Alle nieuws

# Spreken jij en je leveranciers dezelfde (Post-Quantum) taal?

3 months ago

*Deze blog is geschreven door de deelnemers van het PQC Benchmarking-project: TNO, Achmea, Belastingdienst, ABN Amro en ING. De testcase uit deze blog is uitgevoerd door ING, met hulp van Achmea op het gebied van leveranciersstrategie.*

Als quantumcomputers straks krachtig genoeg zijn, loopt onze huidige digitale samenleving groot gevaar. Als gevolg hiervan moeten we onze digitale systemen migreren naar post-quantum cryptografie (PQC). Naast je eigen software en cryptografische oplossingen zul je ook moeten kijken naar producten van je leveranciers als je je IT systemen wil migreren. In deze blogpost delen we onze ervaringen met leveranciers, dus pak deze kans om van onze zoektocht naar post-quantum Hardware Security Modules (HSMs) te leren zodat ook jij het gesprek aan kunt gaan met je leveranciers over PQC!

Vlak voordat we zijn begonnen met ons benchmarkingexperiment, hebben we een e-

mailuitwisseling gehad met een HSM leverancier. Hieronder is deze uitwisseling te lezen.


*"Beste HSM-leverancier,*

*We willen de prestaties van PQC-algoritmes benchmarken op onze PKI-infrastructuur met behulp van HSMs. We zoeken een HSM die de gestandaardiseerde algoritmes implementeert en de juiste interfaces biedt voor aansluiting op onze PKI-software.*

*Ondersteunt uw product deze mogelijkheden?*

*Met vriendelijke groet,*

*Product Owner"*

*"Beste Product Owner,*

*Ja, wij ondersteunen PQC-algoritmen.*
*We werken graag met u samen!"*

Hoewel de eerste reactie positief klonk, bleek later dat er veel meer nuance achter deze vraag zat dan we initieel dachten, waardoor het antwoord niet zo simpel was als een ja of een nee. Als onderdeel van het benchmarkingtraject in het eerste kwartaal van 2025 hebben we contact op moeten nemen met maar liefst **zeven** HSM-leveranciers, voordat we er één konden vinden die aan de behoeften voldeed op het gebied van Post-Quantum Cryptografie (PQC).

Tijdens de eerste gesprekken gaven de meeste leveranciers aan dat ze PQC-gereed waren, maar zodra hun technische teams betrokken raakten, werd duidelijk dat **drie van de zeven leveranciers alleen vroege (niet-gestandaardiseerde) versies van de algoritmen ondersteunden**. Bovendien was ondersteuning voor bepaalde interfaces die integratie met PKI-software makkelijker maken geen prioriteit voor de meeste leveranciers tijdens de beoordelingsperiode. Wel bevestigden de meeste leveranciers dat bredere ondersteuning voor PQC-algoritmen en gerelateerde protocollen op hun ontwikkelingsplanning staat.

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

In de tabel hierboven is de situatie te zien medio februari-maart 2025. Voor een overzicht van de huidige leveranciersaanbiedingen kun je ook de PQC Capabilities Matrix, van het PKI Consortium raadplegen, die actuele informatie bevat over de status van Post-Quantum Cryptografie-ondersteuning.

Om beter de capaciteiten van je leveranciers te kunnen beoordelen, hebben we hieronder wat richtlijnen opgesteld die daarbij kunnen helpen die gebaseerd zijn op onze eigen ervaring.

## Categoriseer leveranciers op basis van risicoprofiel

Niet alle leveranciers vormen hetzelfde risico als het gaat om PQC-gereedheid. Het is daarom verstandig om je leveranciers te categoriseren op basis van een risicoprofiel. Hierbij moet je rekening houden met de gevoeligheid van de gegevens die zij namens jou verwerken en de afhankelijkheid van jouw organisatie van hun cryptografische functies.

Middels deze classificatie kun je leveranciers op een meer gerichte en risicogebaseerde manier benaderen. Voor leveranciers met een hoog risico kun je meer gedetailleerde informatie vragen over hun cryptografische diensten, migratieplannen en tijdlijnen. Je kunt ook strengere eisen stellen, bijvoorbeeld door te stellen dat de PQC tijdlijnen vroegtijdig op elkaar afgestemd moeten worden.

Een gestructureerde, risicogebaseerde aanpak van leveranciersbeheer zorgt ervoor dat aandacht en middelen worden gericht op de systemen waar de impact het grootst is. In ons geval kozen we ervoor om te experimenteren met PKI en HSMs omdat dit een van de meest kritieke componenten is van ons IT-ecosysteem – een die we moeten prioriteren in onze migratie-inspanningen.

## Tijdige en proactieve afstemming is belangrijk

Een belangrijke observatie uit onze benchmarkingervaring is dat leveranciers over het algemeen bereid zijn om te ondersteunen zodat de PQC doelstellingen behaald kunnen worden. We denken dat dit ook nieuw terrein voor is voor de levernaciers en dat ze daarom geïnteresseerd zijn de ervaring van hun klanten. Dit biedt een kans om samen te werken en te experimenteren, wat erg waardevol is vanwege de naderende deadlines.

Als jouw organisatie wordt geclassificeerd als een vroege of urgente adopter van PQC-migratie volgens het PQC-handboek, dan is het van groot belang dat je leveranciers een vergelijkbare urgentie hanteren. Van strategisch oogpunt is het daarom raadzaam om proactief en regelmatig hierover af te stemmen met je leveranciers, vooral met betrekking tot je cryptografische roadmap. Zorg ervoor dat ze zich volledig bewust zijn van de risico's van uitstel, zoals de dreiging van

harvest-now-decrypt-later-aanvallen en het risico als de veranderende regelgeving niet wordt nageleefd.

Onder de NIS2-richtlijn zijn organisaties bijvoorbeeld verplicht om state-of-the-art encryptie te implementeren, waar steeds vaker post-quantum cryptografie onder wordt geschaard.

## Betrek de juiste stakeholders vroegtijdig

Migratie naar PQC-algoritmen is een aanzienlijke transitie, zowel voor je organisatie als voor je leveranciers. Een goed gedefinieerde roadmap om de betrokkenheid van leveranciers te plannen, is essentieel om het proces zo efficiënt mogelijk te maken.

Bij de selectie van de juiste leveranciers voor een succesvolle PQC-migratie is het belangrijk om de juiste **interne stakeholders** al vroeg in het proces te betrekken. Dit proces omvat meer dan alleen inkoop of leveranciersbeheer – je moet ook je cybersecurity- en cryptografie-experts betrekken. Als deze al vroegtijdig betrokken zijn, dan kun je beter beoordelen wat je leveranciers precies aanbieden en wat de gevolgen zouden zijn voor je systeem. Hierdoor kun je beter geïnformeerde beslissingen maken. Het inkoopproces richt zich vaak op algemene vragen zoals “Biedt u quantum-resistente oplossingen aan?”, maar om echt te bepalen of een oplossing bij je behoeftes past, moet je technische vragen stellen en weten hoe je de antwoorden moet interpreteren. Je kunt leveranciersbeheerders trainen om de technische details te begrijpen of hen laten samenwerken met technische beveiligingsexperts om de beoordeling gezamenlijk uit te voeren. Voor ons bood de samenwerking met beveiligingsexperts de beste oplossing.

We weten nu hoe belangrijk het is om je eigen experts te betrekken. Spoor daarnaast ook je leveranciers aan om hun eigen technische specialisten vanaf het begin bij de

gesprekken te betrekken zodat er duidelijk en nauwkeurig gecommuniceerd kan worden. Deze afstemming is essentieel om misverstanden te voorkomen en ervoor te zorgen dat beide partijen gedurende het hele proces op één lijn blijven.

**Tip:** *Ondersteun je leveranciersmanagers door beveiligingsprofessionals de benodigde technische details aan te laten leveren, zodat zij de juiste vragen kunnen stellen. Deze kunnen zij samen evalueren aan de hand van echte leverancierscasussen. Neem daarnaast leveranciersbeheer ook mee in PQC-bewustwordingstrainingen en -projecten.*

***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.*

## Bereid je PQC-vragenlijst voor

Een belangrijke les uit ons benchmarkingproject is dat het stellen van de juiste vragen gesprekken met leveranciers aanzienlijk efficiënter kunnen maken en de kwaliteit daarvan kunnen verhogen. Het helpt om de prioriteiten van je organisatie te verduidelijken en je verwachtingen duidelijk te maken en waar nodig bij te stellen, zodat je minder tijd kwijt bent aan discussies. Een goed gestructureerde PQC-vragenlijst kan dienen als een krachtig hulpmiddel om de gereedheid van leveranciers te beoordelen en efficiënte gesprekken te voeren.

***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?*

**Tip:** *De Nederlandse overheid biedt al voorbeelden die je kunt delen met leveranciers. Pas deze aan op jouw eisen in overleg met je cryptografie-experts: Welke algoritmen zijn opgenomen in jouw cryptografiebeleid? Welke protocollen/interfaces heb je nodig?*

De link naar deze voorbeelden kun je hier vinden.

### *Pas de vragenlijst aan op het type leverancier*

In je beoordeling is het handig om afhankelijk van de relatie met de leverancier – is deze nieuw of een bestaande relatie? – onderscheid te maken in je aanpak. Je kunt het detailniveau ook aanpassen op basis van het risicoprofiel van de leverancier.

#### Nieuwe leveranciers

Bij het onboarden van nieuwe leveranciers moeten cryptografische capaciteiten deel uitmaken van je 'due diligence' en selectieproces voor leveranciers en moeten ze expliciet worden opgenomen in contractclausules. Gebruik de PQC-vragenlijst als integraal onderdeel van je risicobeoordeling, vooral bij leveranciers met een hoger risicoprofiel.

Voor leveranciers in hoogrisicocategorieën kun je meer diepgaande vragen stellen over cryptografische implementatie en migratieplanning.

#### Bestaande leveranciers

Voor huidige leveranciers moet de PQC-vragenlijst worden geïntroduceerd via bestaande governance-structuren – zoals tijdens periodieke prestatiebeoordelingen of strategische afstemmingsvergaderingen – als onderdeel van een open en transparante dialoog.

Grote leveranciers zijn waarschijnlijk al op de hoogte van quantumdreigingen en hebben mogelijk een PQC-strategie. Kleinere leveranciers zijn mogelijk nog niet bekend met de gevolgen van grootschalige quantumcomputers. In zulke gevallen kun je het initiatief nemen om bewustwording te creëren en hen te helpen om je verwachtingen en het opkomende dreigingslandschap te begrijpen.

Je kunt beginnen met een korte introductie over de risico's die jouw organisatie loopt en waarom en wanneer je moet migreren naar PQC. Overweeg daarna om de volgende onderwerpen op te nemen, afhankelijk van het risicoprofiel dat je hebt vastgesteld:

- De naleving door de leverancier van wetgeving en normen die op jouw organisatie van toepassing zijn,
- Of ze een roadmap en strategie hebben voor PQC,
- Hoe hun organisatie ontwikkelingen op cryptografische standaarden bijhoudt,
- Hun houding ten opzichte van cryptografische wendbaarheid,
- Of ze een Cryptographic Bill of Material (CBOM) kunnen leveren,
- Of ze de PQC-gereedheid van hun eigen toeleveringsketen hebben beoordeeld,
- Welke cryptografische algoritmes momenteel worden gebruikt in hun producten en diensten en voor welke algoritmes jij ondersteuning zou willen.

## Belangrijkste inzichten

**PQC is urgent en vereist samenwerking met leveranciers**

- Organisaties die werken aan hun cryptografische inventaris moeten ook de PQC-gereedheid van hun leveranciers beoordelen.
- Organisaties die dringend willen migreren naar PQC moeten direct hun leveranciers betrekken.
- Wetgeving zoals NIS2 vereist het gebruik van state-of-the-art encryptie.
- Leveranciers beweren vaak PQC te ondersteunen, maar in de praktijk is dit mogelijk beperkt of gebaseerd op niet-gestandaardiseerde versies van algoritmes.

**Experimenteren helpt om ervaring op te doen: dit project brengt significante verschillen tussen HSM-leveranciers aan het licht**

- Zeven HSM-leveranciers zijn benaderd; slechts enkelen boden bruikbare ondersteuning voor een Proof of Concept.
- Interfaces zoals PKCS#11 of REST API zijn niet altijd beschikbaar of bruikbaar.
- Veel leveranciers hebben PQC op hun roadmap, maar zijn nog niet volledig gereed.

**Betrek de juiste interne afdelingen**

- Niet alleen inkoop, maar ook cybersecurity-experts moeten vanaf het begin betrokken zijn. Werk samen en leer van elkaar!
- Laat leveranciers ook hun technische experts betrekken bij gesprekken.

**Stel een PQC-vragenlijst op**

Een goede vragenlijst helpt om sneller tot de kern te komen. Stel deze op in samenwerking met je beveiligingsexperts.

- Definieer je eigen PQC-eisen en communiceer deze.

- Pas de vragen aan op nieuwe versus bestaande leveranciers.
- Gebruik risicoprofielen om de benodigde diepgang van gesprekken en eisen te bepalen.

**Proactieve afstemming met leveranciers is cruciaal**

- Continue afstemming helpt om verwachtingen te beheren en tijdig te migreren.

**Neem PQC nu op in nieuwe en bestaande contracten!**

- Dit voorkomt veel afstemming achteraf en versnelt de adoptie

*Bekijk ook de andere blogs in deze serie! In deze serie van vier delen delen we zowel organisatorische als technische resultaten, vanuit vier verschillende perspectieven: Management, Developers, IT Architecten en Vendoren.*

*De eerste afbeelding is gemaakt met behulp van Copilot.*



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