HAPKIDO Deliverable 2.2

Requirement analysis for hybrid quantum-safe electronic document signatures

TNO Public ⟩ TNO 2023 R11745
11 October 2023

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2023 R11745 – 11 October 2023

Requirement analysis for hybrid quantum-safe electronic document signatures

HAPKIDO Deliverable 2.2

Author(s)	Dr. Dayana Spagnuelo, Dr. Alessandro Amadori, Dr. Gabriele Spini
Classification report	TNO Public
Report text	TNO Public
Number of pages	25 (excl. front and back cover)
Number of appendices	0
Sponsor	NWO
Programme name	Research programme cybersecurity
Programme number	NWA.1215.18.002
Project name	HAPKIDO
Project number	060.43667

Summary

The current digital society in which we live heavily relies on secure communications and digital trust services. These are dominantly achieved through Public Key Infrastructures (PKIs), for which the underlying cryptographic implementation is expected to become vulnerable against quantum-capable adversaries in the coming years. The HAPKIDO project studies how to realise the transition of services and systems towards a hybrid state of PKIs which encompasses quantum-safe cryptography next to the classical component. This is a complex problem with challenges in areas ranging from technology governance, to cryptography, and systems integration. In this context, the current deliverable focuses on the system integration challenges, and analyses the requirements a hybrid PKI system must satisfy, and how the transition will impact these systems with respect to computational performance.

There are many different sub-challenges when it comes to making a hybrid PKI system. The scope of this deliverable is electronic document signatures, which are currently implemented through the usage of quantum-vulnerable cryptography. Our work identifies and structures relevant requirements and performance indicators for hybrid generation and verification of PDF documents within PKIs. To do so, we start from existing documentation and standards defining technical requirements and discussing performance aspects of current PKI implementations. We scan them for relevance to our scope, selecting a list of relevant requirements and indicators. We structure and deconflict our selected list, and validate it with the help of experts on the subject, as well as by means of discussion with a designated expert group.

Our work results in four main categories of technical requirements, namely requirements for signature generation, signature validation, signature life-cycle process, and validity status of signatures. We also identify four performance indicators, which can be used to benchmark current classical PKI systems and hybrid ones in order to analyse the impact of their transition. These four indicators are execution time, memory footprint, storage footprint and throughput. We connect each requirement to one or more of these indicators where relevant.

There is no single solution when it comes to transition paths towards hybrid quantum-safe PKI systems that apply to each and every system. The appropriate transition will depend on each specific scenario, and may follow different migration options, depending on the priorities for security and backwards compatibility. As such, in this work we explore four migration options for electronic signatures, and discuss how our requirements and performance indicators can be applied to each of them. This exercise serves a three-fold purpose: 1) it validates the relevance of our results; 2) it guides future HAPKIDO developments, such as the implementation of a proof of concept and the formulation of a migration architecture; and 3) it serves as guidelines to the broader community of scientists and industry actors who wish to be frontrunners in this transition.

Contents

1 Introduction

1.1 Context

HAPKIDO (Hybrid Approach for quantum-safe Public-Key Infrastructure Development for Organizations) is a 5-years project, funded by the Dutch Research Council (NWO), that aims at studying the migration of existing PKI implementations to hybrid quantum-safe PKI implementations. This is done with a holistic approach studying the problem from the perspective of three disciplines: cryptography, technology governance, and systems integration. These are reflected in the three main tracks of the project: technical track, governance track, and evolution track. Each track is divided into several activities carried out in the different work packages (WPs) of the project.

From a technical perspective, HAPKIDO investigates two main problems; WP4 concerns itself with the challenges of using classical and quantum-safe cryptography together, investigating present and future standards for hybrid cryptography and focusing on the creation of various proof of concepts. WP5 focuses on the more fundamental part of hybrid cryptography, investigating the security of combining quantum-safe cryptography and classical cryptography.

Governance of hybrid PKI is studied in two main activities: the societal impact analysis and the migration strategies for organization deploying quantum-safe cryptography.
The first activity studies the expected impacts caused to society when the quantum computer becomes capable of breaking current PKI systems, as well as the threats to critical infrastructures that arise from the advent of a cryptographically-relevant quantum computer. These are studied in WP1. The second activity is subject of research in WP3. It investigates approaches within organizations and designs a serious game to educate about the quantum threat as well as to guide the migration process.

The evolution track concerns three main challenges. Identifying fit-for-purpose migration architectures, ensuring backwards-compatibility, modularity and allowing for a fast and smooth transition into quantum-safe PKIs is the challenge studied in WP6. WP7 aims at building a roadmap to guide such a transition, by providing an analysis of the phases and a tool for its assessment. Finally, WP2, where the current work fits, collects functional and non-functional PKI requirements and analyses the changes that must be performed for a PKI transition.

In the first deliverable of WP2 (deliverable 2.1 [1]), we studied the underlying requirements of existing PKIs. We inspected how such requirements might change over time and which PKI-enabled functionalities are most likely to be impacted by the transition to quantum-safe cryptography. Two use-cases, namely eDelivery and eSeals, are analysed to lay out such requirements. The insights of deliverable 2.1 pave the way for and scope the developments of this current deliverable. We present a summary of the most important findings in the next section.

1.2 Key findings of deliverable 2.1

Deliverable 2.1 focuses on an initial assessment of current PKI-enabled functionalities, on the migration requirements of the underlying cryptography, and on migrating PKI systems as a whole: from classical PKI to a hybrid state which supports both classic and quantum-safe PKI. This first part of the line of work on requirements concerns the study of two use cases identified as relevant to critical societal processes (as defined by Dutch National Coordinator for Security and Counterterrorism[1], see D2.1 for a more in depth explanation), and with potential to identify migration-related challenges, namely: a) electronic registered delivery services; and b) electronic seals.

Electronic registered delivery, or eDelivery, is a service with a protocol ensuring that a party sending electronic data (such as an email) cannot deny sending it, and that the receiving part cannot deny receiving it. According to the definition by the eIDAS regulation[2] (Art. 3(36)), eDelivery services provide evidence related to the handling of data, and protect transmitted data against the risk of loss, theft, damage, or any unauthorised alterations. Deliverable 2.1 identifies various sub-functionalities of eDelivery which can be realised with or without PKI-enabled functionalities (e.g., access control, identification, and authentication), but does not further elaborate on migration options for this use case.

Electronic Seal, or eSeal, is described by eIDAS (Art. 3(25)) as data in an electronic form, logically associated with other data in electronic form, to ensure the latter's origin and integrity. Electronic seals are technically similar to electronic signatures of documents, differing by the fact that seals can only be created by legal persons or entities. One of the issues identified with eSeals is the fact that the validity of an eSeal may be shorter than the required assurance of origin and integrity of the underlying document to which the seal is attached. A challenge of particular interest to this project is the fact that revoking the validity of an electronic seal in face of quantum-capable adversaries should not revoke the legal validity of the document. For this reason, deliverable 2.1 further studies migration options for the preservation of electronic seals. This use case provides a basis for the scope of the current deliverable, which is then further refined in Section 2.1.

In order to study possible migration options, deliverable 2.1 first proposes possible definitions of “hybrid” PKI, which reflect the different understandings of the word “hybrid” among different actors in the migration to quantum-safe cryptography. The hybrid definitions are then interpreted in the context of eSeals, and at least one migration option is derived for each definition. We present here the three definitions, in a slightly rephrased form as to better match the needs of this deliverable.

- **Definition I**: the classical and quantum-safe parts are both present, but users may decide to ignore the quantum-safe part and rely on the classical only (focus on backwards compatibility).
- **Definition II**: the classical and quantum-safe parts are both present, and the PKI system remains secure as long as at least one of the two components is secure (focus on security).

[1] Critical Infrastructure (protection) | National Coordinator for Security and Counterterrorism (nctv.nl)

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73

- **Definition III**: the classical and quantum-safe parts are both present, and the PKI system has two different usage modes; in the first one, Definition I applies. The second usage mode dictates to use both classical and quantum-safe part, and Definition II is valid in this case.

figure 1 shows different ways in which seals can be combined using classical and quantum-safe algorithms to satisfy the different definitions of hybrid.

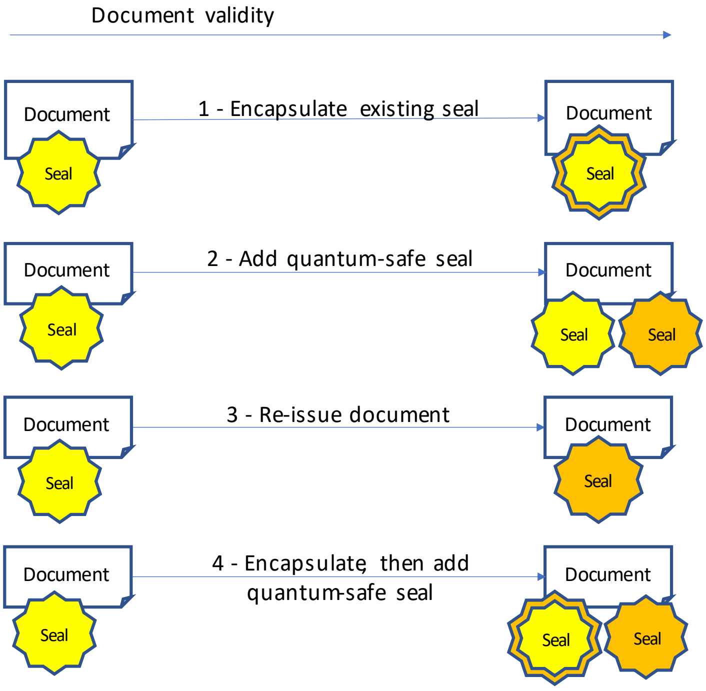
Document validity
Document
Seal
1 - Encapsulate existing seal
2 - Add quantum-safe seal
3 - Re-issue document
4 - Encapsulate, then add quantum-safe seal

Figure 1 - Possible migration options for electronic seals (yellow seal uses classic algorithm; orange seal uses quantum-safe algorithm)

Option 1 contains an encapsulated seal and can realise Definition II or Definition I, depending on the policy for verification of documents. If the policy requires a document to be checked first for its classical component, and then for its quantum-safe component (which contains the content of the classic seal), the document can be considered secure if at least one of the two components remain secure (Definition II). That is because an attempt to tamper with one of the components would be flagged by the verification of the other. On the other hand, if the policy allows the verification of the classical component without imposing the verification of the quantum-safe part (for backwards compatibility), then both parts are present but do not necessarily need to be used in order to verify a document (Definition I).

Option 2 reflects Definition I of hybrid, as both seals are present, but they can be independently verified. Thus, if an entity cannot verify the quantum-safe seal, they can still verify the classical seal. Similarly, **Option 3** assumes the document can coexist in its version with classic seal and its version with quantum-safe seal, thus an entity that cannot verify quantum-safe seals can process the classic version of the document.

And finally, **Option 4** can realise Definition II or Definition III of hybrid, depending on the policy for document verification. Similarly to Option 1, if the policy requires the verification of all components this option realises Definition II. Conversely, if the verification policy does not require the verification of all components the classical part of the encapsulated seal can be verified without the need of verifying its outer layer, in accordance with Definition I. If the encapsulated seal is verified in its entirety, then this option complies with Definition II. As both definitions are valid, Option 4 can also realise Definition III. In this option, the presence of an additional quantum-safe seal serves the purpose of ensuring forward compatibility (for a moment when classical PKI is no longer supported, and verification policies change).

The results of the work conducted in WP2 are not tailored to one particular definition or migration option. Thus, we advise the reader who would like to adopt the contents of our work to read both deliverables (D2.1, and the present document D2.2), and reflect on the definition of hybrid and migration option most appropriate to their own context.

1.3 Purpose of the current deliverable

The current deliverable builds on previous findings (D2.1) and defines requirements for the implementation of hybrid electronic signatures. Additionally, this deliverable gathers indicators for performance, and discusses how they can be used to evaluate and benchmark classic and hybrid implementations.

Work package 2 concerns itself with early stages of HAPKIDO project, by scoping and defining the problem at hand, to guide migration and development. Aligned with the project methodology Action Design Research [2] which defines four stages of research, deliverable 2.1 focuses on problem definition (stage 1), while deliverable 2.2 forms a bridge between this stage and the development-and-evaluation (stage 2) of the hybrid PKI proof of concept (scope of WP4). Additionally, the requirements presented here also serve as input for the development of a fit-for-purpose migration architecture (scope of WP6).

1.4 Deliverable outline

In the remainder of this document, we first clarify the terminology and scope of our requirements and indicators in Section 2. We describe the methodology used for elicitation, structuring, consolidation and validation of requirements and performance indicators in Section 3. Section 4 presents and discusses the proposed performance indicators, while Section 5 introduces the resulting list of requirements, argues their validity, and presents respective performance indicators for each requirement. Finally, Section 6 discusses the applicability of our work, especially in light of the different migration options, and presents the conclusions of this work.

2 Definition of requirements and performance indicators

The objective of this deliverable is the elicitation, structuring and deconfliction of technical requirements for hybrid electronic signatures, and the study of how the migration will impact the implementation of requirements with respect to their computational performance.

To clarify the terminology, a **requirement** must meet the following criteria:

a) It is a singular and documented necessity (or desire) of a stakeholder to solve the problem or achieve the objective of a hybrid quantum-safe PKI system.
b) It is valuable and useful to a stakeholder.

In this work we also propose **performance indicators**. Indicators do not describe a necessity, instead they present a metric or gauge that can be used to reason about the operation of such necessity, once implemented in a system.

2.1 Scope

The scope of this work was decided within the HAPKIDO consortium. Electronic seals, as discussed in the previous section, technically resemble electronic signatures. For this reason, the consortium decided to turn the focus to standards for signatures of electronic documents, in particular the PDF Advanced Electronic Signature (PAdES). This choice was made on one hand, due to the special relevance of PDFs to the HAPKIDO consortium partners, and on the other hand, due to a decision process on project level, that aimed for a use case related to eSeals and eDelivery, while keeping the focus on the technical challenges of digital signing of electronic documents, rather than their organizational and policy aspects; in particular, PAdES is also the focus of the first proof-of-concept developed within HAPKIDO, and we therefore elected to have a compatible scope. Notice that we expect that the requirements for PAdES have equivalents that apply to other form of electronic signature of documents, such as CAdES or XAdES; in this sense, it can be reasonably presumed that the results of this report have relevance to all types of electronic signatures of documents, although a formal analysis and validation of this claim is outside the scope of this report.
The requirements we identify are obtained from specification documents, and describe the structure and actions that govern the process of signing electronic documents and verifying the validity of signatures.

The performance indicators were selected from a pool of topics meant to direct the work towards real needs of HAPKIDO consortium partners. The following topics were proposed and discussed: a) computational performance; b) analysis focused on hybrid certificates; c) revocation processes for hybrid certificates; and d) analysis of requirements focused on Certificate Authorities and End Users.

By means of vote, the topic of computational performance was chosen, and further refined to “definition of performance indicators”. We refer to performance indicators rather than “performance requirements” (more commonly found in the literature) as we refrain from setting operational goals, presenting only the instruments one can use to measure performance in a system. For instance, an indicator could be the maximum memory usage of a given process, while a concrete operational goal would be to keep the maximum memory usage within 1GB. It should be remarked that due the innovative nature of this project, and to the early stage of maturity of hybrid PKI systems, the consortium expressed concerns that performance requirements would not be realistic at this stage. This motivates the choice to focus on performance indicators, rather than concrete values, as expressed at the beginning of this section.

3 Research methodology

This section describes the methods used to produce the findings of this report. In particular, we elaborate on the selected methodology to elicit requirements, to process them in order to obtain the structured and actionable data we aim for, and to validate the entire process.

3.1 Requirements

3.1.1 Elicitation

The requirements elicitation is initially based on desk research. For this we review relevant documentation describing the generation and validation of digital signatures. We selected an initial corpus of documents with support from the consortium partners and expanded it by keyword search (“PAdES + requirements”).

Documentation from consortium partner Logius on PKIOverheid, was considered in this step of the research. However, these documents mostly concern the compliance and organisational requirements that parties must satisfy to become Trust Service Providers (TSP) within PKIOverheid, and not requirements on the generation and validation of signatures. How certificates are used (including implementation guidelines) are out of the scope of Logius documentation, since those are based on ETSI standards.

For the sake of corpus diversity, we include documentation produced outside the European territory, in particular from the Brazilian PKI, which provides a source for controlling that outcomes of work are also internationally relevant, while still being based on ETSI and ISO standards.

The initial list of relevant requirements, with approximately 190 items, was collected from the following documents:

- Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation – ETSI [3]
- Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures - ETSI [4]
- Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles – ETSI [5]
- Requirements for the generation and verification of digital signatures (originally in Portuguese) – ITI [6]
- Requirements for digital signatures policies (originally in Portuguese) – ITI [7]

3.1.2 Structure and deconfliction

To structure and deconflict our list, we analyse each item and filter them according to the scope of this work. In this step we select functional and non-functional requirements for further analysis, following the including criteria:

IC.1. **Requirements referring to AdES or PAdES** – according to decision by the consortium as in scope.[3]

IC.2. **Basic Signatures** – Basic Signatures present sufficient functionalities to test the cryptographic capabilities of hybrid PKI.[4]

Conversely, to keep the scope of the work well-contained, the list of requirements was also filtered, and we removed items fitting the following excluding criteria:

EC.1. **Requirements related to XAdES or CAdES** – which do not pose different cryptographic challenges in comparison to PAdES (this excluding criterium is complementary to IC.1).[5]

EC.2. **More advanced types of signatures** – Signature with Time, Signatures with Long Term Validation Material, and Signatures providing Long Term Availability and Integrity of Validation Material (this excluding criterium is complementary to IC.2).

EC.3. **Revocation requirements** – revocation happens in reference to certificates (not keys), and it is assumed the revocation requirements for hybrid certificates will not necessarily be altered.

EC.4. **Application requirements** – as hybrid PKI will extend on classic PKI systems, it is assumed user interface requirements (e.g., displaying details of document to be signed, displaying details of signer's certificate) are already in place.

EC.5. **Requirements specific to software architecture components** – often referred to as "building blocks", these compose the signature generation and validation application; set aside as input for future HAPKIDO work (WP6), but out of scope for the current work.

EC.6. **Requirements specific to Policies** – we analyse available policies at the time of reporting, but it falls out of scope of the work package to suggest or adapt them. See below for more details.

Elaborating on EC.6, signature policies are additional requirements stipulated by the signing parties that regulate the validity of the signature. Policies can enforce additional rules for the use of signatures as well as their creation, verification, and security requirements. For instance, ETSI has published a policy with additional rules for digital signatures to be considered a qualified electronic signature/seal within the European legal framework [8].

We deem signature policies out of scope of this deliverable as policies do not have an impact on the functional requirements and the performance indicators. Although policies will have an important role in the migration as they can enforce the use of quantum-safe cryptography, possibly in hybrid mode. Therefore, it is reasonable to assume that standardisation institutes will address the current standards for policies to allow the inclusion of quantum-safe cryptography in hybrid mode (e.g., on the basis of already existing standards such as RFC 3125 [9] or ETSI Technical Specification 119 172-1 [10]).

The analysis of the list of requirements against the including and excluding criteria was executed by one researcher. Two other researchers validated this list by challenging the relevance of several requirements, and by discussing them until an agreement was reached.

[3] While ADeS refers to digital signatures on electronic documents in general, the letter which is prepended to ADeS denotes the specific format of the document considered. Therefore, PADeS refers to PDF documents, XADeS to XML, CADeS to CMS, etc.

[4] "Basic signatures" are a concept found in digital signatures for electronic documents. Cryptographically, they still involve regular digital-signature schemes, but the process to sign and verify them and the associated policies are less complex compared to other types of signatures. See exclusion criterium EC.2 for some examples of the more complex types of signatures.

[5] As stated in section 2.1, we expect the requirements for PAdES to have equivalent ones that apply to XAdES and CAdES (among others), although we do not make formal claims in this sense.

This step of the research was executed by the TNO internal team only. As a result, four main categories of requirements emerged, listed below:

- Requirements for **signature generation** – describing the data that is used for signing, how a signature is generated, and statuses of a signature-generation attempt.
- Requirements for **signature verification** – describing the data needed for verification of signatures, and the conditions under which a signature-verification process can succeed.
- Requirements for **processes** – describing non-cryptographic procedures related to the life cycle of the digital signature; and
- Requirements on **validity status** – describing conditions that influence the validity status of a signature.

As a last step to compose our list of requirements, we deconflict them. This was necessary as our initial corpus contained documentation from different standardisation institutes, and several requirements were duplicated, or conveyed a similar message. After requirements from different sources were merged into one document and split into relevant categories, duplicates became self-evident. Whenever a duplicate was found we kept the most encompassing version of the requirement (or adapt them to contain all relevant points) and we referred to all original sources. This is displayed in Tables table 2, table 3, table 4, and table 5, under the column "Original source".

3.1.3 Validation

Validation was done with an approach similar to a *request for comments*. We published a concept version of our requirements, posing specific questions on content or relevance of a given requirement we were unsure about, and invited open feedback about completeness and validity of the entire list. The concept was distributed to consortium partners as they are relevant stakeholders in the development of hybrid PKI systems. Following that, we collected all open questions and discussed them with an expert group composed by the TNO internal team, and one representative from each of HAPKIDO's industry partners, in addition to one academic partner.

The requirements presented in Section 5 are the resulting consolidated list divided in four categories. Where relevant, we comment on the outcomes of the validation by the expert group.

3.2 Performance indicators

3.2.1 Elicitation

Performance indicators are also elicited using desk research. We conduct a literature research using google scholar search engine based on search for keywords "performance + pki". We browse the first 50 hits ordered by descending date, and first 10 hits ordered by relevance. We opt for short number of sources ordered by relevance as it returns several dated references. Articles are selected based on title and abstract: we look for indications that performance is discussed in the document, such as mentions of experiments. Relevant sources are listed below, with two references being non-scientific:

- On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security (2017) [11]
- C-ITS PKI protocol: Performance Evaluation in a Real Environment (2019) [12]
- Evaluating the Performance Impact of PKI on BGP Security (2005) [13]
- A practical study of post-quantum enhanced identity-based encryption (2023) [14]

- PKI4IoT: Towards public key infrastructure for the Internet of Things (2020) [15]
- Performance requirements documentation - IBM [16]
- Requirements specification for PKI – Norwegian government [17]

Indicators are extracted from the body of the relevant documents. This step is more objective and straightforward than the elicitation of requirements, as indicators often appear as variables tested in practical experiments (normally presented in the experiment design, and listed in results tables), or evident from non-functional requirements specifying the minimum performance required for a given system. An initial list of 19 indicators and requirements is selected.

3.2.2 Consolidation and validation

The consolidation of performance indicators is done by extracting the subject indicator from the selected documents, and deconflicting similar indicators. Due to the low volume of our initial list, this step is done by one researcher only, and reviewed by another researcher independently. The resulting list of four performance indicators is validated using the same methodology as the validation of requirements (see 3.1.3).

With the exception of 'throughput', all the remaining indicators explicitly appear more than once in our initial list, thus we have reasons to believe that this list, despite being short, comprises the most relevant indicators in the scope of PKI.

We suggest that performance indicators are used to measure performance of the implementation of functional and non-functional requirements (where applicable). Therefore, in this report we first introduce the indicators in Section 4 before introducing our list of requirements in Section 5.

4 Performance indicators

Indicators present instruments that can be used to measure operations of a systems consistently. The performance indicators we propose can be used to benchmark classic and hybrid post-quantum implementations of functionalities as described in the requirements listed in this document. In table 1 we present the consolidated indicators found to be most relevant in the literature.

Table 1 - Performance indicators

ID	Indicator	Notes
PI.1	Execution time	Time: to be measured with delta of begin time and end time.
PI.2	(Max) Memory usage	Size: to be measured in bytes.
PI.3	Storage usage	Size: to be measured in bytes.
PI.4	Throughput	Speed: number of signature generation/validation (or other operation, depending on requirement) per units of time.

The performance indicators are meant to measure operations of the system; therefore, we suggest they are analysed in combination with requirements that describe a functionality or action to be performed by the system. Our indicators will not yield a meaningful interpretation when applied to requirements describing type and content of data needed for signatures, requirements purely process-related, or conditions for a signature to be considered valid. For this reason, we propose indicators that are applicable to signature generation (5.1), signature validation (5.2), and selected process requirements (5.3). Throughout the next section we suggest indicators that can be used to measure the performance of our requirements[6].

While browsing the literature two other relevant indicators were found but were left out due to the complexity of measurement, and to the fact that they are mostly relevant for production-ready solutions, rather than for the more experimental prototypes that HAPKIDO focus on: 1) latency; and 2) energy consumption. The first one, latency, can only be studied in a meaningful manner with investigation of code and algorithms available in the consolidated PKI libraries, and it would require addition of custom code to them to measure it. Rather than a measure of performance, we interpret latency as one of the reasons for execution time (PI.1) to be higher than expected, and we propose it to be investigated only in that case.

Energy consumption is identified by HAPKIDO partners as a subject of interest in communities of quantum-safe PKI, especially considering the expectation that quantum-safe cryptographic algorithms will have a higher power usage than classic ones. However, measuring energy consumption of a software operation depends not only on its implementation, but also on the hardware that executes it. Due to the yet low-TRL nature of quantum-safe PKIs, we refrain from using energy consumption as a performance indicator in our work, despite recognising it as an important issue.

[6] Our suggestions regarding the applicability of performance indicators might be too narrow for some PKI functionalities, and they should indeed be taken as an indication. We invite the reader to reconsider them for different applications.

5 Requirements

A complete list of requirements was presented to the group of experts (as described in Section 3.1.3), who were requested to provide input about their relevance and completeness. In what follows, we summarize general thoughts that emerged during discussion with the group, and present the requirements already adapted to comply with the feedback received.

5.1 Requirements for signature generation

There were no remarks about requirements under this category other than specific to the terminology used in some descriptions. In general, the group agrees the requirements are relevant to the project.

Table 2 - Signature generation requirements

ID	Requirement	Original source	Performance Indicator
SG.1	At least the following signed fields shall appear in Basic Signatures based on the PDF Advanced Electronic Signature - PAdES standard:	DOC-ICP 15.01 v 04 2.2.1.3	PI.2, PI.3
	a) id-contentType		
	b) id-messageDigest		
	c) id-aa-signingCertificateV2		
	d) id-aa-ets-sigPolicyId [Optional]		
SG.2	The id-aa-signingCertificateV2 attribute shall contain reference to the signer's certificate only. NOTE: This attribute prevents substitution of the referenced certificate with another one with different semantics but the same public key. If the signer holds different certificates related to different signature creation data, it indicates the correct signature verification data to the verifier.	DOC-ICP 15.03 v 08 PA-RB.5.2.1.1.4; ETSI 319 102-1 4.2.5.2	
SG.3	The data to be signed (DTBS) shall be constructed from the information objects that are to be covered by the signature. These are:	ETSI EN 319 102-1 4.2.6	PI.2, PI.3
	a) the Signer's Document or the Signer's Document Representation; and		
	b) the signature attributes selected to be signed together with the Signer's Document.		
SG.4	The DTBS preparation shall take the DBTS formatted (DTBSF) and hash it according to the hash algorithm specified in the cryptographic suite. The result of this process is then used to create the signature (DTBSR).	ETSI EN 319 102-1 4.2.8	PI.1, PI.2, PI.3, PI.4
SG.5	The Signature Creation Device shall take the DTBSR and apply the signature algorithm specified in the cryptographic suite. The result of this process shall be the signature value.	ETSI EN 319 102-1 4.2.9	PI.1, PI.2, PI.3, PI.4

SG.6	Each generated signature shall be verified using the public key from the signer's certificate, and shall meet the validation process requirements.	DOC-ICP 15.01 v 04 2.2.3.8; ETSI EN 319 102-1 4.3.2.4.5	PI.1, PI.2, PI.3, PI.4
SG.7	The status indication of the process for creating digital signatures shall have one of two values:	ETSI EN 319 102-1 4.3.2.4.7	
	OK: The signature has been successfully created; in this case, the Signed Document Object shall also be returned;		
	FAILED: unable to create a signature. In case of an error, it should return additional information allowing the error to be dealt properly.		
SG.8	Before invoking use of the signature creation data, the signature creation system should check that the signing certificate is valid (cryptographically correct, within its validity period and not revoked).	ETSI EN 319 102-1 4.3.2.4.5	PI.1, PI.2, PI.3, PI.4
SG.9	The signature information shall be embedded into the document itself and the ByteRange shall be the entire file, including the signature dictionary […][7].	ETSI EN 319 142.2 4.2.1.b	

5.2 Requirements for signature validation

Validation of signatures is the category of requirements identified with highest importance. That is due to the fact that while a document is signed only once in its lifetime, the verification of the signature happens every time a document is consulted, and has therefore more demands for performance.

Table 3 - Signature validation requirements

ID	Requirement	Original source	Performance Indicators
SV.1	Every digital signature shall be capable of validation. To verify the validity of a digital signature, the verifier shall use:	DOC-ICP 15.01 v 04 2.2.3.1	
	a) the electronic document for which the digital signature was created;		PI.2, PI.3
	b) the digital signature of the electronic document;		PI.2, PI.3
	c) the digital certificate of the signer and its corresponding certification chain;		PI.2, PI.3
	d) the revocation statuses referring to the certificates of the user's certification paths;[8]		PI.2, PI.3, (PI.1, PI.4)

[7] The original requirement from the ETSI document also adds "but excluding the PDF Signature itself". However, adhering to this requirement would pose strict limitations on the type of hybrid PKI used, which is arguably not in the spirit of the original ETSI document. For this reason, we have decided not to include this characterization in our requirements for hybrid PKIs.

[8] One partner points out the fact that in some cases the revocation status is included in the signature itself, at time of signing (for instance, an Online Certificate Status Protocol (OCSP) response). If the verification model is the "chain" model (see Section 5.4, requirement VS.5b), it is not necessary to check the revocation status as the

	e) the signature policy, if present, whose identifier is found in the digital signature;		PI.2, PI.3
	f) one of the algorithms classical or believed to be quantum-safe according to current standards and recommendations.		PI.1, PI.2, PI.4
SV.2	To validate a digital signature, made on an electronic document based on the data mentioned in requirement SV.1, it is necessary to ensure that:	DOC-ICP 15.01 v 04 2.2.3.2	
	a) the cryptographic state of the digital signature is approved, which involves:		
	i. authentication and/or authorship: by deciphering the digital signature generated on the digital content using the public asymmetric cryptographic key contained in the signer's digital certificate;		PI.1, PI.2, PI.4
	ii. integrity: by comparing cryptographic digests, showing that the digital content has not been altered since its digital signature was created by the signer.		PI.1, PI.2. PI.4
	b) the signer's certification path is valid in the time frame adopted for signature verification, which involves checking:		
	i. compliance with the requirements defined in items VS.2 and VS.3;		PI.1, PI.2, PI.3, PI.4
	ii. validity of the digital signature of each entity that issued certificates in the signer’s certificate path.		PI.1, PI.2, PI.3, PI.4
SV.3	The validity of a digital signature shall not be checked if the verifier does not have the data listed in requirement SV.2.	DOC-ICP 15.01 v 04 2.2.3.3	
SV.4	The validation process shall show as a result the status of each signature evaluated in terms of:	ETSI EN 319 102-1 5.1.1 and 5.1.3; DOC-ICP 15.01 v 04 2.2.3.10	
	Approved: when the cryptographic checks of the signature succeeded as well as all checks prescribed by the signature validation policy have been passed.		
	Disapproved: the cryptographic checks of the signature failed, or it is proven that the signing certificate was invalid at the time of generation of the signature, or because the signature is not conformant to one of the base standards to the extent that the cryptographic verification component is unable to process it.		
	Indeterminate: the results of the performed checks do not allow to ascertain the signature to be Approved or Disapproved.		

certificate was valid at the time of signing. The requirement does not specify if the included status information should be used or if a fresh query needs to be made to the issuer's CRL (Certificate Revocation List) or OCSP responder. Therefore, in case a query to retrieve the validation status of a hybrid certificate path needs to be performed via CRL or OCSP, the performance indicators PI.1 and PI.4 are also be applied.

5.3 Requirements for process

The group of experts recognize the relevance of this category of requirements; however, it is noted that these requirements in general are not quantum-safe specific and are likely to overlap with already existing processes for classic PKI.

Because the requirements listed here are non-cryptographic, they are deemed less relevant for HAPKIDO and the future proof of concept.

Table 4 - Process requirements

ID	Requirement	Original source	Performance Indicators
PR.1	In processes related to the life cycle of the digital signature, by technical and procedural means, the following requirements shall be met:	DOC-ICP 15.01 v 04 2.2.1.2	
	a) the digital signature shall be protected against forgery;		
	b) the signed digital content shall be protected from alteration;		
	c) any software or hardware component used in the process shall not cause changes to the digital content;		
	d) any software or hardware component used in the process shall not prevent the digital content from being displayed and viewed before and after each of the processes related to the lifecycle of the digital signature.		
PR.2	Where applicable, the requirements for considering a valid digital certificate may be verified before generating the digital signature. However, if there is any problem or non-conformity with the signer's digital certificate being verified, except in the case of expiration, it is up to the context, application, or business to decide whether the digital signature generation process will be executed or not.	DOC-ICP 15.01 v 04 2.2.2.7	
PR.3	If the signer wishes, the digital signature generation process shall allow the digital content to be visualized before and after the digital signature(s) are executed. Furthermore, the visualized digital content shall match the signed digital content, i.e., the digital content visualized by the signer shall be the content submitted to the digital signature generation process.	DOC-ICP 15.01 v 04 2.2.2.8	
PR.4	The digital signature generation processes shall be able to include and manipulate signed and unsigned attributes defined according to the adopted signature policy.	DOC-ICP 15.01 v 04 2.2.2.10	
PR.5	If a PDF document has embedded XML content and the intention is to sign the PDF, then a PAdES signature shall be used. If you only need to sign the XML content, then it is possible to sign with XAdES, however, this procedure may not protect the PDF as a whole.	DOC-ICP 15.01 v 04 2.2.2.15	

PR.6	The digital signature processes shall allow, when the signers or any interested party involved in the processes wish, the visualization and/or extraction of the signed digital content.	DOC-ICP 15.01 v 04 2.2.4.1	
PR.7	For batch digital signatures, the same requirements defined for processes related to the individual signature life cycle shall apply.	DOC-ICP 15.01 v 04 2.2.5.1	
PR.8	When deemed necessary to perform digital signatures in batch, secure methods, or procedures for accessing the private key of the signer shall be established in such a way as to allow the continuous and secure use of this key during the execution of the digital signature in each digital content belonging to a batch.	DOC-ICP 15.01 v 04 2.2.5.2	PI.1, PI.2, PI.4
PR.9	In the case of digital signatures in batch, for practical reasons, the asymmetric private key of the signer can be enabled only once - for example, with the insertion of the Personal Identification Number - PIN - for the generation of digital signatures in all the batch contents.	DOC-ICP 15.01 v 04 2.2.5.3	PI.1, PI.2, PI.4
PR.10	Signature attributes shall be pieces of information that support the signature and its interpretation and purpose, and which may be covered by the signature together with the signed document. The signature attributes shall be either directly provided by the signer or selected through the application or automatically inserted into the signature by the signature creation system.	ETSI EN 319 102-1 4.2.5.1	PI.2, PI.3
PR.11	Attributes shall either be signed attributes, i.e., attributes that are covered by the signature, or unsigned attributes, i.e., attributes that are not secured by the signature. The set of attributes included in a signature is defined by the signature creation policy used and can also be format specific.	ETSI EN 319 102-1 4.2.5.1	PI.2, PI.3
PR.12	Validation time, usually current-time, can be an input to the signature validation application. Execution of the application with different values for validation time will still return Approved, as long as e.g., no certificate involved in the validation expires or becomes revoked and no cryptographic algorithm is broken. Then it can also return Indeterminate.	ETSI EN 319 102-1 5.1.3	
PR.13	X.509 validation constraints shall indicate requirements for revocation checking and for use in the certificate path validation process as specified in the signature policy [10, pp. clause A.4.2.1, Table A.2 row m].	ETSI EN 319 102-1 5.1.4.2	
PR.14	Cryptographic constraints shall indicate requirements on algorithms and parameters used when creating signatures or used when validating signed objects as specified in the signature policy [10, pp. clause A.4.2.1, Table A.2 row p].	ETSI EN 319 102-1 5.1.4.3	
PR.15	Signature elements constraints shall indicate any requirements additional to X.509 (PR.13) and cryptographic constraints (PR.14) defined above as specified in the signature policy [10, pp. clause A.4.2.1, Table A.2].	ETSI EN 319 102-1 5.1.4.4	

PR.16	The common way to unambiguously identify the signing certificate is by using a property/attribute of the signature containing a reference to it (see SG.2). The certificate can either be found in the signature or it can be obtained using external sources. The signing certificate can also be provided by the driving application. If no certificate can be retrieved, the application shall return the indication Indeterminate.	ETSI EN 319 102-1 5.2.3.4	

5.4 Requirements on validity status

Requirements on validity status of signatures are perceived as relevant by the expert group. A remark is made about the validity models with respect to time. Currently, two modes of verification are supported. The first one, called shell mode, verifies that the certificate is still valid at the moment of the signature verification. The second, called chain mode, verifies that the signature was valid at the time of the signature generation and issuing (VS.5). Although two models are possible, in the scope of this work only the first one is viable, as we consider signatures other than basic out of scope. For validation at the moment of creation of signatures, it is necessary to have a timestamp which is not present in basic signatures.

Table 5 - Validity status requirements

ID	Requirement	Original source	Performance Indicators
VS.1	The affixing of a digital signature shall unequivocally refer to an individual or legal entity and to the electronic document to which it is affixed.	DOC-ICP 15.01 v 04 2.2.2.1	
VS.2	The digital signature will be recognized when affixed during the validity period of the certificate on which it is based, and the restrictions indicated therein are respected.	DOC-ICP 15.01 v 04 2.2.2.2	
VS.3	The digital signature affixed after the expiration or revocation of the certificate on which it is based or that does not respect the restrictions indicated therein is equivalent to the absence of a signature.	DOC-ICP 15.01 v 04 2.2.2.3	
VS.4	A Basic Signature is a signature that can be validated as long as the corresponding certificates are neither revoked nor expired.	ETSI EN 319 102-1 4.3.1	
	NOTE 1: Signature with time can be used to validate a signature when a certificate has been revoked after the signature has been created.		
	NOTE 2: Signatures can then still be validated when certificates expire or become revoked, and also when the security of applied algorithms becomes questionable or used key sizes are no longer state of the art.		
VS.5	The validity model to be used shall be specified as a X.509 validation constraint. Two validity models may be supported:	ETSI EN 319 102-1 5.2.6.4	
	a) all certificates are valid at validation time (shell model); or		
	b) all certificates are valid at the time they were used for issuing a certificate (chain model).		

6 Discussion and Conclusions

Guaranteeing the validity of PKI systems in face of a quantum-capable adversary will become a challenge if not tackled in a timely and structured manner. HAPKIDO investigates how PKIs should migrate to a hybrid state before the quantum threat actualises, in order to prepare for it while maintaining compatibility with current systems. In this work package we focus on the requirements for hybrid PKIs. The first part of our work (D2.1) studies use cases with PKI-enabled functionalities that are deemed crucial for society, and explores the migration alternatives for them. In this work (present deliverable) we collect technical requirements to digitally sign PDF documents, stemming from the use cases of electronic seals/signatures, and present indicators to help measure the performance of their corresponding implementation. We believe our findings to be broadly applicable to digital signatures on electronic documents, although our work focuses on PDF standards.

Our requirements and indicators are agnostic to migration options. This is done purposely as there is still no consensus on a hybrid definition by the quantum-safe PKI community, and the migration options studied in this work package are realisations of those definitions. While no official definition is put forth by standardization bodies, in order to apply the results of the present document, we recommend to study the hybrid definitions and their respective migration options, and pick the most suitable one to the user's scenario.

Within the HAPKIDO consortium there is not yet a clear preference among migration options, although partners agree that it is preferable to maintain only one certificate with classic and quantum-safe keys. For this reason, migration option 3 is the only one ruled out (if one interprets the certificate itself as the document with eSeal, option 3 requires two versions of the same certificate to be signed by the Certificate Authority with classic and quantum-safe keys). For simplicity of implementation and backwards compatibility, option 2 is currently adopted in HAPKIDO.

Here we discuss how one can interpret the requirements according to migration options 1 and 2 (see figure 1). The remaining options share commonalities and their interpretation can be derived from this discussion.

The first migration option presents a document with a seal/signature generated using classic PKI, which is then encapsulated by another quantum-safe seal/signature. To create such document all signature generation requirements apply once with classical PKIs, and another time with quantum-safe cryptography considering the previous signature as part of the document to be signed. To validate such document all signature validation requirements apply once with classical cryptography, and another time with quantum-safe cryptography considering the previous signature as part of the signed document. Note that because this migration option realises hybrid through encapsulation, the outer seal should only be considered for validation if the validation of the inner seal is approved (SV.4).

The second migration option places a quantum-safe seal in a document in addition to a classic one. Similarly to the first option, signature generation and validation requirements apply once for each seal, however independently from each other for this option. Because this migration option realises hybrid definition I (*the classical and quantum-safe parts are both present and do not need to be used at the same time*), a document can be considered valid if at least one seal's validation is approved (SV.4).

Requirements on process and validity status apply more broadly to the life cycle of a digital signature and can be interpreted as relevant to the application or software handling it. This means that their interpretation remains the same for the different migration options. Conversely, performance indicators apply to requirements, and while their interpretation does not change for different migration options, their results might be affected by how the requirements are implemented. For instance, while verifying a document with encapsulated seals (migration options 1 and 4), if signature validation is done separately, it is likely that the implementation will load the signed document to memory twice, and therefore PI.2 (memory usage) will result in the sum of memory usage for each validation. On the other hand, a validation of signatures that is done in batch is likely to load the document only once and PI.2 can be measured only once.

The requirements and performance indicators presented here are validated for their completeness and relevance by HAPKIDO consortium partners on a theoretical level. As requirements and indicators are extracted from recent literature and currently active standards for classic PKI, we have reasons to believe they are also relevant on a practical level. However, tests must be conducted to validate their applicability in the development life cycle of a hybrid PKI-system. Such validation falls outside the scope of this work package. Nevertheless, as our requirements and performance indicators will guide the implementation of HAPKIDO's proof of concept (WP4) and serve as input for the design of the migration architecture (WP6), HAPKIDO's future work will serve as evidence of their applicability.

References

[1] A. Smulders, A. Amadori, G. Spini, L. Spit, N. Bharosa, R. van de Hesseweg, S. Fehr, J. Hament, M. Geerdink, P. van den Berg, J. van den Berge en S. Konings, „D2.1 Requirements Analysis," TNO, 2022.

[2] M. Sein, O. Henfridsson, S. Purao, M. Rossi en R. Lindgren, „Action Design Research," *Management Information Systems Quarterly,* vol. 35, nr. 1, pp. 37-56, 2011.

[3] ETSI, „ETSI EN 319 102-1 V1.3.1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation," 2021.

[4] ETSI, „ETSI EN 319 142-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures," 2016.

[5] ETSI, „ETSI EN 319 142-2 v 1.1.1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles," 2016.

[6] ITI, „DOC-ICP-15.01 V4.0 - Requisitos para geração e verificação de assinaturas digitais na ICP-Brasil," 2021.

[7] ITI, „DOC-ICP-15.03 V8.0 - Requisitos das políticas de assinatura digital na ICP-Brasil," 2021.

[8] ETSI, „ETSI TS 119 172-4 V1.1.1 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists," 2021.

[9] N. Pope, D. Pinkas en J. Ross, „RFC 3125 - Electronic Signature Policies," Internet Engineering Task Force (IETF), 2001.

[10] ETSI, „ETSI TS 119 172-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents," 2015.

[11] F. Haidar, A. Kaiser en B. Lonc, „On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017.

[12] F. Haidar, A. Kaiser, B. Lonc en P. Urien, „C-ITS PKI protocol: Performance Evaluation in a Real Environment," in *2019 15th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, 2019.

[13] M. Zhao, S. W. Smith en D. M. Nicol, „Evaluating the performance impact of PKI on BGP security," in *4th Annual PKI R&D Workshop - Multiple Paths to Trust*, 2005.

[14] D. Verchyk en J. Sepúlveda, „A practical study of post-quantum enhanced identity-based encryption," *Microprocessors and Microsystems,* vol. 99, 2023.

[15] J. Höglund, S. Lindemer, M. Furuhed en S. Raza, „PKI4IoT: Towards public key infrastructure for the Internet of Things," *Computers & Security,* vol. 89, 2020.

[16] IBM, „Performance requirements documentation," [Online]. Available: https://www.ibm.com/docs/en/aix/7.1?topic=implementation-performance-requirements-documentation. [Geopend August 2023].

[17] Norwegian Government Security and Service Organisation, „Requirements specification for PKI in the public sector," 2010.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl