[8] Nationaal Coordinator Terrorismebestrijding en Veiligheid, “Critical Infrastructure (protection),” [Online]. Available: https://english.nctv.nl/topics/critical-infrastructure-protection. [Accessed June 2022].

[9] Tweede Kamer der Staten-Generaal, “Vaststelling van de begrotingsstaten van het Ministerie van Volksgezondheid, Welzijn en Sport (XVI) voor het jaar 2022,” 20 12 2021.

[10] eIDAS, “Regulation (EU) N 910/2014 on electronic identification and trust services for electronic transactions in the internal market and,” *Official Journal of the European Union ,* vol. OJ L 257, pp. 73-114, 23 July 2014.

[11] ETSI, “ETSI TS 119 512 V1.1.1, Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services,” 2020.

[12] ETSI, “ETSI TS 119 142-3 V1.1.1, Electronic Signatures and Infrastructures (ESI); Part 3: PAdES Document Time-stamp digital signatures,” 2016-12.

[13] ETSI, “ETSI TS 103 172 V2.2.2; Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile,” 2013.

[14] European Commission, “eDelivery Exchange documents and data securely and reliably,” [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery. [Accessed 18 March 2022].

[15] FuturTrust, “International Movement for Preservation Service Development,” [Online]. Available: https://pilots.futuretrust.eu/press. [Accessed 14 March 2022].

[16] FuturTrust, “Welcome to the FutureTrust Validation Service (ValS),” [Online]. Available: https://pilots.futuretrust.eu/vals. [Accessed 14 March 2022].

[17] go.eIDAS, “Welcome to the Future of Trust,” 30 July 2019. [Online]. Available: https://blog.eid.as/tag/preservation-service-press/. [Accessed 14 March 2022].

[18] Tweede Kamer der Staten-Generaal, “Gewijzigde motie van het lid van den Berg C.S. ter vervanging van die gedrukt onder nr. 103,” 7 5 2020.

[19] K. Hintzbergen, J. Hintzbergen, H. Baars and A. Smulders, Foundations of Information Security Based on ISO27001 and ISO27002, van Haren, 2015.

11 Appendix 1: Critical Processes

Table 5, overview of critical processes of category A

Critical Processes	Sector (application domain)	Ministry
National transport, distribution and production of electricity	Energy	Economic Affairs and Climate Policy
Gas production, national transport and distribution of gas	Energy	Economic Affairs and Climate Policy
Oil supply	Energy	Economic Affairs and Climate Policy
Drinking water supply	Drinking water	Infrastructure and Water Management
Flood defences and water management	Water	Infrastructure and Water Management
Storage, production and processing of nuclear materials	Nuclear	Infrastructure and Water Management

The list of processes under category B are shown in Table 6. In this table the processes that are taken into account for this project are indicated in bold. These highlighted processes will guide the selection of use cases needed to perform the requirements analysis.

Table 6, overview of critical processes of category B. Indicated in bold the processes in scope of this project.

Critical Processes	Sector (application domain)	Ministry
Regional distribution of electricity	energy	Economic Affairs and Climate Policy
Regional distribution of gas	energy	Economic Affairs and Climate Policy
Internet and data services	ICT/Telecom	Economic Affairs and Climate Policy
Internet access and data traffic	ICT/Telecom	Economic Affairs and Climate Policy
Voice services and text messaging	ICT/Telecom	Economic Affairs and Climate Policy
Geolocation and time information by GNSS	ICT/Telecom	Infrastructure and Water Management
Air traffic control	Transport	Infrastructure and Water Management
Vessel traffic service	Transport	Infrastructure and Water Management
Transport of persons and goods by (main) railway infrastructure	Transport	Infrastructure and Water Management

Critical Processes	Sector (application domain)	Ministry
Transport by (main) road network	Transport	Infrastructure and Water Management
Large-scale production/processing and/or storage of chemicals and petrochemicals	Chemistry	Infrastructure and Water Management
Retail transactions	Financial	Finance
Consumer financial transactions	Financial	Finance
High-value transactions between banks	Financial	Finance
Securities trading	Financial	Finance
Communication with and between emergency services through the 112 emergency number and C2000	Public Order and Safety	Justice and Security
Police deployment	Public Order and Safety	Justice and Security
Personal and organisational record databases	Digital Government	Interior and Kingdom Relations
Interconnectivity between record databases	Digital Government	Interior and Kingdom Relations
Electronic messaging and information disclosure to citizens	Digital Government	Interior and Kingdom Relations
Identification of citizens and organisations	Digital Government	Interior and Kingdom Relations
Military deployment	Defence	Defence