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

TNO 2025 R00000 – 1 August 2025

# D6.2 Hybrid PKI Migration Challenges and Solutions

| | |
|---|---|
| Author(s) | M.J.H. Marcus and A. Amadori |
| Classification report | TNO Intern |
| Title | TNO Intern |
| Report text | TNO Intern |
| Number of pages | 19 |
| Number of appendices | 0 |
| Project name | HAPKIDO |

# Contents

# 1 Introduction

## 1.1 HAPKIDO Project

HAPKIDO is multi-year project focused on a Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations. The project addresses societal, organisational and technical challenges brought about by the threat of quantum computer to digital infrastructures.

The work in this report has been carried out by work package 6, which focuses on technical transition roadmaps for the four sectors in scope of the HAPKIDO project: the financial sector, the healthcare sector, the government sector and the telecom sector.

## 1.2 Work Package Focus

Work package 6 has previously published a generic overview of PKI components and their interdependencies as a foundation for reasoning about technical migration roadmaps [1]. In order to obtain a realistic view of how these components are implemented in practice and identify bottlenecks and potential solutions, representatives of work package 6 interviewed organisations within the Dutch PKI landscape from all four sectors. Note that such interviews have also been conducted as part of the research done for deliverable 3.3 [2], but our approach is of a more technical nature.

From these interviews, we have distilled a number of overarching insights as well as sector-specific insights. We have additionally been able to refine our component overview to reflect the current industry landscape in terms of software and hardware dependencies. Many of the challenges relate to external dependencies, especially for the PKI field, there is a strong dependency on cryptographic hardware and certificate management software, which emphasises the need for a crypto-agile approach to the post-quantum migration process. Even though some PKI standards are currently missing, organisation can take a proactive approach and start testing with the available open-source software packages.

## 1.3 Document Outline

Chapter 2 directly builds upon the component overview provided in deliverable 6.1 [1] and introduces various concrete and crucial PKI processes with diagrams which serve as background information for chapters 3 and 4. Chapter 3 provides a categorisation of the challenges we have identified through the interviews with the four sectors. Chapter 4 provides a one-on-one translation between the categories of challenges presented in chapter 3 and the potential solutions we have identified. Finally, chapter 5 presents the conclusion of this report.

# 2 Refined Component Overview

In order to understand which dependencies are relevant for which aspects of a PKI, we present two phases of PKI operations: Certificate Signing Requests & Renewal and Certificate Validation, and present the most commonly present PKI components during these phases. Some of these concepts have been covered in deliverable 6.1 as well, but we include that information with some extra details here for completeness [1]. We assume that the terms CA and root CA are known to the reader. For a more in-depth introduction to PKI components, we refer to [1].

## 2.1 Certificate Signing Requests and Renewal

The first stage a certificate requestor has to go through is enrolment of a public key into a PKI. This situation is illustrated in Figure 1. This is a standardised process [3]. The dependencies on hardware have been verified through the interviews conducted as part of the research for this report.

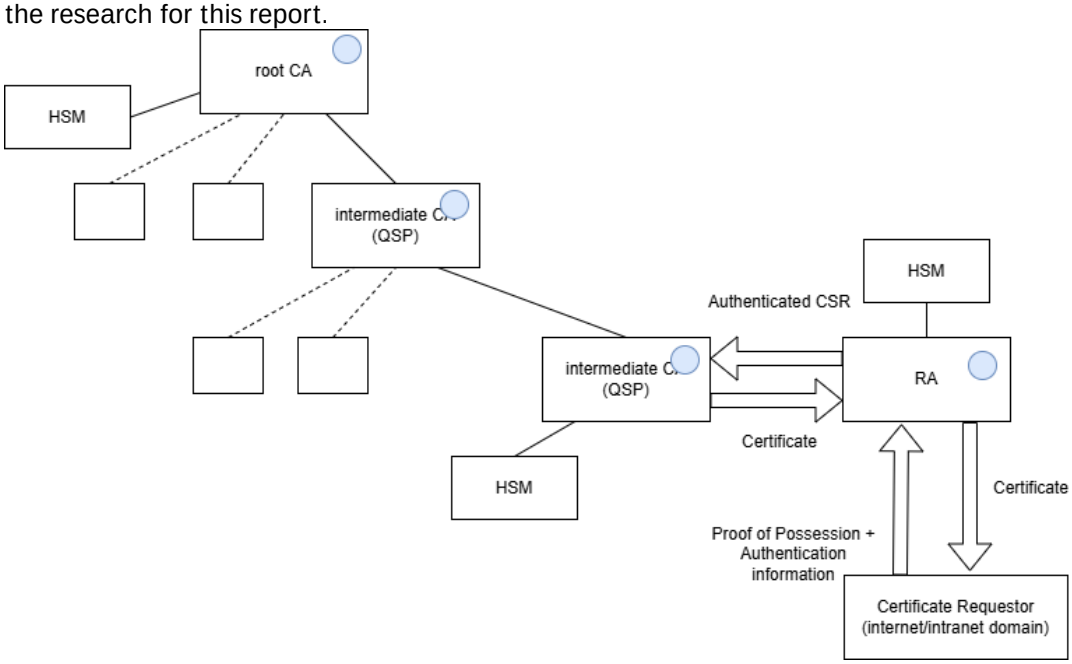


Figure 1: Diagram showing how certificates are requested, how requests are processed, and which PKI authorities are involved. The blue dots represent a dependency on cryptographic hardware and the text in brackets represents an example of such an entity. Here, QSP stands for Qualified Service Provider.

The certificate requestor will have to authenticate themselves to the Registration Authority (RA). The certificate requestor can then present the public key to establish the connection between the certificate requestor and the public key. The RA will check whether the certificate requestor owns the private key that corresponds to the provided public key to make sure the certificate requestor is not trying to register another entity's public key for themselves.

Checking whether the certificate requestor owns the private key of a public-private key pair is done through a proof-of-possession protocol. For public keys related to signing operations, this is fairly simple. The certificate requestor will use their private key to sign the request. For public keys related to key exchange / encryption operations, several approaches exist. Usually, a challenge-response protocol is initiated to prove possession, where the RA will send a nonce encrypted with the public key and the certificate requestor has to decrypt the nonce using their private key and send it back to the RA. This works for both traditional encryption schemes as well as key Encapsulation Mechanisms (KEMs). However, the interactive nature of this proof of possession process is undesirable. Other mechanisms have been proposed - specifically for KEMs - that are non-interactive, but they are currently not standardised [4].

Certificate renewal works similarly to CSRs. If a certificate has not expired yet and has not been revoked, then proof-of-possession is already established through the certificate itself, so in principle no extra protocol is necessary. In practice, it can happen that re-authentication needs to be done.

In principle, it is possible that a certificate requestor delegates the process of generating a public-private key pair to the certificate authorities. In this case, the proof-of-possession protocol can be omitted and the certificate requestor will receive the private key with the certificate from the RA or CA.

Oftentimes, certificate requests and renewal requests are automated through the use of protocols such as SCEP [5], EST [6] and ACME [7].

## 2.2 Certificate Validation

If a certificate is used beyond its expiration date or if the signature on the certificate is not valid for the public key of the issuing CA, then the certificate will be deemed invalid [8]. No communication is necessary to determine this, the user simply needs to verify the signatures in the chain of trust. When certificates have been issued, the only reason to communicate with authorities within the PKI is to determine whether a certificate was revoked before its intended expiration date. Let us take the generic situation when a certificate consumer receives a certificate from a certificate holder, for example the web browser in a webPKI receiving a certificate from a website, they will first check the signature and expiration date. If those are valid, then the certificate consumer has four main methods to deal with revocation: short-lived certificates, retrieving the CRL, OCSP, and OCSP stapling [8] [9] [10].

### 2.2.1 Short-Lived Certificates

A certificate consumer could simply decide to accept the risk that a certificate has been revoked before its expiration date. The benefit is that it removes the need to contact PKI authorities. The downside is the risk it introduces. This risk is higher if the certificates are long-lived – e.g., validity of multiple years. However, if the validity is short, such as 10 days, then the risk might be acceptable. The idea of short-lived certificates that are valid for a few days have become a popular approach [11] [12]. A downside of short-lived certificates is that the CA will need to be more actively involved to process Certificate Signing Requests (CSRs).

### 2.2.2 Retrieving the CRL

If the risk of ignoring potential revocation is too high – which is to be determined by either the user themselves or an overseeing role within an organisation - then the certificate consumer can (be configured to) contact an entity entrusted by the CA, often called the Validation Authority (VA) [13]. The VA tracks all certificates that have been revoked by its respective CA before their expiration date in the so-called Certificate Revocation List (CRL). Sometimes a separate Authority Revocation List (ARL) is tracked with information on revoked PKI authorities. The VA updates these lists at frequent intervals and signs them. The VA sends this signed CRL (and ARL) to the certificate consumers upon request. The certificate consumer can then check whether the provided certificate is on the list, or whether any of the CA certificates within the trust path are on the list. The benefit is that the certificate consumer gets up-to-date revocation information and does not need to divulge which certificate they want the revocation status for, which could reveal for example which website they are visiting and is a drawback of OCSP, which is covered in the next section. The downside is that CRLs can get quite large, which can cause delays when validating certificate information. Especially on the internet, users want to be able to quickly browse to websites, so any delay is undesirable.

### 2.2.3 OCSP

An alternative to retrieving the CRL is the Online Certificate Status Protocol (OCSP), which is visualised in Figure 2. This is standardised in [8].

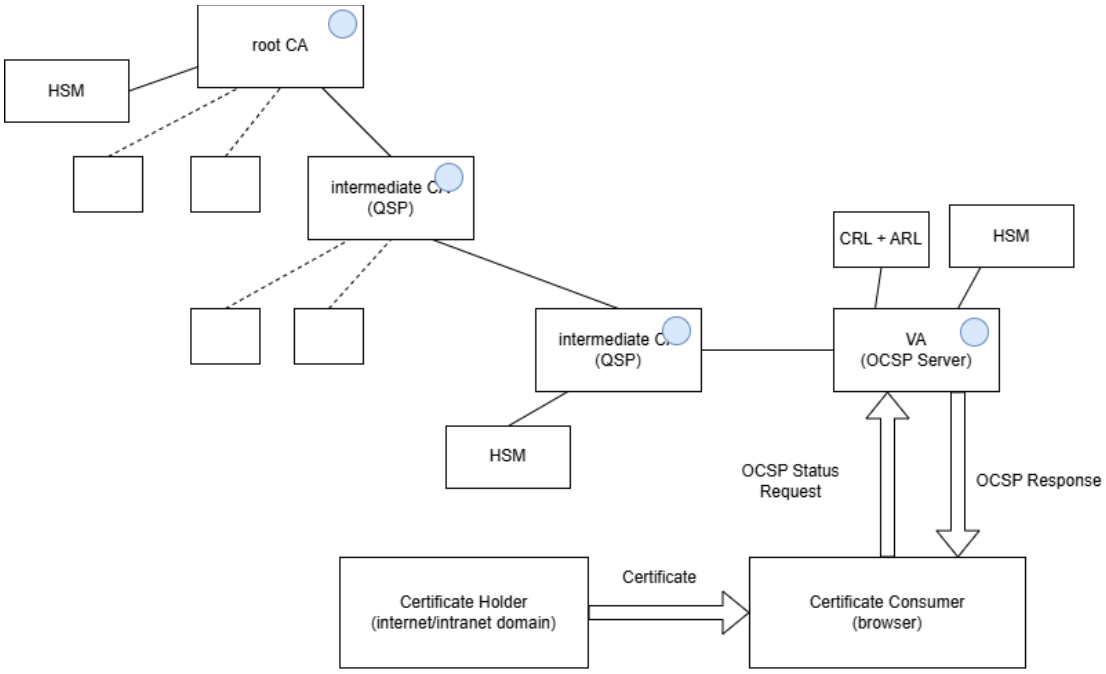


Figure 2: Diagram showing how OCSP works and which PKI authorities are involved. The blue dots represent dependency on cryptographic hardware and the text in brackets represents an example of the respective component.

The certificate consumer will send the provided certificate to the VA, who will then check the CRL (and ARL) on behalf of the certificate consumer. The VA then sends a signed revocation status for the certificate to the certificate consumer. The benefit is that the OCSP response is much smaller than the CRL, but the user does need to share which certificate they want to check for, which can reveal sensitive information as discussed in the previous section.

### 2.2.4 OCSP Stapling

In order to solve the privacy issue with OCSP, OCSP stapling was introduced, which is visualised in Figure 3. This has been standardised in [9] and [10].

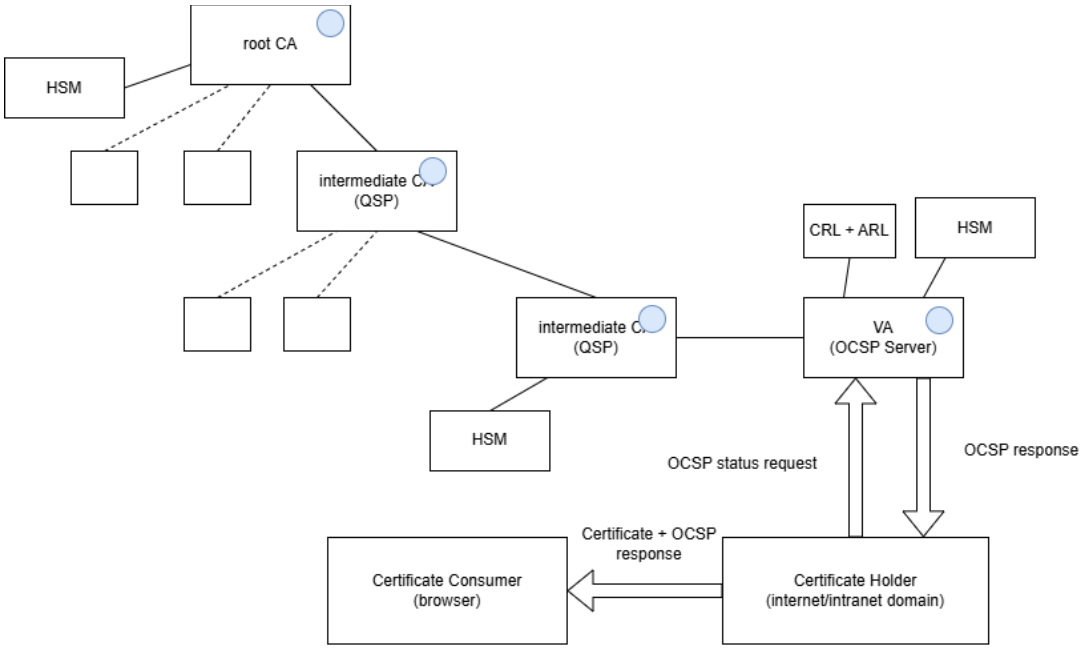


Figure 3: Diagram showing how OCSP stapling works and which PKI authorities are involved. The blue dots represent a dependency on cryptographic hardware and the text in brackets represents an example of the respective component.

With OCSP stapling, the certificate holder has to take a more active role, by proactively communicating with the VA to retrieve OCSP information at regular intervals. This signed OCSP response is valid for a short period of time and can be sent to the certificate consumer at the same time the certificate is sent. The certificate consumer then needs to conduct the normal checks on the certificate and needs to check the validity of the signature on the OCSP response and the expiration date of the signed OCSP response. In essence, the OCSP response is stapled onto the certificate. Since the OCSP responses are short-lived, the probability that the certificate has been revoked in the meantime is fairly low. It seems to have many benefits, but in practice it has seen some challenges. Specifically, OCSP stapling is often not supported and browsers tend to completely ignore revocation checks if OCSP servers are not responding. This can happen when the OCSP server is overloaded or is actively being disrupted .

# 3 Migration Challenges

Using results from previous research and technical and non-technical insights from interviews with PKI experts in all four sectors within the HAPKIDO project's scope, we have distilled the following categories in terms of migration challenges:

1. Software and hardware availability
2. Policy availability
3. Standards availability
4. Externally managed services
5. Hardware limitations
6. Adherence to existing policies
7. Motivation

This is in line with the observation from HAPKIDO deliverable 3.3 and further elaborates on some technical aspects [2].

## 3.1 Software and Hardware Availability

The majority of PKIs in the sectors we have spoken to, use hardware and software from a limited number of vendors. Looking at the figures in chapter 2, all blue dots denote dependency on cryptographic hardware – specifically HSMs. HSM are generally single-purpose hardware that cannot easily be updated to use a different cryptographic scheme. New HSMs need to be built for the newly standardised post-quantum cryptographic primitives. This takes time and can cause delays. Fortunately, there is a variety of vendors who sell HSMs, so PKI practitioners could pivot to a different vendor if their current vendor does not support the necessary schemes yet. However, as shown in [14], different vendors who claim to support the same scheme might actually implement different versions of that scheme, which would break interoperability with the used software for managing and validating keys and signatures.

Additionally, key management is usually done using the EJBCA open source software [15]. Due to the absence of competitive alternatives, there is an implicit vendor lock-in, which means that PKI practitioners will need to wait for new versions of this software before being able to use and manage post-quantum keys.

## 3.2 Policy Availability

For various sectors, there is no specific policy related to post-quantum cryptography, so there is no mandate to use specific schemes or to follow a specific roadmap, even though the European Commission has presented a timeline [16]. Sector-specific policies will be necessary to guide the migration, as many organisation are hesitant to interpret the European policies themselves and risk investing time and money into solutions that are different from the eventual sector-specific policies.

An additional challenge can arise when multiple PKIs are connected by bridge CAs. The new cryptographic policies will need to be coordinated among the policy authorities of the separate PKIs. An example here is the eIDAS regulation [17], which impacts a lot of national PKIs of member states.

## 3.3 Standards Availability

Even though NIST has standardised the required primitives to enable post-quantum cryptography, many PKI-specific protocols have not been updated into a post-quantum or hybrid standard yet. Protocols like OCSP, proof-of-possession protocols for KEMs and hybrid CSRs have not been standardised yet.

## 3.4 Externally Managed Services

In some PKIs, certain services are outsources to external organisations. This can be more efficient or cost-effective, but does introduce a new dependency. The PKI relies on the external organisation to migrate the managed service to post-quantum cryptography.

## 3.5 Hardware Limitations

It is quite evident that HSMs will need to be fully replaced, but they are not the only hardware in use in PKIs. Many organisations also issue smart cards, which need to contain cryptographic information. However, the limited capabilities of smart cards have proven to be an issue for the performance-heavier post-quantum schemes that have been standardised now. There is currently still an on-going on-ramp competition for the standardisation of extra post-quantum signature schemes, that might be more suitable for hardware with limited capabilities, but it is currently unknown when this process will finish.

## 3.6 Adherence to Existing Policies

Currently, there are specific cryptographic policies that have consequences for migration. Specifically, a CA that is higher in the CA hierarchy should always have stronger keys than the CAs below it. This means that the root CA has the strongest keys. Depending on the specific interpretation of these concepts, if a PKI is being replaced, the root CA might have to be replaced first to support the ‘stronger’ post-quantum cryptography. Since post-quantum schemes are younger and less researched, it is possible that new vulnerabilities will be found, so they are not per definition stronger than their classical counterparts.

## 3.7 Incentive

Most organisations take action because policies dictate them to do so. A key factor in the swiftness and accuracy with which policies are implemented are the consequences of noncompliance. In the four sectors within the scope of this report, there is an independent watchdog that can issue fines if noncompliance is established. However, certain sectors are reluctant to issue fines, which could reduce the motivation for organisations in those sectors to take swift action.

# 4 Migration Paths

In this section, we provide some generic insights that are directly relevant for organisation wanting to define a technical migration path for their PKIs. Additionally, for some of the challenges mentioned on the previous section, there are promising solutions that can be used to define migration paths, which we present per challenge.

## 4.1 Generic Insights

### 4.1.1 Carrying Out the Migration

In various sectors, CA migration is not uncommon. Sometimes new generations of CAs are introduced which requires the retirement of existing CAs. For example, PKIOverheid – the PKI of the Dutch government – is retiring their G3 certificates and replacing them with G3+ and G4 certificates [18]. Generally, a parallel PKI is set up that uses a new scheme or different key lengths. New CSRs will only be processed by the new PKI, so if a certificate is renewed or newly generated, it immediately uses the new chain of trust. The old PKI will slowly see fewer and fewer validation requests, because certificates will expire over time and transfer to the new PKI. When all user certificates within the old PKI have expired, the old PKI can be retired and the new PKI will have fully replaced the old one.

A similar situation is posed by the post-quantum migration, which means the same migration strategies can be used. The downside is that two parallel PKIs will need to be managed at the same time, which can give larger overhead and costs. Additionally, users need to be aware of the new root certificate, generally through software/firmware updates. If users have not updated, they will not be able to use the new PKI, so this needs to be orchestrated well. However, such parallel PKIs can only be set up if the other challenges as mentioned in the previous section have been resolved.

### 4.1.2 PQC Support In Software

For specific applications, PQC can only be supported in newer versions. For example, it is not possible to incorporate PQC in TLS 1.2 without altering the standard. Therefore, organisations will need to make sure that the devices in their networks use TLS 1.3, which is a migration of its own. Currently, TLS 1.3 is often supported but not required within company networks. Similarly, OpenSSL version 3.5.0 is the first version to support PQC and clients will need to be updated to version 3.5.0 or higher to be able to use PQC.

## 4.2 Software and Hardware Availability

In terms of hardware availability, it is important to prevent vendor lock-in to stay flexible when other vendors show more suitable timelines for the availability of the required HSMs. There are several aspects to take into consideration when talking to hardware vendors about their post-quantum readiness, such as which version of specific algorithms are supported and which API is supported. For more details, we refer to [19] .

In terms of software availability, the organisation should be aware of the EJBCA roadmap. This is not publicly available, so the EJBCA team will need to be contacted. If this is not adequate, the organisation could coordinate with other organisation to try and contribute to EJBCA, as it is a largely open-source project.

In the meantime, organisations who are willing to proactively prepare for the migration can setup experiments in test environments using open-source implementations of post-quantum algorithms, such as pqc-certificates [20], liboqs [21], the oqs-provider [22] and other initiatives.

## 4.3 Policy Availability

Depending on the type of regulation, either the same or different supervisory bodies have been assigned to the four sectors within the HAPKIDO project's scope. For example, the Dutch Autoriteit Persoonsgegevens (AP) is responsible for the enforcement of laws relating to privacy and personal data, which applies to all sectors. Below is an overview of supervisory bodies that differ per sector that have a role in enforcing regulation related to digital security.

- For the financial sector, De Nederlandsche Bank (DNB) and the Netherlands Authority for the Financial markets (AFM) are supervisory bodies.
- For the Telecommunications sector, the Rijksinspectie Digitale Infrastructuur (RDI) is responsible for the enforcement of telecommunication laws.
- For the healthcare sector, the Inspectie Gezondheidszorg en Jeugd (IGJ) is the supervisory body.
- For the government, no official supervisory body has been assigned to enforce digital security regulation, but there are indications that the RDI will be the supervisory body of the government in the near future [23].

It is recommended for organisations within the sectors to track updates by these supervisory bodies on cryptographic requirements and where possible proactively contact them to obtain timelines for PQC migration.

## 4.4 Standards Availability

To address the unavailability of standards for PKI protocols, several solutions can be identified. There first solution is to use short-lived certificates. If short-lived certificates are an option, the revocation mechanisms as presented in Figure 2 and Figure 3 do not have to

be migrated, which means that there is no need for post-quantum standards for OCSP and OCSP stapling. This will put more pressure on the operational CAs, so it is important that suitable schemes are chosen for the HSMs. Cryptographic agility could be key in this process, since the on-ramp standardisation process by NIST could produce post-quantum signature schemes that increase the performance of the CAs.

Even if short-lived certificates are used, there are still standards that need to be developed, such as hybrid CSRs. If the certificates are used in an application that uses newer communication protocols like kemTLS, proof-of-possession protocols will need to be developed for KEMs enable CSRs. CSRs standards will also need to be extended to support KEM certificates.

If short-lived certificates are not an option, which is the case for certain sectors, or OCSP is mandated for other reasons, then standardisation efforts will need to be intensified to obtain post-quantum and hybrid standards for OCSP and/or OCSP stapling.

## 4.5 Externally Managed Services

Depending on the service, it might be possible to change providers if the external roadmap contains unacceptable delays. This is a type of cryptographic agility related to vendor and service provider management. It requires the organisation to be aware of similar parties that provide the same service and to be in constant dialogue to determine what the best fit is. Similar to cryptographic agility with respect to hardware, it is important to understand what interoperability issues would arise if the organisation would want to switch to a new service provider to understand how challenging it would be to switch.

## 4.6 Hardware Limitations

Currently, it is unclear how performant post-quantum cryptographic, and specifically hybrid cryptography, would be on restricted hardware. There is no immediate solution, but any type of testing facility to understand the implications of new hardware prototypes in realistic PKI environments would greatly benefit our understanding of the impact on PKIs.

## 4.7 Adherence to Existing Policies

The concept of keys of hierarchically higher CAs requiring stronger security can be a topic of debate when it comes to migration, since post-quantum keys are not de facto stronger than classical keys. A resolution can be found in using a conservative approach. Two conservative approaches with respect to post-quantum cryptography are hybrid signatures and hash-based signatures. Since the security of hybrid signatures boils down to the strongest of the classical and post-quantum algorithms used, it is by definition at least as strong as its classical counterpart if the same classical scheme and key length are used in the hybrid signatures. Hash-based signatures are also considered a conservative choice, because the underlying security strength of hash function is well understood, even better than that of classical signatures. It is therefore possible to use hash-based signatures, which as post-quantum signatures, without using the hybrid combination with another classical signature. This makes certificate formats easier as well, as it just requires an extra algorithm to be supported. The downside is that hash-based signatures are very slow to generate, so high

CAs that have to process a high number of CSRs are most likely unsuitable for hash-based signatures. CAs with more downtime, like root CAs, would likely be suitable, since they do not process many CSRs.

## 4.8 Incentive

As emphasised by HAPKIDO deliverable 3.3 [2], incentivising organisations to start the post-quantum migration is a complex challenge. Deliverable 3.3 suggests extrinsic motivators and focuses on governance structures and laws and regulations. We add some intrinsic motivators that could support organisations in kickstarting the migration.
One intrinsic incentive would be to prevent a negative impact on credibility or reputation if it becomes apparent that the organisation will not be able to meet timelines that are set or worse, if they are not ready by the time quantum-capable adversaries appear. In order to understand the actual risk associated with such compromise, organisations should incorporate the quantum threat into their risk assessments methodologies.
Another reason would be to gain a competitive advantage. Frontrunners in post-quantum cryptography migration could more easily attract new customers or gain other types of value.

# 5 Conclusion

Similarly to the research done in deliverable 3.3 [2], we have interviewed PKI practitioners from the four sectors within HAPKIDO's scope and combined the insights from these interviews with the results from previous research to create a structured overview of common PKI services and their dependencies on software and hardware. Compared to the interviews conducted as part of deliverable 3.3, we have taken a more technical approach. As a result of this extended approach we have categorised the identified challenges for PQC migration of PKIs within thee four sectors. Many challenges relate to a dependency on external organisations to provide software, hardware, other services, policies or standards. For hardware dependencies, cryptographic agility can prevent vendor lock-ins and its corresponding risks. The same holds for dependencies on service providers, like managed CAs. Unfortunately, no clear solution is available for the strong dependency on the EJBCA open-source software library within the PKI field. Collaboration is likely the most effective way forward. For standards, organisations can take a proactive stance and contribute to the testing and development of the required standards. For policies, some guidance has been provided by the European Commission with respect to timelines. Sector-specific policies might differ, but it is best to already start the first steps of migration. Other challenges are hardware limitations, key security hierarchies and motivation. For hardware limitations, similarly to standards, the best way forward is to contribute to testing facilities to understand how certain choices affect the PKI landscape. For key security hierarchies, the problem is less severe, because the most likely scenario in practice is that a parallel PKI is set up to enable the migration. Finally, even though extrinsic incentives such as fines are not a suitable means in every sector to kickstart migration, there are arguments that can be used to generate intrinsic motivation within organisations.

# 6 Bibliography


[1] A. Amadori, M. J. H. Marcus and D. Spagnuelo, “HAPKIDO Deliverable D6.1 Overview of Archetype PKI Building Blocks,” HAPKIDO, 2024.

[2] L. C. M. J. N. B. Olivier Rikken, “Quantum Safe Public Key Infrastructure transition – applicability of existing (IT) governance models,” HAPKIDO, 2025.

[3] IETF Network Working Group, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF),* 2005.

[4] T. Güneysu, P. Hodges, G. Land, M. Ounswourth, D. Stebila and G. Zaverucha, “Proof-of-Possession for KEM Certificates using Verifiable Generation,” in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022.

[5] Internet Engineering Task Force, *Simple Certificate Enrolment Protocol,* 2020.

[6] Internet Engineering Task Force, *Enrollment over Secure Transport,* 2013.

[7] Internet Engineering Task Force, *Automatic Certificate Management Environment (ACME),* 2019.

[8] IETF Network Working Group, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* 2008.

[9] Internet Engineering Task Force, *Transport Layer Security (TLS) Extensions: Extension Definitions,* 2011.

[10] Internet Engineering Task Force, *The Transport Layer Security (TLS) Protocol Version 1.3,* 2018.

[11] Internet Security Research Group, “Building a better internet,” 2024.

[12] CA/Browser Forum, “Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates,” Github.com, 2025.

[13] Keyfactor, *What is a Validation Authority?,* 2021.

[14] TNO; Achmea; Dutch Tax Office; ABN Amro; ING, “How to get un-stuck by Architecting for Resilience,” 2025. [Online]. Available: https://pcsi.nl/en/news/how-to-get-un-stuck-by-architecting-for-resilience/.

[15] Keyfactor Inc., “EJBCA® – Open-source public key infrastructure (PKI) and certificate authority (CA) software.,” Github.

[16] NIS Cooperation Group EU PQC Workstream, “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography,” 2025.

[17] European Parliament and Council, “egulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,” *Official Journal of the European Union,* no. L 257, pp. 73-114, 2014.

[18] Logius, “Wees voorbereid, de nieuwe generatie PKIoverheidcertificaten komen eraan!,” [Online]. Available: https://www.logius.nl/onze-dienstverlening/toegang/pkioverheid/wees-voorbereid-de-nieuwe-generatie-pkioverheidcertificaten-komen-eraan. [Accessed 15 08 2025].

[19] PCSI, “Are you and your vendors speaking the same (Post-Quantum) language?,” [Online]. Available: https://pcsi.nl/nl/nieuws/are-you-and-your-vendors-speaking-the-same-post-quantum-language/. [Accessed 3 September 2025].

[20] IETF-Hackathon, “PQC Certificates”.

[21] Open Quantum Safe, “liboqs”.

[22] Open Quantum Safe, “oqs-provider”.

[23] Digitale Overheid, “NIS2-richtlijn,” 20 06 2025. [Online]. Available: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/. [Accessed 15 08 2025].

[24] European Parliament and Council, “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector,” *Official Journal of the European Union,* no. L 333, pp. 1-79, 2022.

[25] Ministerie van Economische Zaken en Klimaat, “Telecommunicatiewet,” *Staatsblad,* 1998.

[26] NCSC, “Cyberbeveiligingswet; Bereid je voor,” [Online]. Available: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn. [Accessed 15 08 2025].

[27] Ministerie van Justitie en Veiligheid, “Samenhangend Inspectiebeeld cybersecurity vitale processen 2024,” 2024.

[28] Ministerie van Volksgezondheid, Welzijn en Sport, “Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg,” *Staatsblad,* no. 253, 2017.

[29] M. M. D. S. Alessandro Amadori, “Overview of Archetype PKI Building Blocks,” HAPKIDO, 2024.

[30] IETF Hackathon, “PQC Certificates”.