Alle nieuws

Are you and your vendors speaking the same (Post-Quantum) language?

3 weeks ago

This blog is written by the participants of the PQC Benchmarking project, from TNO, Achmea, Belastingdienst, ABN Amro and ING. The test case described in this blog was carried out by ING, with aid of Achmea on the vendor strategy.

Our current digital society is being threatened by the advent of large scale quantum computers, urging a post-quantum cryptography (PQC) migration. Migrating your IT systems to quantum-safe cryptography involves not only your own software and cryptographic solutions, but also your supplier's products. In this blogpost, we want to share our experiences on the latter. Learn from our journey of finding PQC-ready Hardware Security Module (HSM) vendors to guide you in talking with your vendors about PQC!

Below is the first response of an email conversation we had just before starting our benchmarking experiment.

> "Dear HSM vendor,
>
> We would like to benchmark the performance of the PQC algorithms on

our PKI infrastructure using HSMs. We are looking for an HSM that implements the standard algorithms and provides the right interfaces for connection to our PKI software.

Does your product support these capabilities?

Best,

Product Owner”

“Dear Product Owner,

Yes, we do support PQC algorithms. We are happy to work together with you!”

While the first response sounds positive, the reality on the readiness/support of the PQC algorithms for the benchmarking turned out to be slightly different. As part of the benchmarking exercise conducted in the first quarter of 2025, we had to reach out to seven HSM vendors to assess their capabilities regarding Post-Quantum Cryptography (PQC) support, before finding one that met our needs.

During the initial discussions, most vendors claimed to be PQC-ready. However, once their technical teams became involved, it became clear that three of the seven vendors only supported early (non-standardized) versions of the algorithms. Additionally, support for certain interfaces, facilitating integration with PKI software, was not a priority for most vendors during the assessment period. That said, most vendors did confirm that broader support for PQC algorithms and related protocols is included in their development roadmaps.

Vendor	Supported Algorithms	Interface	Suitable for PoC	Additional Info
Vendor 1	Dilithium Falcon SPHINCS+	REST API	No	
Vendor 2	ML-DSA-IPD Falcon, SPHINCS+ XMSS, LMS/HSS	PKCS#11	No	
Vendor 3	Dilithium	PKCS#11	No	
Vendor 4	ML-DSA-IPD ML-DSA LMS	REST API	Yes, due to specific support.	Not on dedicated hardware appliances.
Vendor 5	ML-DSA SLH-DSA XMSS, LMS/HSS	REST API PKCS#11 - unclear	Unclear	
Vendor 6	ML-DSA SLH-DSA XMSS/XMSS-MT LMS/HSS	PKCS#11 REST API	Yes	Not used due to config issues
Vendor 7	ML-DSA	PKCS#11	No	Uses SoftHSM emulator

The table shows the situation in February-March 2025. For an overview of current vendor offerings, we recommend reviewing the PKI Consortium's PQC Capabilities Matrix, which provides up-to-date information on the state of Post-Quantum Cryptography support.

In the following, we share guidelines to help you assess your vendor's capabilities based on insights we gained from our own experience.

Categorize Vendors Based on Risk Profile

Not all vendors present the same level of risk when it comes to PQC readiness. It is therefore smart to categorize your vendors based on a risk profile that considers the sensitivity of the data they process on your behalf and your organization's dependency on them for the implementation of cryptographic functions.

This classification enables a more tailored and risk-based approach to vendor engagement. For vendors identified as high-risk, you may need to request more detailed information about their cryptographic services, migration plans, and timelines. You may also choose to define stricter requirements and expect earlier or more rigorous alignment with your own PQC roadmap.

Taking a structured, risk-based approach to supplier oversight ensures that attention and resources are prioritized where the potential impact is greatest. In our case, we chose experimenting with PKI using HSMs because it is one of the pillars of our IT ecosystem – one that we need to prioritize in our migration efforts.

Timely and proactive alignment is important

One key observation of our benchmarking experience is that vendors generally demonstrate strong support and a willingness to assist in achieving PQC objectives. We think that this is also new territory for them, and they are interested

in how customers are experiencing it. This means that there is a window of opportunity to collaborate and experiment, which is especially valuable with the approaching deadlines.

If your organization is classified as an early or urgent adopter of PQC migration, which can be identified using the PQC handbook, it is imperative that your vendors adopt a similar sense of urgency. Maintaining continuous and proactive alignment with your vendors—particularly in relation to your cryptographic roadmap—is therefore strategic. Ensure they are fully aware of the risks associated with delaying migration, such as the threat posed by harvest-now- decrypt-later attacks and the risk of non-compliance with evolving regulatory frameworks.

For example, under the NIS2 Directive, organizations are required to implement state-of-the-art encryption, which increasingly includes preparations for quantum-resilient encryption.

Involve the Right Stakeholders Early

Migrating to PQC algorithms represents a significant transition both for your organisation and your vendors. A well-defined roadmap for supplier engagement is key in managing this process effectively.

In the selection of the right vendors for a successful PQC migration, involve the appropriate internal stakeholders early in the process. This process extends beyond procurement or vendor management functions alone —it must also include your cyber security and cryptography experts. Their timely participation enables a deeper understanding of the technical implications of what vendors are offering and helps ensure well-informed decision-making. The procurement process often focuses on high-level questions such as “Do you provide quantum-resistant solutions?”. However, to truly determine whether a solution fits to your needs, you need to ask technical questions and know how to interpret the answers. You can either train vendor management to grasp the technical details or have them work closely with the technical security experts to conduct the assessment together. For us, the latter option is the way to go.

Similarly, encourage your vendors to involve their technical specialists in discussions from the outset to facilitate clear and accurate dialogue. This alignment is vital for avoiding misunderstandings and ensuring both parties remain on the same page throughout the process.

> ***Tip:*** *Support your vendor management team in asking the right questions by letting the security professionals provide the necessary technical detail and evaluate them together on real vendor cases. Also, include vendor management in PQC awareness training and projects.*

Prepare Your PQC Questionnaire

A key insight from our benchmarking project is that asking the right questions can significantly enhance the efficiency and quality of vendor interactions. It helps clarify your organization's priorities, manage expectations, and reduce the time spent on iterative discussions. A well-structured PQC questionnaire can serve as a powerful tool to assess vendor readiness and steer meaningful conversations.

> ***Tip:*** *The Dutch government already provide examples you can share with vendors. Adapt these to your requirements in consultation with your cryptographic experts: Which algorithms are in your cryptographic policy? Which protocols/interfaces do you need?*

The link to the examples can be found here.

Tailor the Questionnaire to Vendor Type

Differentiate your approach depending on whether you are assessing **new vendors** or **existing vendors** and adjust the level of detail based on the risk profile of each vendor.

New Vendors

When onboarding new vendors, cryptographic capabilities should form part of your due diligence and vendor selection process and be explicitly addressed in contract clauses. Use the PQC questionnaire as an integral part of your risk assessment, particularly where higher risk profiles are identified.

For vendors operating in high-risk categories, consider including more in-depth questions regarding cryptographic implementation and migration planning.

Existing Vendors

For current vendors, the PQC questionnaire should be introduced through existing governance structures—such as during periodic performance reviews or strategic alignment meetings—as part of an open and transparent dialogue.

Larger vendors are likely already aware of quantum threats and may have a PQC strategy in place. However, smaller suppliers may not yet be familiar with the implications of quantum computing. In such cases, take the initiative to raise awareness and support them in understanding your expectations and the emerging threat landscape.

You can start with a brief introduction on the risks that your organization is facing, why and when you need to migrate to PQC. Afterwards consider including the following topics depending on the risk profile you identified:

- The compliance of the vendor with legislations and standards that are applicable to you
- Whether they have a roadmap and strategy in place for PQC,
- How their organization monitors developments on the cryptography standards,
- Their posture on cryptographic agility,
- Where they can provide a Cryptographic Bill of Material (CBOM),
- Whether they have assessed the PQC readiness of their supply chain,
- Which cryptographic algorithms are currently in use in their products and services and what algorithms you expect them to support.

Key take-aways

PQC is urgent and requires collaboration with vendors

- Organizations that are working on their cryptographic inventory should also assess the PQC readiness of their suppliers.
- Organizations that want to migrate urgently to PQC must involve their vendors now.
- Legislation such as NIS2 requires the use of state-of-the-art encryption.
- Vendors often claim to support PQC, but in practice, this might be limited or based on pre-standard algorithms.

Experimenting helps to gain experience: this project shows significant differences between HSM suppliers.

- Seven HSM suppliers were approached; only a few offered usable support for a Proof of Concept.
- Interfaces such as PKCS#11 or REST API are not always available or usable.
- Many vendors have PQC on their roadmap, but are not yet fully ready.

Involve the right internal departments

- Not only procurement but also cyber security experts must be involved from the beginning. Collaborate and educate together!
- Let vendors involve their technical experts in discussions.

Create a PQC questionnaire

A good questionnaire helps to get to the core faster. Create it in collaboration with your security experts.

- Define your own PQC requirements and communicate those.

- Adapt the questions to new vs. existing vendors.
- Use risk profiles to determine the depth of discussions and requirements.

Proactive alignment with vendors is crucial

- Continuous consultation helps manage expectations and migrate in a timely manner.

Include PQC in new and existing contracts now!

This prevents a lot of alignment later and speeds up adoption.

Check out the other blogs in this series as well! In this series of four we share both organizational and technical results, from four different perspectives: Management, Developers, IT Architects and Vendors.

Alleen door samenwerking kunnen we de beste resultaten behalen in de strijd tegen cybercriminaliteit