AIVD | CWI | TNO

Het PQC-migratie handboek

RICHTLIJNEN VOOR HET MIGREREN NAAR POST-QUANTUMCRYPTOGRAFIE

Herziene en uitgebreide tweede editie

December 2024

AIVD | CWI | TNO

Het PQC-migratie handboek

RICHTLIJNEN VOOR HET MIGREREREN NAAR POST-QUANTUMCRYPTOGRAFIE

Herziene en uitgebreide tweede editie

December 2024

De betrokken partijen hebben de grootste zorg en expertise betracht bij het opstellen van dit handboek. Het doel van deze publicatie is het creëren van bewustzijn rond de urgentie van de migratie naar post-quantumcryptografie, alsmede het vergroten van de kennis van cryptografie als integraal onderdeel van cybersecurity. De praktische toepassing van dit handboek is sterk afhankelijk van het type organisatie en de specifieke risico's per organisatie. Het bevat daarom geen standaardbenadering voor alle organisaties en moet mogelijk met begeleiding en advies worden aangevuld.

Aan deze publicatie kunnen dan ook geen rechten worden ontleend en vermelde adviezen kunnen na publicatie van dit handboek verouderd blijken te zijn. AIVD, CWI en TNO zijn in géén geval aansprakelijk voor eventuele gevolgen van de in deze publicatie vermelde adviezen.

Dit document is oorspronkelijk geschreven in het Engels en vertaald met behulp van Microsoft Copilot.

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Auteurs Alessandro Amadori, Thomas Attema, Maxime Bombar, João Diogo Duarte, Vincent Dunning, Simona Etinski, Daniël van Gent, Matthieu Lequesne, Ward van der Schoot, Marc Stevens en cryptologen en adviseurs van de AIVD

Ontwerp C10 Ontwerp

Contact thomas.attema@tno.nl

Samenvatting

Dit handboek biedt organisaties concreet handelingsperspectief en advies om de dreiging van quantumcomputers voor de huidige cryptografie te mitigeren. Het is een uitbreiding van het handboek dat in maart 2023 is gepubliceerd, met zowel een herziene inhoud op basis van recente ontwikkelingen als nieuw materiaal.
Het is onmogelijk te voorspellen wanneer quantumcomputers in staat zullen zijn om de momenteel gebruikte cryptografische systemen in gevaar te brengen. De potentiële impact is echter dusdanig groot dat bepaalde organisaties nu al moeten beginnen met het implementeren van mitigerende maatregelen. Dit geldt bijvoorbeeld voor organisaties die gegevens verwerken die de komende decennia vertrouwelijk moeten blijven en voor organisaties die systemen ontwikkelen die nog decennia in gebruik zullen zijn.
De meest veelzijdige en volledige oplossing wordt *post-quantumcryptografie* (PQC) genoemd. PQC kan worden ingezet op de momenteel gebruikte systemen en computers en biedt beveiliging tegen aanvallen door quantumcomputers. Een andere veelgeprezen, gedeeltelijke oplossing heet *quantum key distribution* (QKD). Veel veiligheidsinstanties bevelen momenteel echter alleen PQC als maatregel aan, vanwege de inherente beperkingen van QKD en bepaalde praktische en veiligheidstechnische zorgen en overwegingen.
De migratie van quantumkwetsbare cryptografie naar PQC wordt een tijdrovend en kostbaar proces. Naar schatting op basis van eerdere migraties kan het meer dan vijf jaar duren. In augustus 2024 werden de eerste PQC-standaarden gepubliceerd door het Amerikaanse National Institute of Standards and Technology (NIST), waarmee de volgende fase in de PQC-migratie aanbrak. Verschillende organisaties zijn al begonnen met de PQC-migratie en autoriteiten en toezichthouders over de hele wereld werken aan PQC-gerelateerde wetgeving en de implementatie daarvan. Dankzij deze PQC-standaarden kunnen nu meer organisaties beginnen met hun PQC-migratie.
Dit handboek volgt een driestappenplan om de quantumdreiging te mitigeren: (1) *diagnose van quantumkwetsbaarheid*, (2) *planning* en (3) *uitvoering*.
De eerste stap, de diagnose van quantumkwetsbaarheid, bevat een aantal "no-regret"-maatregelen die de cyberweerbaarheid van een organisatie vergroten, zelfs los van de quantumdreiging. Met deze maatregelen kunnen organisaties hun cryptografie effectiever beheren en cryptografische veranderingen soepeler doorvoeren. Goed cryptografisch beheer vergemakkelijkt namelijk het identificeren en oplossen van risico's en verkort de reactietijd in het geval van een incident, ook als dit incident niet gerelateerd is aan quantumcomputers.
In concrete is zin het advies aan alle organisaties om te beginnen met een zogenaamde cryptografische inventarisatie, om tot een overzicht te komen van welke cryptografie er allemaal gebruikt wordt. Ten tweede dienen organisaties een risicobeoordeling voor de quantumdreiging uit te voeren en deze te integreren in hun bestaande risicobeheerprocedures. Ten slotte moet elke organisatie haar beleid omtrent cryptografie herzien en bijwerken op basis van de veranderende wet- en regelgeving. Deze informatie zal inzicht geven in de houding die een organisatie moet aannemen ten opzichte van de PQC-migratie. Daarnaast wordt met de beschikbaarheid van deze informatie ook het risico op een overhaaste, foutgevoelige migratie verkleind, wat onnodige kosten en risico's in de toekomst kan voorkomen.
Tijdens de planningsfase is het belangrijk om een speciaal, toegewijd team te vormen dat de migratie overziet en ervoor zorgt dat alle nodige bedrijfsprocessen voor een soepele overgang voorhanden zijn. Dit handboek besteedt extra aandacht aan zogenaamde *urgente adopters*: organisaties die zo snel mogelijk met de PQC-migratie moeten beginnen, omdat de impact van een inbreuk op de cryptografie ergens in de komende decennia onaanvaardbaar zou zijn. Daarnaast biedt dit handboek hulpmiddelen om de gereedheid en volwassenheid van een organisatie voor een PQC-migratie te beoordelen.
Op technisch vlak moeten er bij de ingebruikname van PQC verschillende keuzes worden gemaakt. Niet alle vormen van PQC zijn bijvoorbeeld geschikt voor elke toepassing. Dit handboek biedt concreet advies voor het definiëren van een strategie voor de implementatie van PQC, waarbij rekening wordt gehouden met verschil-

lende toepassingsscenario's. De ingebruikname van PQC kan mogelijk nieuwe eisen aan hardware stellen of vereisen dat er gewisseld wordt naar een leverancier die de relevante vorm van PQC ondersteunt.
De laatste fase van de PQC-migratie is de uitvoering. Tijdens deze fase is het zaak zeer voorzichtig te werk te gaan om geen nieuwe kwetsbaarheden te introduceren. Dit handboek biedt richtlijnen over hoe de migratie kan worden uitgevoerd voor verschillende soorten cryptografie en met de verschillende strategieën die tijdens de planningsfase zijn ontwikkeld. Cryptografie zal in de toekomst blijven veranderen: zo kunnen er bijvoorbeeld nieuwe algoritmes of kwetsbaarheden worden ontdekt, of kunnen verbeteringen in cryptanalyse langere cryptografische sleutels noodzakelijk maken. Daarom is het belangrijk om te werken aan *cryptographic agility* ('cryptografische wendbaarheid'). Een organisatie die *crypto-agile* is, kan snel cryptografische primitieven wijzigen of vervangen zonder organisatorische processen te verstoren. Dit is vooral belangrijk wanneer verbeteringen in cryptografische protocollen of nieuwe kwetsbaarheden worden gevonden. Dit handboek geeft inzicht in hoe crypto-agility in bestaande verandermanagementprocessen kan worden geïntegreerd.

Dankbetuigingen

We willen Ronald Cramer (CWI & Universiteit Leiden) en Maran van Heesch (TNO) bedanken voor hun bijdragen aan de totstandkoming en afbakening van dit handboek. Verder willen we onze dank betuigen aan de vele mensen die hebben bijgedragen aan het herzien en uitbreiden van het PQC-migratiehandboek tot deze tweede editie. De volgende personen willen we in het bijzonder bedanken: Melissa Azouaoui (NXP Semiconductors), Itan Barmes (Deloitte), Nitesh Bharosa (TU Delft), Joppe W. Bos (NXP Semiconductors), Christine Cloostermans (NXP Semiconductors), Oscar Covers (Nederlandse Vereniging van Banken), Gareth T. Davies (NXP Semiconductors), Sander Dorigo (Fox Crypto), Barış Ege (Keysight Technologies), Marie Beth van Egmond (TNO), Dimitri van Esch (Quantum Gateway Foundation), Erik Holkers (DICTU), Andreas Hülsing (TU Eindhoven), Marijn Janssen (TU Delft), Frederik Kerling (TNO), Silke Knossen (KPN), Dion Koeze (NCSC-NL), Ini Kong (TU Delft), Maaike van Leuken (TNO), Anne Nijsten (TNO), Durga Lakshmi Ramachandran (Keysight Technologies), Harld Röling (ABN Amro), Simona Samardjiska (Radboud Universiteit), Tobias Schaap (Auditdienst Rijk), Colin Schappin (Deloitte), Pieter Schneider (MinBZK), Peter Schwabe (Max Planck Institute for Security and Privacy & Radboud Universiteit), Robert Seepers (NCSC-NL), Thom Sijpesteijn (TNO), André Smulders (MinOCW), Thijs Timmerman (KPMG), Daan van der Valk (Deloitte), Marc van Vliet (TNO), Manon de Vries (TNO), Anita Wehmann (MinBZK), Bas Westerbaan (Cloudflare) en Daniël Worm (TNO). Ten slotte willen we de bijdragen aan de eerste editie van dit handboek erkennen: we bedanken Shane Gibbons (CWI & Universiteit Leiden), Loulou Hanna (MinlenW), Larissa Kalle (NCSC-NL), Oscar Koeroo (MinVWS), Daan Planqué (Ericsson), Eamonn W. Postlethwaite (King's College London), Sterre Romkema (MinlenW) en Germain van der Velden (MinlenW).

Dit handboek is gefinancierd door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Inhoud

1 Inleiding

Dit handboek[1] is bedoeld om organisaties te ondersteunen bij het identificeren van de risico's die quantumcomputers vormen voor hun IT-infrastructuren en om concrete strategieën te bieden om deze risico's te mitigeren. Hoewel verschillende eerdere publicaties deze risico's en de urgentie van het implementeren van passende maatregelen al hebben benadrukt, bouwt dit handboek voort op die aanbevelingen door concrete, uitvoerbare richtlijnen te geven. Deze handleiding is met name gericht op organisaties die zich geen uitstel kunnen veroorloven. Zulke partijen worden vaak aangeduid als *urgente adopters*. Aangezien echter vrijwel elke organisatie afhankelijk is van cryptografie, zijn ze allemaal kwetsbaar voor de potentiële bedreiging die quantumcomputers vormen.

Cryptografie is van groot belang in de hedendaagse digitale samenleving en vormt een integraal onderdeel van de cybersecurity van elke organisatie. Sterke cryptografie is essentieel om diefstal van gevoelige of vertrouwelijke gegevens te voorkomen, de integriteit en authenticiteit van gegevens te waarborgen en ongeautoriseerde toegang tot systemen te voorkomen. Zwakke cryptografie vormt daarentegen een onaanvaardbaar risico en kan leiden tot datalekken, ongeautoriseerde toegang, diefstal van bedrijfs- of staatsgeheimen en zelfs ernstigere gevolgen.

Een aanzienlijk deel van de momenteel gebruikte cryptografie wordt verzwakt of zelfs volledig onveilig gemaakt door de aanstaande komst van quantumcomputers. Op dit moment zijn quantumcomputers nog niet krachtig genoeg om cryptografische systemen te breken, maar ze worden steeds verder ontwikkeld. Met enig speculeren verwacht men dat quantumcomputers binnen tien tot twintig jaar in staat zullen zijn om een deel van de veelvoorkomende hedendaagse cryptografie te breken. Cryptografie die veilig is tegen klassieke computers, maar niet tegen quantumcomputers, wordt quantumkwetsbaar genoemd. Cryptografie die ook veilig is tegen quantumaanvallen staat bekend als post-quantumcryptografie (PQC).

Cryptografisch relevante quantumcomputers zijn momenteel nog geen realiteit, maar toch zijn er voor organisaties verschillende dwingende redenen om nu al te beginnen met het aanpakken van de quantumdreiging door de migratie naar PQC te beginnen:

1. ***Store-Now-Decrypt-Later*-aanvallen** | Gevoelige informatie loopt het risico om nu te worden onderschept en opgeslagen en in de toekomst met een quantumcomputer te worden ontsleuteld. Gegevens die een lange periode beschermd moeten blijven lopen daarom nu al het risico om te worden ontsleuteld voordat de beoogde vertrouwelijkheidsperiode is verstreken.

2. **Systemen met een lange levensduur** | Het kan moeilijk of zelfs onmogelijk zijn om systemen met een lange levensduur en vitale infrastructuur na ingebruikname nog bij te werken zodat ze PQC ondersteunen. Zelfs als software-updates mogelijk zijn, kan het zijn dat PQC geavanceerdere hardware vereist die misschien niet meer in te voegen is als het systeem al is ingezet.

3. **Complexiteit van een cryptografische migratie** | Het bijwerken of vervangen van een cryptografische infrastructuur met post-quantum alternatieven is een complexe en tijdrovende taak. Op basis van eerdere migraties wordt verwacht dat een volledige migratie naar PQC vele jaren kan duren. Zo duurde het bijvoorbeeld voor veel organisaties meer dan vijf jaar om te migreren van de kwetsbare SHA-1 naar de veilige opvolger SHA-256, zelfs nadat de benodigde specificaties en implementaties beschikbaar waren.

[1] In 2023 verscheen er een eerdere versie van dit handboek. Deze nieuwe editie is bijgewerkt en uitgebreid op basis van nieuwe inzichten en recente ontwikkelingen. Daarnaast is er nieuw materiaal toegevoegd om de aanbevolen acties en perspectieven nader toe te lichten. Sectie 1.3.1 geeft een gedetailleerd overzicht van de wijzigingen ten opzichte van de versie uit 2023.

4. **State-of-the-Art** | PQC wordt steeds meer beschouwd als de *state-of-the-art (*het hoogste niveau van ontwikkeling*)* binnen de cryptografie en zowel publieke als private organisaties zijn al begonnen met PQC-migratie. Het is essentieel om PQC op tijd te implementeren om interoperabel met deze instanties te blijven en up-to-date te blijven met maatregelen rondom cybersecurity.

5. **No-regrets** | Veel van de stappen in de PQC-migratie kunnen worden beschouwd als zogenaamde *no-regret moves*: deze acties zijn nuttig ongeacht de ontwikkelingen in quantumcomputing. Zo verbetert goed cryptografisch beheer ook de efficiëntie van het afhandelen van andere cryptografische incidenten, zoals het detecteren en vervangen van gecompromitteerde sleutels.

Gelukkig is de PQC-migratie al bezig. Enkele koplopers zijn al begonnen met het implementeren van PQC in hun IT-infrastructuur en regelgevende instanties over de hele wereld bereiden PQC-gerelateerde wetgeving voor of publiceren deze zelf al. Bovendien markeert de recente publicatie van de eerste PQC-standaarden door NIST een nieuwe fase in de migratie: nu deze standaarden beschikbaar zijn, kunnen meer organisaties beginnen met de implementatie van PQC.
Hoewel het moeilijk is om de exacte kosten van de PQC-migratie in te schatten, is het duidelijk dat elke organisatie hiervoor personeel, tijd en geld opzij dient te zetten. Bovendien kan de migratie mogelijk niet beperkt blijven tot het softwaredomein, gezien de hogere eisen die PQC aan hardware stelt.
Om organisaties te helpen migreren naar PQC biedt dit handboek een driestappenbenadering: (1) *diagnose van quantumkwetsbaarheid*, (2) *planning* en (3) *uitvoering*. Alle organisaties wordt aangeraden om te beginnen met de diagnose van quantumkwetsbaarheid. Dit houdt in dat er een inventarisatie wordt gedaan van de cryptografische primitieven en protocollen die momenteel binnen de organisatie worden gebruikt. Tevens moet er geïdentificeerd worden welke gegevens en communicatiekanalen deze cryptografische maatregelen beschermen. Op basis van de daaruit volgende inventaris kan een uitgebreide (quantum-)risicoanalyse worden uitgevoerd, waarbij bijvoorbeeld de urgentie van migratie naar PQC wordt beoordeeld.
Aan de hand van de diagnose kunnen organisaties beginnen met de volgende stappen: de *planning* en *uitvoering* van een gestructureerde PQC-migratie. Het uitstellen van dit proces en vervolgens onder druk overhaast migreren verhoogt het risico op kostbare fouten. Bovendien wordt veel cryptografie beheerd door externe leveranciers. Deze leveranciers hebben tijd nodig om hun producten bij te werken op basis van de veranderende eisen van een organisatie. Het is daarom raadzaam om zo snel mogelijk PQC-gereedheid van leveranciers te eisen.
Ten slotte ontwikkelt het vakgebied van cryptografie zich snel en kunnen nieuwe cryptografische ontwikkelingen in de toekomst nieuwe migraties vereisen, bijvoorbeeld door nieuwere, beter passende standaarden en/of nieuwe beveiligingsaanbevelingen. Om deze reden raden we aan om *crypto-agility* (van *cryptographic agility*: 'cryptografische wendbaarheid') hoog in het vaandel te plaatsen bij het herzien van de bestaande cryptografische infrastructuur. Met crypto-agility kunnen de aanstaande en eventuele toekomstige migraties efficiënter uitgevoerd worden.

1.1 Doel van dit handboek

Het doel van dit document is om middels concrete, uitvoerbare richtlijnen organisaties te ondersteunen bij hun migratie naar post-quantumcryptografie. Dit handboek is specifiek gericht op organisaties waar de impact van een cryptografische kwetsbaarheid ernstig zou zijn, waardoor een snelle start van het PQC-migratieproces noodzakelijk is. Het is echter raadzaam voor alle organisaties om deze overgang zo snel mogelijk te beginnen om de risico's van onvoorziene gebeurtenissen te beperken.
Dit handboek biedt gedetailleerde informatie over de risico's, uitvoerbare strategieën, en de voor- en nadelen van vroege migratie naar PQC. Ook bevat het praktisch advies over het opstellen van een migratieplan

specifiek voor een organisatie. Belangrijk is dat de organisatie uiteindelijk zelf verantwoordelijk blijft voor het ontwikkelen van een migratieplan dat aansluit bij de specifieke risicobereidheid van die organisatie.
Voor een algemeen overzicht van de quantumdreiging voor cryptografie verwijzen we naar eerdere publicaties zoals [MvH20] en [NLNCSA21]. Dit handboek biedt concretere aanbevelingen om organisaties te helpen actie te ondernemen.
We erkennen dat de grote diversiteit aan organisaties op maat gemaakt adviezen voor PQC-migratie vereist. Daarom zijn onze aanbevelingen aangepast op verschillende typen van organisaties, zodat iedereen begeleiding ontvangt die het beste bij de behoeften past. We merken nog op dat zelfs binnen een gegeven organisatie verschillende afdelingen ook verschillende niveaus van urgentie kunnen hebben, afhankelijk van de specifieke gegevens of systemen die zij beheren.

1.2) De dreiging van quantumcomputers

Quantumcomputers vormen een risico voor de veiligheid van veel gegevens en communicatiekanalen die momenteel door cryptografie worden beschermd. Dit risico is echter lastig nauwkeurig te kwantificeren en precieze voorspellingen zijn moeilijk te maken. Deze sectie schetst de overwegingen rondom de risico's die quantumcomputers met zich meebrengen.
Ten eerste hebben bepaalde quantumalgoritmes, met name de algoritmes van Shor en Grover [Sho94; Gro96], de potentie om specifieke cryptografische primitieven te verzwakken of volledig te breken. Het uitvoeren van deze algoritmes vereist een voldoende krachtige quantumcomputer, die zodoende vaak wordt aangeduid als een cryptografisch relevante quantumcomputer. Hoewel zo'n quantumcomputer nog niet (lijkt te) bestaan, is er de afgelopen jaren aanzienlijke vooruitgang geboekt. Als gevolg hiervan heeft de cryptografische gemeenschap zich steeds meer gericht op de ontwikkeling en implementatie van cryptografie die bestand is tegen toekomstige quantumaanvallen. Hoewel er recent nieuwe cryptografische standaarden voor dit domein zijn gepubliceerd, moet de migratie naar deze zogenaamde post-quantumcryptografie in veel systemen nog plaatsvinden.
Er zijn verschillende pogingen gedaan om te voorspellen wanneer een cryptografisch relevante quantumcomputer beschikbaar zal zijn, met schattingen variërend van tien jaar tot "het zal nooit gebeuren". Zulke voorspellingen gaan echter met veel onzekerheden gepaard, aangezien onvoorziene ontwikkelingen de tijdlijnen drastisch kunnen veranderen. Toch is het wel duidelijk dat de impact van een cryptografisch relevante quantumcomputer aanzienlijk zal zijn en dat het risico voor organisaties zal toenemen naarmate ze hun migratie naar PQC langer uitstellen. Daarom raden we organisaties sterk aan om zo snel mogelijk de eerste stappen te zetten richting de PQC-migratie.
Ten tweede hangt het risico af van wat er precies wordt beschermd. Als een systeem of dataset bijvoorbeeld een levensduur heeft die eindigt na verwachte komst van cryptografisch relevante quantumcomputers is het risico al hoog: de dreiging zal dan immers vorm krijgen terwijl de levensduur nog loopt. In dergelijke gevallen moet de migratie prioriteit krijgen en zo snel mogelijk worden uitgevoerd. Functies zoals authenticatie en systeembeschikbaarheid, die niet achteraf kunnen worden aangevallen, lopen risico zodra de quantumdreiging volledig materialiseert. Er kan daarom sprake zijn van een ander urgentieniveau in het migratieproces.
Ten slotte is de duur van het volledige migratieproces onzeker. Op basis van eerdere (en kleinere) cryptografische migraties is het waarschijnlijk dat een volledige transitie meer dan vijf jaar kan duren. Daarom moeten organisaties, afhankelijk van hun risicobereidheid, nu beginnen met de voorbereiding op migratie. Zonder de daadwerkelijke migratie te ondernemen kunnen organisaties beginnen met het identificeren van kwetsbare activa, het prioriteren ervan en het ontwikkelen van een migratieplan. Deze proactieve aanpak minimaliseert de risico's die gepaard gaan met vertragingen en de kosten van onverwachte tegenslagen tijdens de eigenlijke migratie.

1.3 Documentstructuur & leeswijzer

In de basis volgt dit handboek een driestappenaanpak, zoals ook beschreven in [ETSI20a]:

1 In hoofdstuk 2 wordt de diagnose van quantumkwetsbaarheid beschreven. Dit hoofdstuk is primair bedoeld voor strategie- en beleidsmakers en kan de betrokkenheid vereisen van personen met kennis van het type gegevens en bijbehorende componenten binnen een organisatie. Eerst wordt beoordeeld hoe groot de urgentie voor een organisatie is om te migreren. Daarvoor introduceren we het concept van PQC-persona's. Deze persona's helpen organisaties met het bepalen van hun houding ten opzichte van de PQC-migratie. Aan de hand van (visuele) beslisbomen en schema's kan een organisatie identificeren welk persona of welke persona's relevant zijn. Vervolgens moet een inventarisatie worden gedaan van alle cryptografische protocollen en de systemen die deze cryptografie gebruiken.

2 Hoofdstuk 3 schetst de planning van het migratieproces op zowel technisch als organisatorisch vlak. We raden met name urgente adopters aan dit gedeelte grondig te lezen. Na de diagnose zijn het urgentieniveau en de cryptografie die moet worden gemigreerd geïdentificeerd. De volgende stap is om op basis van deze informatie te bepalen welke mitigatiestrategieën voor kwetsbare componenten moeten worden geïmplementeerd. Daarnaast moet in dit stadium de timing van het migratieproces voor verschillende componenten worden bepaald. De doelgroep voor dit hoofdstuk blijft strategie- en beleidsmakers, aangezien zij verantwoordelijk zijn voor het plannen en prioriteren van het migratieproces en het samenstellen van het juiste team om de migratie uit te voeren. Bovendien zal dit hoofdstuk van belang zijn voor (beveiligings)architecten die het migratieproces vanuit technisch perspectief zullen leiden.

3 Hoofdstuk 4 is hoofdzakelijk op een technisch publiek gericht. In dit hoofdstuk worden technische richtlijnen gegeven om te bepalen hoe de cryptografie moet worden gemigreerd. Eerst worden algemene strategieën en overwegingen voor het migreren van cryptografie gepresenteerd. Dit wordt gevolgd door strategieën voor specifieke cryptografische algoritmes en protocollen.

In hoofdstuk 5 besteden we aandacht aan recente ontwikkelingen op het gebied van (post-quantum) cryptografie, inclusief initiatieven rondom PQC-standaardisatie en wetgevende ontwikkelingen. Ook dit hoofdstuk is voornamelijk bedoeld voor een technisch publiek.

Ten slotte biedt hoofdstuk 6 diepgaande technische informatie over een aantal populaire cryptografische constructies. Dit hoofdstuk dient voornamelijk als referentie voor het opzoeken van details rondom de cryptografie die door een organisatie worden gebruikt. Het is niet nodig om dit hoofdstuk in zijn geheel te lezen. De beoogde doelgroep voor dit hoofdstuk bevat technische leiders van het migratieproces en ontwikkelaars/programmeurs in de cryptografie of bredere beveiliging die aan de migratie zullen werken.

1.3.1 Herzieningen en uitbreidingen ten opzichte van de eerste editie

Dit handboek bouwt voort op het PQC-migratiehandboek dat in maart 2023 werd gepubliceerd.
Alle eerdere inhoud is overgenomen, maar herzien om ontwikkelingen die sinds toen hebben plaatsgevonden te weerspiegelen. Daarnaast is het volgende nieuwe materiaal in deze tweede editie opgenomen:

- Sectie 1.6 biedt een lijst met *no-regret moves*;
- Sectie 2.3 behandelt cryptografisch componentbeheer en beschrijft het uitvoeren van een cryptografische inventarisatie;
- Sectie 2.4 geeft een methodologie voor het uitvoeren van een quantumrisicobeoordeling;
- Sectie 3.2.2 weidt uit over veelvoorkomende organisatorische uitdagingen bij volwassen cryptografisch beheer en biedt een strategie om PQC-volwassenheid te beoordelen;;
- Sectie 4.4 is gericht op crypto-agility;
- Hoofdstuk 5 schetst recente internationale ontwikkelingen met betrekking tot de PQC-migratie;
- Sectie 6.5 biedt een overzicht van geavanceerde beveiligingseisen zoals weerstand tegen side-channel attacks en hardwarebeveiliging;
- Sectie 6.6 bespreekt cryptografische softwarelibraries die PQC-algoritmes bevatten.

1.4) Achtergrondinformatie over cryptografie

Voordat we ingaan op de PQC-migratie zelf, leggen we enkele basisbeginselen van cryptografie uit.

	Symmetrisch	Asymmetrisch
Versleuteling	Geauthenticeerde encryptie, Block Cipher + Mode, Stream Cipher	Publieke sleutel-encryptie
Authenticatie / integriteit	Authenticated Encryption, Message Authentication Code	Digitale handtekeningen
Sleutelgeneratie / -verspreiding	(Pseudo) Random Number Generator	Sleuteluitwisseling en -inkapseling

Table 1.1 | Overzicht van enkele bouwblokken om bepaalde cryptografische doelen te bereiken, met symmetrische dan wel asymmetrische cryptografie

Cryptografie richt zich op het beschermen van informatie en communicatiekanalen tegen vijandige entiteiten. Het richt zich op vier hoofdpijlers

- Vertrouwelijkheid zorgt ervoor dat gevoelige data niet worden onthuld aan ongewenste ontvangers;
- Authenticiteit houdt in dat de bron van een bericht wordt geverifieerd;
- Integriteit heeft als doel ervoor te zorgen dat data niet zijn gewijzigd door onbetrouwbare entiteiten;
- Onweerlegbaarheid weerhoudt afzenders en ontvangers ervan hun betrokkenheid bij het verzenden of ontvangen van specifieke berichten ontkennen.

De bouwstenen van cryptografie worden *cryptografische* primitieven genoemd. Dit zijn basale — doch niet eenvoudige — algoritmes waarmee vervolgens ingewikkeldere cryptografische protocollen, algoritmes en schema's kunnen worden gevormd. Voorbeelden van *primitieven* zijn RSA en AES, terwijl TLS en SSH voorbeelden van *protocollen* zijn. Een overzicht van de belangrijkste functionaliteiten en de onderliggende cryptografische primitieven is te zien in tabel 1.1.

Een van de bekendste cryptografische functionaliteiten wordt geleverd door zogenaamde *encryptie-* of *versleutelingsschema's*. Deze schema's beschermen de vertrouwelijkheid van gegevens en voorkomen dat ze worden onderschept door andere partijen. Versleutelingsschema's gebruiken een encryptiesleutel om de gegevens om te zetten in een onleesbare ciphertext, die alleen kan worden ontsleuteld met de juiste decryptiesleutel[2].

Digitale handtekeningen vormen een andere veelgebruikte cryptografische functionaliteit. Deze schema's zijn voornamelijk bedoeld om de authenticiteit en integriteit van data te bewijzen. Er wordt een geheime sleutel gebruikt om de data te ondertekenen. Daarna kan de handtekening worden geverifieerd met behulp van een verificatiesleutel.

Cryptografie vereist cryptografische sleutels om veilig te kunnen werken. Het is dan ook cruciaal dat deze sleutels op een veilige manier tot stand komen. De primitieven die zich hierover ontfermen noemen we mechanismen voor *sleutelgeneratie*.

Binnen de cryptografie onderscheidt men *symmetrische* en *asymmetrische* cryptografie. Bij symmetrische cryptografie worden versleuteling en ontsleuteling (of ondertekening en verificatie in het geval van digitale handtekeningen) uitgevoerd met dezelfde sleutel. In dat geval moeten de betrokken partijen wel van tevoren tot overeenstemming komen over een dergelijke sleutel. Het opzetten van een gezamenlijke (symmetrische) sleutel tussen twee partijen staat bekend als het *sleutelverspreidingsprobleem.*

Asymmetrische cryptografie, ook bekend als *publieke sleutel-cryptografie* (Eng: *public-key cryptography*), omzeilt het sleutelverspreidingsprobleem door twee verschillende sleutels te gebruiken: een *publieke sleutel* en een *geheime sleutel*, die samen een *sleutelpaar* vormen. Eén partij genereert zo'n sleutelpaar en maakt de publieke sleutel openbaar, zodat iedereen berichten kan versleutelen of handtekeningen kan verifiëren. Alleen met de corresponderende geheime sleutel kunnen berichten ontsleuteld of handtekeningen gegenereerd worden: dat is ook de reden dat deze sleutel geheim is.

Symmetrische cryptografie is over het algemeen efficiënter dan asymmetrische cryptografie. Om deze reden worden de minder efficiënte asymmetrische primitieven vaak gebruikt om een symmetrische sleutel te verspreiden, waardoor het probleem van sleutelverspreiding wordt opgelost. Zodra de symmetrische sleutel is verspreid kunnen efficiëntere symmetrische primitieven, zoals AES, worden gebruikt om een communicatiekanaal te beveiligen.

De specifieke asymmetrische primitieven waarmee symmetrische sleutels tussen twee partijen worden opgezet noemen we algoritmes voor *sleuteluitwisseling* (KE, van *key exchange*) of *sleutel inkapselingsmechanismen* (KEM, van *key encapsulation mechanism*). We hanteren in dit handboek de Engelse afkortingen KE en KEM omdat deze in de internationale cryptografische gemeenschap ingeburgerd zijn.

KE's en KEMs verschillen subtiel in de manier waarop ze deze sleutelverspreiding bereiken, maar dit verschil valt buiten de scope van dit document. Daarom zullen we deze twee typen primitieven door elkaar gebruiken. In de meeste toepassingsscenario's speelt het functionele verschil tussen KE's en KEM's geen significante rol. Het vervangen van een KE door een KEM of omgekeerd kan echter technische uitdagingen met zich meebrengen.

Daarnaast bestaan er nog zogenaamde *cryptografische hashfuncties*, die een bericht omzetten in een zogenaamde *digest*. Aan de hand van een gegeven bericht en digest is het makkelijk om te verifiëren of deze met elkaar corresponderen, door simpelweg het bericht te *hashen* en dit met de digest te vergelijken. Het is ech-

[2] Sommige encryptieschema's bieden ook authenticiteit en onweerlegbaarheid

ter zeer moeilijk om het oorspronkelijke bericht uit een gegeven digest terug te halen, of twee verschillende berichten met dezelfde digest te vinden. Hashfuncties vereisen niet altijd een cryptografische sleutel. Als er wel een sleutel wordt gebruikt (zoals bij *keyed hashing*) is dit een symmetrische sleutel. Om deze reden worden hashfuncties vaak onder de symmetrische cryptografie geschaard.
De laatste cryptografische primitieve die we beschouwen zijn zogenaamde *Message Authentication Codes* (MACs). MACs dragen bij aan authenticiteit en integriteit door een tag van een bericht te maken, zodat de ontvanger kan verifiëren of het ontvangen bericht is verzonden door de gewenste partij en tijdens de overdracht niet door iemand anders is gewijzigd. MACs worden normaal gesproken geconstrueerd op basis van hashfuncties of symmetrische bouwblokken.

Dreiging van quantumcomputers

De mate waarin van quantumcomputers bovenstaande primitieven bedreigen varieert. Het quantumalgoritme van Grover [Gro96] geeft in theorie een kwadratische versnelling bij het aanvallen van symmetrische cryptografie. Dit betekent dat het beveiligingsniveau van een hashfunctie of symmetrisch versleutelingsschema effectief wordt gehalveerd. Dit verlies kan worden gecompenseerd door de lengte van de sleutels van symmetrische primitieven te verdubbelen. Gedetailleerdere kostenanalyses van aanvallen op basis van Grover suggereren echter dat deze benadering, het verdubbelen van sleutellengte, mogelijk te conservatief is [JNRV20]. Er is zelfs een groeiende consensus dat quantumcomputers slechts beperkte voordelen bieden bij het aanvallen van symmetrische cryptografie en hashfuncties [GLRS16].
Aan de andere kant wordt de asymmetrische cryptografie die vandaag de dag het meest gebruikt wordt volledig gecompromitteerd door het quantumalgoritme van Shor [Sho94]. Als gevolg hiervan zullen algoritmes zoals RSA, ECDH, ECDSA en EdDSA niet meer veilig zijn zodra een cryptografisch relevante quantumcomputer beschikbaar komt. Daarom wordt verwacht dat quantumcomputers voornamelijk asymmetrische cryptografie zullen beïnvloeden.

Over quantum key distribution

Een van de belangrijkste toepassingen van asymmetrische cryptografie is sleutelverspreiding: het opzetten van een gezamenlijke symmetrische sleutel tussen twee entiteiten. Zo'n sleutel kan vervolgens in symmetrische cryptografie gebruikt worden om communicatiekanalen te versleutelen en te authenticeren. Het combineren van asymmetrische en symmetrische cryptografie op deze manier is doorgaans veel efficiënter dan uitsluitend vertrouwen op asymmetrische cryptografie en is daarom gebruikelijk.
In tegenstelling tot asymmetrische cryptografie maakt *quantum key distribution* (QKD) gebruik van eigenschappen van de quantummechanica om het probleem van sleutelverspreiding op te lossen. De beveiliging van QKD-protocollen is niet afhankelijk van aannames over computationele moeilijkheid en QKD is daarom veilig tegen zowel klassieke als quantum-ondersteunde aanvallen. Om deze reden wordt QKD vaak geprezen als een alternatief voor post-quantumcryptografie. QKD heeft echter bepaalde inherente beperkingen die de toepasbaarheid ervan beïnvloeden. Bovendien geloven veel beveiligingsexperts dat QKD momenteel niet de volwassenheid heeft bereikt om in de meeste toepassingen het gewenste beveiligingsniveau te behalen. Om deze reden moet de migratie naar PQC worden geprioriteerd boven de implementatie van QKD om de quantumdreiging te mitigeren.
Verschillende beveiligingsinstanties delen deze positie over QKD, bijvoorbeeld ANSSI (Frankrijk) [ANSSI20], BSI (Duitsland) [BSI22], NLNCSA (Nederland) [NLNCSA21], NSA (VS) [NSA21b] and UK-NCSC (VK) [NCSC-UK20b]. Bovendien hebben onlangs Nederlandse, Franse, Duitse en Zweedse instanties een standpunt over QKD gepubliceerd [ABNS24], waarin de belangrijkste beperkingen van deze technologie worden toegelicht. Hieronder worden de belangrijkste observaties uit deze standpuntnota samengevat.
Ten eerste kan PQC ingezet worden voor verschillende cryptografische doelen, terwijl QKD alleen een sleutelverspreiding biedt die zelf nog authenticatie met PQC vereist. Ten tweede is QKD geen grondige standaardisatieprocedure ondergaan die het vereiste vertrouwen in cryptografische toepassingen zou bieden.

Ten derde bieden QKD-protocollen momenteel geen bevredigende beveiligingsbewijzen. Hoewel er aanzienlijke vooruitgang is geboekt, vangen de abstracte wiskundige modellen die momenteel worden gebruikt om de beveiliging van QKD te bewijzen de realiteit niet adequaat. Ten vierde heeft QKD last van afstandsbeperkingen. Specifieker: twee partijen die QKD gebruiken moeten verbonden zijn via een quantumcommunicatiekanaal, dat wil zeggen, via een optische vezel of een optisch (*free-space*) communicatiekanaal. Dit communicatiekanaal vereist een laag ruisniveau, wat de maximale afstand beperkt. Deze afstandsbeperking is te overwinnen met het gebruik van *repeaters*. Momenteel is de technologische volwassenheid van niet-vertrouwde repeaters echter onvoldoende om de QKD-afstandsbeperking te overwinnen. Om deze reden moet men vertrouwen op vertrouwde repeaters, waardoor vertrouwde derde partijen toegang krijgen tot de niet-versleutelde gevoelige informatie. *End-to-end*-beveiliging over langere afstanden is momenteel dus onhaalbaar. Ten slotte is voor veilige communicatie met QKD speciale, dure quantumhardware vereist. QKD vereist dus grote investeringen in infrastructuur en de specifieke apparatuur die voor QKD wordt gebruikt introduceert nieuwe aanvalsvectoren.
Al met al is post-quantumcryptografie volwassener, flexibeler en goedkoper dan quantum key distribution. PQC kan quantumkwetsbare cryptografie in alle contexten vervangen, aangezien het kan worden gedraaid op machines die vergelijkbaar zijn met de huidige machines. Er wordt veel onderzoek gedaan naar het verminderen van de huidige beperkingen van QKD en het verbeteren van de beveiligingsgaranties. Voorlopig adviseren we echter om niet te vertrouwen op de beveiliging van QKD-oplossingen.

1.5) Internationale regelgeving en adviezen

Verschillende internationale organisaties hebben richtlijnen gepubliceerd met betrekking tot de dreiging van quantumcomputers. Er is een sterke consensus over de urgentie van het migreren naar quantumveilige cryptografische primitieven en veel organisaties benadrukken het belang van een goed gecoördineerde PQC-migratie. De eerste stap is het inventariseren van de cryptografische componenten die moeten worden gemigreerd en het ontwikkelen van een nauwkeurige roadmap. Om een soepele overgang te waarborgen worden belanghebbenden aangemoedigd om crypto-agile te blijven, zodat ze snel kunnen inspelen op nieuwe ontwikkelingen.
Er zijn echter enkele tegenstrijdigheden rondom specificaties van de implementatie en de tijdslijnen van de PQC-migratie. Sommige EU-lidstaten, zoals Duitsland, Frankrijk en Nederland, pleiten voor de implementatie van PQC in hybride combinaties met gevestigde, maar quantumkwetsbare, cryptografie. Hybride oplossingen verminderen het risico van onontdekte kwetsbaarheden in PQC-primitieven. Omdat hybride oplossingen de complexiteit van de cryptografische oplossing vergroten, kunnen ze echter mogelijk het aanvalsoppervlak vergroten. Om deze reden beveelt het VK hybride oplossingen alleen aan wanneer dit absoluut noodzakelijk is. Ten slotte is er het feit dat de Europese Commissie QKD beschouwt als een mogelijke oplossing om de dreiging van quantumcomputers te mitigeren. Toch zijn beveiligingsinstanties het er over het algemeen over eens dat QKD momenteel niet volwassen genoeg is voor grootschalige adoptie.

1.6) No-regret moves

De gegevens die vandaag worden versleuteld, lopen het risico nu al te worden onderschept om later door quantumcomputers te worden ontsleuteld. Terwijl quantumcomputers gestaag sterker worden, meer qubits controleren en complexere berekeningen uitvoeren, blijft het onduidelijk wanneer de quantumdreiging voor cryptografie zich zal manifesteren. Sommige sceptici beweren zelfs dat een cryptografisch relevante quantumcomputer nooit realiteit zal worden. Desalniettemin zou voor veel organisaties de impact van een quantuminbreuk op hun cryptografische verdediging dermate ernstig zijn, dat het risco niet te negeren is.

De eerste standaarden voor PQC zijn gepubliceerd en de implementatie ervan is al begonnen. Tegelijkertijd vormt post-quantumcryptografie nog steeds een actief onderzoeksgebied, met veel open vragen en veel mogelijkheden voor nieuwe ontwikkelingen. In het bijzonder zullen zowel NIST als ISO hun inspanningen rondom PQC-standaardisatie voortzetten en is de verwachting dus dat de lijst van beschikbare PQC-standaarden in de komende jaren zal groeien.
Bovenstaande onzekerheden, die betrekking hebben op zowel de risico's van quantumcomputers als de bijbehorende mitigatiemaatregelen, kunnen terughoudendheid bij het starten van de PQC-migratie veroorzaken. Het uitstellen van de migratie is echter riskant. Gelukkig kunnen de eerste stappen van de PQC-migratie zoals beschreven in dit handboek worden beschouwd als zogenaamde *no-regret moves*: deze acties zijn nuttig ongeacht de ontwikkelingen in quantumcomputing en post-quantumcryptografie. Hieronder vatten we een aantal no-regret moves in de context van de PQC-migratie samen.

Beoordeel afhankelijkheden in de toeleveringsketen (sectie 2.1) | Cryptografie is doorgaans opgenomen in IT-producten en organisaties vertrouwen op hun leveranciers om deze cryptografische algoritmes bij te werken. Adequaat risicomanagement omvat het inventariseren van dergelijke afhankelijkheden. Vervolgens kunnen organisaties het gesprek met hun leveranciers aangaan over PQC-migratiestrategieën om tot afstemming te komen. Omgekeerd is het ook belangrijk om te onderzoeken welke organisaties worden beïnvloed door uw cryptografische beslissingen.

Zet cryptografisch componentbeheer op (sectie 2.3) | Cryptografische implementaties kunnen net als andere software bugs en kwetsbaarheden bevatten, zelfs als een cryptografisch relevante quantumcomputer nooit werkelijkheid wordt. Zorgvuldig beheer van alle cryptografische componenten kan organisaties helpen om dergelijke kwetsbaarheden efficiënt te identificeren en op te lossen. Bovendien kan cryptografisch componentbeheer de responstijden bij incidenten aanzienlijk verkorten en daardoor de impact beperken in het geval van bedreigde sleutels of certificaatverval. Het is een belangrijke stap in het realiseren van crypto-agility. Verder is cryptografiebeheer een essentiële stap om een quantumrisicobeoordeling uit te voeren.

Herzie cryptografisch beleid (sectie 2.3 en 4.4) | Het cryptografische beleid van een organisatie kan herziening vereisen op basis van zowel technische als regelgevende ontwikkelingen. Beleidslijnen moeten voldoen aan de wetgeving, anticiperen op veranderingen in regelgeving en dienen de bevindingen van de quantumrisicobeoordeling te weerspiegelen.

Voer een risicobeoordeling uit (sectie 2.4) | Organisaties moeten de quantumdreiging opnemen in hun bredere risicomanagementprocedures. De quantumrisicobeoordeling is essentieel om te bepalen wanneer en hoe de migratie naar post-quantumcryptografie moet plaatsvinden.

Schat de kosten van migratie (sectie 3.3) | Voor verschillende aspecten van de PQC-migratie is een gedetailleerd kostenoverzicht noodzakelijk, bijvoorbeeld voor het bepalen van de optimale timing voor de migratie van verschillende delen van de cryptografische infrastructuur. Een uitgebreid kostenoverzicht, dat zowel financiële overwegingen als capaciteitskwesties in acht neemt, zal besluitvormingsprocessen efficiënter maken en onnodige vertragingen voorkomen.

Inventariseer vereisten rondom regelgeving (hoofdstuk 5) | In veel sectoren zijn passende cryptografische algoritmes een verplichte cybersecurity-maatregel. De verwachting is dat regelgevende instanties de implementatie van nieuwe PQC-standaarden zullen vereisen en binnenkort tijdlijnen zullen publiceren waarin kwetsbare cryptografische standaarden worden afgeschaft. Om deze reden is het belangrijk om niet alleen op de hoogte te blijven van technische ontwikkelingen, maar ook van regelgevende veranderingen.

Zorg voor een backup-plan | In het geval van onvoorziene ontwikkelingen, zoals een doorbraak in quantumcomputing of een aanval op een gevestigde cryptografische standaard, kan het nodig zijn om af te wijken van het oorspronkelijke migratieplan. Plan hoe u de bedrijfscontinuïteit kunt waarborgen en uitval in dergelijke gevallen kunt vermijden.

Werk samen met gelijksoortige organisaties | De PQC-migratie is een wereldwijde uitdaging die gezamenlijk moet worden aangepakt. Veel organisaties staan voor vergelijkbare uitdagingen en samenwerking zal daarom een effectieve en efficiënte PQC-migratie mogelijk maken. Organisaties kunnen ervaringen en lessen met elkaar delen, zowel op technisch als organisatorisch niveau. Bovendien is samenwerking essentieel om interoperabiliteit tussen organisaties te behouden.

1.7) Cryptografische volwassenheid

Zelfs buiten PQC-migratie gerekend is het voor organisaties uiterst waardevol om een bepaald niveau van volwassenheid te bereiken in het beheer van hun cryptografische componenten. In feite kan het bereiken van cryptografische volwassenheid worden beschouwd als een no-regret move: waardevol ongeacht de quantumdreiging. Een organisatie wordt als volwassen beschouwd met betrekking tot haar cryptografiebeheer als:

- ze een volledig overzicht heeft van haar cryptografische componenten;
- ze inzicht heeft in de risico's met betrekking tot haar cryptografie;
- ze een cryptografisch beleid heeft dat in overeenstemming is met relevante regels en voorschriften;
- ze de voorgaande punten continu bijhoudt en bijwerkt.

Allereerst zal goed cryptografiebeheer een organisatie niet alleen helpen om de PQC-migratie te faciliteren, maar ook om risico's met betrekking tot cryptografie in het algemeen te beperken. Hoewel cryptografische volwassenheid uiteindelijk tijd en moeite bespaart, is het voor veel organisaties moeilijk te implementeren of te onderhouden. Voordat een organisatie als cryptografisch volwassen kan worden beschouwd, zijn er een aantal vereiste stappen. Een schematisch overzicht van veelvoorkomende organisatorische uitdagingen met betrekking tot cryptografiebeheer vóór en tijdens de PQC-migratie is te vinden in figuur 1.1. De figuur toont hoe een goed uitgevoerde PQC-migratie cryptografische volwassenheid zal bewerkstelligen.
Zoals uit de figuur blijkt, is een essentiële eerste stap in een cryptografische migratie het erkennen wanneer de migratie moet plaatsvinden. Hoewel dit eenvoudig klinkt, is een gebrek aan urgentie van besluitvormers een typisch knelpunt. Daarna moet een diagnose worden uitgevoerd. Een volwassen organisatie zou efficient componentbeheer moeten hebben dat continu een cryptografische inventaris bijwerkt. Als dit nog niet het geval is, biedt de PQC-migratie een goede gelegenheid om het cryptografisch beheer van een organisatie te verbeteren. Het implementeren van gecentraliseerd cryptografiebeheer binnen een organisatie kan bijvoorbeeld leiden tot beter inzicht en effectiever beheer.
Vervolgens moet een quantumrisicobeoordeling duidelijk maken welke data en systemen onder welk niveau van dreiging van een quantumcomputer vallen. De methodologie die in sectie 2.4 wordt beschreven biedt handvatten om de dreiging van een quantumcomputer te beoordelen. De quantumrisicobeoordeling moet continu worden herhaald om een nauwkeurig overzicht van de huidige risico's te geven. Volwassen organisaties zouden doorgaans toegewijde systemen en personeel moeten hebben om alle soorten risico's waarmee een organisatie wordt geconfronteerd te beheren. Het opnemen van de risico's die door een potentiële dreiging worden geïntroduceerd, is een essentiële stap om deze risico's goed te beheren. Met integratie in bestaande strategieën voor risicomanagement kan een verbinding worden gelegd tussen risico's en hun effecten op kernbedrijfsprocessen.

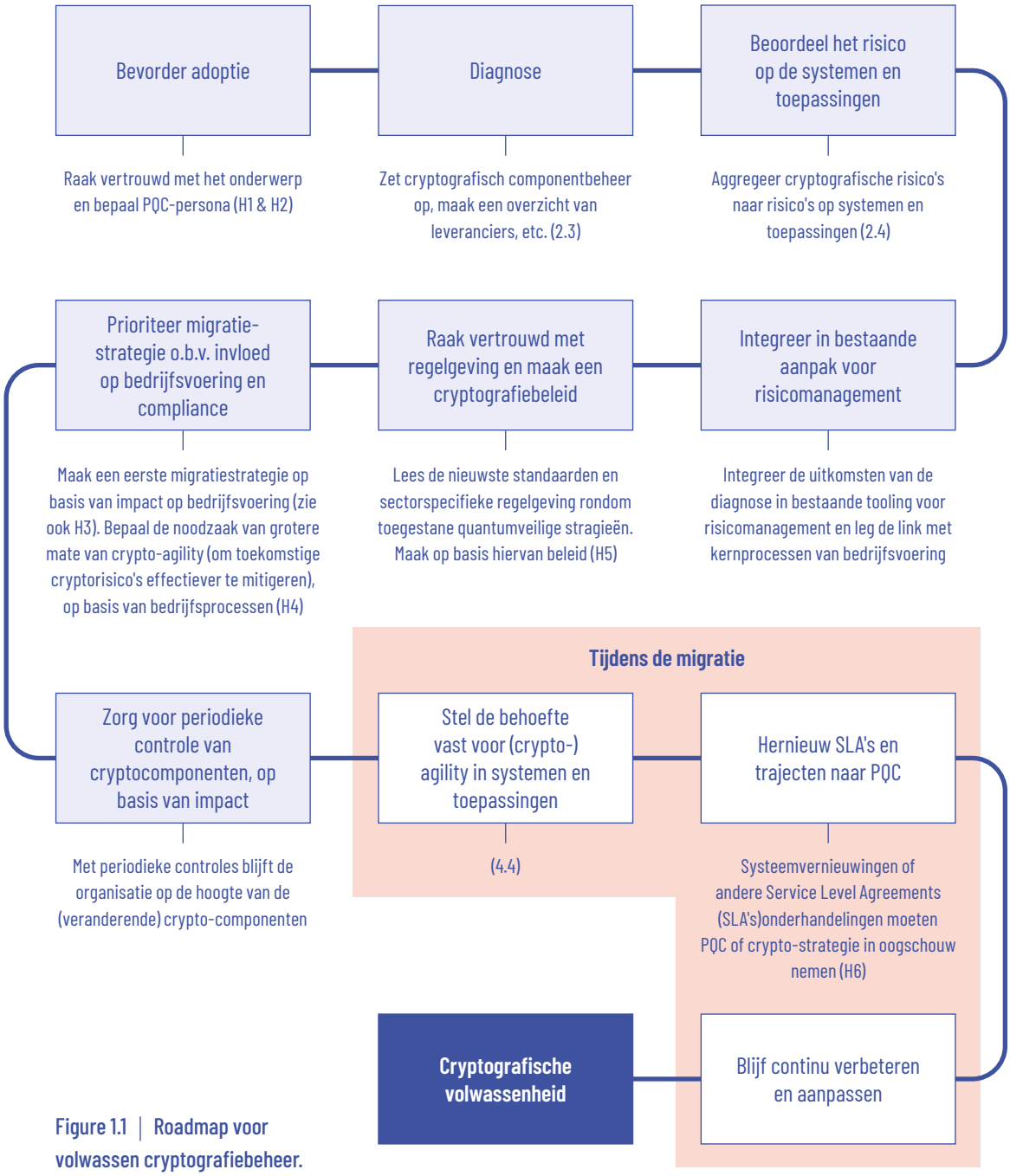


Figure 1.1 | Roadmap voor volwassen cryptografiebeheer.

Hoewel organisaties hun afhankelijkheden en cryptografische componenten zelf kunnen beheren, zal er ook regelgeving zijn die voor best practices rondom cryptografisch beheer en de migratie naar PQC voorschrijft. Daarom is het voor elke organisatie essentieel om bewust te zijn van toepasselijke regelgeving. Op basis van deze regelgeving en eigen doelstellingen zou een volwassen organisatie een goed beleid voor cryptografisch beheer moeten hebben. De inhoud en vorm van een dergelijk beleid worden uitgelegd in sectie 2.3.1.
Volwassen organisaties moeten een prioriteitenlijst opstellen van welke systemen, applicaties, gegevens, et cetera in welke volgorde moeten worden gemigreerd. Deze prioriteitenlijst moet relevante regelgeving naleven en inzichten in de risico's voor de organisatie als geheel in acht nemen. Bovendien moet deze prioritering identificeren welke toekomstige risico's moeten worden aangepakt, bijvoorbeeld door een hoger niveau van wendbaarheid te bewerkstelligen. Zoals eerder vermeld moeten deze stappen (diagnose, risicobeoordeling,

beleid en prioritering) periodiek worden herzien om een actueel overzicht van de huidige status te behouden. Ten slotte kan een volwassen organisatie tijdens de migratie een hoger niveau van crypto-agility implementeren, vooral voor de data in systemen in eigen beheer. Voor componenten in extern beheer moet beoordeeld worden of de migratietijdlijnen van de betreffende leveranciers met overeenkomen met de eigen tijdlijnen en doelstellingen. Als dat niet het geval is, moeten de organisatie nieuwe leveranciers vinden of zelf de cryptografie gaan beheren. Een overzicht van verschillende soorten crypto-agility volgt in sectie 4.4.

Als een organisatie een hoge mate van crypto-agility heeft bereikt, kunnen cryptografische algoritmes en systemen gemakkelijker worden aangepast om te voldoen aan nieuwe standaarden en beveiligingspraktijken en om nieuwe bedreigingen het hoofd te bieden. Dit toont aan dat de organisatie volwassen is in het gebruik van cryptografie en eventuele aanpassingen snel kan doorvoeren om haar niveau van veiligheid te handhaven.

2 Diagnose van quantum-kwetsbaarheid

Samenvatting

Dit hoofdstuk bevat concrete richtlijnen voor organisaties om het risico en de urgentie van de migratie naar PQC-standaarden te bepalen, inclusief een overzicht van wat ze nodig hebben om met deze migratie aan de slag te gaan. Het eerste deel van dit hoofdstuk geeft organisaties handvatten om hen te helpen beslissen of ze nu al de eerste stappen van de PQC-migratie moeten zetten. Dit gebeurt door organisaties in te delen in verschillende persona's, zodat elke (deel)organisatie zich met ten minste één van deze persona's kan identificeren. Het tweede deel bevat concrete adviezen voor het doen van een PQC-diagnose, een eerste stap die elke organisatie moet nemen in de PQC-migratie.
De persona of persona's van een organisatie zijn afhankelijk van een aantal factoren, zoals het soort data dat door de organisatie wordt verwerkt, de systemen waarmee de organisatie werkt, het dreigingsniveau en de afhankelijkheid van andere organisaties. Op basis van deze factoren kunnen drie hoofdpersona's onderscheiden worden: *urgente adopters*, *reguliere adopters* en *cryptografie-experts*. Urgente adopters zijn organisaties die nu al stappen in de PQC-migratie moeten zetten, of dat al hadden moeten doen. Daarnaast zijn er reguliere adopters: organisaties die voorlopig meer een reactieve houding ten aanzien van de PQC-migratie kunnen aannemen. Ze kunnen vanwege hun systemen de verdere ontwikkeling van PQC-standaarden afwachten alvorens met de migratie te beginnen. Cryptografie-experts zijn ten slotte organisaties die cryptografische kennis of infrastructuur aan andere organisaties leveren en deze onderhouden. Dit hoofdstuk bevat informatie voor organisaties om te beslissen met welke persona('s) zij zich identificeren.
Als een organisatie tot de urgente adopters behoort, luidt het advies om zo spoedig mogelijk met de PQC-diagnose aan de slag te gaan. In dit stadium worden de benodigde data verzameld over de huidige beveiligings-architectuur om te beslissen welke systemen als eerste moeten worden gemigreerd. Voor deze stap moeten vier documenten worden opgesteld: een risicobeoordeling; een inventaris van de binnen de organisatie gebruikte cryptografische systemen; een inventaris van de door de organisatie verwerkte data en een inventaris van de leveranciers van de cryptografische systemen. Organisaties die niet behoren tot de urgente adopters kunnen over het algemeen wachten met het uitvoeren van deze PQC-diagnose. In sommige gevallen kan het echter toch nuttig zijn om nu al met deze diagnose te beginnen, aangezien het onderdeel is van de no-regret stappen.

De volgende hoofdsukken richten zich op advies voor de urgente adopters. Het is van vitaal belang dat PQC-persona's nauwkeurig worden bepaald, om ervoor te zorgen dat alle organisaties die nu stappen moeten ondernemen richting PQC-migratie dit ook daadwerkelijk doen.

2.1 PQC-personas

Voordat organisaties beginnen aan de PQC-migratie, moeten ze bepalen wanneer ze de migratie moeten beginnen. Om organisaties te helpen bij deze keuze en om de verschillende behoeften van organisaties bij het uitvoeren van de PQC-migratie het beste aan te pakken, hebben we het landschap van organisaties onderverdeeld in een klein aantal categorieën, genaamd PQC-persona's. Ten eerste stelt dit ons in staat om te iden-

tificeren welke organisaties zo snel mogelijk stappen moeten zetten richting migratie en welke organisaties nog even kunnen wachten. Ten tweede stelt dit ons in staat om advies op maat te geven aan verschillende organisaties met een vergelijkbare structuur. We hebben verschillende, concrete stappen opgesteld voor de verschillende persona's, verschillend in mate van urgentie, tijdslijnen, risicoanalyse en aandachtspunten. We hebben de volgende kenmerken gebruikt om deze verdeling te maken:

- **Aanvalsoppervlak** | Welke infrastructuur biedt een organisatie aan / hebben ze in beheer die vatbaar is voor aanvallen van een quantumcomputer?
- **Type systemen** | Wat voor systemen gebruikt een organisatie en wat is de impact als een systeem niet meer (goed) functioneert?
- **Type data** | Wat voor soort data en informatie verwerkt een organisatie in termen van criticaliteit, gevoeligheid en consequenties van onbevoegde en onontdekte aanpassingen?
- **Tijdsdruk** | Hoe snel moet PQC-migratie gebeuren om de veiligheid van data en systemen te waarborgen?
- **Afhankelijkheid van andere organisaties** | Hoe zijn verschillende organisaties afhankelijk van elkaar?
- **Dreigingsniveau** | Hoe realistisch is het dat een kwaadwillende met een quantumcomputer besluit om deze organisatie aan te vallen?

The PQC-persona's kunnen in drie categorieën onderverdeeld worden:

Urgente adopters | Organisaties die gevoelige data verwerken of kritieke of langlevende infrastructuren aanbieden. Deze organisaties moeten zo snel mogelijk de eerste stappen op het gebied van de PQC-migratie zetten. Binnen deze categorie is een onderscheid gemaakt tussen de verschillende soorten organisaties die snel moeten schakelen, afhankelijk van de reden waarom ze het risico lopen aangevallen te worden door een quantumcomputer

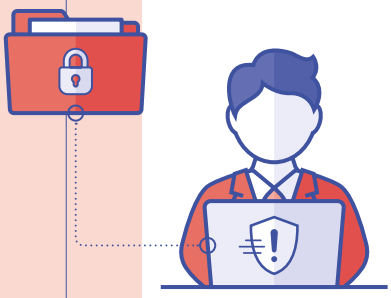
Reguliere adopters | Organisaties die niet beschikken over gevoelige data of vitale infrastructuur (of infrastructuur met een lange levenduur) met een hoog risico op aanvallen. Deze organisaties kunnen bijvoorbeeld wel gevoelige data verwerken, maar alleen als het onwaarschijnlijk is dat die data op dit moment worden opgeslagen voor ontsleuteling door een toekomstige quantumcomputer.

Cryptografie-experts | Organisaties die cryptografische standaarden of infrastructuur verstrekken. In tegenstelling tot urgente adopters hebben cryptografie-experts het grootste deel van de benodigde cryptografische kennis voor de PQC-migratie al in huis. Daarnaast zijn ze ook verantwoordelijk voor cryptografische systemen van andere organisaties.

Deze handleiding richt zich voornamelijk op het geven van advies en concrete stappen aan urgente adopters. Het belangrijkste doel van dit hoofdstuk is dan ook om organisaties te laten bepalen of ze een urgente of reguliere adopter zijn. De volgende hoofdstukken bevatten uitgebreid advies voor urgente adopters, maar er is ook advies voor de andere twee categorieën.

2.1.1 Urgente adopters

Binnen de persona 'urgente adopters' zijn verschillende subpersona's te onderscheiden. Deze subpersona's vormen geen verdere onderverdeling van de persona 'urgente adopters', maar zijn vooral voorbeelden van urgente adopters. Deze voorbeelden zijn gebaseerd op de verschillende risico's die quantumcomputers voor urgente adopters met zich meebrengen. Over het algemeen is het advies identiek voor deze subpersona's, maar voor bepaalde subpersona's worden sommige actiepunten meer benadrukt dan voor andere. Meer informatie hierover staat in het volgende hoofdstuk.



Verwerkers van persoonlijke informatie

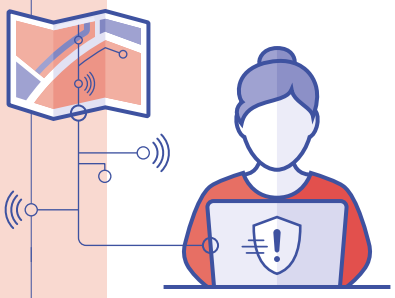
Organisaties die **persoonlijke informatie met een lange vertrouwelijkheidstermijn** verwerken. Deze organisaties zijn wettelijk verplicht om dergelijke persoonlijke informatie te beschermen. Store-now-decrypt-later-aanvallen vormen het belangrijkste risico waarmee deze organisaties worden geconfronteerd. Persoonlijke informatie is alle informatie die betrekking heeft op een geïdentificeerde of identificeerbare persoon. Hierbij is onder andere te denken aan burgerservicenummer (BSN), telefoonnummer, creditcardnummer, gezondheidsgegevens, uiterlijk of adres. Dergelijke data zijn vatbaar voor store-now-decrypt-later-aanvallen als er andere partijen zijn voor wie deze data zelfs over 20 jaar of meer interessant zijn. Hoewel de meeste organisaties persoonlijke informatie verwerken, is deze persona gericht op persoonlijke informatie waarvoor een quantumcomputer vandaag al een grote bedreiging vormt. Voor meer gevoel over hoe deze risico's beoordeeld kunnen worden, zie sectie 2.4.1. Dit betekent bijvoorbeeld dat sportclubs, webshops en onderwijsinstellingen niet onder deze persona vallen. Voorbeelden van organisaties die wel onder deze persona vallen zijn overheden, organisaties in de zorg zoals ziekenhuizen, financiële instellingen en verzekeraars.
Van belang is dat er momenteel géén wetten zijn specifiek gericht zijn op het beschermen van persoonlijke informatie tegen quantumcomputers of het gebruik van PQC om dit risico te verminderen. Het is echter waarschijnlijk dat beheerders van deze data verantwoordelijk worden gehouden als in de toekomst een quantumcomputer wordt gebruikt voor het ontsleutelen van op dit moment reeds opgeslagen data.

Verwerkers van organisatorisch gevoelige informatie

Organisaties die **organisatorisch gevoelige informatie met een lange vertrouwelijkheidstermijn verwerken**. Denk hierbij aan staatsgeheimen, transacties, notulen, handelsgeheimen en andere informatie die vertrouwelijk is voor entiteiten buiten de organisatie. Store-now-decrypt-later-aanvallen vormen het belangrijkste risico waarmee deze organisaties worden geconfronteerd. Dergelijke data zijn vatbaar voor store-now-decrypt-later-aanvallen als er andere partijen zijn voor wie deze data interessant zijn, zelfs pas over 20 jaar of meer. Voorbeelden van

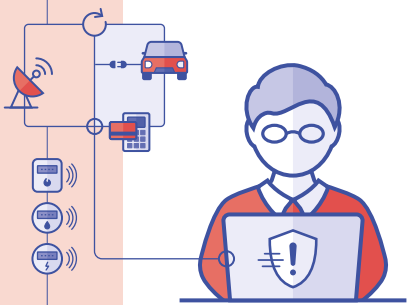
dergelijke organisaties zijn het leger, nationale inlichtingendiensten, overheden, financiële organisaties, kennisinstituten en universiteiten.
Het belangrijkste verschil tussen persoonlijke informatie en organisatorisch gevoelige informatie is dat persoonlijke informatie geheim moeten blijven om de privacy van individuen te beschermen, terwijl organisatorisch gevoelige informatie geheim moeten blijven om een organisatie te beschermen. Bij een datalek van persoonlijke informatie overtreedt een bedrijf wetten met betrekking tot persoonlijke informatie, terwijl een datalek van organisatorisch gevoelige informatie waarschijnlijk zou leiden tot het verlies van kennis of het concurrentievoordeel van een bedrijf, een verminderde staatsveiligheid of een algemene negatieve impact op de economie.

Aanbieders van vitale infrastructuur



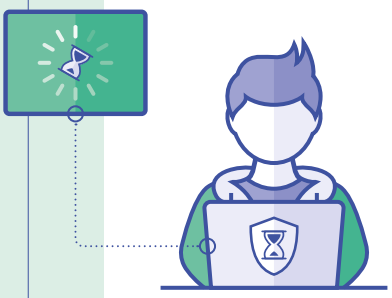
Organisaties **die systemen aanbieden die cruciaal zijn voor het functioneren van grote groepen mensen**, zoals dorpen, steden, provincies of zelfs landen. Er bestaan tal van dergelijke systemen; de meeste voorzien in basisbehoeften van grote groepen mensen, zoals water, elektriciteit, transport, communicatie en gezondheidszorg. Een gebrekkige werking van deze systemen kan resultaten hebben met verschillende mate van impact. Meestal leidt een storing ertoe dat het dagelijks leven van mensen ernstig wordt verstoord, maar soms zijn de gevolgen verstrekkender en is er sprake van ernstige schade, letsel of zelfs overlijden. Er zijn talloze voorbeelden van cyberaanvallen op kritieke infrastructuur. Eén van de meest opvallende is de aanval van Triton-malware in een Saoedische petrochemische fabriek, specifiek bedoeld om mensenlevens in gevaar te brengen. Wilt u meer lezen over deze en andere voorbeelden, zie dan [Wei21].
Het verschil met de eerste twee persona's is tweeledig. Enerzijds is beschikbaarheid bij deze organisaties van groter belang dan integriteit en betrouwbaarheid. Anderzijds is de risicobereidheid bij deze organisaties veel lager, aangezien defecten een veel grotere impact hebben. Om deze twee redenen kan het migratieproces er anders uitzien. Voorbeelden van aanbieders van kritieke infrastructuren zijn energie- of waterbedrijven, vervoersorganisaties zoals treinmaatschappijen of luchthavens, communicatiebedrijven zoals telecommunicatienetwerken, webbrowsers en zorgaanbieders zoals ziekenhuizen.

Aanbieders van systemen met een lange levensduur



Dit zijn organisaties die **systemen met een lange levensduur** aanbieden, omdat ze anders niet rendabel zijn. Het grootste risico waarmee deze organisaties worden geconfronteerd, is dat de systemen die de komende tien jaar worden geproduceerd waarschijnlijk nog altijd in gebruik zullen zijn op het moment dat quantumcomputers beschikbaar komen. Daarom moeten deze systemen snel kunnen worden bijgewerkt naar quantumveilige standaarden. Post-quantumcryptografie stelt doorgaans andere (meestal zwaardere) eisen aan hardware dan de huidige cryptografie, waardoor bij de productie van systemen met een levensduur van meer dan 20 jaar reeds met deze hardware-eisen rekening dient te worden gehouden. Voorbeelden zijn satellieten, betaalautomaten, auto's, telecommunicatienetwerken, energieleveranciers, slimme meters, smart industry (4.0) en sensornetwerken.

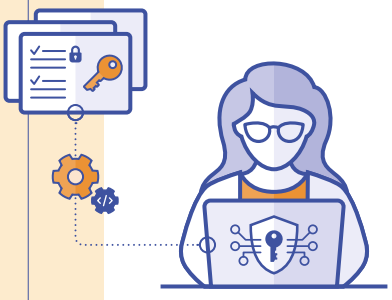
2.1.2 Reguliere adopters



Deze categorie omvat elke organisatie die niet behoort tot een van de persona's van de urgente adopters. Deze organisaties verwerken data of bieden systemen aan, maar de data lopen momenteel geen risico op store-now-decrypt-later-aanvallen en de systemen zijn niet van kritieke aard en hebben een kortere levensduur. Van belang is dat deze organisaties in latere stadia wel vatbaar kunnen zijn voor aanvallen met behulp van een quantumcomputer, maar dat het voor deze organisaties vooralsnog gunstiger is om verdere standaardisatie van PQC af te wachten, omdat vroege migratie met extra risico's komt, zoals eerder genoemd. Deze organisaties kunnen nu echter wel al stappen zetten en dienen ook alert te blijven op mogelijke wijzigingen in het advies of hun eigen persona('s). Meer informatie hierover staat in het volgende hoofdstuk. De meeste organisaties zijn reguliere adopters, zoals winkeliers, scholen en sportclubs.

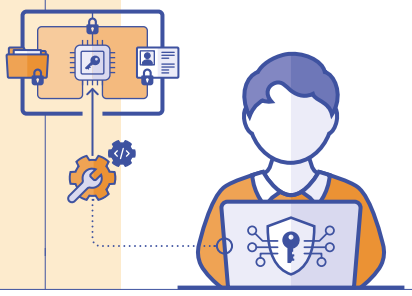
2.1.3 Cryptografie-experts

Dit document probeert dit soort organisaties geen directe adviezen te geven, aangezien zij zelf alle nodige kennis in huis zouden moeten hebben. Om een aantal redenen worden ze hier toch benoemd. Ten eerste is het voor de belangrijkste groep van urgente adopters belangrijk om te weten dat deze groep bestaat en wat ze ervan kunnen verwachten. De meeste urgente adopters nemen cryptografische systemen bij cryptografie-experts af. Urgente adopters die naar PQC willen migreren, moeten deze leveranciers kunnen vragen of hun producten quantumveilig zijn en zo niet, wanneer ze verwachten dat hun producten quantumveilig zijn. Ten tweede geeft het hierboven genoemde toch indirect adviezen voor de cryptografie-experts. Ze moeten voorbereid zijn op vragen van hun klanten in verband met PQC, zoals wanneer PQC in hun producten geïntegreerd zal zijn en welke algoritmes ze van plan zijn te implementeren. Daarom moeten ze ook zo snel mogelijk beginnen met het migreren van hun producten naar PQC-standaarden.



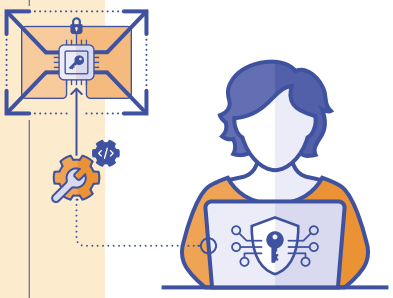
Standaardisatieorganen

Organisaties die **cryptografische standaarden en/of protocollen** definiëren. Dit zijn standaarden voor een scala aan toepassingen, waarbij op de één of andere manier gebruik wordt gemaakt van cryptografie. De meeste van deze standaarden worden gebruikt voor communicatie of beveiliging, zoals beveiligde communicatie, beveiligde dataopslag, bescherming van systemen of TLS. Deze organisaties opereren bijna altijd op nationaal of internationaal niveau vanwege het belang van interoperabiliteit tussen regio's en landen. Voorbeelden zijn NIST, ETSI, IETF, TLS, IEEE, ISO/IEC, TCG, ANSI, W3C en ENISA.



Aanbieders van cryptografische infrastructuur

Organisaties die **cryptografische infrastructuur ontwikkelen, implementeren of onderhouden die door andere bedrijven kan worden gebruikt**. Deze organisaties opereren veelal op nationaal of internationaal niveau. Voorbeelden zijn aanbieders van beveiligingsbeheer en ontwikkelaars van cryptografische libraries.



Aanbieders van cryptografie die verder gaat dan veilige communicatie

Organisaties die **infrastructuur ontwikkelen, implementeren of onderhouden op basis van cryptografische protocollen die worden gebruikt voor doelen die verder gaan dan veilige communicatie**. Van belang is dat dit soort cryptografie niet noodzakelijk sterkere veiligheidsgaranties oplevert. De door deze organisaties ontwikkelde cryptografische protocollen worden voor verschillende doelen gebruikt en kunnen op verschillende principes zijn gebaseerd. Voorbeelden van zulke protocollen zijn blockchain, Zero-Knowledge Proofs, Multi-Party Computation en Idemix. Deze persona wordt apart vermeld omdat de ontwikkelde cryptografie dermate kan verschillen dat deze organisaties andere maatregelen moeten treffen dan bij meer standaard cryptografische functionaliteiten. Aangezien deze vormen van cryptografie vaak relatief recent praktisch geworden zijn, zijn de meeste organisaties van deze persona momenteel start-ups die een van de genoemde technieken gebruiken voor specifieke use-cases.

2.1.4 Persona's bepalen

In deze sectie wordt uitgelegd hoe een organisatie haar persona('s) kan bepalen.

Niveaus van cryptografie

Over het algemeen zijn er drie niveaus van cryptografie waarvoor een organisatie verantwoordelijk is, namelijk 1) haar eigen cryptografische infrastructuur; 2) haar cryptografische kennis; 3) de cryptografische infrastructuur voor het leveren van diensten of producten aan andere organisaties.

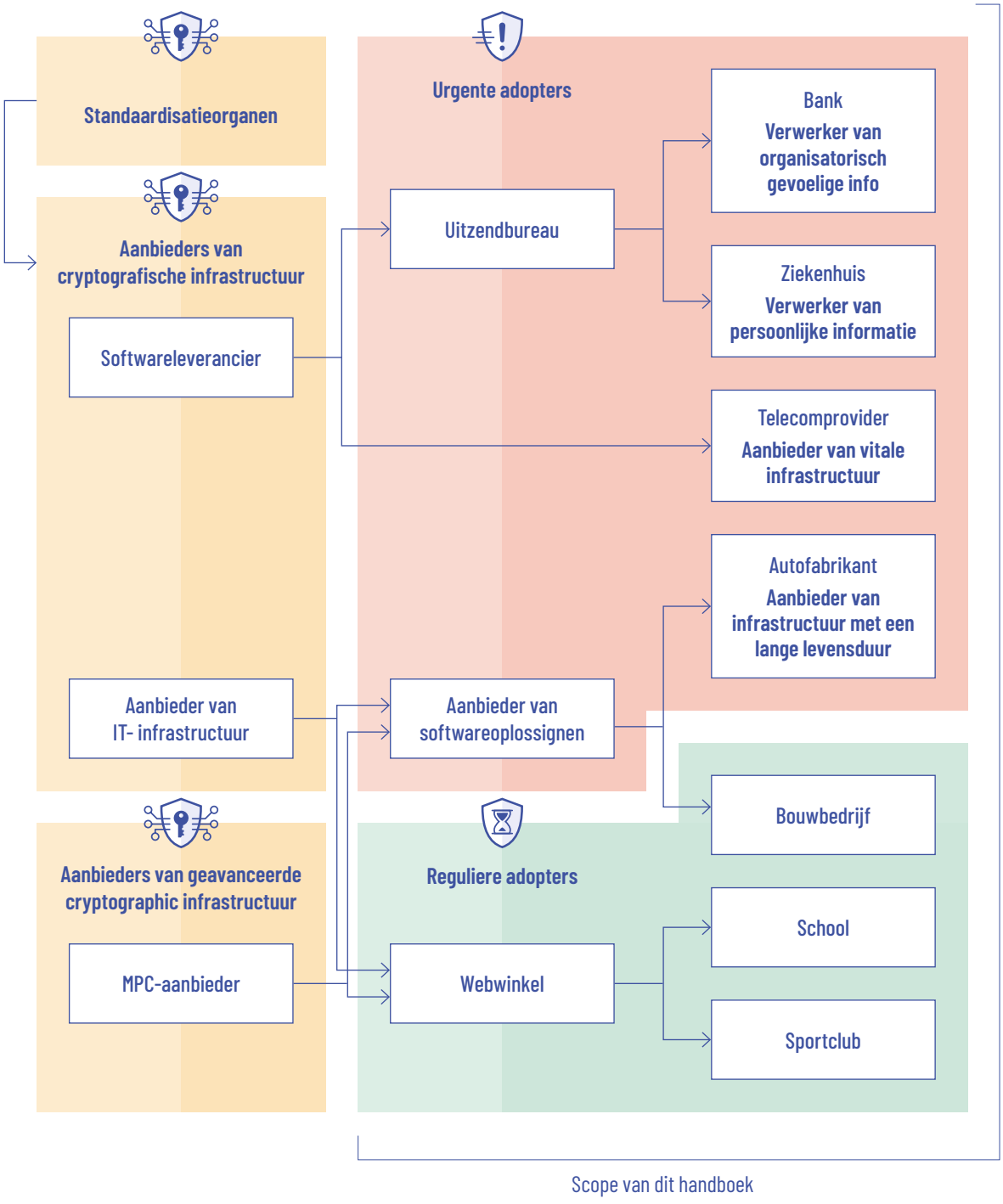
Er dient rekening gehouden te worden met elk van deze drie niveaus bij de migratie naar PQC en het beïnvloedt daarom welk type persona een organisatie is. Niveau 3 wordt apart behandeld omdat aanvallen op deze leverende organisatie via zogenaamde supply-chain aanvallen kunnen doorwerken naar de organisaties aan wie zij leveren. Een supply-chain is een keten van organisaties waarbij elke organisatie levert aan de volgende organisatie in de keten. Een voorbeeld van bepaalde organisaties die een supply-chain vormen, is te vinden in figuur 2.1.

In dit diagram geven de pijlen aan dat organisaties aan elkaar leveren (bijv. de software leverancier levert aan het wervingsbureau en de telecomprovider). Aanvallen op organisaties hoger in de supply-chain kunnen ook een risico vormen voor organisaties verderop in de supply-chain. Een voorbeeld van een supply-chain aanval is de SolarWinds hack in 2020. Bij deze aanval plaatsten hackers een kwaadaardige code in een van de producten die door softwarebedrijf SolarWinds werd aangeboden. Na deze toevoeging verzond SolarWinds (zonder het te weten) deze als een update naar duizenden organisaties, waaronder grote multinationals en de Amerikaanse overheid, zodat de hackers vervolgens toegang kregen tot data, netwerken en systemen. Voorbeelden van leveranciers zijn IT/softwareleveranciers zoals Microsoft en IBM, cloudproviders en antivirus/IDS-leveranciers.

De persona bepalen

Bij het bepalen van haar persona moet een organisatie rekening houden met alle drie de hierboven genoemde niveaus van cryptografie. Ten eerste moet het zijn eigen infrastructuur overwegen om met één of meer geschikte persona('s) te komen. Ten tweede kan een organisatie zich identificeren als bepaalde persona's vanwege de cryptografische kennis die het bezit. Dit resulteert in een cryptografie-experts persona. Ten slotte erft een organisatie dezelfde persona als alle organisaties waaraan het levert, omdat het dezelfde

adviezen moet volgen als de organisaties waaraan het levert. Anders vormt het een te groot risico voor de organisaties waaraan het levert. Dit erven van persona's gaat zelfs verder in de supply-chain, wat betekent dat een organisatie alle persona's erft van organisaties die lager in de supply-chain staan. Als voorbeeld betekent dit dat in figuur 2.1 het wervingsbureau zowel een organisatorisch gevoelige als persoonlijke gegevensbeheerder is, de software leverancier ook een langlevende infrastructuurleverancier is, en de software provider zowel een organisatorisch gevoelige gegevensbeheerder, persoonlijke gegevensbeheerder als leverancier van kritieke infrastructuur is.



Figuur 2.1 | Visueel voorbeeld van organisaties met hun PQC-personas.

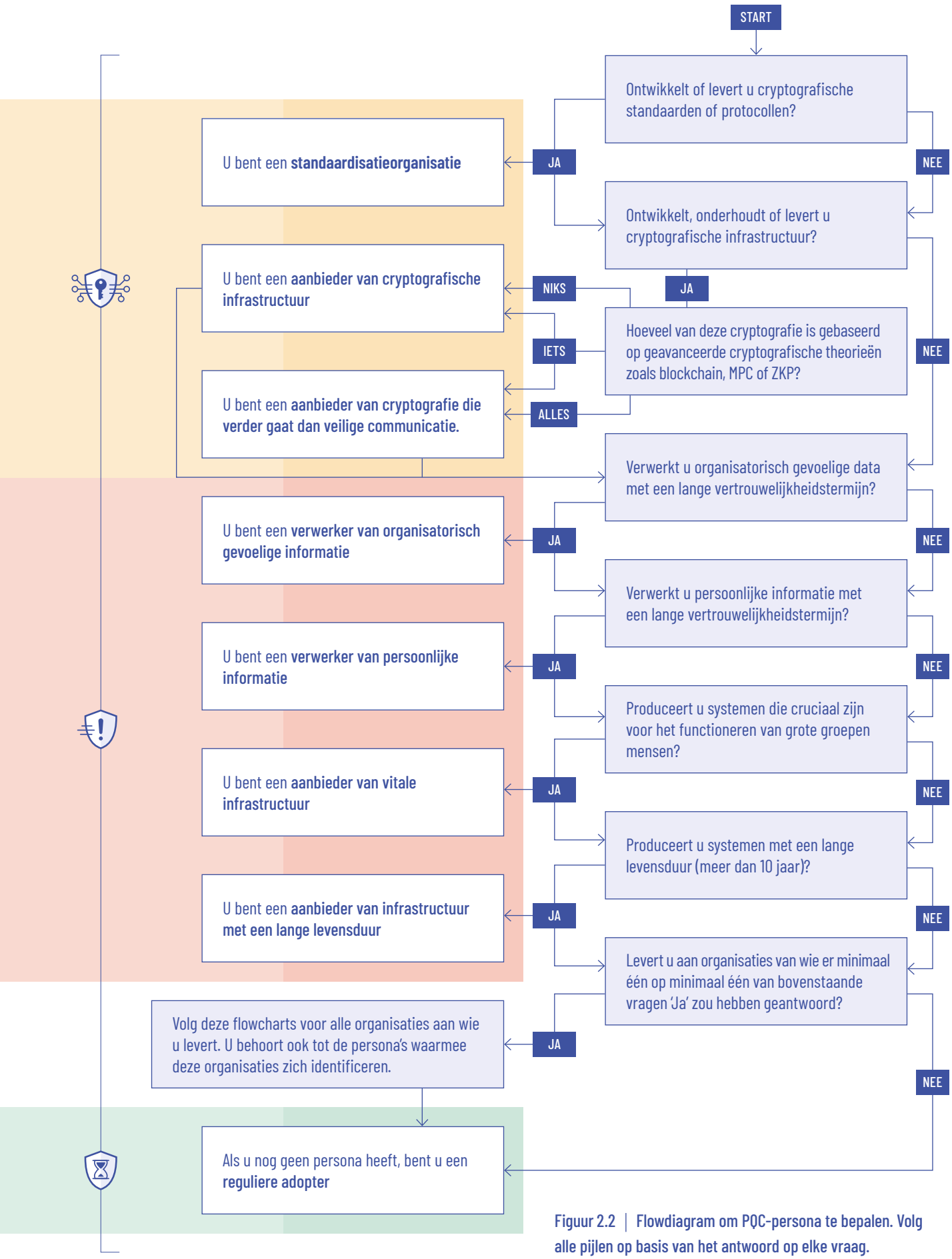
Door al deze persona's samen te nemen, zou elke organisatie zichzelf moeten kunnen identificeren als een urgente of reguliere adopter en mogelijk ook als een cryptografie-expert. Als een organisatie een urgente adopter is, kan het zich identificeren als meerdere van de subpersona's.
Daarnaast moet worden opgemerkt dat de persona('s) van een organisatie in de loop van de tijd kunnen veranderen, omdat de risico's waaraan zij worden blootgesteld in de loop van de tijd kunnen veranderen. We adviseren om zorgvuldig opnieuw te beoordelen als welke persona de organisatie identificeert en dit elke keer te herhalen als de organisatie nieuwe stappen zet in de PQC-migratie. We benadrukken ook dat sommige organisaties misschien denken dat ze reguliere adopters zijn, terwijl ze in de praktijk een urgente adopter zijn vanwege hun eigen cryptografische infrastructuur of de infrastructuur van een van de organisaties waaraan ze leveren. Daarom adviseren we organisaties om conservatief te zijn bij het bepalen van hun PQC persona. Op het grensvlak tussen een urgente of reguliere adopter wordt geadviseerd om het advies in sectie 3.2 te volgen, aangezien deze sectie verdere richtlijnen geeft over wanneer ze bepaalde componenten moeten migreren.
De beste manier om erachter te komen welke persona('s) van toepassing zijn op een organisatie of de organisaties waaraan ze leveren, is door de beschrijvingen van alle bovenstaande persona's te lezen en te zien welke beschrijving(en) van toepassing zijn op de relevante organisaties. Daarnaast is de flowchart in figuur 2.2 bedoeld als visuele hulp bij het bepalen van hun PQC persona('s).

Advies voor organisaties met meerdere persona's

Zoals hierboven vermeld, kunnen sommige urgente adopters tot meerdere subpersona's van urgente adopters behoren. Financiële instellingen zijn bijvoorbeeld zowel verwerkers van persoonlijke informatie als verwerkers van organisatorisch gevoelige informatie. Hoewel het advies in het volgende hoofdstuk hierdoor niet verandert, vormen de verschillende subpersona's wel een indicatie van de actiestappen waarop een organisatie zich meer dient te focussen. De eerste actiestappen (zie 'De diagnose van quantumkwetsbaarheid uitvoeren' in het volgend hoofdstuk) zijn identiek voor de verschillende subpersona's. Voor de vervolgstappen moet de diagnose duidelijk maken welk cryptografische systeem onder welke persona valt en dus welke actiestappen prioriteit hebben voor dit systeem.

Interoperabiliteit tijdens de PQC-migration

De PQC-migratie kan vaak niet door organisaties individueel worden uitgevoerd, vanwege afhankelijkheden tussen verschillende organisaties. Deze afhankelijkheid kan zowel op organisatorisch als op technisch niveau voorkomen. Coördinatie tussen deze organisaties is cruciaal tijdens de PQC-migratie om interoperabiliteit tussen verschillende organisaties te behouden. Dit kan op verschillende manieren gebeuren. Als een organisatie A direct afhankelijk is van een organisatie B, moet organisatie B migreren naar PQC-standaarden vóórdat organisatie A dit kan doen. Vaak zijn afhankelijkheden tussen organisaties niet zo lineair, maar vinden ze plaats in de vorm van een bepaalde netwerkstructuur. Als dit het geval is, moeten alle organisaties die betrokken zijn in deze netwerkstructuur hun PQC-migratie coördineren om zowel de interoperabiliteit als de veiligheid van hun data en systemen te waarborgen. Organisaties moeten dan rekening houden met alle PQC-persona's van de respectieve organisaties bij het uitvoeren van de PQC-migratie.
Voor aanbieders van cryptografie die verder gaat dan alleen veilige communicatie wordt benadrukt dat sommige veelgebruikte geavanceerde cryptografische protocollen niet quantumveilig zijn.



Figuur 2.2 | Flowdiagram om PQC-persona te bepalen. Volg alle pijlen op basis van het antwoord op elke vraag.

2.2 Diagnose van quantumkwetsbaarheid

Zodra een organisatie haar persona heeft vastgesteld, kan zij vaststellen of zij moet doorgaan met de migratie, met als eerste stap de diagnose van quantumkwetsbaarheid.

Urgente adopters

Organisaties die tot de urgente adopters behoren moeten zo snel mogelijk met hun PQC-diagnose aan de slag, zodat ze de migratie zo snel mogelijk kunnen realiseren. De rest van dit document is vooral bedoeld om dergelijke organisaties door het migratieproces te leiden.

Reguliere adopters

Tot reguliere adopters behorende organisaties hoeven nog niet te reageren op de quantumdreiging. Deze organisaties moeten er echter wél voor zorgen dat ze in een optimale conditie verkeren om in de toekomst te migreren. De volgende aanbevelingen zijn van toepassing.

Ten eerste moeten deze organisaties ervoor zorgen dat ze up-to-date zijn met de nieuwste beveiligingsrichtlijnen (bijvoorbeeld migreren van TLS 1.2 naar TLS 1.3) en de voorkeur geven aan crypto-agile oplossingen. Zie sectie 4.4. voor meer informatie over crypto-agility. Ze moeten daarnaast rekening houden met het feit dat toekomstige updates een impact zullen hebben op de prestaties van cryptografische algoritmes. Deze organisaties kunnen al beginnen met het uitvoeren van de risicoanalyse- en diagnosestappen van het migratieplan dat wordt beschreven in sectie 2.2.1.

Ten tweede moeten deze organisaties goed geïnformeerd blijven en de standaardisatieontwikkelingen volgen. Een paar jaar na de publicatie van de post-quantumnormen worden er naar verwachting nieuwe aanbevelingen aangekondigd die specifiek zijn gericht op deze organisaties, rekening houdend met de ontwikkelingen en lessen die zijn geleerd van urgente adopters. Tot slot willen sommige organisaties die als reguliere adopters worden geïdentificeerd proactief handelen en verder gaan met het toepassen van het migratieplan dat in deze handleiding wordt beschreven, met name door te beginnen met de quantumkwetsbaarheid diagnose. Er zijn verschillende redenen om dit te doen, waaronder: de organisatie staat op het punt om grote infrastructuurinvesteringen te doen; de organisatie verandert haar activiteiten of de organisatie heeft nieuwe klanten, waardoor de risicobeoordeling verandert. Hoe dan ook, deze stappen zullen op een gegeven moment moeten worden genomen, dus het kan geen kwaad om nu de eerste migratiestappen te starten.

Cryptografie-experts

Organisaties die als cryptografie-experts gelden, dienen ook te beginnen met het toepassen van de migratieaanbevelingen op de eigen infrastructuur. Omdat deze organisaties de leveranciers van cryptografische systemen zijn, vertrouwen alle andere actoren in de supply-chain op ze. Daarom moeten ze gereed zijn voor het implementeren van quantumveilige algoritmes zodra de standaarden beschikbaar zijn.

Cryptografie-experts dienen duidelijk met hun klanten te communiceren om de migratieplanning te vergemakkelijken voor organisaties waaraan ze leveren. Ze moeten daartoe voor elk van hun producten aangeven of het bestand is tegen quantumaanvallen. Als dat niet het geval is, moeten ze quantumveilige alternatieve oplossingen voorstellen en duidelijk aangeven wanneer ze van plan zijn dergelijke oplossingen aan te bieden.

2.2.1 De diagnose van quantumkwetsbaarheid uitvoeren

Nadat een organisatie heeft besloten om met de PQC-migratie aan de slag te gaan, bestaat de eerste stap uit het uitvoeren van een diagnose om de huidige situatie met betrekking tot de cybersecurity in de organisatie in kaart te brengen. In deze stap worden de benodigde data verzameld om te beslissen welke systemen als eerste moeten worden gemigreerd, de afhankelijkheden te identificeren en te anticiperen op de gevolgen van de migratie.
Let op dat een organisatie deze informatie niet per se in een bepaalde volgorde hoeft te vergaren. Zo kunnen verschillende soorten informatievergaring of beoordelingen in parallel uitgevoerd worden. Een organisatie kan er bijvoorbeeld voor kiezen om eerst een gedeeltelijke risicoanalyse uit te voeren en de eerste inventaris vervolgens alleen voor de hoog risico componenten in hun organisatie te doen.
Over het algemeen dient een organisatie te beschikken over de volgende informatie voor het opstellen van een geschikt migratieplan:

- Inventaris van alle cryptografische componenten die gebruikt worden in de organisatie;
- Inventaris van alle data die verwerkt wordt door de organisatie;
- Inventaris van alle leveranciers van cryptografische componenten;
- Risicoanalyse.

Inventaris van cryptografische componenten

Om de migratie uit te voeren, is het noodzakelijk om alle cryptografische componenten binnen een organisatie te identificeren, inclusief componenten die binnenkort de organisatie zullen binnenkomen. Richtlijnen voor het opstellen van een cryptografische inventaris zijn te vinden in sectie 2.3. Dit is een belangrijke stap om ervoor te zorgen dat alle componenten correct worden gemigreerd. Als één algoritme kwetsbaar blijft voor een quantumaanval, kan dit dienen als een toegangspunt voor een grotere aanval op het hele systeem. Daarom moet een organisatie streven naar een uitputtende lijst van alle gebruikte cryptografie, zowel software als hardware. De verzamelde informatie moet zo gedetailleerd mogelijk zijn, inclusief het algoritme, de sleutelgrootte, het gebruik, etc. De informatie zal worden gebruikt om te bepalen of een cryptografisch component kwetsbaar is voor quantumaanvallen en welke quantumveilige oplossing in plaats daarvan kan worden gebruikt. Voor componenten die niet door de organisatie zelf worden beheerd, moeten de leveranciers worden geïdentificeerd. Deze inventaris kan de vorm aannemen van een Configuration Management Database (CMDB). Eerdere cryptografische migraties hebben aangetoond dat het maken van een inventaris van cryptografische componenten het belangrijkste en moeilijkste deel van de diagnose is. Organisaties moeten er rekening mee houden dat deze stap aanzienlijk veel tijd in beslag zal nemen.
Daarnaast is een dergelijke inventaris buiten de scope van dit migratieproject ook nuttig. Het hebben van een volledig beeld van de exacte cryptografische algoritmes die worden ingezet, kan helpen bij het identificeren van kwetsbaarheden in het huidige systeem. Dergelijke kwetsbaarheden zijn verre van ongewoon en moeten worden verholpen. Daarom zal een goede inventaris van alle cryptografie helpen bij het verminderen van zowel quantum- als niet-quantumdreigingen. Bovendien kan het onderhouden van een cryptografische inventaris deel uitmaken van een meer algemeen cryptografisch beleid. Een cryptografische inventaris kan helpen bij het identificeren van niet-conform cryptografiegebruik. Daarbij komt wel dat vanwege de voortdurend veranderende aard van cryptografische landschappen, deze inventaris ook continu moet worden bijgewerkt. Bovendien is een dergelijk overzicht zeer gevoelig omdat het kwetsbaarheden van een organisatie bevat. Het is daarom van het grootste belang dat het goed beveiligd is en niet toegankelijk is voor onbevoegden.

Inventaris van data

Om een migratie te plannen, zal een lijst van de data die door een organisatie worden verwerkt helpen om goede beslissingen te nemen. In principe is een uitputtende lijst van de data niet noodzakelijk, maar een lijst van soorten gegevens, met in ieder geval de volgende informatie:

- Type data (data in rust, data in overdracht of data in gebruik);
- Locatie van de data;
- Waarde van de data (vertrouwelijkheid, beschikbaarheid);
- Classificatie van data;
- Risicobeoordeling voor elke dataverzameling.

Inventaris van cryptografische afhankelijkheden

Bij de meeste organisaties wordt een aanzienlijk deel van de cryptografische componenten (hardware en software) geleverd door externe leveranciers. Een groot deel van de migratie bestaat dan ook uit het ervoor zorgen dat leveranciers migreren en nieuwe quantumveilige oplossingen aanbieden, of anders om nieuwe leveranciers te vinden. Het doel van deze inventaris is om de cryptografie supply-chain te identificeren. Let daarbij op dat het wordt verwacht dat leveranciers niet altijd expliciet zullen zijn over hun (gebrek aan) ondersteuning voor PQC. Voor elke leverancier wordt aanbevolen om op te sommen welke producten er geleverd worden, of er lopende contracten met hen zijn en hoe contact met hen kan worden opgenomen. Deze lijst moet ook certificeringsinstanties omvatten. Naast de officiële leveranciers van cryptografische componenten moet een organisatie ook interne communicatiemiddelen (instant messaging, samenwerkingsplatforms) en schaduw IT overwegen. De organisaties waaraan wordt geleverd zullen een soortgelijke beoordeling van hun afhankelijkheden maken en kunnen vereisen dat een leverancier zijn intenties met betrekking tot PQC duidelijk communiceert. Voor de leverende organisatie is het niet noodzakelijk om een uitputtende lijst van alle klanten te maken, maar houd dit in gedachten bij het beslissen over een geschikte strategie.

Risicobeoordeling

Elke organisatie beoordeelt regelmatig het risico van aanvallen op haar IT-structuur en de mogelijke gevolgen (financieel, reputatie, juridisch, etc.). Richtlijnen voor het uitvoeren van een quantumrisicobeoordeling zijn te vinden in sectie 2.4. Het risico wordt beoordeeld op basis van verschillende parameters: de waarde van de informatie, de kwetsbaarheid en de dreiging. De eerste fase van de risicobeoordeling bestaat uit het herbeoordelen van het risico op de huidige IT-infrastructuur in het nieuwe scenario waarin een aanvaller toegang heeft tot een grootschalige quantumcomputer. De quantumdreiging heeft geen invloed op de waarde van de informatie: de waardevolle componenten blijven hetzelfde. Het creëert echter wel nieuwe kwetsbaarheden; informatie die werd beschermd door cryptografische algoritmes die als veilig werden beschouwd tegen niet-quantum aanvallers, is niet beschermd tegen quantumaanvallers. Bovendien moet men anticiperen op nieuwe dreigingen: aanvallers die zich richten op de nieuwe kwetsbaarheden die door deze situatie worden gecreëerd. Daarom moet het risico opnieuw worden beoordeeld. Een goede risicobeoordeling zal van vitaal belang zijn om te beslissen welke systemen als eerste moeten worden gemigreerd.

2.3) Cryptografisch componentbeheer

Het creëren van een inventaris van cryptografische componenten is essentieel voor een succesvolle diagnose en planning voor iedere organisatie die wil migreren naar post-quantum cryptografie. Asset management is een centraal onderdeel van het levenscyclusbeheer van software, hardware, diensten en artefacten. In het bijzonder is het onderhouden van cryptografische componenten belangrijk voor risicomanagement, incident response en compliance.

Het belang van het opbouwen van een cryptografische inventaris als eerste stap naar quantum-gereedheid wordt ook erkend door Europese [BSI22] en Amerikaanse instanties [CISA23; NIST21] evenals door internationale organisaties voor standaardisatie [ETSI20c; PCI22; GSMA24].

2.3.1 Cryptografisch beleid

Voordat een organisatie kan beginnen met cryptografische inventarisatie, is het essentieel om het cryptografisch beleid van de organisatie te identificeren en te begrijpen. Deze voorbereidende stap zorgt ervoor dat cryptografische taken in lijn zijn met wettelijke vereisten en organisatorische beveiligingsdoelen en definieert de rollen en verantwoordelijkheden met betrekking tot cryptografische taken. Cryptografisch beleid helpt bij:

- Het vaststellen van procedures voor sleutelgeneratie, distributie, opslag, vervanging en vernietiging;
- Het definiëren van de levenscyclus van cryptografische sleutels;
- Het definiëren van algoritmes en parameters voor gegevensversleuteling en gegevensintegriteit;
- Het bieden van mechanismen om authenticatie en autorisatie te waarborgen;
- Het bieden van richtlijnen om ongeautoriseerde gegevenswijziging te voorkomen;
- Het toestaan en verbieden van specifieke protocollen en protocolversies;
- Het specificeren van roadmaps en deadlines voor cryptografische migraties;
- Andere gerelateerde onderwerpen.

Begrijpen van wat nodig is om te voldoen aan regelgeving is een ander belangrijk aspect. Verschillende industrieën en regio's hebben specifieke regels en normen met betrekking tot gegevensbescherming. Deze normen fungeren als leidende principes voor hoe cryptografie wordt geïmplementeerd en beheerd binnen een organisatie. Bijvoorbeeld, financiële instellingen moeten mogelijk voldoen aan de Payment Card Industry Data Security Standard (PCI DSS) [PCI22], terwijl zorgverleners moeten voldoen aan de Health Insurance Portability and Accountability Act (HIPAA) [US96]. Organisaties in verschillende sectoren die gevoelige informatie verwerken, vooral die betrokken zijn bij IT-technologie, financiën, gezondheidszorg en softwareontwikkeling, voldoen vaak aan de ISO-27001-norm [ISO22a]. Daarnaast benadrukt de Algemene verordening gegevensbescherming (AVG) (Eng: General Data Protection Regulation (GDPR)) [EU16b] het gebruik van cryptografie om het risico te verlagen, met name in de context van datalekken, en verplicht het om geschikte technische en organisatorische maatregelen te nemen om de beveiliging van verwerkingssystemen en -diensten te waarborgen, inclusief het gebruik van cryptografie voor pseudonimiseren en anonimiseren. Ten slotte vereist de NIS2-richtlijn [EU22a] dat entiteiten degelijke cryptografische maatregelen implementeren om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te beschermen.
Het identificeren van cryptografisch beleid is een strategische benadering voor het creëren van een cryptografische inventaris. Ten eerste helpt het bij het prioriteren van componenten door duidelijk te definiëren wat bescherming nodig heeft en het niveau van bescherming dat vereist is. Ten tweede geeft het inzicht in de locatie van de componenten en helpt het bij het efficiënt lokaliseren. Het kennen van de specifieke plaatsen en contexten waarin cryptografische maatregelen nodig zijn maakt een gerichte en efficiënte inventarisatie mogelijk, wat tijd en middelen bespaart. Bovendien kan het nuttig zijn om gerelateerde onderwerpen tot cryptografie te identificeren, zoals gegevensclassificatie, ICT-risicomanagement, risicomanagement van derden en incidentrespons. Deze twee aspecten zullen ondersteunen bij het opstellen van een plan voor de volgende stap: het definiëren van een strategie voor cryptografische inventarisatie.

2.3.2 Vaststellen van een strategie voor cryptografische inventarisatie

Zodra het cryptografisch beleid is geïdentificeerd en vastgesteld, is de volgende stap het definiëren van een strategie voor cryptografische inventarisatie. Deze strategie dient als een gestructureerde aanpak voor het

identificeren, evalueren en documenteren van cryptografische componenten binnen een organisatie. Het definiëren van een dergelijke strategie kan in verschillende stappen worden gedaan, hoewel het nodig kan zijn deze aan te passen aan een specifieke organisatie:

1. **Definiëren van het doel** | Stel het doel vast van de inventarisatie van cryptografische componenten. Het doel kan zijn het waarborgen van naleving, het uitvoeren van onderhoud, het bijwerken van cryptografische maatregelen;
2. **Definiëren van scope** | Bepaal de type componenten die moeten worden gedocumenteerd en wat prioriteit heeft. Dit kunnen sleutels, metadata van cryptografische algoritmes en certificaten omvatten, afhankelijk van hun criticaliteit en wat relevant is voor de organisatie;
3. **Definiëren van inventarisatiemethodologie** | Identificeer de tools en technieken die moeten worden ingezet voor inventarisatie. Dit omvat het selecteren van geschikte tools, het bepalen van de systemen die moeten worden onderzocht en het verdelen van taken onder teamleden;
4. **Definiëren van data-analyse** | Specificeer het type informatie dat nodig is voor elk type component en het detailniveau dat benodigd is. Dit kan metrieken omvatten voor het evalueren van de effectiviteit, naleving en risico's die verband houden met ieder cryptografische component;
5. **Rapportage** | Stel vast hoe de verzamelde gegevens moeten worden geïnventariseerd en geanalyseerd. Definieer de vorm en de structuur voor het rapporteren van bevindingen, zodat de informatie op een duidelijke en bruikbare manier wordt gepresenteerd;
6. **Review** | Bepaal op welke manier en hoe vaak de inventaris moet worden herzien en bijgewerkt. Dit zorgt ervoor dat de cryptografische inventaris actueel en relevant blijft, en eventuele wijzigingen in componenten en beleid aanpakt.

Na het definiëren van een strategie kan het proces van het uitvoeren van de inventarisatie van cryptografische componenten in systemen beginnen.

2.3.3 Uitvoeren van cryptografische inventarisatie

Om een uitputtende cryptografische componenten inventarisatie te garanderen, is het cruciaal om alle diensten te lokaliseren die afhankelijk zijn van de principes van vertrouwelijkheid, authenticiteit, integriteit en onweerlegbaarheid (zie sectie 1.4). Deze diensten omvatten bijvoorbeeld instant messaging, cloudopslag, virtuele conferenties, veilige bestandsoverdracht, digitale zegels en handtekeningen op juridisch bindende contracten, banktransacties, toegangscontrole via smartcards (fysiek) of tokens in VPN (digitaal), authenticatiemechanismen zoals wachtwoordlogin en tweefactorauthenticatie, e-mailcommunicatie, elektronisch stemmen, IoT-beheer, OS-booting, software-updates en digitaal rechtenbeheer.
Een initiatief omtrent het ontdekken van cryptografische assets, het creëren en het beheren van een cryptografische inventaris wordt uitgevoerd door het National Cybersecurity Center of Excellence (NCCoE), dat de speciale publicatie [NCCoE23] heeft uitgebracht als een van de resultaten van het project Migration to Post-quantum Cryptography. In deze publicatie wordt het proces van het ontdekken van cryptografische assets onderzocht, en daarbij proberen ze de uitdagingen en mogelijke oplossingen te identificeren. Het rapport identificeert drie hoofddoelen waarin cryptografische componenten worden gebruikt en moeten worden gedetecteerd voor een uitputtende inventaris:

- Softwareontwikkeling;
- Operationele systemen en applicaties;
- Netwerkverkeer.

Softwareontwikkeling | Cryptografische softwarelibraries helpen softwareontwikkelaars bij het creëren en beheren van een breed scala aan cryptografische componenten. Dit varieert van het aanmaken en gebruiken van cryptografische sleutels tot het uitvoeren van versleutelings- en handtekeningalgoritmes, tot het beheren van wachtwoorden en tokens. Typische voorbeelden van cryptografische libraries die in softwareontwikkeling worden gebruikt, zijn OpenSSL [OpenSSL03], Bouncy Castle [BC24a], Libsodium [Libsodium13], Crypto++ [Dai23] en wolfCrypt [Wol24b].
Bij softwareontwikkeling wordt de inventarisatie uitgevoerd door te inspecteren welke cryptografische library vereist is en welke cryptografische functionaliteiten worden geïmporteerd en gebruikt in de ontwikkeling. Hoewel identificatie en inventarisatie van cryptografische operaties en/of cryptografische materialen (zoals sleutels, tokens en inloggegevens) handmatig in codeontwikkeling kunnen worden geïmplementeerd (bijvoorbeeld bij codebeoordeling), is dit proces foutgevoelig. Het is wenselijk om statische en/of dynamische analysetools te integreren in de software development life cycle in de ontwikkelomgeving en/of in de continuous integration/continuous development (CI/CD) pipeline om dit proces te automatiseren.

Operationele systemen en applicaties | Operationele systemen worden constant gebruikt om dagelijkse taken binnen een organisatie uit te voeren, zoals VPN-verbindingen, tweefactorauthenticatie (2FA), inloggen via inloggegevens, versleuteling en ontsleuteling van gegevens in rust (bijvoorbeeld gegevens in databases) en veilig opstarten en updaten van besturingssystemen. Deze diensten worden mogelijk gemaakt door het gebruik van uitvoerbare en niet-uitvoerbare cryptografische componenten.
Uitvoerbare componenten omvatten cryptografische software, firmware, hardware en softwarelibraries. Zelfs als een organisatie niet ontwikkelt met behulp van cryptografische libraries, zijn uitvoerbare cryptografische componenten nodig om hun activiteiten te ondersteunen. Een voorbeeld is de OpenSSL-library die is geïntegreerd in de meeste Linux-distributies en wordt ondersteund door onder andere CISCO AnyConnect, dat vaak wordt gebruikt in VPN-verbindingen voor werken op afstand.
Niet-uitvoerbare componenten zijn cryptografische gegevens die ofwel in rust zijn en worden bereikt via beveiligde protocollen zoals 2FA, of worden gebruikt of gegenereerd door de uitvoerbare componenten. Voorbeelden zijn persoonlijke inloggegevens, OpenPGP-sleutels, sleutelopslagplaatsen en X.509-certificaten.

Netwerkverkeer | Het is daarnaast mogelijk om te identificeren welk IT-component cryptografie gebruikt door netwerkverkeer te monitoren. Het is mogelijk om een netwerk scanning tool te gebruiken om te detecteren welk type cryptografische algoritmes en beveiligingsmaatregelen worden uitgewisseld en gebruikt. Communicatie kan plaatsvinden intern, in de cloud of via onbetrouwbare netwerken met entiteiten van buiten de organisatie. Elke laag van het OSI-model (van ISO) voor internetcommunicatie wordt beschermd door een beveiligd protocol, daarom is het essentieel om ze allemaal grondig te onderzoeken. Tabel 2.1 geeft een overzicht van voorbeelden van beveiligde protocollen voor elke laag van het OSI-model.
Sommige beveiligingsprotocollen werken op meer dan één niveau van het OSI-model. Dit hangt af van de verschillende toepassingen waarvoor deze protocollen worden gebruikt en het soms onduidelijke verschil tussen lagen 5, 6 en 7. Zo worden digitale certificaten in X.509-formaat bijvoorbeeld gebruikt om een HTTPS-verbinding in TLS op te zetten, wat werkt op niveau 6, maar ze kunnen ook worden gebruikt voor e-mail of documentondertekening en verificatie. Voor een meer diepgaand overzicht van de meest gebruikte protocollen kunt u sectie 4.3 raadplegen.
Het is van belang dat een geschikte tool wordt gebruikt om de relevante OSI-lagen van netwerkcommunicatie te onderzoeken en dat het gebruik van de scanner in de systemen is toegestaan. Een voorbeeld van hoe netwerkverkeer kan worden geïnspecteerd zijn verschillende open-source poortscanners zoals nmap [Lyo24] en testssl.sh [Wet24] alsmede netwerkscanners zoals Wireshark [Wir24] en tcpdump [Gro24] om TLS-verkeer te scannen. Deze tools kunnen helpen om een overzicht van het netwerk te creëren en te identificeren waar cryptografie wordt gebruikt. Vervolgens kan het combineren van deze netwerkanalyse met agent-based detectie zorgen voor een nauwkeuriger en volledig onderzoek.

Niveau	Laag	Toepassing	Beveiligde protocollen
7	Toepassing	PKI, Web of Trust, e-mail, webbrowsen	PGP, S/MIME, SSH, X.509
6	Presentatie	PKI	SSH, TLS, X.509
5	Sessie	PKI, FTP, wachtwoordauthenticatie	PAP, SMB, SSH, X509
4	Transport	TCP, UDP	QUIC
3	Netwerk	IP-routing, VPN	IPSec
2	Datalink	Wifi, ethernet	WPA3, MACsec
1	Fysiek	Kabel, golf	-

Table 2.1 | Beveiligde protocollen die in het OSI-model gebruikt worden voor communicatie.

2.3.4 Format van cryptografische inventaris: CBOM

Er zijn verschillende manieren om een cryptografische inventaris op te bouwen en te beheren, en de manier waarop deze wordt gecreëerd en beheerd moet passen bij een organisatie en hun gebruikssituatie. Het gebruik van een standaardformaat voor een cryptografische inventaris is echter wenselijk omdat het een meer gestroomlijnde manier biedt om een inventaris te creëren, te beheren en te analyseren; bijvoorbeeld, het kan niet alleen gemakkelijk worden beheerd door de organisatie zelf, maar ook door hun leveranciers en hun klanten. Deze functie voegt transparantie toe en voorkomt interoperabiliteitsproblemen tussen gebruikers en leveranciers.
De *cryptographic bill of materials* (CBOM) is een machinaal leesbaar standaardformat dat is gebaseerd op de bestaande *software bill of materials* (SBOMs) van CycloneDX [Cyc24]. CBOM's zijn bedoeld om zowel de gebruikte cryptografie vast te leggen, inclusief metadata over dit gebruik, als om afhankelijkheden tussen cryptografische algoritmes bij te houden, terwijl ze ook een middel bieden om een klassieke en quantumveiligheids-kwetsbaarheidsscore aan de gevonden componenten te koppelen. De standaard is ontwikkeld door IBM met als doel het creëren van een inventaris die gespecialiseerd is in cryptografische componenten. Sinds april 2024 worden CBOM's volledig ondersteund in versie 1.6 van de CycloneDX SBOMs [OWA24].
Een CBOM kan een zeer gedetailleerde en grondige cryptografische inventaris opleveren die elk type cryptografisch component opsomt: veilige protocollen, cryptografische algoritmes, cryptografische sleutels, cryptografische materialen zoals ciphertexts, handtekeningen, hashes, initialisatievectoren, tokens en artefacten zoals digitale certificaten, referenties, wachtwoorden en nog meer. Tabel 2.2 geeft enkele voorbeelden van het soort informatie dat beschikbaar is voor verschillende cryptografische componenten.

Component	Voorbeeld	Data
Protocol	TLSv1.2	versie, ciphersuite
Algoritme	AES-128-GCM, SHA512withRSA	soort primitieve (handtekening, versleuteling), parameters, *mode of operation*, *execution environment* (CPU-architectuur), NIST-veiligheidsniveau, functionaliteiten
Sleutel	RSA-2048 pub-key	soort sleutel (publiek/geheim), lengte, levensduur, status (actief, bedreigd), soort opslag (SW, HW)
Certificaat	X.509	ontvanger, uitgever, geldigheid, format, extensies, publieke sleutel, handtekening, etc.

Tabel 2.2 | Soort informatie dat in CBOM's kan voorkomen.

```
...
   {
         "type" "crypto-asset",
         "bom-ref" "oid1.3.18.0.2.32.104",
         "name" "tlsv12",
         "cryptoProperties" {
               "assetType" "protocol",
               "protocolProperties" {
                     "tlsCipherSuites"  [
                           "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519)",
                           "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519)",
                           "TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)",
                           "TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)"
                     ]
               }
         }
   }
...
   {
         "type" "crypto-asset",
         "bom-ref" "oid2.16.840.1.101.3.4.1.6",
         "name" "AES",
         "cryptoProperties" {
               "assetType" "algorithm",
               "algorithmProperties" {
                     "variant" "AES-128-GCM",
                     "primitive" "ae",
                     "mode" "gcm",
                     "implementationLevel" "softwarePlainRam",
                     "implementationPlatform" "x86_64",
                     "certificationLevel" "none",
                     "cryptoFunctions" ["keygen", "encrypt", "decrypt", "tag"]
               },
               "classicalSecurityLevel" 128,
               "nistQuantumSecurityLevel" 1
         }
   }
...
```

Figuur 2.3 | Voorbeeld van een CBOM.

In figuur 2.3 wordt een fragment van een CBOM getoond dat geconstrueerd is uit de webserver *nginx* en gepubliceerd door IBM [IBM24]. In dit voorbeeld worden het protocol TLS v1.2 en de cryptografische primitieve AES-128-GCM vermeld als cryptografische componenten van nginx.
Daarnaast zijn CBOM's zo gestructureerd dat het mogelijk is om afhankelijkheden van cryptografische componenten bij te houden. De CBOM in het voorbeeld van zo-even beschrijft dat TLS v1.2 en AES-128-GCM zijn gedetecteerd; figuur 2.4 laat zien hoe deze componenten van andere afhangen. De officiële gids [OWA24] geeft meer en gedetailleerdere voorbeelden van hoe CBOM's zijn gestructureerd.
Hoewel het CBOM-formaat dergelijke informatie kan opslaan, is er geen garantie dat al deze gegevens ook daadwerkelijk worden aangeleverd door de scanningtools die CBOM's produceren. Deze tools hebben vaak moeite met het in kaart brengen van alle afhankelijkheden en het identificeren van specifieke elementen zoals *IV*'s, *nonces* en wachtwoorden. Een andere noemenswaardige beperking van CBOM's is het feit dat ze geen procedures rondom sleutelbeheer vastleggen (bijv. hoe een sleutel wordt gegenereerd, geladen en opgeslagen). Ook richten de bestaande velden zich vooral op cryptografische componenten die in software zijn ontdekt en minder op netwerkverkeer.

```
...
   {
         "ref" "TLS v1.2",
         "dependsOn" [
               "libcrypto.so"
         ],
         "dependencyType" "uses"
   },
   {
         "ref" "libcrypto.so",
         "dependsOn" [
               "AES-128-GCM",
               "SHA256", "
               HMAC-DRBG"
         ],
         "dependencyType" "uses"
   },
...
```

Figuur 2.4 | Afhankelijkheden zoals weergegeven in een CBOM.

2.3.5 Tools voor cryptographische inventarisatie

Het inventariseren van componenten, het analyseren van inventarissen en het verhelpen van mogelijke dreigingen zijn drie belangrijke aspecten voor tools die werken met cryptografische componenten. Inventarisatie helpt bij het identificeren van alle cryptografische componenten om ervoor te zorgen dat zwakke algoritmes en kwetsbaarheden niet over het hoofd worden gezien. In de daaropvolgende inventaris analysefase worden deze elementen beoordeeld op zwakke punten, naleving van het huidige beleid en potentiële risico's. Remediëring pakt geïdentificeerde problemen aan en versterkt het systeem tegen mogelijke aanvallen.
Houd er rekening mee dat om een optimale levenscyclusbeheer van componenten te waarborgen de inventarisatie-, analyse- en remediëringstappen deel uitmaken van een continu proces waarbij het nodig is om regelmatig opnieuw te beoordelen en updates uit te voeren om potentiële bedreigingen tijdig te mitigeren.
Daarnaast wordt het beste resultaat bereikt wanneer automatische tools voor cryptografische inventarisatie worden gebruikt in combinatie met handmatige taken; het is essentieel om sanity checks uit te voeren op de uitkomst van de tools en te zien of de uitkomst van dergelijke tools in lijn is met de strategie die is gedefinieerd voor het inventarisatieproces. Bovendien kunnen tools geen inzicht geven in alle beveiligingsmaatregelen die elders zijn genomen voor gegevensopslag of sleutelgeneratie.
Een ander voorbeeld van een tekortkoming van tools is het analyseren van geïsoleerde systemen zoals *hardware security modules* (HSM's) en *trusted execution environments* (TEE's) waar geen scanning mogelijk is. Daarnaast kunnen deze tools geen verbanden leggen tussen verschillende cryptografische elementen: bijvoorbeeld een link tussen een digitaal certificaat en het bijbehorende sleutelpaar.
Naast dat het belangrijk is om tools te gebruiken die een cryptografische inventaris creëren, moet een inventaris ook beheerd worden zodat actie kan worden ondernomen. Zodra een goed beeld van de cryptografische componenten is vastgesteld, kunnen de benodigde acties worden bepaald. Het is goed om te onthouden dat ook het rapporteren niet volledig kan worden geautomatiseerd. Hoewel tools kunnen helpen bij het creëren en onderhouden van de cryptografische inventaris door de juiste gegevens en initiële analyse te verstrekken, is handmatige inspanning belangrijk om de rapporten te interpreteren, de context te begrijpen en de juiste acties te bepalen.
Er zijn verschillende open-source en afgeschermde tools beschikbaar om te helpen bij het starten met een cryptografische inventaris. Een onvolledig overzicht van tools die worden gebruikt in het NCCoE-onderzoek kan gevonden worden in de eerder genoemde NCCoE-publicatie [NCCoE23].

Integratie van CBOM's

Een noemenswaardig voorbeeld van het integreren van CBOM's in open-source diensten is in Github. In december 2023 kondigde Github aan dat CodeQL kan worden gebruikt om CBOM's te creëren [Cha23]. CodeQL is een statische code-analyse-engine die code gehost op Github analyseert op beveiligingskwetsbaarheden. Statische analysetools worden gebruikt om broncode te scannen zonder de code uit te voeren. Dergelijke tools worden gebruikt in codeontwikkeling om de codekwaliteit in de gaten te houden en mogelijke beveiligingsproblemen op te sporen. CodeQL kan worden gebruikt om cryptografische componenten in software te vinden. Voor elk cryptografisch component dat CodeQL vindt, rapporteert het de exacte locatie in de broncode. Een open-source tool om de output van CodeQL om te zetten in een geldige CBOM, genaamd CryptoBOM-forge, is te vinden op GitHub [Res24].

2.4) Quantumrisico-beoordeling

Nadat een organisatie een goed beeld heeft van de cryptografie die ze gebruiken in hun (belangrijkste) systemen, is de volgende stap het beoordelen van het risico van quantumcomputers voor deze systemen. In dit hoofdstuk wordt een concreet stappenplan gegeven voor het uitvoeren van een quantumrisico-beoordeling. Dit hoofdstuk helpt bij het kwantificeren van de risico's van verschillende systemen en het prioriteren van welke systemen als eerste moeten worden gemigreerd. Let op dat de methodologie specifiek bedoeld is voor risico's met betrekking tot cryptografie; andere potentiële risico's voor organisaties geïntroduceerd door quantumcomputers vallen buiten de scope. Dit hoofdstuk is grotendeels gebaseerd op de inhoud van de publicatie "Quantum Risicomethodologie voor cryptografie" door TNO in 2024 [dVBDvV24].
In deze sectie gaan we ervan uit dat er al een cryptografische inventaris is gemaakt, of dat de informatie over de cryptografische componenten die nodig zijn voor het uitvoeren van deze risicobeoordeling gemakkelijk kan worden verkregen. Concreet bestaat het quantumrisico uit drie componenten:

- De **quantumkwetsbaarheid** van de cryptografie die wordt gebruikt op systeem- of applicatieniveau. Dit wordt beoordeeld op basis van de sterkte van de bekende quantumaanvallen;
- De verwachte **impact** van een quantumaanval op het systeem. Dit is gebaseerd op de gevolgen als de cryptografie zou worden gebroken, rekening houdend met het doel waarvoor de cryptografie wordt gebruikt;
- De geschatte **tijd en moeite** die nodig is om naar post-quantum cryptografie te migreren. De schattingen zijn voornamelijk gebaseerd op bekende uitdagingen in de migratie en ervaringen van eerdere cryptografische migraties.

In de volgende secties worden concrete stappen beschreven om te beoordelen met welke aanvallers rekening gehouden moeten worden en ieder van de drie componenten van het quantumrisico. Ten slotte worden in de laatste sectie deze componenten tot één risicoscore tussen 0 en 4 gecombineerd, die kan worden gebruikt in een PQC-migratieplan of algemene processen voor risicomanagement.

2.4.1 Realistische aanvallers met quantumcomputers

Voordat een (quantum)risico-beoordeling kan worden uitgevoerd, moet een organisatie identificeren welke aanvallers realistisch gezien de organisatie zullen aanvallen. Voor de quantumrisico-beoordeling gaan we ervan uit dat een aanvaller geïnteresseerd is in het aanvallen van de organisatie als geheel, en niet specifieke systemen van de organisatie.

Momenteel verwachten experts dat er een realistische dreiging is van quantumcomputers binnen 10-20 jaar, waarbij de voorspelde waarschijnlijkheid toeneemt van 25% over 10 jaar tot meer dan 60% over 20 jaar[MP23]. Aangezien quantumcomputers in het begin erg duur zullen zijn, is het aannemelijk dat voornamelijk statelijke actoren of zeer gemotiveerde en capabele aanvallers ze zullen gebruiken om cryptografische infrastructuren aan te vallen. Hun motivatie zal voornamelijk politiek, militair en economisch van aard zijn, bijvoorbeeld gericht op het veroorzaken van verstoringen en het verzamelen van inlichtingen over andere bevolkingen. Deze dreigingen zijn daarom het meest relevant voor organisaties met een reeds bestaande dreiging van statelijke actoren, met name van cybermachten. Bovendien zijn organisaties die vitale infrastructuur leveren of beheren of die waardevolle geheimen hebben die meer dan 10 jaar veilig moeten blijven, in scope.
Bij twijfel kunt u het nationale dreigingslandschap van uw nationale inlichtingen- of cybersecurityorganisaties raadplegen. In het jaarverslag 2023 van de Nederlandse inlichtingendienst (AIVD) worden dergelijke voorbeelden van doelwitten van staten gegeven [AIVD23]. Ze waarschuwen onder andere expliciet overheden, de defensie-industrie en prominente technologiebedrijven voor de constante dreiging van spionage. Specifiek over de dreiging van statelijke actoren werd in 2022 een document gepubliceerd door de AIVD, de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) [NCTV22].
Aangezien quantumcomputing naar verwachting grotendeels via de cloud beschikbaar zal zijn, zal de stap van statelijke actoren naar andere gemotiveerde aanvallers naar verwachting kort zijn. In dit geval zullen aanvallers met bijvoorbeeld een financieel doel ook quantumaanvallen kunnen uitvoeren die hen in staat stellen geld te stelen of commercieel gevoelige informatie te verkrijgen. Hoewel (quantum) cloud-gebaseerde aanvallen enkele jaren extra in de toekomst liggen en duur zullen zijn voor een aanvaller, betekent dit uiteindelijk dat elke organisatie die te maken heeft met gemotiveerde aanvallers deze dreiging zal ondervinden binnen een decennium van degenen die te maken hebben met statelijke actoren. Dit betekent dat als ze kwaadaardige actoren als bedreigingen hebben, het slechts een kwestie van tijd is voordat deze actoren ook deze kwetsbaarheden kunnen uitbuiten. Vanwege de exploitatiekosten zullen voornamelijk grote multinationals, organisaties die werken aan hightech of innovatieve oplossingen, of andere doelen met hoge opbrengsten risico lopen.

2.4.2 Quantumkwetsbaarheid

We verdelen de kwetsbaarheid van cryptografische algoritmes die in een applicatie worden gebruikt in drie verschillende *quantumkwetsbaarheid*-scores:

0: Het algoritme is quantumveilig en hoeft met de huidige kennis niet te worden gemigreerd.

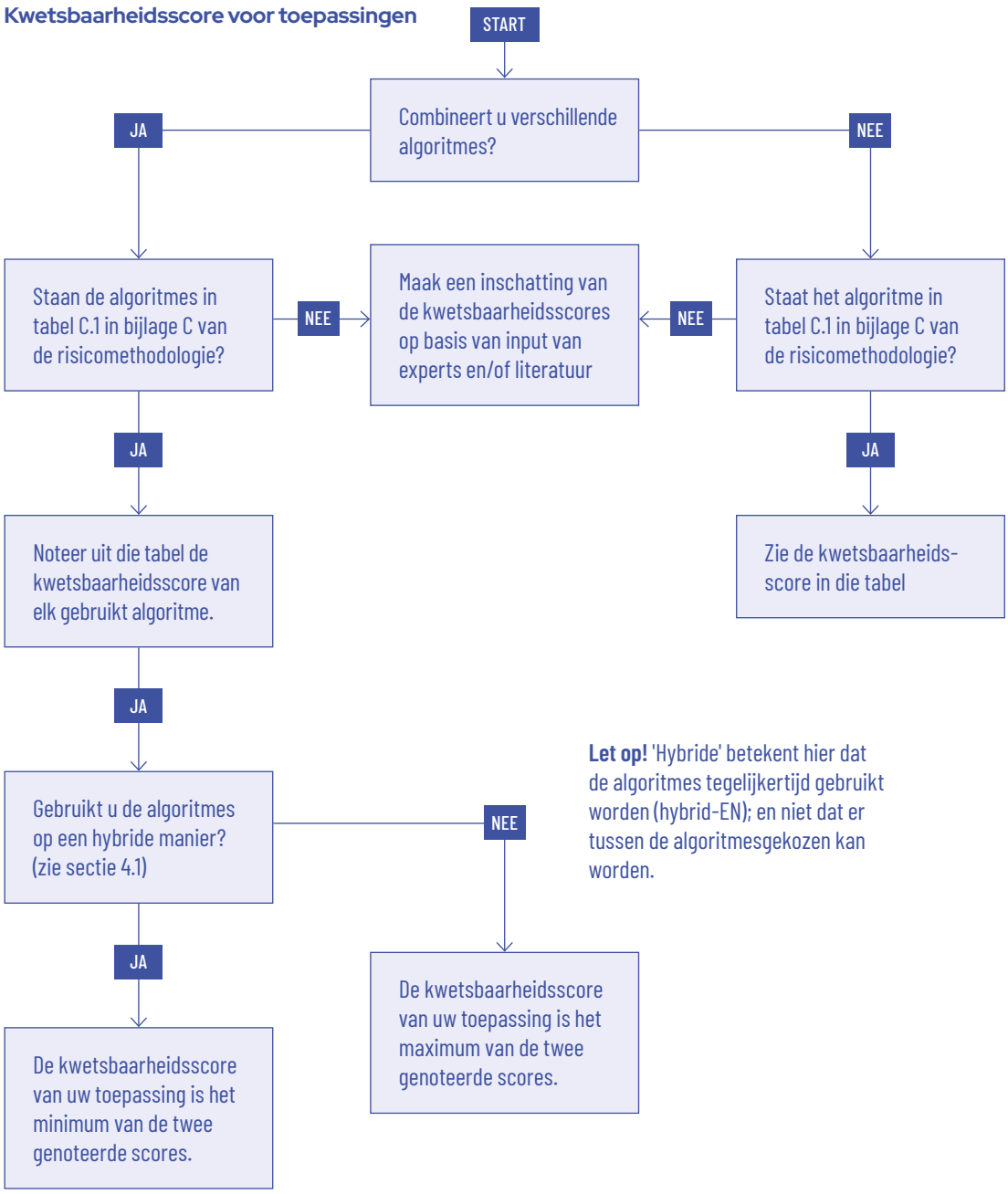
1: Het algoritme loopt (nog) geen gevaar om door een quantumcomputer te worden gebroken, maar zal in de toekomst aandacht nodig hebben. Een prominent voorbeeld hiervan zijn symmetrische algoritmes en hashfuncties. Er zijn quantumaanvallen tegen sommige van deze primitieven bekend, maar deze worden in de nabije toekomst niet als praktisch uitvoerbaar beschouwd.

2: Het algoritme is niet veilig tegen quantumcomputers en moet worden vervangen door een quantum-safe alternatief

Een lijst van veel voorkomende cryptografische algoritmes en hun quantumkwetsbaarheid-scores is te vinden in [dVBDvV24, Bijlage C].

Quantumkwetsbaarheid op applicatieniveau

In de praktijk worden verschillende cryptografische algoritmes vaak gecombineerd om één cryptografische oplossing te vormen. Zo laat het protocol TLS gebruikers een keuze te maken uit een lijst van verschillende cryptografische algoritmes om een bepaalde sessie te beschermen en gebruikt het publieke sleutel-cryptografie om een sleutel voor een symmetrisch algoritme op te zetten. In deze voorbeelden is de quantumkwetsbaarheid op applicatieniveau in feite de hoogste kwetsbaarheidsscore van alle algoritmes. Intuïtief kan een aanvaller namelijk simpelweg het zwakste cryptografische algoritme kiezen om het systeem aan te vallen. Alleen in het geval dat een hybride-EN constructie wordt gebruikt, waarbij meerdere cryptografische algoritmes in lagen worden gebruikt, is de kwetsbaarheidsscore op applicatieniveau het *minimum* van de kwetsbaarheidsscores van de individuele algoritmes.



Figuur 2.5 | Flowdiagram om de quantumkwetsbaarheidsscore van een systeem te vinden.

In figuur 2.5 staat een flowdiagram om organisaties te helpen bij het vinden van de quantumkwetsbaarheid van een systeem. Let op dat dit flowdiagram combinaties van algoritmes beoordeelt die worden gebruikt om één netwerkverbinding (of iets vergelijkbaars) te beschermen. Als één applicatie cryptografie gebruikt om twee verbindingen te beschermen, moet het flowdiagram voor beide verbindingen afzonderlijk worden gevolgd.

2.4.3 Impactanalyse

Het doel van de *impactscore* is om te meten hoe groot de gevolgen zijn voor een organisatie in het geval dat de cryptografie van een systeem wordt gebroken. Om de impactanalyse uit te voeren, is het belangrijk om te beoordelen of het realistisch is dat een aanvaller de organisatie zou aanvallen.
De verwachte impact wordt opnieuw verdeeld in drie niveaus (1, 2 en 3). Merk op dat we nu beginnen bij 1 in plaats van 0, aangezien er altijd enige vorm van impact zal zijn als een systeem wordt gecompromitteerd.
Figuur 2.6 kan worden gebruikt om de verwachte impact te beoordelen in het geval dat de cryptografie van een systeem wordt gebroken. De intuïtie achter ieder niveau is als volgt:

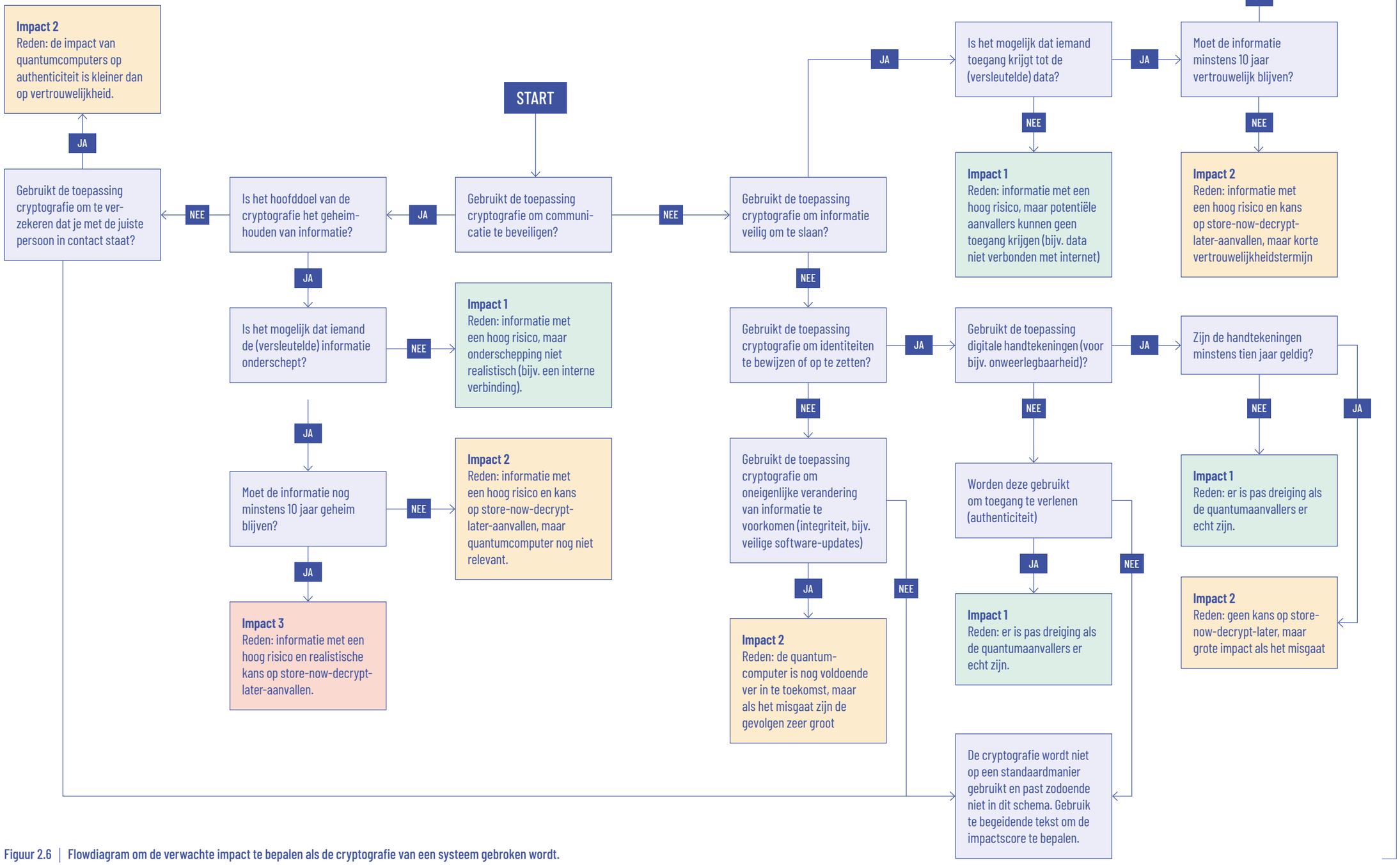
1: Er is geen significante impact die aandacht vereist. Dit is bijvoorbeeld het geval als de cryptografie geen gevoelig systeem beschermt, als de dreiging meer dan tien jaar in de toekomst is, als er geen realistische aanvaller voor het systeem bekend is, of wanneer er reeds andere veiligheidsmaatregelen zijn getroffen.

2: In dit geval bestaat er een realistische aanvaller die impact kan maken, maar niet op de korte termijn. Bijvoorbeeld: gevoelige gegevens die weliswaar in versleutelde vorm kunnen worden onderschept, maar niet meer relevant zijn wanneer ze kunnen worden ontsleuteld. Een ander voorbeeld is een systeem dat een hoog risico is voor het bedrijf, bijvoorbeeld het verifiëren van identiteiten of het beveiligen van de software-updates die mensen installeren. In deze gevallen is er een hoog risico en een grote kans op een aanval op het systeem wanneer een quantumcomputer beschikbaar is.

3: Ten slotte wordt de hoogste impactscore gegeven wanneer de impact al zo groot is dat er onmiddellijk op gehandeld moet worden. Dit is het geval als er een realistische aanvaller is die nu berichten kan onderscheppen die nog steeds gevoelig zijn wanneer zodra een cryptografisch relevante quantumcomputer werkelijkheid wordt. Het gaat dan om gegevens die nog steeds een significante impact hebben op organisaties of individuen over tien tot twintig jaar. Voorbeelden hiervan zijn staatsgeheimen, intellectueel eigendom, vertrouwelijke contracten en speciale persoonlijke informatie.

Let op: de impactscore is altijd een momentopname van de huidige situatie. De impact kan veranderen als de gevoeligheid van de applicatie of de tijdslijn voor een relevante quantumcomputer verandert. Bovendien kan het veranderen als het systeem wordt bijgewerkt. Daarom wordt geadviseerd om de risicobeoordeling periodiek te herhalen als onderdeel van de reguliere aanpak rondom risicomanagement.

Impactscore voor toepassingen



Figuur 2.6 | Flowdiagram om de verwachte impact te bepalen als de cryptografie van een systeem gebroken wordt.

2.4.4 Migratiemoeite

Tot slot is het belangrijk om in te schatten hoeveel inspanning en tijd de migratie naar post-quantumcryptografie zal kosten en hoeveel onvoorziene uitdagingen kunnen worden verwacht. Deze sectie richt zich alleen op het inschatten van de tijd die nodig is om naar PQC te migreren. In de praktijk is er meer van belang voor een succesvolle PQC-migratie, zoals personeel en financiële middelen. Voor richtlijnen over het inschatten van deze middelen verwijzen we naar hoofdstuk 3. De *migratiemoeite-score* kan net als de vorige scores drie waarden aannemen:

1: Er worden geen grote uitdagingen verwacht en de tijd om een systeem volledig naar PQC te migreren wordt geschat op maximaal twee jaar.

2: De migratie is niet eenvoudig, maar er worden ook geen grote hindernissen verwacht. De verwachte tijd om te migreren is maximaal 8 jaar.

3: De migratie wordt moeilijk en het is moeilijk te voorspellen welke uitdagingen er verwacht worden. Dit is bijvoorbeeld het geval als er veel afhankelijkheden zijn, er een gebrek aan prioriteit is, het systeem fysiek moeilijk te bereiken is of als er vertragende andere factoren spelen. In dit geval zal de migratie naar PQC meer dan 8 jaar duren.

De moeite voor het migreren naar PQC hangt af van veel factoren, die sterk variëren per organisatie. Daarom is er geen algemene manier om tot een migratiemoeite-score te komen en moet de organisatie dit zelf beoordelen. In het de rest van dit hoofdstuk worden veelvoorkomende factoren beschreven die een organisatie kunnen helpen bij het beoordelen van de migratiemoeite.

Volwassenheid van beheer binnen de organisatie | Organisaties die een goed levenscyclusbeheer hebben, zoals een up-to-date inventaris van hun software, cryptografie en certificaten, zullen gemakkelijker de cryptografische componenten kunnen vinden en migreren die moeten worden gemigreerd

Afhankelijkheid van standaardisatie en wetgeving | Soms kunnen organisaties niet zelf migreren omdat ze gebonden zijn aan bepaalde regelgeving of gedwongen zijn een gestandaardiseerd algoritme te gebruiken. Deze processen kunnen lang duren en organisaties hebben hier vaak geen invloed op. Aan de andere kant kan regelgeving ook de adoptie van PQC versnellen.

Afhankelijkheid van externe leveranciers | Veel organisaties zullen software of hardware van externe leveranciers gebruiken. Dit kan de migratie versnellen als de leverancier al werkt aan PQC-oplossingen, in dat geval kan de organisatie zich zelf concentreren op hoe de uiteindelijke update soepel kan worden uitgevoerd. Aan de andere kant werkt een leverancier mogelijk niet aan PQC, bijvoorbeeld vanwege een gebrek aan prioriteit, omdat de software niet langer wordt onderhouden of de leverancier niet langer bestaat. Ook compatibiliteit tussen verschillende systemen die door verschillende organisaties worden beheerd, zal een belangrijke factor zijn die de PQC-migratie vertraagt.

Afhankelijkheid van externe hardware | Vaak wordt hardware gebruikt om cryptografische processen te versnellen of te beheren. Zo worden *hardware security modules* (HSM's) bijvoorbeeld vaak gebruikt om cryp-

tografische sleutels te maken en te beheren. De HSM moet het PQC-algoritme eerst ondersteunen voordat een andere applicatie het algoritme kan gebruiken. Ook wordt er speciale hardware gebruikt om cryptografische operaties te versnellen. Als deze hardware het PQC-algoritme niet ondersteunt, kan dit een aanzienlijke impact hebben op de snelheid van het systeem. In dat geval moet nieuwe hardware worden geïnstalleerd, wat tijd en geld kost of zelfs onmogelijk kan zijn in bepaalde omgevingen in de OT (Operationele Technologie).

Beperkingen in hardware | Vergelijkbaar met hardware-afhankelijkheden, kunnen de bandbreedte, opslag, snelheid en de ondersteunde bewerkingen ook de moeite vergroten die nodig is om naar PQC te migreren. De PQC-algoritmes zullen andere vereisten hebben in vergelijking met de huidige algoritmes. Low-end apparaten kunnen moeite hebben om hieraan te voldoen. Voorbeelden zijn smartcards, IoT-apparaten, OT-systemen en high-end systemen die veel cryptografische bewerkingen uitvoeren, zoals bedrijfsnetwerkapparaten.

Software in eigen beheer | Als een applicatie of systeem zelf wordt beheerd, moet de vereiste expertise in huis zijn om het systeem naar PQC te migreren. Als dit het geval is, kan de tijd om te migreren aanzienlijk afnemen. Aan de andere kant kan het een grote hindernis zijn als een organisatie de expertise niet heeft.

2.4.5 Quantumrisico-scores

Als laatste stap worden de drie individuele scores gecombineerd tot één *quantumrisico-score* tussen 0 en 4. De quantumrisico-score verwijst naar de systemen in de organisatie. De quantumrisico-scores worden gedefinieerd in figuur 2.7. Een quantumkwetsbaarheid-score van 0 leidt altijd tot een quantumrisico-score van 0, omdat het systeem al adequaat is beschermd. De vier scores zijn als volgt gedefinieerd:

0: **Risicoscore 0 (geen risico)** | Alle quantumdreigingen zijn adequaat gemitigeerd.

1: **Risicoscore 1 (laag risico)** | Er is op lange termijn een risico, maar dit vormt momenteel geen prioriteit.

2: **Risicoscore 2 (middelgroot risico)** | Er is actie vereist, maar de huidige cryptografie is op korte termijn nog veilig of de migratie wordt als eenvoudig geschat.

3: **Risicoscore 3 (groot risico)** | Er is op korte termijn prioriteit nodig, omdat de verwachte impact groot is en/of de migratie naar PQC naar verwachting lang zal duren.

4: **Risicoscore 4 (acuut risico)** | Het systeem loopt nu al risico, bijvoorbeeld omdat de verwachte migratiemoeite in combinatie met de vertrouwelijkheidstermijn van gegevens langer is dan de verwachte tijd totdat een quantumcomputer in staat zal zijn om de cryptografie te breken. In dit geval is er een realistische dreiging die onmiddellijk aandacht behoeft, mogelijk ook van hoger managementin het geval van grote impact op de bedrijfsvoering.

Afhankelijk van de PQC-persona van een organisatie kunnen bepaalde risico's wel of niet acceptabel zijn. Bijvoorbeeld, een reguliere adopter kan zich veroorloven langer te wachten met het migreren van een systeem met quantumrisico-score 1 of 2. Aan de andere kant moeten urgente adopters mogelijk al beginnen

met het prioriteren van systemen met een quantumrisico-score van 1 of 2, omdat de verwachte schade veel groter is als het systeem wordt gebroken. Uiteindelijk hangt de manier waarop organisaties systemen met verschillende quantumrisico-scores prioriteren af van hun algehele risicomanagementproces, beschikbare middelen en de algemene risicobereidheid van de organisatie.

Kwetsbaarheid	Impact	Migratiemoeite	Risico
0	1 2 3	1 2 3	0
1	1	1	1
1	1	2	1
1	1	3	1
1	2	1	1
1	2	2	1
1	2	3	1
1	3	1	1
1	3	2	2
1	3	3	2
2	1	1	1
2	1	2	1
2	1	3	2
2	2	1	2
2	2	2	2
2	2	3	3
2	3	1	3
2	3	2	4
2	3	3	4

Figuur 2.7 | Het omzetten van de scores van de drie componenten naar één risicoscore per toepassing.

Stap 2

3 Plannen van de migratie

Samenvatting

Dit hoofdstuk biedt concrete richtlijnen en advies voor organisaties die hun migratie naar post-quantumcryptografie (PQC) willen plannen. Het is voornamelijk bedoeld voor urgente adopters, maar ook voor reguliere adopters die proactief willen handelen.

In dit hoofdstuk wordt ervan uitgegaan dat een organisatie al de diagnosefase heeft doorlopen zoals beschreven in hoofstuk 2. Om te beslissen welke componenten als eerste moeten worden gemigreerd, is in het bijzonder de informatie uit sectie 2.2.1 over de huidige beveiligingsarchitectuur van een organisatie vereist. Daarnaast is de uitkomst van een quantumrisicobeoordeling nodig om te beginnen met het plannen van wanneer systemen moeten worden gemigreerd.

Met deze informatie zal dit hoofdstuk u helpen bij het bepalen van twee zaken. Het eerste deel van dit hoofdstuk helpt bij het bepalen wanneer de migratie moet plaatsvinden. De eerste NIST-standaarden zijn gepubliceerd in augustus 2024 en we verwachten binnen enkele jaren gecertificeerde softwarelibraries en standaarden omtrent de ingebruikname van PQC. Sommige organisaties kunnen het zich veroorloven om te wachten tot deze beschikbaar zijn, terwijl andere vandaag al moeten beginnen met migreren, mogelijk zelfs naar algoritmes die nog niet zijn gestandaardiseerd. Dit zal invloed hebben op het migratiebeleid. Het eerste deel van dit hoofdstuk biedt alle nodige informatie om te beslissen welk migratiescenario op een organisatie van toepassing is.

Het tweede deel van dit hoofdstuk bevat advies over hoe de migratie gepland moet worden. Hier wordt besloten welke cryptografische componenten moeten worden vervangen, waarmee ze moeten worden vervangen en in welke volgorde ze moeten worden vervangen. Dit omvat prioritering, het identificeren van afhankelijkheden en het anticiperen op enkele gevolgen van de migratie, zoals de noodzaak om sommige gegevens tijdelijk te isoleren. Na zorgvuldige planning van de migratie biedt het volgende hoofdstuk begeleiding bij de uitvoering van de migratie.

Hoewel dit document de migratiestappen (diagnose-planning-uitvoering) opeenvolgend beschrijft, hoeft een organisatie in de praktijk niet te wachten tot een stap volledig is voltooid voordat de volgende stap wordt gestart. Organisaties moeten beginnen met het identificeren van hun meest vitale componenten, een eerste migratiefase plannen voor deze vitale onderdelen en doorgaan met deze migratie, terwijl ze parallel actief werken aan het uitbreiden van de diagnose naar een groter deel van hun infrastructuur, dat in een tweede fase zal worden gemigreerd.

3.1 Tijdlijnen van de migratie

Gezien het feit dat systemen mogelijk op korte termijn moeten worden gemigreerd, is het nu tijd om te beslissen wanneer de migratie moet plaatsvinden. Dit wordt bepaald door drie variabelen: de tijd X die een component veilig moet blijven; de migratietijd Y; en de tijd Z tot quantumcomputers asymmetrische cryptografie kunnen breken. Er moet op tijd gemigreerd worden zodat $X + Y < Z$. Deze ongelijkheid staat ook bekend als

de ongelijkheid van Mosca, genoemd naar de onderzoeker die het introduceerde. Hoe dichter de waarde van $X + Y$ bij Z ligt, hoe urgenter de migratie is. Natuurlijk kunnen en moeten organisaties hoe dan ook al beginnen met de voorbereiding op de migratie door de no-regret moves uit te voeren
In de quantumrisico-beoordeling van sectie 2.4, wordt in bepaalde gevallen de impactscore direct beïnvloed door de tijd dat een component veilig moet blijven. Dit is het geval als de impact van niveau 3 is, vanwege de mogelijkheid van een store-now-decrypt-later-aanval. In dit geval wordt geadviseerd om zo snel mogelijk de migratie te beginnen. Daarnaast komt de migratiemoeite-score direct overeen met Y, de tijd die nodig is om de migratie uit te voeren. Hier komen de migratiemoeite-scores ruwweg op de volgende manier met de parameter *Y* overeen:

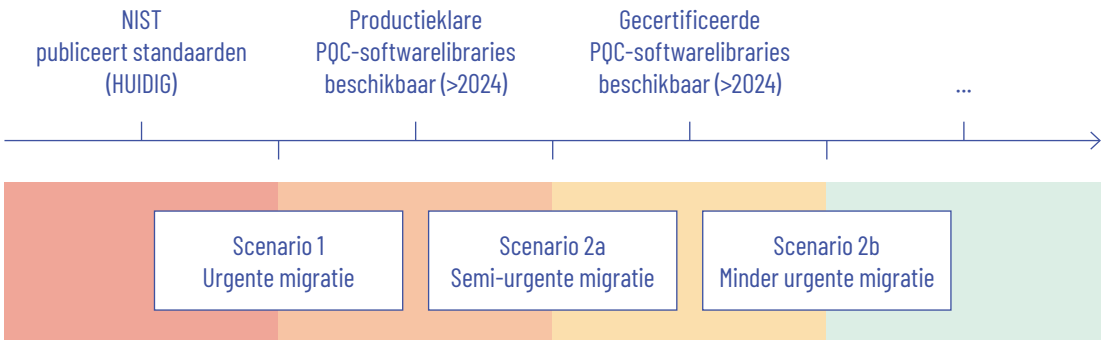
Migratiemoeite-score	*Y*
1	0-2 jaar
2	5-8 jaar
3	>8 jaar

Tabel 3.1 | Relatie tussen migratiemoeite en de parameter *Y*.

Daarnaast moet men rekening houden met het traject voor gecertificeerde implementaties van PQC-standaarden. Er zijn drie mijlpalen in dit traject, waarvan de eerste in augustus 2024 werd bereikt met de publicatie van de eerste PQC-standaarden door NIST. In figuur 3.1 worden deze mijlpijlen weergegeven, samen met zekere migratiescenario's. Alle data en systemen moeten gemigreerd worden volgens zo'n scenario met bijbehorende mijlpaal *M*, zodanig zodat de migratietijd $X + Y + M$ minder is dan Z.

De waarde van *M* schatten | Het is moeilijk te bepalen wanneer gecertificeerde of productie-niveau PQC-softwarelibraries voor algemeen gebruik zullen verschijnen. Verschillende PQC-libraries zullen namelijk gericht zijn op het optimaliseren van de algoritmes voor verschillende gebruikssituaties, zoals smartcards of IoT-apparaten. Ervaring uit vergelijkbare situaties is daarom zeer waardevol bij het bepalen van *M*. Daarnaast kunnen eindgebruikers invloed hebben op deze tijdlijnen. (Software)leveranciers zouden momenteel al moeten beginnen met het ontwikkelen van PQC-software. Door direct contact opnemen met leveranciers kan men invloed hebben op wanneer zulke software wordt gepubliceerd. Ook kan de wens voor dergelijke software worden uitgesproken binnen relevante community's of fora online.

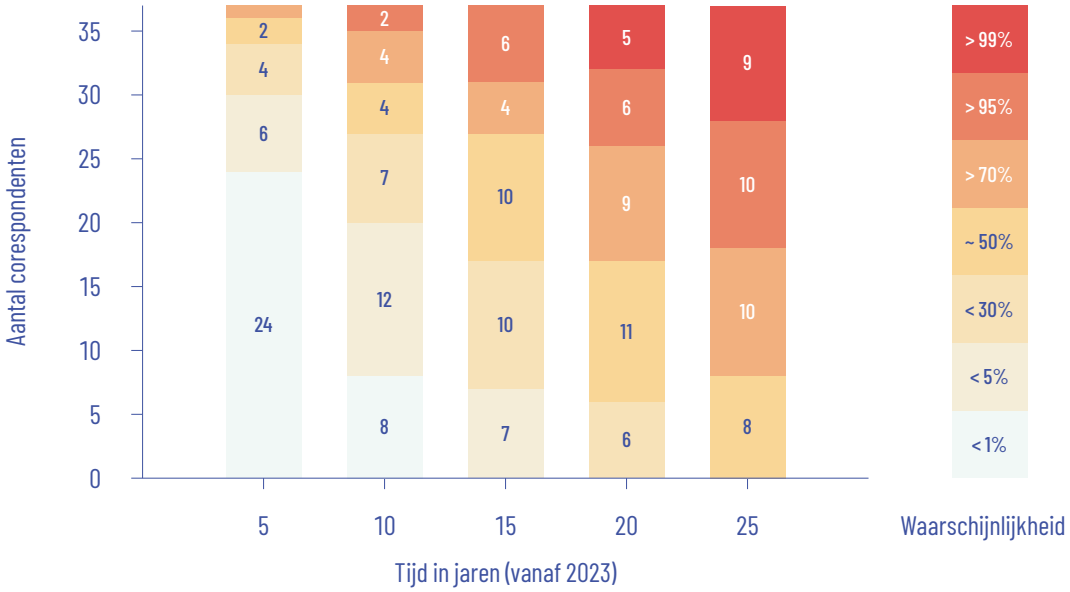
De waarde van *Z* schatten | Zelfs experts zijn het er niet over eens wanneer quantumcomputers in staat zullen zijn om quantumkwetsbare asymmetrische cryptografie te breken. Om een geïnformeerde schatting te geven, voert onderzoeker Michele Mosca jaarlijks een enquête uit, waarbij een selectie van experts op het gebied van quantumcomputing wordt gevraagd hun mening te geven over de waarschijnlijkheid dat een quantumcomputer RSA-2048 zal breken in 5, 10, 15, 20 en 30 jaar. Het resultaat van de recentste enquête [MP23] wordt weergegeven in figure 3.2. Uit deze figuur blijkt dat het een conservatieve schatting is dat quantumcomputers asymmetrische cryptografie zullen breken in 2040, terwijl dit volgens een minder conservatieve schatting al in 2030 gebeurt.
Merk op dat de tijd om de migratie uit te voeren per organisatie en zelfs per component zal variëren. Dit kan te wijten zijn aan het feit dat bijvoorbeeld librarydocumentatie, commerciële ondersteuning en algemene kennis van PQC completer zullen zijn als de migratie later begint. Daarom is het van cruciaal belang dat elk systeem uiteindelijk migreert naar productie-niveau of gecertificeerde implementaties van NIST PQC-standaarden. De exacte timing van de migratie zal afhangen van de risicobereidheid van de organisatie.



Figuur 3.1 | Tijdlijn voor verschillende migratiescenario's.

Gecertificeerde softwarelibraries

Voor sommige organisaties zal het essentieel zijn om te migreren naar Scenario 1, wat betekent dat er gemigreerd moet worden naar PQC-standaarden vóór er gecertificeerde libraries beschikbaar zijn. Dit brengt extra nadelen met zich mee: het gebruik van niet-gecertificeerde libraries kan leiden tot certificeringsproblemen en het gebruik van code die niet van productie-niveau is, kan leiden tot beveiligingsproblemen. Deze nadelen moeten in overweging worden genomen bij de keuze van een migratiescenario. Hierbij is het belangrijk om op te merken dat de momenteel meest gebruikte cryptografiestandaard, FIPS 140-2, al hybride schema's toestaat. Dit betekent dat het mogelijk is om ten minste die certificering te verkrijgen. Voor meer informatie over de hybride benadering verwijzen we naar de paragraaf over hybride oplossingen in sectie 4.1.



Figuur 3.2 | Enquête onder experts over het breken van RSA-2048 met een quantumcomputer [MP23].

Bepalen van het migratiescenario

Als onderdeel van de quantumrisico-beoordeling is er een algehele risicoscore per systeem geïdentificeerd. Afhankelijk van het risico dat een systeem loopt en de risicobereidheid van de organisatie ten opzichte van het systeem, moet meer of minder prioriteit worden gegeven aan het migreren van het systeem. Afhankelijk van de verhouding tussen risicoscore en risicobereidheid kunnen organisaties besluiten wel of niet te wachten tot alle drie de mijlpalen zijn bereikt. Dit leidt vervolgens naar een van de drie scenario's (urgente, semi-urgente of minder urgente migratie).

In hoofdstuk 4 wordt advies gegeven over hoe asymmetrische primitieven gemigreerd moeten worden afhankelijk van het specifieke scenario. In de rest van dit document zullen we scenario's 2a en 2b samen beschouwen, simpelweg als scenario 2. Dit komt omdat het advies voor deze scenario's tot op zekere hoogte hetzelfde is. Dit advies zou kunnen veranderen zodra de bovenstaande mijlpalen zijn bereikt.

Overkoepelende strategie

Aangezien het onmogelijk is om alle systemen en data in één keer te migreren, is een overkoepelende strategie vereist. Het wordt aanbevolen om verouderde protocollen eerst te migreren naar protocollen die momenteel worden aanbevolen door de NCSC-NL. Dit zal het componentbeheer en de agility van zowel de cryptografie als de organisatie als geheel testen. Pas als dit is gedaan, wordt aanbevolen om te beginnen met de migratie naar PQC. Op deze manier kan een organisatie al beginnen met het moderniseren van haar migratieproces om de uiteindelijke overgang te versoepelen.

3.2 Advies voor het plannen van de migratie

Het tweede deel van dit hoofdstuk bevat advies voor het plannen van de migratie. Het hoofddoel is tweeledig:

1. Voor elk cryptografische component beslissen of het vervangen moet worden, en zo ja, identificeren waarmee het vervangen moet worden.
2. De volgorde bepalen waarin verschillende cryptografische componenten moeten worden gemigreerd.

Deze sectie biedt nuttige handvatten om te helpen beslissen welke cryptografische componenten moeten worden vervangen en geeft suggesties voor manieren om ze te vervangen (zie hoofdstuk 4). De prioritering hangt af van de risicoanalyse die in het vorige hoofdstuk is opgesteld, maar moet ook rekening houden met de afhankelijkheden en de gevolgen van de migratie voor een specifieke bedrijfsvoering.

3.2.1 Plannen van bedrijfsprocessen

Omdat bedrijfsprocessen een wezenlijk onderdeel van de migratie vormen, is het belangrijk dat de planningsfase dit in overweging neemt. Op de eerste plaats dient een migratiemanager te worden aangesteld die verantwoordelijk is voor de uitvoering van de migratie. Dit moet iemand zijn met kennis van de organisatie in haar geheel en met toegang tot alle delen van de organisatie. De migratiemanager moet alle betrokken medewerkers van het bedrijf instrueren over de verschillende stappen van de migratie en de tijdlijnen daarvan. Ten tweede moeten er voldoende middelen voor de noodzakelijke migratiestappen worden vrijgemaakt, zoals tijd, financiën en faciliteiten. Ten slotte zullen er tijdens het migratieproces momenten zijn waarop bepaalde diensten en delen van de organisatie moeten worden geïsoleerd en uitgeschakeld. Deze 'downtime' moet zorgvuldig worden gemanaged en vooraf worden gepland om het effect op de continuïteit van de organisatie tot een minimum te beperken.
Een zorgvuldige planning houdt rekening met de migratiepaden van andere organisaties om zo ook de interoperabiliteit te behouden. Daarom is het verstandig om te overwegen de migratie samen met een groep van soortgelijke organisaties te plannen. In sommige gevallen is dit zelfs noodzakelijk omdat cryptografische systemen en systemen tussen organisaties dusdanig met elkaar verbonden zijn. Ook als dit niet het geval is, kan het samen uitvoeren van een migratieplanning voordelig zijn omdat de werklast voor het plannen van de migratie dan kan worden verdeeld. Voor meer advies over de planning van bedrijfsprocessen verwijzen we naar een technisch rapport [ETSI20a] van standaardisatieorgaan ETSI.

3.2.2 PQC-volwassenheidsbeoordeling

Voor een succesvolle migratie is het zaak om de grootste problemen te identificeren die de migratie van een organisatie (kunnen) belemmeren of vertragen. Het groeimodel dat wordt beschreven in [KJB24] kan inzicht bieden in welke aspecten van de migratie het belangrijkst zijn en welke technische en niet-technische uitdagingen er zijn. In het rapport worden vijftien belangrijke migratie-uitdagingen opgesomd en verder uitgewerkt:

1. Migreren van *legacy*-systemen;
2. Gebrek aan PQC-standaarden;
3. Gebrek aan besluitvorming over de meest geschikte algoritmes voor verschillende use-cases;
4. Gebrek aan testen en benchmarking;
5. Gebrek aan certificering voor PQC-software en -hardware en aan hoogwaardige implementaties;
6. Gebrek aan inzicht in de impact van quantumcomputing en gerelateerde risico's en kwetsbaarheden;
7. Gebrek aan urgentie binnen een enkele organisatie;
8. Gebrek aan langetermijnvisie op voordelen voor de organisatie;
9. Gebrek aan gekwalificeerd personeel met PQC-kennis;
10. Gebrek aan urgentie en planning voor de organisatie;
11. Gebrek aan urgentie onder belanghebbenden;
12. Gebrek aan leiderschap onder belanghebbenden;
13. Gebrek aan samenwerking onder belanghebbenden;
14. Gebrek aan beleid en juridische implicaties;
15. Technische complexiteit van de migratie.

Deze uitdagingen staan niet op zichzelf en beïnvloeden elkaar. Het aanpakken ervan kan een domino-effect hebben: hoe eerder een organisatie actie onderneemt binnen haar ecosysteem, hoe gemakkelijker het zal zijn om de volgende uitdagingen op te lossen. Pogingen om deze problemen afzonderlijk aan te pakken zullen het migratieproces daarentegen aanzienlijk moeilijker maken. Het rapport raadt collectieve acties en sterke samenwerkingen dan ook sterk aan als eerste stappen voor migratie. Om een overzicht te krijgen van deze uitdagingen kan het groeimodel in het rapport worden geraadpleegd om een overzicht te krijgen van het migratietraject.

Dit groeimodel wordt gepresenteerd als een beoordelingsmatrix en clustert de vijftien bovenstaande uitdagingen in acht hoofdprioriteiten:

- Samenwerking;
- Bewustwording;
- Bestuur;
- Beleid en regelgeving;
- Beschikbaarheid van PQC;
- Hybride aanpak;
- Strategieën voor cryptografische beveiliging;
- Kennis over de PQC-migratie.

Elk van deze prioriteiten is onderverdeeld in vijf verschillende groeistadia. Door de aspecten te identificeren waaraan een organisatie mogelijk moet werken, krijgt men een duidelijk beeld van de voortgang en de benodigde acties. Dit gestructureerde raamwerk dient als een waardevol beoordelingsinstrument, waarmee een organisatie haar huidige status binnen elke prioriteit kan evalueren. De matrix is te vinden in tabel 3.2.

	1. Samenwerking	2. Bewustwording	3. Bestuur	4. Beleid & regelgeving	5. Beschikbaarheid van PQC	6. Hybrid aanpak	7. Strategieën voor cryptografische veiligheid	8. Kennis van de PQC-migratie
Niveau 0	**1.0 Geen betrokkenheid** De organisatie is niet betrokken bij het ecosysteem. De organisatie is niet verbonden of actief betrokken.	**2.0 Onbewust** Het ontbreekt de organisatie aan bewustzijn van de PQC-migratie. De organisatie is onvoorbereid en heeft de relevantie en het voordeel van PQC nog niet erkend.	**3.0 Bestuursvacuüm** Er is een gebrek aan formeel bestuur voor migratie in het ecosysteem. Er zijn geen richtlijnen, regels of mechanismen voor besluitvorming, coördinatie en verantwoording.	**4.0 Geen formeel beleid of regels** Er zijn geen formele certificeringsprocessen voor PQC. Er is een gebrek aan regelgeving en beleid voor PQC-migratie.	**5.0 Beperkte kennis over PQC** De organisatie bezit geen kennis van de kernconcepten met betrekking tot de PQC-migratie. De organisatie herkent de noodzaak van PQC niet.	**6.0 Beperkte kennis over PQC** De organisatie bezit geen kennis van de kernconcepten met betrekking tot de PQC-migratie. De organisatie herkent de noodzaak van PQC niet.	**7.0 Reactieve & ad-hoc praktijken** De organisatie heeft een reactieve benadering rondom beveiliging en risico-beheer. Cryptografische algoritmes en protocollen worden ad-hoc geïmplementeerd.	**8.0 Beperkte kennis over PQC-migratie** De organisatie bezit beperkte kennis over de PQC-migratie en weet niet wat er gedaan moet worden. De organisatie is zich niet bewust van de quantumdreiging en de voordelen van PQC.
Niveau 1	**1.1 Communicatie & monitoring** De organisatie erkent het belang van samenwerking in het ecosysteem. De organisatie stelt communicatiekanalen in het ecosysteem in en monitort de PQC-migratie.	**2.1 Erkend bewustzijn** Er zijn discussies over de PQC-migratie. De organisatie erkent dat verandering noodzakelijk is en erkent de potentiële impact van de quantumdreiging op het bestaande systeem.	**3.1 Erkenning van beoordeling & planning** De organisatie erkent de noodzaak van migratiebestuur in het ecosysteem. De organisatie identificeert gedeelde doelstellingen voor de migratie.	**4.1 Opkomende inzichten & overwegingen** De organisatie erkent de noodzaak van enig niveau van beleid en regelgeving.	**5.1 Basisbegrip van PQC** De organisatie heeft basale kennis van de PQC-migratie. De organisatie heeft echter geen technische inventarisatie van de bestaande systemen uitgevoerd.	**6.1 Basisbegrip van PQC** De organisatie heeft basale kennis van de PQC-migratie. De organisatie heeft echter geen technische inventarisatie van het bestaande systeem uitgevoerd.	**7.1 Gedefinieerd beleid & procedures** De organisatie heeft cryptografisch beleid en richtlijnen gedefinieerd die gaccepteerde algoritmes en sleutelbeheerpraktijken beschrijven.	**8.1 Kennis van de bestaande infrastructuur** De organisatie heeft een cryptografische inventarisatie uitgevoerd, kent de bestaande infrastructuur en weet waar PQC moet worden toegepast.
Niveau 2	**1.2 Belanghebbenden identificeren** De organisatie identificeert potentiële richtingen voor de PQC-migratie. De organisatie ontwikkelt plannen om verwachtingen voor de PQC-migratie te delen met belanghebbers.	**2.2 Groeiende bewustwording** De organisatie zoekt informatie over PQC. Er is een groeiend bewustzijn van PQC. De organisatie begrijpt de reikwijdte van PQC echter niet volledig.	**3.2 Gedeelde bestuursprincipes** Organisaties in het ecosysteem gaan in discussie over gedeelde bestuursprincipes. Organisaties stellen de fundamentele waarden en verwachtingen voor de PQC-migratie vast.	**4.2 Gedeelde inzichten & discussies** De organisatie gaat in discussie en deelt inzichten in het ecosysteem over PQC-richtlijnen en informele industriestandaarden.	**5.2 Technische inventarisatie** De organisatie beoordeelt de bestaande infrastructuur en identificeert potentiële gebieden waar PQC kan worden geïmplementeerd. De organisatie begrijpt de reikwijdte van PQC echter niet volledig.	**6.2 Technische inventarisatie** De organisatie beoordeelt de bestaande infrastructuur en identificeert potentiële gebieden waar PQC kan worden geïmplementeerd. De organisatie begrijpt de reikwijdte van PQC echter niet volledig.	**7.2 Benadering op basis van risico** De organisatie heeft een risicogebaseerde benadering voor cryptografische beveiliging. Er worden risicobeoordelingen uitgevoerd om kwetsbaarheden en bedreigingen te identificeren. Het gebruik van cryptografische algoritmes is afgestemd op industriestandaarden en compliance.	**8.2 Kennis van PQC** De organisatie heeft kennis van de beperkingen en uitdagingen van de verschillende PQC-algoritmes. De organisatie begrijpt waar de hybride aanpak kan worden toegepast en geïmplementeerd in de bestaande systemen.
Niveau 3	**1.3 Gecoördineerde inspanningen** De organisatie werkt samen met het ecosysteem om coördinatie voor de PQC-migratie te bevorderen. Organisaties werken samen om een gedeelde visie en collectieve doelen te benutten.	**2.3 Geïnformeerd bewustzijn** De organisatie verkent verschillende mogelijkheden met betrekking tot de PQC-migratie. De organisatie heeft een dieper begrip van PQC en identificeert gebieden in de bestaande systemen die PQC nodig hebben.	**3.3 Bestuursstructuur** De organisatie stelt een formele structuur vast, zoals de oprichting van bestuurscommissies voor de PQC-migratie. De organisatie stemt in met rollen en verantwoordelijkheden die besluitvorming vergemakkelijken.	**4.3 Hiaatanalyse & voorbereiding** De organisatie identificeert beleids- en regelgevingshiaten met betrekking tot de PQC-migratie. De organisatie evalueert de potentiële risico's en gevolgen die gepaard gaan met de geïdentificeerde hiaten in beleid en regelgeving.	**5.3 Testspecificatie & use-cases** De organisatie voert tests uit met PQC. De organisatie identificeert testscenario's en use-cases van PQC. De organisatie voert interoperabiliteitstests uit en valideert functionaliteit, prestaties en veerkracht.	**6.3 Testspecificatie & use-cases** De organisatie voert tests uit met PQC. De organisatie identificeert testscenario's en use-cases van PQC. De organisatie voert interoperabiliteitstests uit en valideert functionaliteit, prestaties en veerkracht.	**7.3 Proactieve benadering** De organisatie hanteert een proactieve benadering van cryptografische beveiliging. Er worden geavanceerde cryptografische controles geïmplementeerd om vitale componenten te beschermen. Crypto-agility wordt benadrukt in de beveiligingsstrategie.	**8.3 Kennis van selectie van PQC** De organisatie heeft kennis van de selectie van verschillende PQC-algoritmes. De organisatie verkrijgt inzicht en verduidelijkt de kennis die nodig is voor implementatie en adoptie. Een roadmap, tijdlijn, doelen en middelen worden gedefinieerd.
Niveau 4	**1.4 Gezamenlijke acties** Organisaties werken samen om de nodige ondersteuning en middelen voor de PQC-migratie te bieden. Ze nemen actief deel aan gezamenlijke projecten, initiatieven en coördineren inspanningen om het hele ecosysteem te bevoordelen.	**2.4 Strategisch bewustzijn** De organisatie stemt haar bewustzijn af op haar strategische doelen voor de PQC-migratie. De organisatie maakt plannen om een soepele PQC-migratie te bereiken.	**3.4 Implementatie & handhaving** De vastgestelde bestuursstructuur en -principes worden in de praktijk gebracht. De organisatie implementeert en handhaaft actief de bestuursmechanismen om compliance, transparantie en verantwoording te waarborgen.	**4.4 Vrijwillige richtlijnen** Vrijwillige maatregelen en informele richtlijnen worden geïntroduceerd die criteria, procedures en vereisten beschrijven voor de bestaande systemen om quantumveilig te worden. Deze dienen als aanbevelingen en zijn niet wettelijk bindend.	**5.4 Pilots & validatie** De organisatie voert een pilotimplementatie van PQC uit. De organisatie monitort prestaties, verzamelt feedback. De organisatie werkt samen met belanghebbers om bruikbaarheid en effectiviteit te beoordelen.	**6.4 Pilots & validatie** De organisatie voert een pilotimplementatie van PQC uit met een hybride aanpak. De organisatie monitort prestaties, verzamelt feedback. De organisatie werkt samen met belanghebbenden om bruikbaarheid en effectiviteit te beoordelen.	**7.4 Voortdurende verbetering van cryptografische maatregelen** De organisatie verbetert haar cryptografische beveiligingsmaatregelen. Er is voortdurende evaluatie en adoptie van nieuwe cryptografische algoritmes en protocollen. Crypto-agility wordt benadrukt in de beveiligingsstrategie.	**8.4 Kennis van implementatie van PQC** De organisatie heeft een strategisch plan om PQC in de bestaande systemen te implementeren. De organisatie verkrijgt kennis over de implementatie van PQC.
Niveau 5	**1.5 Gezamenlijke sacties & continue dialoog** Organisaties onderhouden een continue dialoog binnen het ecosysteem. Er is voortdurende communicatie, rapportage, feedback en samenwerking tussen leiders om ervoor te zorgen dat de gedeelde visie en doelen worden doorgegeven.	**2.5 Vooruitziend bewustzijn** De organisatie kijkt vooruit en blijft op de hoogte van de laatste ontwikkelingen in PQC. De organisatie is zich bewust van de evolutie van PQC en plant strategisch voor toekomstige uitdagingen.	**3.5 Continue evaluatie & aanpassing** De organisatie beoordeelt de effectiviteit van het bestuurskader in het ecosysteem en maakt de nodige aanpassingen om aan de veranderende behoeften te voldoen. Het vastgestelde bestuur ondergaat continue evaluatie en aanpassing.	**4.5 Verplicht beleid & regelgeving** Beleid en regelgeving voor PQC worden wettelijk verplicht. Regelgevende instanties introduceren wettelijke mandaten die PQC vereisen voor standaarden, processen en compliance-eisen waaraan alle relevante organisaties moeten voldoen.	**5.5 Geschaalde implementatie** De organisatie selecteert de PQC-algoritmes om te implementeren en past deze toe in de bestaande systemen. Een succesvolle adoptie leidt tot verdere opschaling en integratie van PQC.	**6.5 Geschaalde implementatie** De organisatie selecteert de PQC-algoritmes om te implementeren met een hybride aanpak en past deze toe in de bestaande systemen. Een succesvolle adoptie leidt tot verdere opschaling en integratie van PQC met een hybride aanpak.	**7.5 Volwassen & veerkrachtige cryptografische beveiliging** De organisatie reageert zeer snel op cryptografische bedreigingen. Crypto-agility is een fundamenteel onderdeel van de beveiligingsstrategie van de organisatie. Crypto-agility wordt binnen de organisatie opgeschaald, waardoor snelle aanpassing aan toekomstige cryptografische standaarden mogelijk is.	**8.5 Kennis van het gebruik van PQC** Een succesvolle adoptie leidt tot verdere opschaling en integratie van PQC. De organisatie volgt prestaties, verzamelt gegevens en verzamelt feedback. De organisatie deelt kennis en ervaring in lijn met de beste praktijken in de industrie.

Tabel 3.2 | Matrix om het groeimodel te beoordelen.

Bovendien wordt er momenteel een online versie van het beoordelingsinstrument ontwikkeld die in januari 2025 openbaar zal worden gemaakt. Hoewel het rapport zich voornamelijk richt op infrastructuren met publieke sleutel-infrastructuren, zijn de achterliggende principes en strategieën veelzijdig en kunnen ze worden aangepast aan iedere overgang naar PQC van een organisatie.

3.2.3 Technische planning

Het technische deel van de planning moet zich richten op aspecten zoals welke cryptografie moet worden gemigreerd, wanneer deze moet worden gemigreerd en welke methoden moeten worden gebruikt.

Onderlinge afhankelijkheid van systemen

Een belangrijk doel van deze planning is het identificeren van de afhankelijkheden tussen de verschillende cryptografische systemen en het bepalen van de migratievolgorde. Als systeem A afhankelijk is van systeem B, beslis dan of A of B eerst moet worden gemigreerd. Dergelijke afhankelijkheden moeten duidelijk worden uit de inventarisatie. Het post-quantumprotocol kan in eerste instantie als optioneel worden beschouwd totdat alle bijbehorende systemen zijn gemigreerd. Op die manier kan een organisatie de interoperabiliteit tussen de systemen tijdens de migratie behouden.

Vervangen van cryptografie

Nadat de cryptografische inventaris is opgesteld en de afhankelijkheid van cryptografische systemen is uitgezocht, kan de vervanging van cryptografische systemen daadwerkelijk gepland worden. De organisatie moet voor elk cryptografisch systeem eerst besluiten of deze moet worden vervangen, opnieuw ontworpen, buiten gebruik gesteld of anderszins moet worden aangepast. Deze beslissing is afhankelijk van verschillende factoren, zoals het belang van het systeem voor de organisatie, de gevolgen van de gebrekkige werking van het systeem, het risico dat het systeem wordt aangevallen, maar ook van de beschikbare middelen. Zodra is besloten dat een systeem moet worden vervangen of opnieuw moet worden ontworpen, moet de organisatie in de volgende stap beslissen met welke quantumveilige oplossing het systeem moet worden vervangen. Suggesties hiervoor volgen in hoofdstuk 4. We raden bovendien aan om crypto-agility in deze overwegingen mee te nemen, zodat de implementatie snel kan worden bijgewerkt als er in de toekomst nieuwe standaarden of regels uitkomen. Zie sectie 4.4 voor meer informatie over crypto-agility.
Het is belangrijk om cryptografische systemen ook tijdens de migratie te beschermen. Dit kan op vele manieren worden gedaan. De gemakkelijkste manier is door de traditionele cryptografische bescherming van het systeem te behouden totdat het systeem wordt beschermd door de nieuwe quantumveilige oplossing. Als dat geen optie is, moet het systeem worden geïsoleerd.

Isolatie van data of systemen

In sommige gevallen is isolatie van data/systemen de enige manier om deze volledig te beschermen. Dit geldt met name voor verwerkers van persoonlijke en organisatorisch gevoelige informatie. Er zijn verschillende gevallen waarin isolatie wordt geadviseerd of zelfs noodzakelijk is. Ten eerste biedt isolatie van data bescherming tegen store-now-decrypt-later-aanvallen. Het risico op een dergelijke aanval kan worden weggenomen door deze data fysiek te scheiden van het netwerk. Dit geldt met name voor data tijdens overdracht, aangezien deze aanvallen worden uitgevoerd door het onderscheppen van data via een communicatiekanaal. Informatie in rust is minder kwetsbaar voor store-now-decrypt-later-aanvallen. Isolatie van systemen is ook nuttig wanneer een systeem niet kan worden beschermd tijdens de migratie. Aangezien migratie een ingewikkeld proces is, is het wellicht niet mogelijk alle systemen tegelijkertijd te updaten. Hierdoor moet voor sommige systemen of data de huidige cryptografische beveiliging worden verwijderd voordat de quantumveilige beveiliging kan worden toegepast. Het kan ook zo zijn dat het momenteel te duur is om bepaalde systemen te migreren, maar dat een organisatie deze toch wil beschermen. In beide gevallen is het mogelijk de vereiste

bescherming te behouden door het isoleren van het kwetsbare systeem. Na afloop van de vereiste migratiestappen kan het systeem vervolgens weer uit de isolatie gehaald worden. Het is belangrijk om te beseffen dat isolatie een enorme impact heeft op de functionaliteit en beschikbaarheid van de data. Zolang een systeem is geïsoleerd, kan het niet worden gebruikt. Dit is een belangrijk aspect waarmee organisaties rekening moeten houden bij de overweging systemen te isoleren. In sommige scenario's is het isoleren dan ook geen optie.

Hardware vervangen

Door de migratie moet hardware mogelijk worden vervangen. Bij een grootschalige vervanging van hardware moet de organisatie bij de planning van de migratie rekening houden met de beschikbaarheid van het nieuwe product en de implementatietijd.

Testen

Nieuwe implementaties op zowel hardware- als softwareniveau moeten een testfase doorlopen. Deze testfase is zeer belangrijk en moet goed worden voorbereid. De tests zullen uitwijzen of de nieuwe algoritmes compatibel zijn met de overige infrastructuur en of ze daadwerkelijk de beloofde beveiliging bieden.

3.3 Kosten van de migratie

Een essentieel onderdeel van het plannen van de PQC-migratie is het schatten van de kosten en het toewijzen van middelen. Uitgebreide kostenramingen moeten meegenomen worden bij het nemen van strategische PQC-beslissingen en het prioriteren van acties. Zo heeft de federale overheid van de VS de totale kosten van de PQC-migratie tussen 2025 en 2035 geschat op 7,1 miljard dollar [US24]. Daarnaast moeten de federale instanties hun kostenramingen jaarlijks bijwerken.

De reikwijdte en complexiteit van de PQC-migratie kan worden bepaald op basis van de quantumkwetsbaarheidsdiagnose en in het bijzonder de cryptografische inventaris. De complexiteit wordt daarnaast beïnvloed door de wettelijke vereisten van de organisatie en de quantumrisico-beoordeling. Vervolgens moet een organisatie de benodigde mankracht en expertise schatten om de PQC-migratie uit te voeren, waarbij rekening wordt gehouden met welke delen van de cryptografische infrastructuur direct onder de controle van de organisatie vallen en welke delen door hun leveranciers worden beheerd. Verder zijn er verschillende tools en diensten beschikbaar om te helpen bij de PQC-migratie. Door de kosten te schatten kan een goed geïnformeerde beslissing worden genomen over welke tools en diensten moeten worden aangeschaft.

Bepaalde producten moeten mogelijk worden vervangen als deze geen PQC ondersteunen en de leverancier niet van plan is om PQC in nieuwe versies op te nemen. Bovendien vereisen PQC-algoritmes vaak meer rekenkracht, waarvoor de momenteel gebruikte cryptografische hardware mogelijk niet voldoende is. Als blijkt dat de huidige hardware niet meer voldoende is, moet deze ook worden vervangen.

Een bijkomende overweging met betrekking tot de kosten van de PQC-migratie is mogelijke 'downtime'. In het ideale geval kan een organisatie haar downtime en de impact op bedrijfsactiviteiten tot een minimum beperken, maar er kunnen zich altijd onvoorziene omstandigheden voordoen. Om dezelfde reden moet er een backup-plan zijn en een robuuste procedure bestaan voor het herstellen van de communicatie-infrastructuur van een organisatie.

Ten slotte biedt de PQC-migratie een uitstekende kans om de cryptografische beleidslijnen en processen van een organisatie naar een hoger niveau te tillen. Dit is bijvoorbeeld wenselijk omdat de huidige PQC-migratie waarschijnlijk niet de laatste cryptografische migratie zal zijn. Er worden nog steeds nieuwe cryptografische primitieven ontwikkeld en gestandaardiseerd, wat de mogelijkheid biedt voor toekomstige verbeteringen. Ook kunnen toekomstige ontwikkelingen in de cryptoanalyse ervoor zorgen dat aanpassingen of verdere cryptografische migraties nodig zijn. De kosten van deze toekomstige uitgaven kunnen worden verminderd door nu te investeren in crypto-agility.

Stap 3

4 Uitvoeren van de migratie

Samenvatting

Dit hoofdstuk biedt informatie en richtlijnen over hoe de migratie moet worden uitgevoerd. Het biedt richtlijnen voor het migreren van onveilige cryptografie en protocollen. Deze richtlijnen bieden zowel algemene als specifieke stappen om succesvol over te stappen naar een quantumveilige omgeving. Veel stappen zijn afhankelijk van wanneer de organisatie de migratie daadwerkelijk gaat uitvoeren, daarom is het aanbevolen om eerst het migratiescenario te bepalen in het vorige hoofdstuk. Verder is het belangrijk om nu al te beginnen met het werken aan de crypto-agility van de componenten. De belangrijkste aanbeveling voor bijna alle protocollen is om een hybride oplossing te gebruiken.

4.1 Algemene strategieën

De laatste fase van de migratie is de uitvoering van het plan dat in het vorige hoofdstuk is opgesteld. Idealiter is op dit punt een volledig overzicht van cryptografische componenten beschikbaar, en is er een plan gemaakt waarin wordt beschreven naar welke quantumveilige alternatieven de kwetsbare componenten moeten worden gemigreerd. Als alternatief kan een organisatie ervoor kiezen om al te beginnen met het migreren van componenten met hoge prioriteit voordat het volledige plan is voltooid en de laatste fase daarmee parallel uit te voeren met de andere fases. Houd er rekening mee dat IT-omgevingen voortdurend veranderen. Een inventaris van componenten die twee jaar geleden is gemaakt zal hoogstwaarschijnlijk niet het huidige cryptografische landschap van een organisatie beschrijven. Daarom is het belangrijk om deze inventaris continu up-to-date te houden.
Deze sectie geeft een aantal algemene strategieën die kunnen worden toegepast in de PQC-migratie. De twee secties daarna bespreken in detail hoe cryptografische primitieven en protocollen te migreren.

Waarschuwing | Het migratieplan dient nauwgezet te worden toegepast. De vervanging van bepaalde cryptografische systemen door andere zou immers nieuwe kwetsbaarheden kunnen introduceren. Een onjuist gekozen vervangend algoritme of een fout in de nieuwe configuratie kan het beveiligingsniveau verlagen. Bovendien is het aanvalsoppervlak groter tijdens de migratiefase. Zelfs als een organisatie deze taak uitbesteedt, moet ze een bepaald inzicht in PQC behouden om de verschillende afwegingen rondom elke vervangende oplossing te begrijpen. Daarnaast is quantumveilige asymmetrische cryptografie minder goed ingeburgerd dan traditionele asymmetrische cryptografie. Om hetzelfde niveau van vertrouwen te krijgen, moet er nog jarenlang grondig cryptoanalytisch werk worden verricht. Toch mag dit geen argument zijn om de migratie uit te stellen: hybride-EN schema's bieden immers een beveiligingsniveau dat minstens even sterk is als dat van van het gebruikte traditionele algoritme, waardoor de dreiging van quantumcomputers strikt minder wordt.

Migratie van primitieven versus migratie van protocollen

Voordat we de migratie van primitieven en protocollen bespreken, moet eerst een belangrijk onderscheid worden gemaakt. Cryptografische primitieven staan over het algemeen niet op zichzelf, maar worden gebruikt als een bouwblok in een groter protocol. Dit betekent dat de meeste organisaties nooit direct te maken krijgen met de details van cryptografische primitieven. In plaats daarvan gebruiken ze softwarelibraries die veelgebruikte protocollen zoals TLS aanbieden, die onder de motorkap cryptografie gebruiken. Deze softwarelibraries bieden wel verschillende cryptografische keuzes, zoals welke primitieven of sleutelgroottes moeten worden gebruikt. De organisatie is over het algemeen echter niet zelf verantwoordelijk voor het implementeren van de cryptografische algoritmes in deze softwarelibraries. Het direct migreren van primitieven is daarom vaak alleen aan de orde in het geval dat een organisatie direct te maken heeft met de details van de cryptografie in deze softwarelibraries en mogelijk haar eigen protocollen implementeert. Aan de andere kant volstaat het voor veel organisaties de protocolversie bij te werken, bijvoorbeeld van TLS 1.2 naar TLS 1.3. Het eerste deel van hoofdstuk 6 bevat een lijst met de belangrijkste cryptografische primitieven, hun basiskenmerken en of ze al dan niet quantumveilig zijn. Dit hoofdstuk bevat ook de belangrijkste post-quantumprimitieven.

Migratie van symmetrische cryptografie

In theorie kan een quantumcomputer symmetrische cryptografie, inclusief hashfuncties, efficiënter aanvallen dan klassieke computers met het algoritme van Grover. Over het algemeen leidt het resulterende (theoretische) quantumvoordeel niet tot een volledige breuk van symmetrische cryptografie, maar vereist het wel grotere cryptografische sleutels om hetzelfde veiligheidsniveau te behouden. Gedetailleerdere analyses hebben echter aangetoond dat het onwaarschijnlijk is dat het bovenstaande quantumvoordeel in de praktijk benut kan worden. Daarom is de verwachting dat symmetrische primitieven veilig blijven tegen quantumaanvallen, zelfs zonder de sleutelgrootte te vergroten. Om deze reden benadrukken we dat het van belang is om de migratie van asymmetrische cryptografie te prioriteren. Voor meer details verwijzen we naar sectie 4.2.3.

Migratie van asymmetrische cryptografie met hybride constructies

Een cryptografisch relevante quantumcomputer zal in staat zijn om bepaalde asymmetrische cryptografie te breken, waardoor alle bijbehorende veiligheidsgaranties komen te vervallen. Encryptieschema's en mechanismen voor sleuteluitwisseling en -inkapseling die de vertrouwelijkheid van gegevens beschermen zijn kwetsbaar voor store-now-decrypt-later-aanvallen. Om deze dreiging te mitigeren, is het essentieel om op tijd naar PQC te migreren. Digitale handtekeningen, die worden gebruikt voor authenticatie en integriteit, hebben geen last van store-now-decrypt-later-kwetsbaarheden, waardoor hun migratie naar PQC mogelijk minder urgent is. Er is daarnaast speciale aandacht vereist voor systemen met een lange levensduur, zoals vitale infrastructuren, satellieten en operationele technologie. Zulke systemen, die momenteel ontwikkeld en ingezet worden, kunnen namelijk moeilijk of zelfs onmogelijk geupdate worden in de toekomst.

Hybride constructies

Hybride constructies maken gelijktijdig gebruik van zowel vertrouwde (quantumkwetsbare) cryptografie als post-quantumcryptografie binnen een enkel protocol. Om het resulterende protocol te breken zou een aanvaller beide algoritmes moeten breken. Daarom is het hybride schema als geheel minimaal even veilig als elk algoritme afzonderlijk.

De insteek van hybride constructies is het verminderen van de beveiligingsrisico's als gevolg van de beperkte volwassenheid van de post-quantumalgoritmes. Tegelijkertijd biedt de hybride constructie meer veiligheid tegen quantumaanvallers dan het quantumkwetsbare, beproefde algoritme alleen zou doen.

Naast deze wiskundige beveiliging beschermt het implementeren van quantumkwetsbare en post-quantumalgoritmes in hybride ook tegen implementatiefouten van PQC. Tot slot zijn hybriden specifiek interessant om te gebruiken in omgevingen waar PQC nog niet is toegestaan of vertrouwd. Het gebruik van PQC

in combinatie met een vertrouwd, quantumkwetsbaar algoritme laat toe om PQC gebruiken én te voldoen aan de bestaande regelgeving. Hybride constructies worden met name aanbevolen voor organisaties die quantumveilige cryptografie willen inzetten voordat nieuwe gecertificeerde implementaties van de gestandaardiseerde algoritmes beschikbaar zijn, bijvoorbeeld als de gegevens van de organisatie nu al vatbaar zijn voor store-now-decrypt-later-aanvallen. Het belangrijkste nadeel van deze techniek is dat het een overhead kan veroorzaken (in tijd en/of geheugen) omdat nu twee cryptografische algoritmes moeten worden uitgevoerd voor een enkele encryptie of handtekening. Aangezien de meeste post-quantum algoritmes al relatief meer kosten met zich meebrengen in vergelijking met quantumkwetsbare cryptografie, zouden deze extra kosten behapbaar moeten zijn. In typische scenario's wordt de hybride oplossing namelijk slechts één keer gebruikt om een (symmetrisch) sleutelpaar op te zetten om de rest van een verbinding te versleutelen. In deze scenario's zijn de extra kosten van de hybride oplossing laag in vergelijking met de gehele verbinding.

Waarschuwing | Als producten beweren hybride encryptie of handtekeningen te gebruiken, moeten organisaties ervoor zorgen dat dit overeenkomt met de bovenstaande beschrijving, dat wil zeggen, dat het tegelijkertijd gebruik maakt van vertrouwde (quantumkwetsbare) algoritmes EN post-quantumalgoritmes voor de encryptie of handtekening. Dit mag niet worden verward met de keuze tussen het gebruik van quantumkwetsbare OF post-quantumalgoritme voor encryptie (zie hieronder). Bovendien wordt hybride encryptie ook vaak gebruikt om een combinatie van symmetrische en asymmetrische cryptografie aan te duiden, waarbij de asymmetrische cryptografie meestal wordt gebruikt om een sleutel voor het symmetrische algoritme op te zetten. Dit is ook niet de hybride-EN-strategie waar we in dit stuk op doelen.

Downgrade-aanvallen

Sommige hybride benaderingen lopen risico op *downgrade-aanvallen*. Dit is het geval wanneer een systeem hybride-OF in plaats van hybride-EN implementeert zoals hierboven beschreven. Hybride-OF, ofwel optioneel post-quantum, gaat over een situatie waarin zowel het quantumkwetsbare algoritme als het post-quantumalgoritme op de server zijn geïmplementeerd. Om met de server te communiceren, kan een client er in dit geval ervoor kiezen om het quantumkwetsbare dan wel het quantumveilige protocol te gebruiken en is het niet verplicht om beide te gebruiken. Een dergelijke configuratie is gunstig voor *backwards compatability*. Deze compatibiliteit is bijzonder handig om interoperabiliteit te bieden tijdens de vroege ontwikkelingsfase en tijdens het testen. Dergelijke oplossingen brengen echter een belangrijk risico met zich mee: een aanvaller kan doen alsof hij geen post-quantumprotocollen ondersteunt en de server dwingen om te communiceren met behulp van het quantumkwetsbare algoritme. Dit staat bekend als een *downgrade-aanval*. Zelfs als de kwaadwillende entiteit het quantumkwetsbare primitieve niet kan breken, kan hij nog steeds store-now-decrypt-later-aanvallen uitvoeren. Daarom wordt over het algemeen aanbevolen dat interne systemen hybride gebruiken in de hybride-EN-vorm zoals hierboven beschreven. Voor extern gerichte systemen kan dit echter omslachtiger zijn en kan hybride-OF de enige optie zijn. Er moet beleid en strategie worden gevormd om te bepalen wanneer en hoe dergelijke systemen hybride algoritmes correct kunnen gebruiken.

Migratie van asymmetrische cryptografie met van tevoren gedeelde sleutels

Een andere manier om asymmetrische cryptografie quantumveilig te maken, is door gebruik te maken van symmetrische cryptografie en de sleutels vooraf te delen (Eng: *pre-shared keys*). Op deze manier kan communicatie tot stand gebracht worden zonder enige vorm van asymmetrische cryptografie. Het vereist echter dat sleutels op een fysieke manier worden van tevoren gedeeld, bijvoorbeeld via een USB-stick. Het opzetten van dergelijke sleutels is hierdoor meestal een omslachtig proces en slecht schaalbaar in complexe infrastructuren met veel deelnemende partijen. Bovendien is het valideren van certificaten niet mogelijk omdat publieke sleutelcryptografie wordt omzeild. Maar als dergelijke vooraf gedeelde sleutels eenmaal zijn vastgesteld, is dit een erg veilige en efficiënte aanpak.

Het advies is daarom om hybride constructies te gebruiken, tenzij het systeem aan elk van de volgende eisen voldoet:

1. Het systeem moet worden gemigreerd vanuit scenario 1.
2. Het systeem valt onder de volledige controle van de organisatie en is volledig betrouwbaar.
3. Het systeem communiceert alleen met volledig gecontroleerde systemen met dezelfde betrouwbaarheid.
4. Er is een praktische manier om de geheime sleutels tussen de communicatiesystemen te delen.
5. De netwerken waarin deze communicerende systemen bestaan, zijn hoogst vertrouwelijk en de indeling verandert niet vaak.
6. Het toevoegen of verwijderen van knooppunten aan deze netwerken gebeurt niet vaak en is niet praktisch.

TLS en IPSec zijn voorbeelden van protocollen waarbij vooraf gedeelde sleutels kunnen worden gebruikt.

4.2) Aanbevolen cryptografische primitieven

Tijdens het uitvoeren van de PQC-migratie moeten specifieke keuzes gemaakt worden, waaronder het kiezen welke post-quantum primitieve in de praktijk moet worden gebruikt. Dit kan een uitdagende taak zijn en vereist expertise en kennis. Deze sectie presenteert een tabel met aanbevolen cryptografische primitieven (tabel 4.1) en een tabel met de corresponderende aanbevolen parameters (tabel 4.2). Daarnaast wordt uitgelegd wat de nuances en de rationale zijn achter deze aanbevelingen. Het is belangrijk op te merken dat deze tabellen niet uitputtend zijn. Bijvoorbeeld, alhoewel SHA-2 en SHA-3 aanbevolen algemene hashfamilies zijn, zijn ze mogelijk niet geschikt voor alle toepassingsscenario's. Voor bijvoorbeeld wachtwoord-hashing zijn over het algemeen speciale hashfuncties zoals Argon2 vereist. In de praktijk is er een breed spectrum aan toepassingsscenario's die mogelijk cryptografische primitieven vereisen die verder gaan dan die in deze sectie worden besproken. Deze sectie is bedoeld om softwareontwikkelaars en beveiligingsarchitecten te begeleiden, ervan uitgaande dat ze een bepaald niveau van bekendheid met cryptografie hebben. Voor een verdere bespreking van de aanbevolen cryptografische primitieven verwijzen we naar hoofdstuk 6. Daarnaast zijn er enkele tools die begeleiding kunnen bieden bij het maken van een geïnformeerde keuze over de meest geschikte cryptografische primitieve, afhankelijk van specifieke gebruiksscenario's en beveiligingseisen. Meer informatie is te vinden in sectie 6.4.

4.2.1 Sleuteluitwisseling en -inkapseling en digitale handtekeningen

Onlangs heeft NIST de standaarden gepubliceerd voor asymmetrische primitieven ML-KEM [NIST24a], het sleutelinkapselingsmechanisme dat voorheen bekend stond als CRYSTALS-Kyber, en ML-DSA [NIST24b], het digitale handtekeningalgoritme dat voorheen bekend stond als CRYSTALS-Dilithium. Deze primitieven zijn allebei gebaseerd op wiskundige roosters. Tijdens het PQC-standaardisatieproces van NIST zijn deze primitieven grondig onderzocht en ze worden daarom als klaar voor praktische implementatie beschouwd. We raden aan deze primitieven in een hybride modus te implementeren, gecombineerd met reeds bestaande en veelgebruike primitieven gebaseerd op elliptische krommen. Dit is om ervoor te zorgen dat kwetsbaarheden in PQC-implementaties en mogelijke doorbraken in de cryptoanalyse van roosters niet onmiddellijk de cryptografie onveilig maken. Beide standaarden specificeren drie parametersets, die overeenkomen met beveiligingsniveaus 1 (of 2 in het geval van ML-DSA), 3 en 5. We raden aan de primitieven waar mogelijk te gebruiken met de sterkste parameterset, beveiligingsniveau 5, en beveiligingsniveau 3 als een acceptabel alternatief te beschouwen (zie tabel 4.2). De ML-KEM-standaard specificeert beveiligingsniveau 3 als de standaardoptie; onze aanbevelingen kunnen daarom als iets conservatiever worden beschouwd.

Functionaliteit	Soort	Aanbevolen	Acceptabel	Uitgefaseerd
Sleuteluitwisseling of - inkapseling	Asymmetrisch	ML-KEM[1]	FrodoKEM[1] Classic McEliece[1]	ECDH[3] RSA[3]
Digitale handtekening zonder toestand (*stateless*)	Asymmetrisch	ML-DSA[2] SLH-DSA	FN-DSA[2]	ECDSA[3] EdDSA[3] RSA[3]
Digitale handtekening met toestand (*stateful*)	Asymmetrisch	XMSS LMS HSS		
Hashfunctie	Hash	SHA-2 SHA-3	BLAKE2	MD5 SHA-1
Block Cipher	Symmetrisch	AES	Camellia	(T)DES IDEA Blowfish
Stream Cipher	Symmetrisch	AES-CTR ChaCha20		RC4
Versleuteling	Symmetrisch	AES-CTR ChaCha20		
Geauthenticeerde versleuteling (met *Associated Data*)	Symmetrisch	AES-GCM(-SIV) AES-OCB ChaCha20-Poly1305		
Message Authenticati-on Code (MAC)	Symmetrisch	CMAC-AES HMAC-SHA-2 KMAC	CMAC-Camelia BLAKE2-MAC	CBC-MAC

Tabel 4.1 | Aanbevolen cryptografische primitieven.

Primitieve	Aanbevolen	Acceptabel
ML-KEM[4]	ML-KEM-1024[1]	ML-KEM-768[1]
ML-DSA[4]	ML-DSA-87[2]	ML-DSA-65[2]
SLH-DSA	SLH-DSA-(SHA2/SHAKE)-256(s/f) SLH-DSA-(SHA2/SHAKE)-192(s/f)	SLH-DSA-(SHA2/SHAKE)-128(s/f)
AES	AES-256	AES-128
SHA-3	SHA-3-256 SHA-3-384 SHA-3-512 (c)SHAKE256	SHA-3-224 (c)SHAKE128
SHA-2	SHA-256 SHA-384 SHA-512	SHA-224

Tabel 4.2 | Aanbevolen parameterkeuzes voor cryptografische primitieven.

[1] We bevelen aan om dit algoritme te gebruiken in een hybride constructie met ECDH. [2] We bevelen aan om dit algoritme te gebruiken in een hybride constructie met ECDSA or EdDSA. [3] Bestand tegen klassieke aanvallen en kan deel uitmaken van een hybride constructie. [4] BSI, ANSSI, uWBH (AIVD) bevelen NIST-niveau 5 of 3 aan. NSA CNSA 2.0 eist niveau 5.

De derde PQC-standaard gepubliceerd door NIST is het op hashfuncties gebaseerde digitale handtekeningalgoritme SLH-DSA, voorheen bekend als SPHINCS+. Aangezien de veiligheid van dit algoritme uitsluitend afhangt van de veiligheid van de onderliggende hashfunctie, wordt SLH-DSA beschouwd als een iets conservatievere keuze dan de op roosters gebaseerde tegenhanger ML-DSA. Daarom wordt het niet noodzakelijk geacht om dit schema in een hybride combinatie met elliptische kromme-primitieven te implementeren. Om dezelfde reden beschouwen we beveiligingsniveau 1 als een acceptabele implementatie van SLH-DSA.
FN-DSA, voorheen bekend als Falcon, is een tweede op roosters gebaseerd digitaal handtekeningalgoritme. Samen met ML-KEM, ML-DSA en SLH-DSA is het geselecteerd voor standaardisatie. In tegenstelling tot de andere primitieven is de FN-DSA-standaard echter nog niet afgerond. Daarom raden we momenteel het gebruik van ML-DSA en SLH-DSA boven FN-DSA aan.
Ten slotte erkennen we dat er scenario's kunnen zijn waarin een hoger niveau van zekerheid gewenst is. Voor deze scenario's zijn FrodoKEM en Classic McEliece alternatieve mechanismen voor sleutelinkapseling. Deze primitieven zijn gebouwd op basis van conservatievere veiligheidsaannames en gaan zodoende gepaard met conservatievere veiligheidsanalyse. Het is daarom minder waarschijnlijk dat de onderliggende aannames ongeldig blijken te zijn en daardoor cryptoanalytische aanvallen haalbaar worden. Het nadeel is echter dat deze extra zekerheid ten koste gaat van de performance van de algoritmes. Bovendien zijn FrodoKEM en Classic McEliece nog niet gestandaardiseerd. Totdat dit het geval is, beschouwen we deze primitieven slechts als acceptabel, hoewel we lopende initiatieven om ze te standaardiseren sterk steunen. Bij het implementeren van deze schema's raden we aan de recentste parametersets te volgen die gericht zijn op veiligheidsniveau 5 of 3.

4.2.2 Digitale handtekeningen met een toestand (*stateful algorithms*)

Naast SLH-DSA zijn er nog meer standaarden voor digitale handtekeningen op basis van hashfuncties: XMSS, LMS en HSS. Deze primitieven zijn zelfs efficiënter en kunnen daarom de voorkeur genieten boven de eerder genoemde digitale handtekeningalgoritmes. Ze hebben echter één significant nadeel: ze zijn *stateful*, wat betekent dat ze een interne 'toestand' hebben die bijgehouden moet worden. Deze algoritmes kunnen met een gegeven sleutelpaar slechts een beperkt aantal handtekeningen produceren en vereisen daarom zorgvuldig beheer van deze interne toestand of *state*. Concreet moet na elk gebruik van de privésleutel de toestand worden bijgewerkt. Als de toestand verloren gaat (of onnauwkeurig wordt bijgehouden) is het algoritme onveilig. Daarom zijn handtekeningalgoritmes met een toestand alleen toepasbaar in specifieke scenario's, waarin dergelijk zorgvuldig beheer van de toestand mogelijk is. Als ze echter correct worden geïmplementeerd, bieden handtekeningalgoritmes met een interne toestand een efficiënte en conservatieve digitale handtekeningsfunctionaliteit. NIST heeft uitgebreide richtlijnen gepubliceerd voor het implementeren van *stateful* handtekeningalgoritmes [NIST20a].

4.2.3 Symmetrische cryptografie

In theorie kunnen symmetrische primitieven worden aangevallen met het quantumalgoritme van Grover in kwadratisch minder stappen dan een klassieke *bruteforce-aanval* zou vereisen. Dit zou een halvering van het veiligheidsniveau betekenen, wat kan worden tegengegaan door de sleutellengte te verdubbelen. Dit betekent dat een sleutellengte van 128 bits moet worden vermeden, en sleutels van 256 bits aanbevolen worden. Gedetailleerdere analyses van aanvallen op basis van Grover tonen echter aan dat de kosten ervan ten minste vergelijkbaar zijn met de kosten van een klassieke aanval [JNRV20]. De belangrijkste reden is dat, in tegenstelling tot de quantumaanval, de klassieke aanval kan worden geparalleliseerd. Daarom is het waarschijnlijk dat 128-bits symmetrische sleutelprimitieven voorlopig ook veilig blijven, zelfs als er quantumcomputers zijn die quantumkwetsbare asymmetrische cryptografie kunnen breken.

Over het algemeen raden we aan om waar mogelijk 256-bit-sleutels te gebruiken en 128-bit-sleutels als een acceptabel alternatief te beschouwen. De belangrijkste conclusie is dat organisaties prioriteit moeten geven aan de migratie van asymmetrische primitieven. We raden zelfs aan dat organisaties alleen middelen toewijzen aan het updaten van de symmetrische sleutels als ze ál hun asymmetrische primitieven naar post-quantumalternatieven hebben gemigreerd.

4.3) Migreren van protocollen

Deze sectie beschrijft hoe protocollen naar een quantumveilige versie kunnen worden gemigreerd. Er worden verschillende veelgebruikte protocollen besproken en voor elk protocol wordt ten minste één oplossing gegeven om naar PQC te migreren. Voor elk van deze oplossingen worden actiepunten genoemd voor systeembeheerders, softwarelibrary-ontwikkelaars en personeel dat verantwoordelijk is voor het beveiligingsbeleid binnen de organisatie. Hoewel dit advies nog op een vrij abstract niveau is, biedt het wel handvatten voor enkele van de relevante partijen. De gangbare protocollen die deze sectie worden behandeld zijn TLS, SSH, S/MIME, PGP, IPSec en X.509. Veel van deze protocollen worden gedefinieerd in een type document genaamd een RFC (Request for Comments). Dit zijn standaardisatiedocumenten die worden geproduceerd door de Internet Engineering Task Force (IETF). Conceptstandaarden worden Internet Drafts genoemd.

TLS

Beschrijving | TLS garandeert de vertrouwelijkheid, authenticiteit en integriteit van communicatie via internet [Res18].

Huidige versie | TLS 1.3 [Res18].

Standaardisatiedocumenten | RFC 8446 [Res18].

Normaal gebruik | TLS wordt gebruikt in verschillende domeinen zoals HTTPS en beveiligde e-mail.

Voor de migratie van TLS naar PQC zijn er twee opties: het gebruik van vooraf gedeelde sleutels (optie 1) en de hybride benadering (optie 2).

Opmerking voor systeembeheerders | Het advies luidt om voor elk scenario en elke optie TLS 1.3 te gebruiken. Zorg er bovendien voor dat ofwel **AES-256-GCM** ofwel **ChaCha20-Poly1305** is geïntegreerd in de gekozen versleutelingssuites voor geauthentiseerde versleuteling met bijbehorende dataversleutelingen.

TLS, optie 1: van tevoren gedeelde sleutels

Te implementeren beleid | Hoewel het beleid van use case tot use case kan verschillen, moet er een strikt beleid worden opgesteld voor het delen van deze symmetrische sleutels om te voorkomen dat ze in de handen van kwaadwillende actoren komen en per ongeluk met het verkeerde systeem worden gedeeld. Bovendien dient er een beleid te worden opgesteld dat duidelijk definieert welke systemen gebruik mogen maken van TLS met vooraf gedeelde sleutels. Ten slotte moet het gebruik van deze vooraf gedeelde sleutels in het sleutelbeheer worden vermeld. Vooraf gedeelde sleutels moeten minimaal 256-bits zijn om store-now-decrypt-later aanvallen te voorkomen. Een lagere bitsleutel kan echter ook acceptabel zijn, rekening houdend met hoe lang de informatie vertrouwelijk moet blijven, zoals eerder besproken. Ten slotte is een duidelijk beleid nodig waarin wordt aangegeven wanneer en hoe de omschakeling van vooraf gedeelde sleutels naar hybride of volledig post-quantumsleutels moet worden uitgevoerd.

Opmerking voor systeembeheerders | Uiteraard moet de systeembeheerder TLS configureren om vooraf gedeelde sleutels te gebruiken. Deze informatie is te vinden in de documentatie van de TLS-leverancier. Neem contact op met de TLS-leverancier als de TLS-implementatie geen vooraf gedeelde sleutels ondersteunt.

Softwarelibrary-ontwikkelaars | Een gedetailleerd technisch overzicht van het implementeren van vooraf gedeelde sleutels in TLS is gedefinieerd in RFC 4279 [ET05] en RFC 5487 [IETF09]. Softwarelibrary-ontwikkelaars moeten ervoor zorgen dat hun TLS-implementatie voldoet aan deze standaarden

TLS, optie 2: hybride constructie

Er is een Internet Draft die aangeeft hoe de hybride sleuteluitwisseling verloopt. Dit is een handig hulpmiddel om te begrijpen hoe de hybride oplossing in TLS kan worden geïmplementeerd, zie [IETF24].

Te implementeren beleid | Cruciaal beleid is een gesprek met de systeembeheerder en eventueel cryptografische experts over de toegestane versleutelingssuites die kunnen worden gebruikt om quantumveiligheid te waarborgen. Volgens de eerdere uitleg over store-now-decrypt-later aanvallen hoeft u misschien niet alle systemen quantumveilig te maken. Daarom is het absoluut noodzakelijk om te bepalen welke systemen deze gewijzigde TLS zouden gebruiken. Dit is vooral belangrijk omdat de RFC momenteel wordt opgesteld en ongetwijfeld zal worden bijgewerkt. Deze veranderingen moeten dan ook in het beleid worden weerspiegeld. Ten slotte moet er sprake zijn van een duidelijk beleid dat aangeeft wanneer en hoe de overgang van de hybride benadering naar volledig PQC moet worden uitgevoerd.

Opmerking voor systeembeheerders | De systeembeheerder moet de TLS configureren om deze hybride benadering te gebruiken. Deze informatie vindt u in de documentatie van de TLS-leverancier. Overweeg om van TLS-leverancier te veranderen of neem contact op met de TLS-leverancier als de TLS-implementatie deze RFC niet ondersteunt.

Softwarelibrary-ontwikkelaars | Softwarelibrary-ontwikkelaars kunnen deze experimentele functie op basis van de RFC implementeren. Uiteraard zullen er meer herzieningen van dit concept worden gepubliceerd. Oftewel, we verwachten dat implementaties in de loop van de tijd zullen veranderen.

SSH

Beschrijving | SSH stelt partijen in staat om op afstand veilige netwerkdiensten uit te voeren.

Huidige versie | SSH-2 [LY06].

Standaardisatiedocumenten | RFC 8446 [LY06].

Normaal gebruik | SSH wordt veelal gebruikt om op afstand ergens in te loggen en op afstand opdrachten uit te voeren. Aangezien het SSH-protocol géén vooraf gedeelde sleutels accepteert, moeten alle scenario's de hybride benadering gebruiken.

Er is een Internet Draft over hybride sleuteluitwisseling die illustreert hoe hybride SSH kan worden geïmplementeerd, zie [KSFH+20].

Te implementeren beleid | Cruciaal is een gesprek met de systeembeheerder en eventueel cryptografische experts over de toegestane versleutelingen die kunnen worden gebruikt om quantumveiligheid te waarborgen. Volgens de eerdere uitleg over store-now-decrypt-later aanvallen hoeft u misschien niet alle systemen

quantumveilig te maken. Daarom is het absoluut noodzakelijk om te bepalen welke systemen deze gewijzigde versie van SSH zouden gebruiken. Dit is vooral belangrijk omdat de RFC momenteel wordt opgesteld en ongetwijfeld zal worden bijgewerkt. Deze veranderingen moeten dan ook in het beleid worden weerspiegeld. Ten slotte moet er sprake zijn van een duidelijk beleid dat aangeeft wanneer en hoe de overgang van de hybride benadering naar volledig post-quantum moet worden uitgevoerd.

Opmerking voor systeembeheerders | De systeembeheerder moet SSH configureren om deze hybride benadering te gebruiken. Deze informatie vindt u in de documentatie van de SSH-leverancier. Overweeg om van SSH-leverancier te veranderen of neem contact op met de SSH-leverancier als de SSH-implementatie deze RFC niet ondersteunt.

Softwarelibrary-ontwikkelaars | Softwareontwikkelaars kunnen deze functie op basis van de RFC implementeren. Uiteraard zullen er meer herzieningen van dit concept worden gepubliceerd. Met andere woorden verwachten we dat implementaties in de loop van de tijd zullen veranderen.

S/MIME

Beschrijving | S/MIME ondersteunt vertrouwelijkheid en authenticatie voor MIME-data (audio, afbeeldingen...).

Huidige versie | S/MIMEv4 [Hou02].

Standaardisatiedocumenten | RFC 8551 [SRT19] and RFC 3369 [Hou02].

Normaal gebruik | S/MIME wordt vaak gebruikt in beveiligde e-mailcommunicatie.

Op dit moment is er weinig onderzoek naar post-quantum S/MIME. OpenQuantumSafe biedt een fork van OpenSSL aan met een quantumveilige S/MIME, dat ofwel een hybride benadering toepast of alleen post-quantum primitieven gebruikt [OQS S/MIME24]. Ze stellen echter dat deze library niet is bedoeld voor productieomgevingen, hetgeen het gebruik in de echte wereld beperkt.

Alle scenario's moeten worden gebaseerd op de hybride benadering aangezien dit protocol geen vooraf gedeelde sleutels accepteert.

Te implementeren beleid | Waarschijnlijk is het meest ideale beleid om per e-mail geen informatie uit te wisselen die langer vertrouwelijk moet blijven dan het begin van de ontsleutelingsfase van store-now-decrypt-later aanvallen. Elke uitwisseling van dergelijke informatie moet als een beveiligingsincident worden gemarkeerd. Als de leverancier een productiewaardige quantumveilige versie van S/MIME implementeert, moet er beleid worden geïmplementeerd dat het juiste gebruik en de omschakeling naar deze nieuwe versie aangeeft. Ten slotte moet er sprake zijn van een duidelijk beleid dat aangeeft wanneer en hoe de overgang van de hybride benadering naar volledig post-quantum moet worden uitgevoerd.

Opmerking voor systeembeheerders | Als de leverancier een productiewaardige quantumveilige versie van S/MIME implementeert, moet de systeembeheerder deze nieuwe versie van S/MIME volgens het vastgestelde beleid configureren. Neem ook contact op met de huidige S/MIME-leverancier om naar PQC te informeren.

Softwarelibrary-ontwikkelaars | De bovengenoemde OpenQuantumSafe-library kan worden gebruikt als basis om de S/MIME-library quantumveilig te maken. Dit moet expliciet worden bestempeld als een experimentele functie en de ontwikkelaar moet nieuwe ontwikkelingen op dit gebied blijven volgen.

PGP

Beschrijving | PGP ondersteunt vertrouwelijkheid en authenticatie van data en diensten voor sleutel- en certificaatbeheer.

Huidige versie | OpenPGP [IETF07] en GnuPGP [MJ21].

Standaardisatiedocumenten | RFC 4880 [IETF07].

Normaal gebruik | PGP wordt vaak gebruikt in beveiligde e-mailcommunicatie.

Opmerking voor systeembeheerders | Elke uitwisseling van dergelijke informatie moet als een beveiligingsincident worden gemarkeerd. U kunt ook contact opnemen met de huidige PGP-leverancier om naar quantumveiligheid te informeren. De organisatie moet nieuwe ontwikkelingen op dit gebied blijven volgen.

Softwarelibrary-ontwikkelaars | Het bijhouden van RFC-ontwerpen en wetenschappelijke literatuur op dit gebied is absoluut noodzakelijk om PGP naar een quantumveilige versie te migreren.

IPSec

Beschrijving | IPSec versleutelt en authentiseert IP-pakketten tussen communicerende partijen.

Huidige versie | IPSec-v3 [FK11].

Standaardisatiedocumenten | RFC 6071 [FK11].

Normaal gebruik | IPSec wordt vaak gebruikt in VPNs.

Er zijn twee opties: gebruik van vooraf gedeelde sleutels (optie 1) en de hybride aanpak (optie 2).

IPSec, option 1: van tevoren gedeelde sleutels

Te implementeren beleid | Hoewel het beleid van use case tot use case kan verschillen, moet er een strikt beleid worden opgesteld voor het delen van deze symmetrische sleutels. Verder moet er een beleid worden opgesteld dat duidelijk definieert welke systemen IPSec met vooraf gedeelde sleutels mogen gebruiken. Ten slotte moet het gebruik van deze vooraf gedeelde sleutels in het sleutelbeheer worden vermeld. Het is belangrijk dat de partijen die de symmetrische vooraf gedeelde sleutels gebruiken ervoor zorgen dat de sleutels ten minste 256 bits lang zijn om store-now-decrypt-later aanvallen te voorkomen. Een lagere bit-sleutel kan echter ook acceptabel zijn, rekening houdend met hoe lang de informatie vertrouwelijk moet blijven, zoals eerder besproken. Ten slotte is het belangrijk dat er een duidelijk beleid is dat aangeeft wanneer en hoe de omschakeling van vooraf gedeelde sleutels naar ofwel een hybride benadering ofwel een volledig post-quantumsleutel moet worden uitgevoerd.

Opmerking voor systeembeheerders | Uiteraard moet de systeembeheerder IPSec configureren om van tevoren gedeelde sleutels te gebruiken. Deze informatie vindt u in de documentatie van de IPSec-leverancier. Overweeg om van IPSec-leverancier te veranderen (ten minste voor de systemen die gebruik moeten gaan maken van vooraf gedeelde sleutels) of neem contact op met de IPSec-leverancier als de IPSec-implementatie geen vooraf gedeelde sleutels ondersteunt.

Softwarelibrary-ontwikkelaars | Een gedetailleerd technisch overzicht van dit proces is gedefinieerd in RFC 7296 [KHNE+14]. Softwareontwikkelaars moeten ervoor zorgen dat hun IPSec-implementatie aan deze standaarden voldoet. Er is ook een Internet Draft die handig kan zijn voor ontwikkelaars om met vooraf gedeelde sleutels quantumveiligheid te realiseren [FKMS20].

IPSec, optie 2: hybride constructie

ETSI TR 103 617 is een nuttig technisch hulpmiddel om quantumveiligheid in IPSec te realiseren [ETSI18].

Te implementeren beleid | Belangrijk is een gesprek met de systeembeheerder en eventueel cryptografische experts over de toegestane versleutelingssuites die kunnen worden gebruikt om quantumveiligheid te waarborgen. Volgens de eerdere uitleg over store-now-decrypt-later aanvallen hoeft u misschien niet alle systemen quantumveilig te maken. Daarom is het absoluut noodzakelijk om te bepalen welke systemen deze gewijzigde TLS zouden gebruiken. Dit is vooral belangrijk omdat de RFC momenteel wordt opgesteld en ongetwijfeld zal worden bijgewerkt. Deze veranderingen moeten dan ook in het beleid worden weerspiegeld.

Ten slotte moet er sprake zijn van een duidelijk beleid dat aangeeft wanneer en hoe de overgang van de hybride benadering naar volledig post-quantum moet worden uitgevoerd.

Opmerking voor systeembeheerders | De systeembeheerder moet IPSec configureren om deze hybride benadering te gebruiken. Deze informatie vindt u in de documentatie van de IPSec-leverancier. Overweeg om van IPSec-leverancier te veranderen (ten minste voor de systemen die gebruik moeten gaan maken van een hybride systeem) of neem contact op met de IPSec-leverancier als de IPSec-implementatie deze hybride benadering niet ondersteunt.

Softwarelibrary-ontwikkelaars | Library-ontwikkelaars kunnen deze functie implementeren op basis van het technische rapport van ETSI [ETSI18]. Uiteraard zullen er meer herzieningen van dit concept worden gepubliceerd. Met andere woorden verwachten we dat implementaties in de loop van de tijd zullen veranderen.

X.509

Beschrijving | X.509 bewijst eigendom van een publieke sleutel.

Huidige versie | X.509v3 [ITU19].

Standaardisatiedocumenten | RFC 5280 en ITU-T X.509 [ITU19].

Normaal gebruik | X.509 wordt vaak gebruikt om websites te authenticeren in HTTPS. Aangezien het X.509-protocol geen vooraf gedeelde sleutels accepteert, moeten alle scenario's de hybride benadering overwegen. De ITU-T heeft al een variant van hybride (meerdere algoritmes) certificaten gestandaardiseerd in sectie 9.8 van [ITU19]. Dit is gebaseerd op de verlopen Internet Draft van Truskovsky et al. [TGFK+18]. In de literatuur worden deze certificaten vaak katalysatorcertificaten genoemd. Daarnaast ontwikkelt de IETF nieuwe Internet Drafts [OGPK+24b; OGPK+24a] die een alternatieve vorm van hybride certificaten bieden, zogenaamde samengestelde certificaten. Natuurlijk zullen meer root CA's en CA's post-quantum certificaten gaan aanbieden, dus het is belangrijk om up-to-date te blijven met de markt.

Te implementeren beleid | Volgens de eerdere uitleg over store-now-decrypt-later aanvallen hoeft u misschien niet alle certificaten compatibel te maken met de hybride oplossing. Daarom is het absoluut noodzakelijk om te bepalen welke systemen dit X.509-certificaat zouden gebruiken. Verder dient in dit verband

opgemerkt te worden dat cryptografische en protocol-libraries dan compatibel moeten worden gemaakt met de nieuwe certificaten.

Tot slot moet er sprake zijn van een duidelijk beleid dat aangeeft wanneer en hoe de overgang van de hybride benadering naar volledig post-quantum moet worden uitgevoerd. Communicatie en planning met de CA of root-CA is essentieel om dit alles te realiseren.

System Administrators | De systeembeheerder moet X.509-certificaten zodanig configureren dat ze compa-tibel zijn met de hybride benadering.

Softwarelibrary-ontwikkelaars |Softwarelibrary-ontwikkelaars kunnen deze experimentele functie implementeren op basis van de RFC en de ITU-T. Uiteraard zullen er meer herzieningen van dit concept worden gepubliceerd.

4.4) Crypto-agility

Crypto-agility (van *cryptographic agility*: 'cryptografische wendbaarheid') is een principe met als doel dat een organisatie zich met minimale inspanning aan kan passen aan risico's rondom het gebruik van cryptografie. Concreet verwijst crypto-agility naar het structureren van technologie, processen en beleid op een manier waarop de cryptografie die bij een organisatie wordt gebruikt, efficiënt kan worden geconfigureerd. Dit betekent dat de cryptografie kan worden bijgewerkt, gewijzigd of volledig vervangen met minimale inspanning en nadelige gevolgen zoals downtime tot een minimum beperkt worden. Crypto-agility kan helpen op verschillende niveaus van cryptografie: het kan helpen om het ongeldig maken van cryptografische sleutels te vergemakkelijken, parameters bij te werken, een cryptografisch algoritme te vervangen door een ander algoritme of een implementatie van een cryptografisch algoritme te vervangen.
Crypto-agility kan niet zomaar worden gekocht, maar vereist afstemming op verschillende lagen binnen een organisatie. Er bestaan technische oplossingen die bijvoorbeeld automatisch problemen met cryptografie kunnen detecteren of de implementatie van een cryptografisch algoritme kunnen configureren/vervangen. Maar daarnaast moet crypto-agility ook worden geïntegreerd in bedrijfsprocessen en bedrijfsbeleid, om ervoor te zorgen dat de technische oplossingen rondom crypto-agility ook correct kunnen worden ingezet. Zo kan crypto-agility worden geïntegreerd in processen voor inkoop en change management. Ook moet crypto-agility worden opgenomen in het bredere cryptografische beleid om bepaalde oplossingen binnen een organisatie te verplichten.
De PQC-algoritmes die momenteel zijn of worden gestandaardiseerd zijn nog niet veel in de praktijk getest. Daarom is het waarschijnlijk dat specificaties, parameters of zelfs gehele algoritmes in de toekomst moeten worden bijgewerkt. Met crypto-agility kan dit worden gedaan met minimale moeite en beperkte verstoringen. Vooral als ervoor wordt gekozen om bepaalde cryptografische componenten gedeeltelijk te migreren voordat daadwerkelijke standaarden en gevalideerde implementaties beschikbaar zijn, moet een organisatie voorbereid zijn om de cryptografische componenten eenvoudig te kunnen veranderen zodra de relevante standaarden beschikbaar zijn of een nieuwe implementatie wordt aanbevolen. Dit is anders dan bij de momenteel gebruikte, quantumkwetsbare cryptografie, waarvoor standaarden en goede parameterkeuzes al lang en breed zijn vastgesteld en veranderingen minder vaak voorkomen.
Crypto-agility draagt niet alleen bij aan het soepele verloop van een migratie naar PQC, maar ook aan het beheer van cryptografie in het algemeen. Daarom beschouwen we het invoeren van crypto-agility in een organisatie als een no-regret move. Het kan immers nu al helpen bij het sneller identificeren van potentiële kwetsbaarheden en het verkorten van reactietijden in geval van een incident.

Desalniettemin blijft crypto-agility een enigszins abstract concept in de praktijk. Het beschouwen van specifieke modaliteiten of vormen van crypto-agility kan helpen om het doel explicieter te maken. In dit hoofdstuk geven we eerst richtlijnen over hoe crypto-agility kan worden opgenomen in technologie, processen en beleid. Daarna beschrijven we verschillende vormen van crypto-agility en veelvoorkomende uitdagingen om deze te bereiken. Tot slot bespreken we overwegingen bij het kiezen van een passende strategie omtrent crypto-agility.

Technische maatregelen voor crypto-agility

Op technisch niveau kunnen verschillende maatregelen worden getroffen om soepele overgangen tussen cryptografische algoritmes, parameters of implementaties te garanderen. Een startpunt voor crypto-agility is wederom duidelijke kennis over welke cryptografie wordt gebruikt en waar. Het bijhouden van een up-to-date cryptografische inventaris helpt enorm bij het controleren, identificeren en snel bijwerken van kwetsbare cryptografie. In sectie 2.3 worden technische oplossingen gepresenteerd die kunnen helpen bij het onderhouden van een dergelijke inventaris.

Daarnaast vormt compatibiliteit een grote uitdaging bij het beheer van cryptografie. Zo kunnen er bijvoorbeeld problemen optreden als een nieuw algoritme wordt geïnstalleerd bij één client, maar nog niet aan de andere kant van de verbinding. Het onderhouden van een gecentraliseerde cryptografische inventaris maakt het gemakkelijker om te controleren of een update tegelijkertijd in de gehele organisatie wordt uitgevoerd. Een ander onderdeel van cryptografiebeheer omvat het beheer van cryptografische sleutels en certificaten. Er bestaan tools die het mogelijk maken om het maken, verdelen en intrekken van cryptografische sleutels en certificaten (gedeeltelijk) te automatiseren.

De volgende fase waarin crypto-agility kan worden meegenomen, is tijdens de ontwikkeling van systemen die cryptografie gebruiken. Om een cryptografisch algoritme eenvoudig door een nieuwe te kunnen vervangen, kunnen aanroepen (calls) naar cryptografische functies in de broncode zoveel mogelijk worden geabstraheerd. Bovendien kunnen Continuous Integration/Continuous Deployment (CI/CD) pipelines worden benut om cryptografische functionaliteiten te testen. Op deze manier kunnen onjuiste toepassingen of compatibiliteitsproblemen van cryptografie vroegtijdig worden opgespoord. Bovendien kan deze informatie de prestaties van andere tools voor het detecteren van componenten verbeteren.

Systemen die cryptografie gebruiken kunnen worden ingericht om meerdere algoritmes tegelijkertijd te ondersteunen en andere systemen te laten kiezen welk algoritme voor iedere verbinding moet worden gebruikt. Dit kan het algehele systeem flexibeler en (backwards) compatibel maken. Aan de andere kant kan dit ook nieuwe kwetsbaarheden introduceren, zoals downgrade-aanvallen [NCSC-NL24].

Tot slot kan crypto-agility worden verbeterd door rekening te houden met de hardware-eisen van (toekomstige) cryptografische algoritmes. PQC zal meer capaciteit vereisen qua opslag, bandbreedte, enzovoort. Daarom is het belangrijk om te beoordelen of de huidige hardware geschikt is om in de toekomst PQC te draaien. Als dit niet het geval is, is het belangrijk om na te denken over alternatieve manieren om de hardware te upgraden of te vervangen. Meer informatie over de specifieke vereisten voor verschillende PQC-alternatieven is te vinden in hoofdstuk 6.

Crypto-agility in processen

Naast technische oplossingen kan en moet crypto-agility ook worden afgedwongen door deze op te nemen in bestaande processen. Afhankelijk van de volwassenheid van een systeem kunnen organisatorische maatregelen ook gemakkelijker worden aangenomen in vergelijking met technische oplossingen, vooral voor systemen die al in gebruik zijn. Door crypto-agility expliciet te documenteren in processen, kunnen blinde vlekken en knelpunten in het proces om cryptografie bij te werken gemakkelijker worden opgespoord. Bovendien vergroten processen de afstemming tussen betrokken belanghebbenden (zowel intern als extern) en kunnen ze worden doorgegeven als mensen weg gaan. Uiteindelijk leidt dit tot minder fouten bij updates van

cryptografie en dus tot minder verspilling van middelen zoals tijd en geld. Door de stappen van crypto-agility duidelijk te documenteren tijdens het uitvoeren van het proces, wordt een vorm van controle verkregen, wat ook wenselijk is voor crypto-agility.

Om crypto-agility in processen op te nemen, moet ten eerste de scope van de agility worden beschreven. Dit kan bijvoorbeeld gaan over welke vorm van crypto-agility het beoogt te bereiken en wanneer het proces moet beginnen en eindigen. Dit zal ook helpen bij het identificeren van de gerelateerde processen. Veelvoorkomende processen waarin crypto-agility kan worden meegenomen, zijn processen met betrekking tot inkoop, change management, ontwikkeling en publicatie van software en incidentresponsbeheer.

Crypto-agility moet worden meegenomen in inkoopprocessen met betrekking tot de aanschaf van nieuwe software- en hardwarecomponenten. Door crypto-agility mee te nemen kan er voor worden gezorgd dat het component in de toekomst correct kan worden bijgewerkt. Ook is het beoordelen en testen van de (geclaimde) agility-functies van een product een belangrijke stap voor crypto-agility. Voor hardware moet het in staat zijn om al verschillende algoritmes of parameters te ondersteunen, of dit moet in de toekomst gemakkelijk kunnen worden bijgewerkt. Houd er rekening mee dat het opnemen van agility vanaf het begin van de levenscyclus van een systeem doorgaans veel gemakkelijker is dan het implementeren ervan in bestaande systemen. Daarom zijn inkoopprocessen bijzonder nuttig om crypto-agility op te nemen. Dit komt ook nauw overeen met cryptografisch beleid, dat een bepaald niveau van agility voor nieuwe producten kan verplichten.

Daarnaast kunnen processen met betrekking tot de ontwikkeling en publicatie van software crypto-agility vergroten door middel van tests. Zo kan een proces bijvoorbeeld dicteren hoe en wanneer cryptografie kan worden getest om compatibiliteitsproblemen of andere kwetsbaarheden te voorkomen. Ook in het geval dat er cryptografie moet worden geüpdatet, moet worden beschreven hoe dit soepel kan worden geregeld als onderdeel van een software-release.

Processen voor change management beschrijven hoe organisaties efficiënt veranderingen in de organisatie kunnen doorvoeren. Een dergelijk proces kan bijvoorbeeld beschrijven waarom een verandering moet plaatsvinden, hoe deze moet worden geïmplementeerd en hoe de organisatie zich kan aanpassen aan de verandering. Voor crypto-agility is het belangrijk om te beschrijven hoe een update of vervanging van cryptografie moet worden georganiseerd. Bijvoorbeeld, dit kan beschrijven wie verantwoordelijk is voor welke cryptografie en hoe ervoor moet worden gezorgd dat de hele organisatie tegelijkertijd dezelfde wijzigingen in cryptografie doorvoert. Personen die doorgaans betrokken zijn bij een dergelijk proces zijn management of beleidsmakers die een wijziging in de cryptografie moeten goedkeuren, of softwareontwikkelaars/veiligheidsarchitecten die de update daadwerkelijk moeten installeren of uitvoeren.

Ten slotte beschrijven incidentresponsprocessen hoe een organisatie moet reageren in geval van een incident. Er kan bijvoorbeeld beschreven worden welke stappen moeten worden genomen in het geval dat een cryptografische sleutel is gecompromitteerd. Aangezien reactietijd vaak een belangrijke eis is, kan het beschrijven van stappen met betrekking tot crypto-agility helpen om het algehele proces te stroomlijnen. Door bijvoorbeeld continu alle cryptografie die in een organisatie wordt gebruikt te monitoren als onderdeel van een algeheel risicobeoordelingsproces, kunnen risico's vroegtijdig worden opgespoord. Ook kan het proces, in geval van een incident, helpen om te identificeren wie verantwoordelijk is voor welke beslissingen en bijvoorbeeld hoe een cryptografische sleutel snel moet worden ingetrokken.

Crypto-agility in beleid

Crypto-agility moet ook worden opgenomen in het beleid rondom cryptografisch beheer. Voor een uitgebreide uitleg van cryptografische beleidsmaatregelen verwijzen we naar sectie 2.3.1. Een logische manier om crypto-agility op te nemen is door technische en procedurele maatregelen voor crypto-agility verplicht te stellen, wat met name van toepassing is voor nieuwe systemen. Bovendien kan cryptografisch beleid voorschrijven dat een cryptografische inventaris periodiek moet worden bijgewerkt en personen verantwoordelijk worden gemaakt voor het beheer van cryptografie. Zo zou het beleid bijvoorbeeld kunnen specificeren wie verantwoordelijk is voor het controleren en bijhouden van de veiligheid van de gebruikte cryptografie, of

wie een update moet goedkeuren en uitvoeren indien dit gewenst is. Verder zou cryptografisch beleid kunnen specificeren hoe en wanneer de processen waarin crypto-agility is opgenomen moeten worden getest om te zorgen dat ze correct functioneren. Ook in beleidsmaatregelen rondom inkoop kan crypto-agility in acht worden genomen. Leveranciers kunnen bijvoorbeeld verplicht worden gesteld om binnen een bepaalde tijd na standaardisatie over te schakelen naar nieuwe PQC-algoritmes. Tot slot is een veelvoorkomend obstakel tijdens het bijwerken of vervangen van cryptografie dat een cryptografisch beleid slechts één algoritme of parameterset toestaat. Daardoor moet eerst het beleid worden bijgewerkt wanneer een migratie naar een nieuw algoritme of parameterset moet worden uitgevoerd. Een cryptografisch beleid moet hiervoor ruimte bieden door meer opties toe te staan. Aan de andere kant moeten organisaties ervoor zorgen dat hun cryptografisch beleid geen verouderde, achterhaalde of uitgefaseerde keuzes voor algoritmes of parameters bevat die niet meer veilig zijn.

4.4.1 Vormen van crypto-agility

Op basis van de resultaten van een cryptografieworkshop in 2019 [OPAB+19] presenteerde het Nederlandse Nationaal Cyber Security Centrum (NCSC) hun visie op de verschillende vormen van crypto-agility. De reden waarom organisaties crypto-agility willen, hangt af van hun context. Zorgvuldig kijken naar wat vereist is in welke context helpt om een beter begrip te verkrijgen van wat daadwerkelijk nodig is om een adequaat niveau van crypto-agility te bereiken met betrekking tot de gewenste doelen. In de rest van deze sectie zullen de verschillende vormen van crypto-agility worden uitgelegd en veelvoorkomende uitdagingen om deze te bereiken, worden besproken. Voor verdere discussie over de verschillende manieren om naar crypto-agility te kijken, verwijzen we naar [ASWH+23].

Migratie-agility

Dit is waarschijnlijk de bekendste vorm van crypto-agility. Het doel is om in staat te zijn om het ene cryptografische algoritme te vervangen door een ander. Daarom is dit de belangrijkste vorm van crypto-agility die nodig is om te migreren van quantumkwetsbare cryptografie naar post-quantumcryptografie. Het is belangrijk om ervoor te zorgen dat migratie-agility wordt geïmplementeerd bij iedere toepassing van het algoritme voor een dienst of applicatie. Het niet bijwerken van het algoritme of de parameters op iedere plek kan compatibiliteitsproblemen veroorzaken wanneer de ene kant van de communicatie de nieuwe configuratie gebruikt terwijl de andere kant nog steeds de oude configuratie gebruikt. Dit is vooral moeilijk als verschillende instanties van het algoritme worden beheerd door verschillende (externe) entiteiten. Daarnaast kan het niet verifiëren dat het algoritme overal in de organisatie is bijgewerkt kwetsbaarheden introduceren omdat een aanvaller simpelweg het deel zal aanvallen waar de oude configuratie nog in gebruik is. Tot slot kan hardwarecompatibiliteit een obstakel zijn voor migratie-agility, aangezien de hardware bijvoorbeeld grotere sleutels of ciphertexts moet kunnen ondersteunen. Verder kunnen huidige hardwareversnellers niet compatibel zijn met het nieuwe algoritme, waardoor het veel langzamer wordt. Maatregelen om deze vorm van crypto-agility te vergroten en de bijbehorende risico's te beperken, zijn onder andere het implementeren van cryptografisch componentbeheer, het abstraheren van de code die verantwoordelijk is voor de cryptografische operaties zodat deze slechts op één locatie hoeft te worden gewijzigd, en het hebben van een goed overzicht en communicatielijnen met interne en externe afhankelijkheden. Bovendien kan het ondersteunen van meerdere algoritmes of parametersets in een "OF"-modus helpen om deze (tijdelijke) compatibiliteitsproblemen te verhelpen. Dit kan echter ook het risico van downgrade-aanvallen introduceren, waarbij een aanvaller opzettelijk een zwakker algoritme kiest om aan te vallen [NCSC-NL24]. Daarom moeten de ondersteunde algoritmes worden gecontroleerd en verwijderd zodra ze niet langer nodig zijn voor compatibiliteit of niet langer veilig zijn.

Compliance-agility

Deze vorm van agility verwijst naar cryptografische infrastructuur die eenvoudig opnieuw kan worden geconfigureerd om gelijktijdig te voldoen aan verschillende (regionale) regelgeving. In dat geval zullen er meerdere "versies" van hetzelfde systeem zijn, elk met een andere cryptografische configuratie. Het is cruciaal om een goed overzicht te hebben van hoe die configuraties eruitzien en waar ze worden gebruikt. In het geval dat deze vorm van agility gewenst is om de cryptografie aan te passen aan veranderende regelgeving, is het vergelijkbaar met migratie-agility, maar met de extra vereiste dat er een vorm van controle aanwezig is om snel te voorzien wanneer een wijziging in regelgeving van toepassing is op een bepaald stuk cryptografie. Zo kan een land bijvoorbeeld het gebruik van een nieuwe set parameters voor vertrouwelijke informatie verplicht stellen. Daar komt nog bij dat migratie-agility slechts één systeem bijwerkt, terwijl er bij compliance-agility verschillende versies van hetzelfde systeem, die voldoen aan verschillende regelgeving, tegelijkertijd functioneren.

Implementatie-agility

In plaats van het cryptografische algoritme bij te werken, is het doel hier om op applicatieniveau de hele implementatie van een algoritme te kunnen vervangen. Dit kan bijvoorbeeld wenselijk zijn als er een nieuwe versie van de implementatie wordt uitgebracht. Voor implementatie-agility gelden vergelijkbare risico's als voor migratie-agility. Zo zijn compatibiliteits- en afhankelijkheidsproblemen ook hier een uitdaging. Daarnaast vereist het wijzigen van implementaties doorgaans het doorlopen van complexe processen in organisaties. Zo kan een bedrijf beleid en/of CI/CD-oplossingen hebben om de software te testen voordat deze kan worden vrijgegeven. Het is belangrijk om op de hoogte te zijn van deze processen en hun tijdsduur in acht te nemen voor de migratietijd. Aan de andere kant kunnen CI/CD-oplossingen ook een geweldige kans zijn om geautomatiseerde tests van cryptografische implementaties voor bekende kwetsbaarheden of andere fouten te integreren.

Platform-agility

Deze vorm van agility verwijst naar cryptografische algoritmes die naadloos integreren met verschillende platformtypen. Deze vorm van agility is voornamelijk van belang voor organisaties die daadwerkelijk cryptografische implementaties aan klanten leveren. Het houdt in dat dezelfde cryptografische algoritmes moeten kunnen draaien op veel verschillende apparaten, ongeacht de hard- en software die wordt gebruikt. Vooral bij het draaien van cryptografie op bepaalde apparaten kunnen problemen ontstaan wanneer een nieuw cryptografisch algoritme niet op de bestaande hardware past en deze hardware moeilijk te vervangen is. Bovendien vereisen sommige post-quantumalgoritmes complexere operaties die moeilijk te implementeren en uit te voeren zijn op deze apparaten. Het is raadzaam om deze overwegingen in acht te nemen.

Andere vormen van agility

Daarnaast zijn er in [OPAB+19] nog vier andere vormen van crypto-agility geïdentificeerd. Waarschijnlijk zijn deze echter voor een groot deel van de organisaties niet relevant. Dit kan omdat ze te geavanceerd, specifiek of riskant zijn. We raden aan om deze vormen van agility alleen te na te streven als een organisatie de cryptografische systemen die ze bouwen volledig begrijpt en deze vormen van agility echt nodig zijn. De vormen zijn security strength agility, retirement agility, composability agility en context agility:

- Security strength-agility verwijst naar systemen die dynamisch de veiligheidsparameters van de cryptografie kunnen wijzigen op basis van de algehele systeemconfiguratie. Dit kan veel moeite besparen voor organisaties die hun systemen continu in veel verschillende contexten met verschillende eisen inzetten. Aan de andere kant, voor (de meerderheid van) organisaties waarvoor dit niet het geval is, is deze vorm van agility mogelijk niet de moeite waard om na te streven.

- Composability-agility verwijst naar het bouwen van cryptografie op een manier die het gemakkelijk maakt om te combineren met andere cryptografische bouwstenen. Deze vorm van agility is bijzonder nuttig in de context van de PQC-migratie, waar hybride-EN composities van cryptografie naar verwachting als voorlopige oplossing zullen worden gebruikt. We verwachten echter dat voornamelijk de cryptografische experts die daadwerkelijk de cryptografie bouwen deze vorm van agility zullen inzetten.
- Retirement-agility verwijst naar systemen die automatisch verouderde of onveilige cryptografische algoritmes deactiveren.
- Context-agility verwijst naar cryptografische systemen die automatisch afleiden uit de context welk algoritme en beveiligingssterkte moet worden gebruikt. Bijvoorbeeld, het kiezen van een sterker (versie van een) algoritme op basis van de classificatie van de gegevens die moeten worden versleuteld. Hoewel dit een nuttige vorm van agility is, bestaat het risico dat per ongeluk onvoldoende veilige parameters worden gekozen en daardoor onvoldoende bescherming wordt geboden. Voor de meeste organisaties, die niet vaak de veiligheidsgraad hoeven te veranderen, is het veiliger om deze beslissingen handmatig te nemen.

4.4.2 Het kiezen van een geschikte strategie voor crypto-agility

Technische oplossingen, processen en beleidsmaatregelen zijn allemaal belangrijk om een systeem meer crypto-agile te maken. In de praktijk is het voor veel organisaties waarschijnlijk echter gemakkelijker om crypto-agility in processen op te nemen dan in technische en beleidsmatige oplossingen. Aan de andere kant kunnen technische oplossingen een zeer effectieve manier zijn een cryptografische wijziging te versnellen, terwijl beleidsmaatregelen een goede katalysator kunnen zijn om crypto-agility af te dwingen.

Het bepalen van welke maatregelen geschikt zijn en hoeveel crypto-agility vereist is voor een bepaald systeem of supply-chain kan een uitdagende taak zijn. Desalniettemin is het mogelijk om te redeneren over de vereiste snelheid van een cryptografische verandering op basis van het risicoprofiel van een toepassing, de persona van een organisatie en de gewenste vorm van crypto-agility.

Voor oudere systemen die al in gebruik zijn, zijn technische oplossingen zoals het abstraheren van aanroepen van cryptografie in de code moeilijk achteraf in te voeren. Voor toepassingen of producten die nog niet in productie zijn, raden we daarom sterk aan om crypto-agility al mee te nemen in het ontwerp van het product of de toepassing ervan te onderzoeken. Dit kan ook worden bevorderd door deze aspecten op te nemen in processen rondom de inkoop van nieuwe systemen.

Houd er rekening mee dat de mogelijkheden voor het opnemen van technische oplossingen rondom crypto-agility ook beperkt kunnen worden door de algehele volwassenheid van de organisatie zelf. Het automatisch bijwerken van de parameters van een bepaald cryptografisch algoritme kan bijvoorbeeld alleen gebeuren als er een goede, up-to-date cryptografische inventaris beschikbaar is.

Voor veel vormen van crypto-agility en veel organisaties is wat vertraging bij het wijzigen of bijwerken van cryptografie acceptabel zolang deze tijdsduur grotendeels zeker is. Zo hoeft een organisatie die compliance-agility in hun product vereist voor een release in een ander land de cryptografie niet binnen enkele minuten te kunnen vervangen. Een productrelease kan immers weken duren, dus is het wellicht voldoende om de cryptografie binnen enkele weken te kunnen vervangen. Dit geldt alleen als de organisatie er voldoende vertrouwen in heeft dat er geen significante vertragingen zullen zijn.

In sommige situaties is het echter wel erg belangrijk om zeer snel te kunnen reageren en grote zekerheid te hebben over eventuele vertragingen. Dit is bijvoorbeeld het geval voor een organisatie die migratie-agility vereist om te reageren op nieuw ontdekte kwetsbaarheden in de cryptografie die gebruikt wordt voor het beschermen van persoonlijke gegevens.

Al met al zal het evalueren van de technische, procesmatige en beleidsgeoriënteerde aspecten van crypto-agility en het testen ervan helpen bij het inschatten of de tijdsduur acceptabel is of niet. Als de vertraging bij een verandering in cryptografie onaanvaardbaar is gezien het risicoprofiel en de gewenste vorm van agility, moet een organisatie verder onderzoek doen naar mogelijkheden om de efficiëntie van het proces te verbeteren.

5 Recente ontwikkelingen

Samenvatting

In dit hoofdstuk bespreken we recente ontwikkelingen en lopende inspanningen in het PQC-migratieproces. We beginnen met het bespreken van de huidige status van verschillende standaardisatie-initiatieven, met een focus op het NIST-standaardisatieproces, dat het meest geavanceerd en uitgebreid is. We onderzoeken ook wetgeving die PQC-migratie verplicht stelt, samen met flexibelere richtlijnen en aanbevelingen die aan verschillende organisaties worden gegeven. Het hoofdstuk sluit af met inzichten en opgedane ervaringen op basis van eerdere migraties.

5.1 Status van verschillende standaardisatie-initiatieven

Sinds de bewustwording dat quantumcomputers een bedreiging vormen voor de cryptografische systemen die momenteel in gebruik zijn, zijn er veel inspanningen geleverd om deze dreiging te mitigeren. De meeste van deze inspanningen zijn geconsolideerd door standaardisatieprocessen die ons in staat stellen om algoritmes te specificeren die bestand zijn tegen quantumdreigingen, hun veiligheid en efficiëntie te testen, en richtlijnen te bieden voor hoe deze algoritmes moeten worden geïmplementeerd en geïntegreerd in grotere IT-systemen. Deze sectie biedt een overzicht van verschillende standaardisatie-initiatieven rondom PQC. Een kort overzicht van post-quantumcryptografie wordt gepresenteerd in sectie 6.3.1.

Aangezien de impact van een grootschalige quantumcomputer op symmetrische cryptografie als klein wordt beschouwd [NIST16c] (het verdubbelen van de grootte van de sleutels zou dezelfde veiligheid moeten bieden als zonder quantumcomputers), richten we ons voornamelijk op asymmetrische cryptosystemen, namelijk sleutelinkapselingsmechanismen (KEMs, van *key encapsulation mechanism*) en algoritmes voor digitale handtekeningen (DSA's, van *digital signature algorithm*). In de volgende subsectie geven we vervolgens een samenvatting van het standaardisatieproces van NIST, het grootste standaardisatieproces waarop de meeste internationale cryptografische instanties zich baseren. We geven ook enige basisinformatie over de huidige staat van het proces. We eindigen de sectie met basisinformatie over andere voltooide, lopende en in voorbereiding zijnde standaardisatieprocessen en gerelateerde inspanningen.

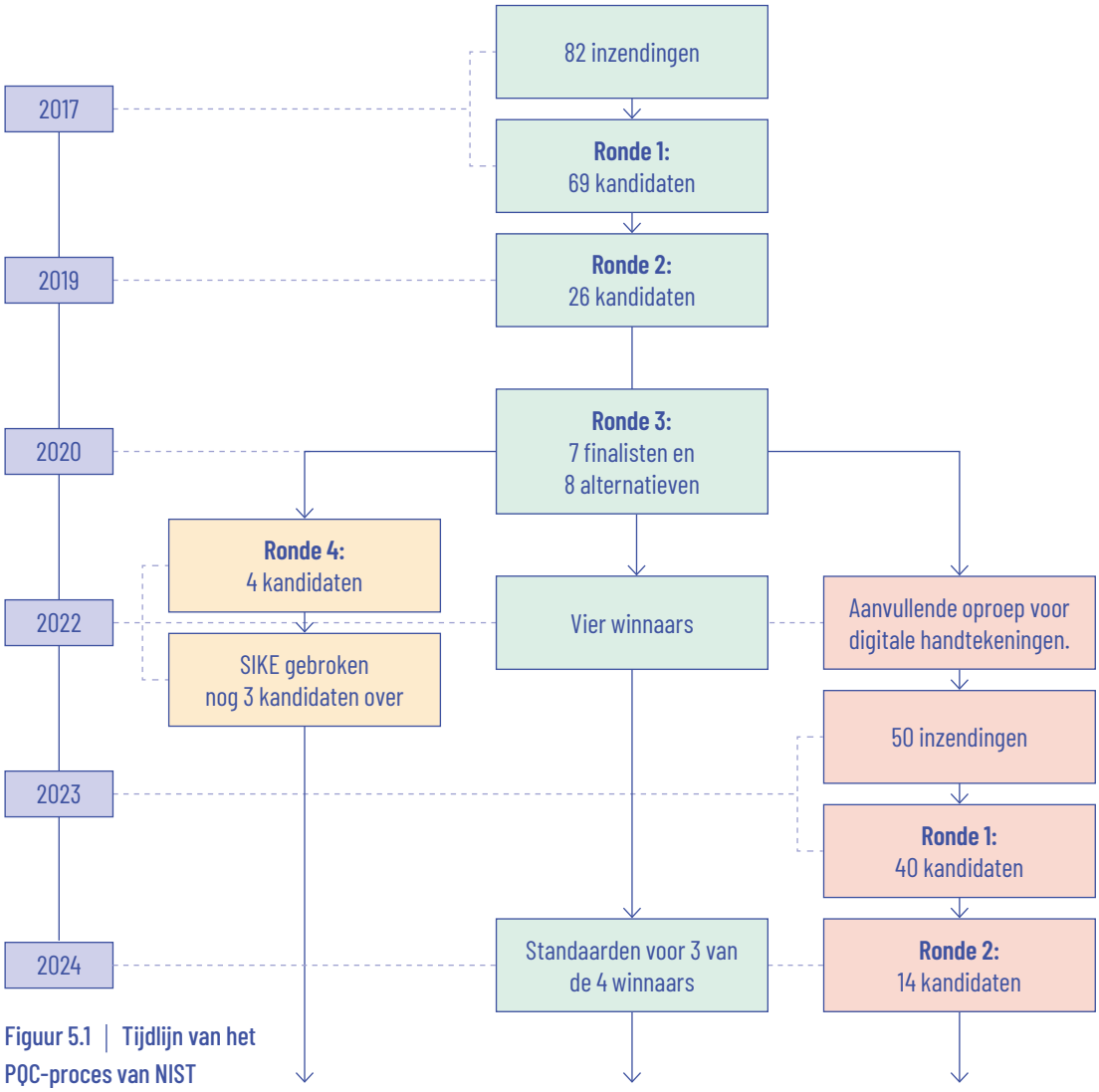
5.1.1 PQC-standaardisatieprocedure van NIST

In 2016 begon het National Institute of Standards and Technology (NIST) met de standaardisatie van publieke-sleutel encryptie (PKE)/sleutel inkapselingsmechanismen (KEM), en digitale handtekeningen algoritmes (DSA). Na drie grote fasen, die publieke beoordelingen en evaluaties omvatten, selecteerde NIST in juli 2022 de volgende kandidaten voor standaardisatie: een sleutelinkapselingsmechanisme bekend als CRYSTALS-Kyber (nu hernoemd naar ML-KEM) en drie digitale handtekeningalgoritmes, namelijk CRYSTALS-Dilithium (hernoemd naar ML-DSA), Falcon (hernoemd naar FN-DSA) en SPHINCS+ (hernoemd naar SLH-DSA). De eerste standaarden werden in augustus 2024 uitgebracht als Federal Information Processing Standards (FIPS) [NIST24a; NIST24b; NIST24c].

Naam	Functionaliteit	Veiligheidsaanname	Standaard
ML-KEM	Sleutelinkapseling/encryptie	Gestructureerde roosters	[NIST24a]
ML-DSA	Digitale handtekening	Gestructureerde roosters	[NIST24b]
Falcon (FN-DSA)	Digitale handtekening	Gestructureerde roosters	nog niet beschikbaar
SLH-DSA	Digitale handtekening	Hashing (zonder toestand)	[NIST24c]

Tabel 5.1 | Overzicht van de algoritmes die door NIST geselecteerd zijn voor standaardisatie.

Daarnaast zijn er vier extra KEMs doorgegaan naar een laatste, vierde ronde met de intentie om een van hen te standaardiseren. Sinds mei 2023 zijn er nog drie kandidaten in deze ronde, namelijk Classic McEliece, Bike en HQC. Deze zijn alle drie gebaseerd op zogenaamde foutcorrigerende codes. Om de veiligheidsaannames waarop PQC gebaseerd is diverser te maken, heeft NIST nog een extra oproep gedaan specifiek voor digitale handtekeningen. Hiervan werden de tweede-ronde kandidaten in oktober 2024 bekendgemaakt. De tijdlijn in de figuur representeert de tijdsvakken van de vier rondes en de extra oproep in het standaardisatieproces, waar het begin van iedere oproep grofweg overeenkomt met het moment waarop de kandidaten door NIST bekend werden gemaakt.



Figuur 5.1 | Tijdlijn van het PQC-proces van NIST

Standaardisatie van hash-gebaseerde digitale handtekeningen met een interne toestand | Voorafgaand aan het hoofdproces van PQC-standaardisatie dat in deze sectie wordt beschreven, zijn in 2020 al twee quantumveilige digitale handtekeningen gestandaardiseerd door NIST [NIST20a]. Hun belangrijkste kenmerk is er een interne toestand moet worden bijgehouden van een aantal geheime gegevens die niet opnieuw mogen worden gebruikt. Merk op dat SLH-DSA [NIST24c] deze vereiste niet heeft: dit algoritme is *stateless*. Voor meer details kunt u het einde van deze subsectie raadplegen, waar meer informatie over stateful hash-gebaseerde handtekeningen schema's staat.

Evaluatiecriteria

Het belangrijkste criterium voor het evalueren van cryptografische schema's was de veiligheid. Concreet moesten de kandidaten aantoonbaar sterke veiligheidskenmerken bevatten, bekend als IND-CCA2 (semantische veiligheid met betrekking tot adaptieve gekozen ciphertext-aanvallen) voor key encapsulation mechanisms, en EUF-CMA (existentiële onvervalsbaarheid met betrekking tot adaptieve gekozen berichtaanvallen) voor digitale handtekeningen. Naast theoretische veiligheid moesten de kandidaten ook veiligheid in de praktijk waarborgen met betrekking tot bekende aanvallen. Hiervoor bood NIST 5 veiligheidscategorieën aan die dienden als een nieuwe maatstaf om de veiligheid van de cryptografische schema's te vergelijken. Elke categorie was gedefinieerd om vergelijkbare veiligheid te bieden als goed geanalyseerde symmetrische cryptografische schema's zoals AES en collision-resistant hashfuncties. Uiteindelijk concentreerden de inzendingen zich voornamelijk op niveaus 1, 3 en 5, die respectievelijk overeenkwamen met AES-128, AES-192 en AES-256.

Het standaardisatieproces

Hier geven we een samenvatting van de verschillende fasen van de selectie van de standaarden.

Selectie van de eerste kandidaten | De eerste ronde waarin alle kandidaten die zowel aan de indieningsvereisten als de minimale acceptatiecriteria voldeden, werden geëvalueerd. Na feedback van de cryptografische gemeenschap en op basis van de bovengenoemde evaluatiecriteria koos NIST vervolgens kandidaten die doorgingen naar de tweede ronde. De tweede en derde ronde waren gewijd aan grondigere analyses en verdere experimentele verificatie die uiteindelijk resulteerden in de kandidaten die werden gekozen voor standaardisatie. Meer details over de eerste drie rondes zijn te vinden in de NIST-samenvattingen van de rondes, zie [NIST19b], [NIST20b] en [NIST22].

De vierde ronde | Na drie ronden werden er een sleutelinkapselingsmechanisme (ML-KEM [NIST24a]) en drie digitale handtekeningen (ML-DSA [NIST24b], FN-DSA en SLH-DSA [NIST24c]) als volwassen genoeg beschouwd en geselecteerd voor standaardisatie[1]. Omdat drie van deze schema's zijn gebaseerd op vergelijkbare veiligheidsaannames met betrekking tot gestructureerde roosters, wil NIST ook algoritmes selecteren die zijn gebaseerd op andere veiligheidsaannames. Hierdoor gingen er ook vier KEMs doornaar een extra vierde ronde: BIKE, Classic McEliece en HQC die gebaseerd zijn op foutcorrigerende codes, en SIKE, die gebaseerd is op zogenaamde isogenieën. SIKE onderging echter een aantal baanbrekende aanvallen in de zomer van 2023, te beginnen met [CD23], waardoor het niet meer overwogen wordt voor standaardisatie. De vierde ronde bestaat daardoor nog drie KEMs, waarvan er ten minste één tegen 2025 moet worden gestandaardiseerd.

Aanvullende oproep voor digitale handtekeningen | Naast de vierde ronde riep NIST ook op tot een aanvullende ronde voor digitale handtekeningen met als doel meer algemene handtekeningenschema's te introduceren die niet zijn gebaseerd op gestructureerde roosters, evenals handtekeningenschema's die korte handtekeningen en snelle verificatie hebben, wat relevant is voor bepaalde toepassingen. Hoewel het primaire doel is om de handtekeningen te diversifiëren door meer variatie in de onderliggende aanname van

[1] In Oktober 2024 was de standaard voor FN-DSA nog niet gepubliceerd.

digitale handtekeningen te introduceren, verklaarde NIST dat inzendingen die zijn gebaseerd op gestructureerde roosters nog steeds in overweging zouden worden genomen als ze significant beter presteren dan ML-DSA en FN-DSA in relevante toepassingen en aanvullende relevante veiligheidskenmerken bieden.

Hash-gebaseerde digitale handtekeningen met een toestand | In oktober 2020 koos NIST ervoor om twee bestaande quantumveilige schema's voor digitale handtekeningen te standaardiseren in NIST SP 800-208: LMS (al gestandaardiseerd in IRTF RFC 8554) en XMSS (al gestandaardiseerd in IRTF RFC 839) [NIST20a; IETF19; IETF18]. Dit zijn de eerste twee quantumveilige schema's die door NIST zijn gestandaardiseerd, nog vóór het standaardisatieproces dat hierboven is beschreven. Hun veiligheid is gebaseerd op de moeilijkheid van het inverteren van een cryptografische hashfunctie. Ze zijn daardoor een conservatieve optie zijn voor quantumveiligheid. LMS en XMSS (MT) zijn gestandaardiseerd voor specifieke toepassingen die 1) voor de lange termijn zijn, 2) niet kunnen wachten op het hoofdstandaardisatieproces en 3) niet praktisch zijn om achteraf bij te werken. In tegenstelling tot SLH-DSA hebben deze twee schema's een *interne toestand* (ze zijn *stateful*, terwijl SLH-DSA *stateless* is). Omdat deze interne toestand belangrijk en gevoelig is, vereisen deze algoritmes daarom strikte operationele procedures. Daarom heeft NIST in SP 800-208 gespecificeerd dat sleutelmateriaal binnen een gecertificeerde cryptografische module moet worden gegenereerd en nooit mag worden geëxporteerd. Wiggers et al. hebben een document opgesteld om richtlijnen te bieden voor operationele en technische aspecten in het beheer van de toestand en backup voor LMS en XMSS(MT) [WBKG+24]. Dit bevat oplossingen binnen de strikte eisen van NIST, maar ook daarbuiten.

5.1.2 Andere standaardisatie-initiatieven

Naast het standaardisatieproces van NIST zijn er andere standaardisatie-initiatieven geweest die hebben geresulteerd of zullen resulteren in nieuwe cryptografische standaarden. De meeste hiervan waren echter veel kleiner van omvang en sommige waren alleen gericht op specifieke domeinen. Hier vermelden we enkele van de recent voltooide en lopende PQC-standaardisatieprocessen en bespreken we de processen die in voorbereiding zijn. Voor sommige hiervan vermelden we alleen hun bestaan, maar gaan we niet in detail vanwege een gebrek aan redelijk toegankelijke documentatie.

International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC)
ISO en IEC zijn internationale organisaties die standaarden ontwikkelen voor vrijwel alle industrieën. In het bijzonder hebben ze een gezamenlijke technische commissie (JTC 1) opgericht met de naam Information Technology om specifiek standaarden voor informatie- en communicatietechnologie te ontwikkelen. Ter voorbereiding op de post-quantum migratie hebben ze gezamenlijk een document uitgebracht waarin de noodzaak van post-quantum migratie en de wiskundige problemen die ten grondslag liggen aan toekomstige post-quantum standaarden worden beschreven. Als onderdeel van de ISO/IEC 14888-serie hebben ze al hash-gebaseerde handtekeningen met een interne toestand gestandaardiseerd in ISO 14888-4 [ISO24], inclusief LMS, XMSS, HSS, and XMSS-MT. Daarnaast ontwikkelt ISO/IEC JTC1 een PQC-amendement op ISO/IEC 18033-2 [ISO06]. Dit is nog niet officieel uitgebracht, maar naast de NIST-standaarden wordt verwacht dat ISO/IEC ook de sleutelinkapselingsmechanismen FrodoKEM [ABDL+21] en Classic McEliece [ABCC+20] zal standaardiseren, die qua veiligheidsaannames als conservatiever worden beschouwd dan ML-KEM.
Naast hun standaardisatie-inspanningen werkt ISO nauw samen met andere internationale organisaties zoals het International Accreditation Forum (IAF), die certificeringen bieden waarmee sommige producten voldoen aan ISO-standaarden door middel van zorgvuldige audits. Dit vergroot het vertrouwen dat klanten hebben in producten en diensten, en voor sommige industrieën zijn dergelijke certificeringen zelfs contractuele vereisten. Daarom kunnen ISO-standaarden in industriële omgevingen als nog belangrijker worden beschouwd dan NIST-standaarden.

Internet Engineering Task Force (IETF) | De IETF is een wereldwijd erkende organisatie die specifiek verantwoordelijk is voor de ontwikkeling van standaarden voor het internet via zogenaamde Requests For Comments (RFC's). Het bijzondere van de IETF is dat het een volledig open proces is met openbare mailinglijsten en vergaderingen. Hoewel de status van post-quantumcryptografie bij de IETF nog op het niveau van Internet drafts is (er is nog geen RFC uitgebracht), is het zeer actief en is er in het bijzonder een specifieke werkgroep genaamd Post-Quantum Use In Protocols (PQUIP)[2] opgericht op experimentele basis door de Internet Engineering Steering Group (IESG) om de ontwikkeling van de PQC-standaarden te coördineren. IESG is van plan om het in 2025 te herzien, wanneer de eerste RFC's naar verwachting officieel zullen worden uitgebracht. Daartoe werkt PQUIP nauw samen met de Cryptographic Forum Research Group (CFRG)[3], die RFC's uitbrengt waarin de verschillende cryptografische standaarden worden beschreven, evenals met meer specifieke werkgroepen zoals LAMPS[4], die zich richten op veilige e-mailcommunicatie; IPSECME[5], betrokken bij de integratie van post-quantumcryptografie in de IPsec-suite voorprotocollen die veel worden gebruikt in VPN's; COSE[6], gewijd aan het ontwikkelen van standaarden voor het beveiligen van gegevensobjecten met behulp van Concise Binary Object Representation (CBOR); of de TLS[7] en ACME[8] werkgroepen die respectievelijk verantwoordelijk zijn voor het standaardiseren van het Transport Layer Security-protocol en het specificeren van conventies voor geautomatiseerd certificaatbeheer. De status van post-quantum integratie is te vinden op https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc. Daarnaast werkt de PQUIP-werkgroep aan een gids die een overzicht biedt aan ontwikkelaars van het post-quantum landschap (van bedreigingen tot algoritmes). Het huidige concept van dit document is beschikbaar op https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/. Het kan worden gezien als een aanvulling op deze handleiding, maar is geen vervanging. Bijvoorbeeld, het PQUIP-document biedt geen duidelijk tijdschema over wanneer de daadwerkelijke migratie moet beginnen, wat wij wel doen in hoofdstuk 2. Daarnaast geeft onze section 4.4 een completer beeld over crypto-agility.

European Telecommunications Standards Institute (ETSI) | ETSI is een onafhankelijke, non-profit standaardisatieorganisatie gevestigd in Europa. Het wordt door de Europese Unie erkend als een van de belangrijkste standaardisatie-instellingen voor telecommunicatie. Wat betreft post-quantumcryptografie richt ETSI zich voornamelijk op het ondersteunen van implementaties van algoritmes die door NIST zijn gestandaardiseerd in plaats van de algoritmes zelf te standaardiseren. In juli 2020 publiceerde ETSI een richtlijn voor post-quantum migratie [ETSI20a]. Recentere rapporten van hun technische commissie CYBER richten zich op concreet advies over het gebruik van quantum-veilige hybride sleuteluitwisseling [ETSI20b] en het bieden van technische beschrijvingen van sleutelinkapselingsmechanismen [ETSI21a] en digitale handtekeningen [ETSI21b] die zijn ingediend voor de derde ronde van het NIST-standaardisatieproces

Korean Post-Quantum Cryptography (KpqC) | De eerste ronde van een competitie door het Zuid-Koreaanse onderzoekscentrum voor PQC begon in november 2022. Na een jaar van evaluatie kondigde het team vier KEMs en vier digitale handtekeningen aan die doorgaan naar de volgende ronde, waar hun veiligheid en efficiëntie verder zullen worden beoordeeld. Van de vier digitale handtekeningen die in de tweede ronde worden geëvalueerd, zijn er twee gebaseerd op roosters, één op multivariabele polynomen en één op symmetrische primitieven. Van de vier KEMs die in de tweede ronde zitten zijn er twee gebaseerd op roosters en twee op foutcorrigerende codes. De exacte tijdlijn voor het standaardisatieproces is nog niet duidelijk, maar de Zuid-Koreaanse overheid is van plan om haar nationale cryptografiesystemen tegen 2035 om te zetten naar PQC.

[2] https://datatracker.ietf.org/wg/pquip/about/
[3] https://datatracker.ietf.org/rg/cfrg/about/
[4] https://datatracker.ietf.org/wg/lamps/about/
[5] https://datatracker.ietf.org/group/ipsecme/about/
[6] https://datatracker.ietf.org/wg/cose/about/
[7] https://datatracker.ietf.org/group/tls/about/
[8] https://datatracker.ietf.org/wg/acme/about/

Chinese Association for Cryptologic Research (CACR) | In 2018 startte CACR een competitie voor symmetrische en asymmetrische cryptografische algoritmes. Na twee rondes kondigde CACR in januari 2020 de winnaars van de competitie aan. Meerdere algoritmes werden geselecteerd als de eerste-, tweede- en derde rangs kandidaten. Het resultaat van deze competitie is enigszins anders dan het NIST-standaardisatieproces, aangezien CACR geen standaardisatie-instelling is, maar eerder een onderzoeksorganisatie. Het doel van deze competitie was dus niet om nieuwe schema's te standaardiseren, maar eerder om nieuwe ontwerpen van post-quantum schema's aan te moedigen die in de toekomst mogelijk gestandaardiseerd kunnen worden.

Standaarden voor specifieke domeinen | In oktober 2010 standaardiseerde het American National Standards Institute (ANSI) een schema gebaseerd op een gestructureerd lattice-probleem met de bedoeling het voornamelijk te gebruiken voor de Amerikaanse financiële sector. Het aanvankelijk gestandaardiseerde schema werd later verbeterd door de zwakke parameters te vervangen en zo het gewenste beveiligingsniveau te bereiken, en de standaard werd in februari 2017 bijgewerkt. De details hiervan zijn te vinden in [ANSI10]. In februari 2024 kondigde de Global System for Mobile Communications Association (GSMA) richtlijnen aan voor post-quantum migratie voor verschillende gebruiksscenario's in mobiele communicatie [GSMA24].

5.2) Post-quantumcryptografie en wetgeving

Gestandaardiseerde cryptografische algoritmes worden aannemelijk veel vaker in de praktijk toegepast. Over het algemeen wordt aanbevolen om alleen gestandaardiseerde algoritmes te gebruiken. Echter, cryptografische standaarden zijn niet inherent verplicht en, tenzij aanvullende regelgeving van kracht is, kunnen organisaties ervoor kiezen om ze te negeren. Daarentegen creëert passende wetgeving een sterke stimulans voor organisaties om te beginnen met de migratie naar post-quantumcryptografie. Ze stellen wettelijke verplichtingen vast en ze houden organisaties verantwoordelijk voor hun cryptografische beslissingen.
Het belang van het reguleren van cyberbeveiligingsmaatregelen, en dus het inzetten van cryptografie, is duidelijk aangetoond. Ten eerste is het migreren van cryptografie een tijdrovende en dure onderneming, waarvan de voordelen mogelijk niet onmiddellijk zichtbaar zijn, vooral omdat de quantumdreiging zich pas in de toekomst zal manifesteren. Daarom kunnen organisaties de voorkeur geven aan winsten op de korte termijn boven risicobeperking op de lange termijn op het gebied van cyberbeveiliging. Investeren in post-quantumcryptografie zou een organisatie zelfs in een concurrentienadeel kunnen brengen. Het reguleren van het correcte gebruik van cryptografie zorgt voor een gelijk speelveld, waardoor alle organisaties dezelfde of vergelijkbare maatregelen moeten nemen.
Bovendien beoogt wetgeving kleinere organisaties te beschermen die zelf niet over de kennis van de nieuwste cryptografische dreigingen beschikken. Het belang van wetgeving wordt verder benadrukt door het feit dat cryptografie vaak publieke aangelegenheden beschermt, zoals nationale veiligheid, openbare veiligheid en privacy. In deze situaties kan de markt wellicht niet voldoende prikkels creëren voor het inzetten van passende cryptografische maatregelen. Daarnaast maakt wetgeving een consistente inzet van standaarden mogelijk; zonder wetgeving kunnen organisaties inconsistente keuzes maken, wat de interoperabiliteit en controleerbaarheid beperkt.
Deze sectie geeft enkele voorbeelden van wetgeving die het gebruik van cryptografie voorschrijft. Deze voorbeelden tonen aan hoe het gebruik van post-quantumcryptografie steeds meer verplicht zal worden. Dit overzicht is verre van compleet en we adviseren organisaties om de relevante regelgevende instanties en wetgevingen in hun regio en sector te inventariseren. Over het algemeen verplicht wetgeving het gebruik van gestandaardiseerde en goed bestudeerde cryptografische algoritmes. Aangezien PQC-standaarden nog nieuw zijn of zelfs nog in ontwikkeling, verklaart dit waarom wetgeving die expliciet het gebruik van post-quantumcryptografie vereist nog schaars is. Echter wordt verwacht dat naarmate meer standaarden

worden afgerond, wetgeving snel zal volgen en zal beginnen met het uitfaseren van oudere cryptografische standaarden die niet in staat zijn om te beschermen tegen quantumaanvallers. Om deze reden is het belangrijk om de wetgevende ontwikkelingen bij te houden.

5.2.1 ISO/IEC 27000-serie

De ISO/IEC 27000-serie is misschien wel de bekendste set internationale cyberbeveiligingsstandaarden, gericht op het waarborgen van robuuste informatiebeveiligingsbeheerprocessen. Deze set standaarden wordt wereldwijd in veel verschillende sectoren en formeel door meerdere overheden en organisaties nageleefd. Het naleven van de ISO/IEC 27000-serie is niet inherent verplicht, maar wordt algemeen beschouwd als een best practice. Bovendien kunnen regelgevende instanties in sommige sectoren naleving van deze standaarden vereisen.
Deze standaarden bieden geen technische cryptografische vereisten, maar specificeren wel de noodzaak van cryptografische beleidslijnen en controles, en het inzetten van passende cryptografische technieken op basis van een risicobeoordeling. Meer gedetailleerde richtlijnen en specificaties met betrekking tot cryptografie zijn te vinden in andere ISO/IEC-standaarden en richtlijnen. Bijvoorbeeld, ISO/IEC 18033 specificeert een set gestandaardiseerde primitieven die kunnen worden gebruikt binnen deze cryptografische beleidslijnen. Momenteel biedt deze standaard nog geen post-quantum publieke sleutels. Echter is de werkgroep ISO/IEC JTC 1 SC27 WG2 momenteel wel een post-quantum amendement op ISO/IEC 18033 aan het ontwikkelen.

5.2.2 Richtlijnen van Network and Information Systems (NIS)

De NIS-richtlijn [EU16a] biedt wetgeving die gericht is op het bereiken van een hoog niveau van cyberbeveiliging in de lidstaten van de Europese Unie. In 2018 trad deze in werking en in 2023 werd deze vervangen door zijn opvolger, de NIS2-richtlijn [EU22a]. NIS2 specificeert 18 sectoren en alle middelgrote tot grote EU-bedrijven in deze sectoren moeten aan deze wetgeving voldoen. De reikwijdte van de NIS2-richtlijn gaat veel verder dan cryptografie, en het biedt geen gedetailleerde of specifieke vereisten voor het gebruik van cryptografie. Echter, NIS2 specificeert wel de verplichting om proportionele cryptografische maatregelen in te zetten, rekening houdend met zowel de blootstelling van een organisatie aan risico's als de stand van zaken in cryptografie.

5.2.3 Algemene verordening gegevensbescherming (AVG)

De AVG (Eng: *General Data Protection Regulation (GDPR)*) [EU16b] is een uitgebreide wet die de bescherming van privacy en persoonlijke informatie van EU-burgers verplicht stelt. De gegevensbeschermings-autoriteiten in de verschillende EU-lidstaten zijn verantwoordelijk voor het toezicht op de naleving van de AVG. Het niet naleven van de AVG kan resulteren in aanzienlijke boetes. De AVG schrijft het gebruik van specifieke cryptografische algoritmes niet voor, maar impliceert wel het gebruik van cryptografie terwijl rekening wordt gehouden met de staat van de techniek (Artikel 32).

5.2.4 Federal Information Security Modernization Act (FISMA)

De FISMA [Uni02] verplicht Amerikaanse federale agentschappen en hun aannemers om een reeks cyberbeveiligingsmaatregelen in te zetten. FISMA delegeert de specificatie van cryptografische algoritmes aan het Amerikaanse National Institute for Standards and Technology (NIST). Om te voldoen aan FISMA, moet specifiek cryptografie die is gestandaardiseerd door NIST, in Federal Information Processing Standards (FIPS), worden gebruikt. FIPS-standaarden dekken nu al een breed scala aan cryptografische algoritmes, en recentelijk zijn er nieuwe PQC FIPS-standaarden toegevoegd als resultaat van de NIST PQC-competitie.

Aparte hogere FIPS-standaarden specificeren vervolgens welke cryptografische algoritmes zijn goedgekeurd, verwijzend naar de overeenkomstige FIPS-standaarden van deze algoritmes. Dit toont duidelijk de modulaire aard van deze Amerikaanse wetgeving aan.

5.2.5 Memorandum van het Witte Huis (VS)

Al in 2022 gaf het Witte Huis van de VS een memorandum uit waarin het beleid van de regering met betrekking tot quantumcomputing werd beschreven, met de nadruk op zowel de risico's als de kansen van quantumtechnologie [US22] Dit memorandum definieert concrete acties voor Amerikaanse overheidsinstanties om een tijdige mitigatie van de quantumdreiging te waarborgen. Bijvoorbeeld, het beschrijft de oprichting van verschillende (industriële) werkgroepen en nieuwe PQC-migratieprojecten. Hoewel het niet de inzet van specifieke cryptografische algoritmes verplicht stelt, vereist dit memorandum wel dat veel Amerikaanse organisaties beginnen met de PQC-migratie.
In juli 2024 publiceerde het White House Office of Management and Budget (OMB) een strategie voor de overgang van federale informatiesystemen naar PQC, in lijn met het memorandum. Binnen een jaar na de goedkeuring van de eerste PQC-standaarden door NIST (ongeveer een jaar vanaf de herfst van 2024), zal de OMB richtlijnen uitgeven, in samenwerking met de Cybersecurity and Infrastructure Security Agency (CISA) van het Department of Homeland Security, NIST en het Office of the National Cyber Director (ONCD), waarin agentschappen worden geïnstrueerd om een PQC-migratieplan te ontwikkelen en prioriteit te geven.

5.2.6 Commercial National Security Algorithm Suite (CNSA)

In de CNSA [NSA21a] vereist de National Security Agency (NSA) van de Verenigde Staten een specifieke set cryptografische algoritmes voor het beschermen van Amerikaanse nationale veiligheidssystemen (NSS). Deze vereisten verwijzen naar de FIPS-standaarden van NIST. In 2022 werd de CNSA 2.0 gepubliceerd, waarin NSS-eigenaren, -operators en -leveranciers worden geïnformeerd over de toekomstige cryptografische vereisten. In het bijzonder specificeert CNSA 2.0 vier quantum-veilige publieke-sleutelalgoritmes - CRYSTALS-Kyber, CRYSTALS-Dilithium, XMSS en LSS - en kondigt deze aan dat de inzet ervan verplicht zal worden. Specifieker definieert CNSA 2.0 een overgangsperiode. Afhankelijk van de cryptografische toepassing zal naleving van CNSA 2.0, en dus de inzet van PQC, verplicht zijn in 2030 of 2033. Tot die tijd zal naleving van CNSA 2.0 eerst optioneel en later de voorkeur hebben.

5.2.7 Wetgeving voor specifieke domeinen

Naast het algemene regelgevingskader zijn er veel sectoren met specifieke wetgeving die is afgestemd op hun behoeften. Bijvoorbeeld, de Digital Operational Resilience Act (DORA) [EU22b] heeft als doel een hoog niveau van operationele weerbaarheid te bereiken in de financiële sector van de Europese Unie. DORA vereist dat financiële instellingen "leidende praktijken en standaarden" in cryptografie toepassen, en zal daarom binnenkort (impliciet) het gebruik van post-quantumcryptografie vereisen.
In de VS verplicht de Health Insurance Portability and Accountability Act (HIPAA) [US96] de gezondheidszorgsector om patiëntendossiers te beveiligen, bijvoorbeeld door het toepassen van geschikte cryptografische technieken. Als laatste voorbeeld reguleert de European Electronic Communications Code (EECC) [EU18] elektronische communicatienetwerken in de EU en vereist het gebruik van sterke cryptografie om de impact van beveiligingsincidenten te minimaliseren.

5.3 Internationale PQC-richtlijnen en -adviezen

Enkele internationale organisaties ook minder juridisch bindende richtlijnen gegeven voor een succesvolle implementatie van naar post-quantumcryptografie.

5.3.1 Europese commissie

Op 11 april 2024 heeft de Europese Commissie een uitgebreide set aanbevelingen [EU24] uitgegeven aan haar lidstaten met betrekking tot de overgang naar post-quantumcryptografie. Hoewel dit slechts aanbevelingen zijn, verwijzen ze expliciet naar de NIS2-richtlijn (zie sectie 5.2.2), waarmee de cruciale rol van PQC in het bereiken van een hoog niveau van cyberveiligheid in de hele EU wordt onderstreept. De aanbeveling moedigt lidstaten aan om hun inspanningen tijdens de migratie naar PQC te coördineren en samen te werken om een gedetailleerde, uniforme routekaart te ontwikkelen. De commissie heeft nog geen specifieke PQC-algoritmes goedgekeurd, maar pleit voor de ontwikkeling van normen op EU-niveau, samen met een grondige analyse van deze algoritmes. Voor de praktische overgangsfase wordt aanbevolen om hybride cryptografische oplossingen te gebruiken, die post-quantum algoritmes combineren met de momenteel gebruikte algoritmes. Daarnaast heeft de Europese Commissie Quantum Key Distribution (QKD) nog niet uitgesloten als mogelijke oplossing, hoewel veel veiligheidsinstanties van de lidstaten QKD onvoldoende volwassen achten en het gebruik ervan afraden.

5.3.2 Duitsland, Frankrijk en Nederland

Verschillende EU-lidstaten hebben specifieke richtlijnen gegeven over de overgang naar post-quantumcryptografie via hun nationale cybersecurity-instanties. Hoewel de richtlijnen in Duitsland [BSI24b], Frankrijk [ANSSI23] en Nederland [NCSC-NL23; Fiche24] elk hun nuances hebben, zijn ze het over het algemeen eens met de aanbevelingen van de Europese Commissie en ondersteunen ze het gebruik van hybride cryptografische constructies. De situatie is eenvoudiger voor digitale handtekeningen dan voor sleutelinkapseling, aangezien het voldoende is om handtekeningen met twee verschillende algoritmes te verstrekken en de handtekening alleen te accepteren als beide geldig zijn. In tegenstelling tot de Europese Commissie stellen deze drie instanties echter vraagtekens bij de volwassenheid van QKD en de haalbaarheid van het gebruik van QKD als maatregel om de quantumdreiging te mitigeren.

Specifieke algoritmes | Alle drie de instanties presenteren veiligheid als het belangrijkste criterium voor het selecteren van post-quantumalgoritmes. Ze gaan mee in de standaardisatiekeuzes van NIST voor ML-KEM [NIST24a], ML-DSA [NIST24b] en SLH-DSA [NIST24c]), maar geven waarschuwingen rondom FN-DSA. In het bijzonder geven ze aan dat FN-DSA lastig op een veilige manier te implementeren is zodat het bescherming biedt tegen side-channel aanvallen en daarom raden ze het gebruik van dit algoritme niet aan. Daarnaast wordt er gepleit voor twee andere KEMs: FrodoKEM [ABDL+21] en Classic McEliece [ABCC+20]. De eerste van deze twee kan worden beschouwd als een variant van ML-KEM die niet afhankelijk is van zekere algebraïsche structuur. De tweede is een directe aanpassing van een ouder cryptosysteem van McEliece[McE78] waarmee Classic McEliece het oudste cryptosysteem is dat momenteel ongebroken is. Deze kenmerken maken deze twee algoritmes conservatievere keuzes dan de NIST-standaarden en de instanties hebben veel vertrouwen in hun veiligheid.

Conservatievere parametersets | Bij het implementeren van post-quantumcryptografie zijn alle instanties het erover eens dat alleen de conservatiefste parameters die door een externe organisatie zijn gestandaardiseerd moeten worden gebruikt. In het bijzonder pleiten ze voor het gebruik van de parameters die behoren tot beveiligingscategorieën 3 en 5 voor de NIST-normen en raden ze aan te wachten op de toekomstige ISO/

IEC en IETF-normen met betrekking tot FrodoKEM en Classic McEliece. Deze zorgen rondom veiligheidsniveau worden enigszins gedeeld door NIST, waar men van mening is dat de parameters voor beveiligingscategorie 3 standaard moeten worden gebruikt voor ML-KEM [NIST24a, Section 8].

Crypto-agility en flexibiliteit | Alle drie de instanties benadrukken dat roadmaps voor PQC-migratie flexibel moeten blijven met het oog op nieuwe (technologische) ontwikkelingen. In het bijzonder benadrukt een informatieblad van de Nederlandse overheid [Fiche24] het belang van investeren in onderzoek en innovatie. Alle drie de agentschappen dringen aan op de ontwikkeling van crypto-agility om de overgang van een bepaald cryptografisch algoritme naar een ander te vergemakkelijken.

Tijdlijn | Een detail uniek aan het rapport van ANSSI is dat het ook een tijdlijn geeft voor de implementatie van quantumveilige cryptografie:

- **Stap 1 (tot 2025)** De organisaties van het grootste belang, die overeenkomen met wat wij in hoofdstuk 2 urgente adopters noemen, moeten hun migratie starten door hun crypto-agility te verbeteren. Post-quantumcryptografie is nog optioneel, maar als het wordt gebruikt, moet het worden gebruikt binnen in een hybride constructie.
- **Stap 2 (van 2025 tot 2030)** Quantumveiligheid moet door commerciële organisaties als een belangrijke prioriteit worden gezien. Commerciële organisaties moeten een duidelijke migratiestrategie definiëren, te beginnen met een cryptografische inventarisatie (zie sectie 2.2.1). Post-quantumcryptografie moet worden geïmplementeerd in een hybride constructie, met een ander meer gevestigd maar quantumkwetsbaar cryptosysteem. ANSSI zal beginnen met het verstrekken van certificeringen van producten die aan deze richtlijnen voldoen.
- **Stap 3 (vanaf 2030)** ANSSI verwacht dat post-quantumalgoritmes tegen 2030 betrouwbaarder zullen zijn en dat hun veiligheid beter zal worden begrepen. In het bijzonder is de verwachting dat post-quantumcryptografie als een op zichzelf staande vervanging voor de huidige cryptografie gebruikt kan gaan worden, wat efficiënter is dan hybridisatie.

Implementatie | Naast hun aanbevelingen biedt het Duitse BSI ook een open-source softwarelibrary aan voor cryptografie. Deze library heet Botan, is geschreven in C++ en is beschikbaar op Github. Botan biedt een breed scala aan cryptografische algoritmes en protocollen aan en biedt zowel quantumkwetsbare als quantumveilige cryptografie aan die voldoet aan de eigen richtlijnen.

5.3.3 Verenigd Koninkrijk

Het UK National Cyber Security Centre (UK-NCSC) is een cybersecurity-instantie van het Verenigd Koninkrijk en maakt deel uit van een grotere inlichtingen- en veiligheidsorganisatie, bekend als GCHQ (Government Communications Headquarters). In hun whitepaper uit 2020 [NCSC-UK20a] adviseren zij net als BSI en ANSSI om zo snel mogelijk over te stappen naar quantumveilige algoritmes [NCSC-UK22], maar ontmoedigen zij de migratie naar algoritmes die niet gestandaardiseerd zijn.

Kijk op standaarden | In hun whitepaper uit 2023 [NCSC-UK23] sluit UK-NCSC zich aan bij de NIST-standaardisatie en beveelt het gebruik van ML-KEM aan als een algemene PKE/KEM en ML-DSA als een algemene digitale handtekeningalgoritme. Voor specifieke toepassingen, zoals het ondertekenen van firmware en software, waar snelheid minder belangrijk is, bevelen zij het gebruik van de stateless SLH-DSA de stateful LMS en XMSS aan. Deze laatste twee worden alleen voor gebruik aanbevolen als het mogelijk is om de toestand gedurende de levensduur van de geheime sleutel op een betrouwbare manier te beheren.

Kijk op hybride constructies | In de eerste whitepaper uit 2020 ondersteunde UK-NCSC impliciet hybride constructies: schema's die eerder gebruikte algoritmes combineren met een post-quantumalgoritme, om zo een soepelere overgang naar quantumveilige cryptografie mogelijk te maken. Niettemin benadrukt UK-NCSC dat het gebruik van hybride schema's geen ideale oplossing is vanwege de implementatiekosten, complexiteit en gebrek aan efficiëntie. Hun standpunt is daarom dat hybride schema's alleen moeten worden gebruikt als hun toepassing noodzakelijk is. Dat kan zijn als het algoritme dat wordt vervangen deel uitmaakt van een groter en zeer complex systeem; als een systeem een hoog beveiligingsniveau vereist (bijvoorbeeld gevoelige gegevens beschermt) en als het moeilijk is om traditionele asymmetrische algoritmes te verwijderen. Maar zelfs in deze gevallen moeten organisaties uiteindelijk streven naar alleenstaand gebruik van post-quantumalgoritmes, aangezien hybride schema's geen extra bescherming bieden tegen een grootschalige quantumcomputer en alleen een overhead in de implementatie zouden introduceren.

Kijk op QKD | In zowel de whitepaper uit 2023 als een blogpost uit hetzelfde jaar geeft UK-NCSC aan dat het gebruik van QKD[9] voor sleutelverspreiding niet de efficiëntste of veiligste maatregel is. Dat komt omdat het hardware vereist die nog in ontwikkeling is. Daarom moedigt UK-NCSC het gebruik van QKD voor de bescherming van gevoelige gegevens niet aan.

Kijk op migratie van protocollen en diensten | Het UK-NCSC heeft opgemerkt dat, als onderdeel van de overgang naar de nieuwe post-quantum algoritmes, protocollen en services die op deze protocollen vertrouwen opnieuw moeten worden ontworpen om te voldoen aan de hogere eisen die door de geïmplementeerde algoritmes worden gesteld. UK-NCSC heeft de volgende uitdagingen in de PQC-migratie geïdentificeerd: *legacy*-systemen die moeilijk te upgraden zijn, sectorspecifieke protocollen en protocollen die draaien op apparaten met beperkte rekenkracht. Ze merken echter op dat voor veel gebruikssituaties de overgang "stilletjes" kan worden uitgevoerd via software-updates en ze moedigen deze aanpak aan wanneer dit mogelijk is.

5.4 Lessen van reeds uitgevoerde PQC-migraties

Sommige organisaties en beheerders van bekende software zijn al begonnen met de migratie naar post-quantumcryptografie. In deze sectie geven we een overzicht van praktijkervaringen, beschrijven we de uitdagingen die zijn ondervonden en vatten we samen welke lessen die hieruit te trekken zijn.

5.4.1 PQC-migraties van Google

Google is een pionier in het integreren van post-quantumcryptografie in de interne infrastructuur. Hun migratieproces begon zelfs voordat NIST de eerste algoritmes voor standaardisatie aankondigde. Als gevolg hiervan dient hun experiment als een belangrijk voorbeeld van een succesvolle migratie naar post-quantumcryptografie. Googles interne communicatie wordt beveiligd met een eigen protocol genaamd ALTS (Application Layer Transport Security)[Google17]. ALTS is een systeem voor wederzijdse authenticatie en transportversleuteling, vergelijkbaar met mTLS (mutual Transport Layer Security), maar volledig ontwikkeld door Google om aan hun specifieke behoeften te voldoen. Om ALTS te upgraden naar een post-quantumversie, koos Google voor hybride encryptie om de veiligheidsrisico's te beperken in geval van problemen. Op basis van eerdere experimenten kozen ze NTRU-HRSS [HRSS17] als hun primaire post-quantumencryptieschema, met plannen om over te schakelen naar ML-KEM zodra de standaarden zijn afgerond. Dit zou geen significante uitdaging moeten vormen, aangezien ze al streefden naar grote mate van crypto-agility. Zie [Google22b] voor meer details.

[9] Quantum-key distribution (QKD) gebruikt eigenschappen van de quantummechanica voor veiligheidsgaranties, in plaats van wiskundige problemen die veel rekenkracht vereisen

De migratie naar post-quantum ALTS werd besproken op Real World Crypto 2023 [KPMS23], en werd makkelijker dankzij Googles volledige controle over zowel server- als clientimplementaties van het protocol. Het integreren van de post-quantumlaag bracht echter verschillende uitdagingen met zich mee. In het bijzonder vereiste het gebruik van zogenaamde ephemeral keys (een soort 'tijdelijke sleutel' die alleen voor een specifieke iteratie wordt gebruikt) in het ALTS-protocol het genereren van nieuwe sleutels voor elke sessie, wat kostbaar is, vooral als de server nog niet is gemigreerd. Daarom overwogen ze het cachen van de publieke sleutel om dit probleem te verlichten. Helaas veroorzaakte deze aanpak problemen met sleutellengtes, wat resulteerde in onverwachte stackoverflows op bepaalde architecturen. Om dit aan te pakken, verplaatsten ze de sleutel naar het heap-geheugen, maar dit introduceerde latentieproblemen die niet waren voorzien tijdens de initiële benchmarks. Deze latentieproblemen ontstonden door de allocatietijd wanneer duizenden post-quantumsessies werden geïnitieerd, wat protocolupdates vereiste.
Kortom, de ervaring van Google benadrukt dat migreren naar post-quantumcryptografie een langdurig proces is, dat uitgebreide tests in verschillende scenario's vereist vanwege onverwachte problemen.

5.4.2 Project rondom post-quantum-TLS van Google en Cloudflare

TLS (Transport Layer Security) is een van de belangrijkste pilaren van het wereldwijde web, dat praktisch elke verbinding tussen computers over het internet beveiligt. TLS wordt typisch gebruikt voor twee doelen: authenticatie en encryptie. Authenticatie wordt gebruikt om ervoor te zorgen dat een gebruiker kan verifieren dat hij met de juiste server praat door middel van een digitale handtekening in de vorm van een certificaat. Encryptie wordt gebruikt om ervoor te zorgen dat de informatie die van client naar server en vice versa wordt verzonden, vertrouwelijk blijft. Hiervoor stelt het protocol eerst op een veilige manier een gedeelde symmetrische sleutel op met behulp van een sleuteluitwisselingsprotocol (wat een asymmetrische primitieve is). Vervolgens wordt symmetrische cryptografie gebruikt om de rest van het gesprek te versleutelen.
TLS 1.3 [Res18] is de nieuwste versie van het TLS-protocol, uitgebracht in augustus 2018, met veel beveiligings- en prestatieverbeteringen ten opzichte van versie 1.2. TLS 1.3 is echter gemaakt zonder specifieke aandacht voor PQC en het integreren van post-quantumalgoritmes brengt bepaalde uitdagingen met zich mee. Dit is vooral waar als men zowel vertrouwelijkheid (door het wijzigen van de sleuteluitwisseling) als authenticatie (door het gebruik van quantum-veilige digitale handtekeningen) in overweging wil nemen, maar ze kunnen afzonderlijk worden behandeld.
Het CRPQ2-project (Combined Elliptic-Curve and Post-Quantum) was een serie vroege experimenten met het ontwerpen van quantumveilige varianten van het mechanisme voor sleuteluitwisseling in TLS 1.3. Dit project, dat in 2019 plaatsvond, werd geleid door Google en Cloudflare [VK19]. Ze overwogen een hybride sleuteluitwisseling: X25519 samen met ófwel het rooster-gebaseerde NTRU-HRSS [HRSS17], óf met SIKE [JACC+21] (voor de variant CRPQ2b). We merken op dat SIKE tegenwoordig niet meer als veilig wordt beschouwd, maar aangezien ze een hybride sleuteluitwisseling gebruikten, leidde CRPQ2b niet tot veiligheidsverliezen in vergelijking met de huidige implementatie van TLS 1.3. Sindsdien is NTRU-HRSS vervangen door de conceptversie van ML-KEM [OBr23; AVW23]). In dit experiment implementeerde Cloudflare de serverzijde, terwijl Google ondersteuning toevoegde voor hybride KEMs in hun eigen browser, Chrome[10]. Aangezien rooster-gebaseerde KEMs over het algemeen extreem snel zijn, was de overhead in termen van rekenkracht van het gebruik van quantumveilige algoritmes bijna niet merkbaar. Sommige berichten in het TLS-protocol, namelijk de ClientHello en de ServerHello, bevatten echter ook de publieke sleutels en de ciphertext, die gezamenlijk de Maximum Transmission Unit (MTU) kunnen overschrijden, d.w.z. de maximale pakketgrootte die over het netwerk kan worden verzonden - over het algemeen 1400 bytes. In deze situatie moeten de handshake-berichten worden verdeeld over meerdere TCP-pakketten, waardoor het risico op pakketverlies toeneemt en mogelijk latentieproblemen ontstaan wanneer pakketten opnieuw moeten worden verzonden.

[10] Mozilla heeft ondersteuning voor hybride KEMs toegevoegd aan versie 123 van Firefox in het begin van 2024.

De TLS-standaard staat toe dat de pakketten op deze manier worden gesplitst, maar aangezien dit in een pre-quantum-wereld uiterst zeldzaam was, zijn veel clients en servers niet correct geïmplementeerd en negeren ze volgende pakketten, wat leidt tot onverwachte afbreking van het protocol. In het bijzonder zijn uitgebreide tests nog steeds nodig om deze slechte implementaties op te sporen en ervoor te zorgen dat leveranciers ze repareren. De IETF werkt momenteel aan de standaardisatie van hybride sluiteluitwisseling in TLS 1.3 [IETF24]. Dit probleem met de grootte kan nog problematischer worden met quantumveilige authenticatie. Over het algemeen worden er veel handtekeningen en publieke sleutels opgenomen in een enkele handshake. Ook al staat de standaard voor TLS 1.3 een certificaatketen van 16 MB toe, zullen veel apparaten in de praktijk veel kortere ketens al afwijzen. In deze situatie stelt Cloudflare dat de toepassing van quantumveilige authenticatie eenvoudiger zou zijn als er 6 handtekeningen en 2 publieke sleutels in 9 kB passen [Wes21].
Er worden ook andere oplossingen onderzocht. Er is bijvoorbeeld voorgesteld om tussenliggende certificaten te verwijderen [KSFH+20] of zelfs om sommige handtekeningen te vervangen door KEMs [SSW20] in een nieuwe variant die bekend staat als KEMTLS. Al deze voorstellen vereisen echter dat het protocol daadwerkelijk wordt gewijzigd. Dat zou vele jaren duren en er is augustus 2024 nog geen consensus bereikt. De geïnteresseerde lezer kan meer informatie over deze KEMTLS-variant en de experimenten van Cloudflare ermee vinden in [CW21].

5.4.3 Post-quantum-TLS bij Meta

Meta is ook actief geweest in de migratie naar post-quantumcryptografie en heeft bijgedragen aan de NIST-inzendingen BIKE [ABBB+21] en Classic McEliece [ABCC+20] Net als Google kozen ze ervoor om hun interne communicatieverkeer te migreren, waarbij hun controle over alle eindpunten en de vatbaarheid voor store-now-decrypt-later-aanvallen de belangrijkste redenen waren om dit als eerste test te doen [LTAN+24]. Concreet kozen ze voor een hybride aanpak, waarbij Kyber (nu gestandaardiseerd als ML-KEM) in een hybride constructie werd gebruikt met sluiteluitwisseling op basis van een elliptische kromme (X25519). Ze implementeerden hybride constructie voor sleuteluitwisseling in hun eigen, open-source TLS-softwarelibrary genaamd Fizz [Meta24]. . Voor PQC gebruikten ze de open-source software van liboqs [SM16]. Hun oorspronkelijke plan was om ML-KEM-768 (NIST-niveau 3) als de standaardkeuze voor sleuteluitwisseling in te stellen. Na het ervaren van problemen met de ClientHello die niet in één pakket past en het onderzoeken van verschillende oplossingen, schaalden ze echter terug naar de kleinere parameterset van ML-KEM-512 (NIST-niveau 1). Bovendien ondervonden ze crashes in liboqs na de uitrol van hybride sleuteluitwisseling naar hun interne communicatie. De crash werd veroorzaakt door multithreading, wat de noodzaak benadrukt om implementaties goed te testen voordat erop wordt vertrouwd.

5.4.4 PQC in communicatie-apps

Signal | Het Signal-protocol [Mar13; MP16] is een cryptografisch protocol dat end-to-end-encryptie biedt voor spraak- en tekstberichten. Het wordt sinds 2013 ontwikkeld en bijgehouden voor de Signal-berichtenapplicatie en is sindsdien geïntegreerd in veel andere apps voor communicatie zoals WhatsApp [Wha16] en Google Messages for Android [Google22a]. Het is een van de meest wijdverspreide protocollen voor instant messaging ter wereld en wordt dagelijks door miljarden mensen gebruikt [Mil24]. De veiligheid ervan berust onder andere op een protocol voor sluiteluitwisseling dat X3DH (triple Diffie-Hellman) heet [MP16]. In september 2023 kondigde Signal aan dat een PQC-variant van hun protocol, bekend als PQXDH [Signal24b] was geïntegreerd in de Signal-berichtenapplicatie [Signal24a]. Deze quantumveilige variant voegt ondersteuning toe voor een hybride mechanisme voor sleuteluitwisseling. In de documentatie wordt de keuze van het algoritme vrijgelaten aan de programmeur, hoewel Signal vermeldt dat zij zelf ML-KEM gebruiken. Aangezien Signal alle eindpunten van het protocol voor hun berichtenapplicatie beheren, ondervonden zij geen specifieke uitda-

gingen bij de implementatie. Echter, kort na de release van dit protocol werd het formeel geverifieerd (zie [BJKS24]), wat leidde tot nieuwe aanvallen op de hybride sleuteluitwisseling in vroege versies van PQXDH. Dit resulteerde in aanpassingen van het protocol.

iMessage | iMessage is de belangrijkste app voor instant messaging van Apple en exclusief geïmplementeerd op hun platforms. Het is vergelijkbaar met het eerder genoemde Signal-protocol, maar gebruikt een ander ontwerp voor de sleuteluitwisseling, wat op zijn beurt andere uitdagingen met zich meebrengt. In februari 2024 verbeterde Apple iMessage met de introductie van het PQ3-protocol, waarmee quantumveiligheid wordt geboden via het ML-KEM-algoritme [Jac24; Apple24]. Dit protocol is ook recent formeel geverifieerd [BLS24].

5.4.5 Samenvatting van opgedane ervaringen

Deze praktijkvoorbeelden tonen aan dat hybride sleuteluitwisseling een haalbare oplossing is, waardoor het theoretisch eenvoudig is om quantumveilige vertrouwelijkheid te bereiken. In de praktijk moeten er echter nog vele uitdagingen worden overwonnen. De grotere lengte van publieke sleutels kan de rekentijd verhogen door de geheugentoewijzing, of zelfs geheugenproblemen veroorzaken in omgevingen met beperkte rekenkracht. Uitgebreide tests op verschillende architecturen zijn noodzakelijk om deze problemen te identificeren voordat de post-quantumvarianten in productie kunnen worden gebruikt. Dit proces is eenvoudiger wanneer alle eindpunten door één entiteit worden beheerd (bijvoorbeeld voor interne migratie). Formele verificaties hebben aangetoond dat het gebruik van hybride constructies voor sleuteluitwisseling ook leiden tot nieuwe aanvallen. Er moeten dus verdere controles worden uitgevoerd, hoewel deze niet noodzakelijk technische moeilijkheden opleveren.
Het bereiken van quantumveilige authenticatie is uitdagender. Huidige quantumveilige algoritmes voor digitale handtekeningen hebben de neiging in grotere handtekeningen te resulteren of tragere verificatie te bereiken. Dit kan leiden tot efficiëntieproblemen en de migratie minder aantrekkelijk maken. Dit is vooral problematisch voor de Web Public Key Infrastructure, die gebaseerd is op ketens van certificaten. Hoewel er al enkele ideeën zijn voorgesteld om de protocollen te verbeteren, zouden deze veranderingen in de kern van de protocollen verisen. Dit kan alleen worden ingevoerd als er consensus is, wat op zijn beurt meer tijd zal vergen en de migratie zou uitstellen. De nieuwe oproep van NIST specifiek voor quantumveilige handtekeningen zal van het grootste belang zijn voor deze toepassing.
Aan de positieve kant: er zijn scenario's waarin quantumveilige handtekeningen mogelijk eenvoudig kunnen worden geïmplementeerd. Bijvoorbeeld bij hardware root of trust-systemen zoals *Trusted Platform Modules* (TPM). Hier wordt een publieke sleutel direct op een chip gebrand en worden handtekeningen geverifieerd voor firmware-updates. Dit is bijzonder geschikt voor IoT-apparaten en kan hardware mogelijk maken die op de lange termijn quantumveilig is.

6 Achtergrond voor primitieven

Samenvatting

Het doel van dit hoofdstuk is om softwarelibrary-ontwikkelaars te helpen bij het selecteren van verschillende primitieven voor opname in hun libraries. Ook is het de insteek om organisaties te helpen begrijpen welke primitieven ze moeten kiezen kiezen en hoe ze deze moeten configureren bij het migreren naar een quantumveilige versie van een protocol. Dit hoofdstuk is ook bedoeld als hulpmiddel bij de inventarisatie en risicobeoordelingen. Vanwege het beoogde publiek en de te bespreken informatie wordt in dit hoofdstuk een redelijke hoeveelheid cryptografische achtergrondkennis verondersteld. We geven een lijst van de belangrijkste cryptografische primitieven die in gebruik zijn. Voor elke primitieve presenteren we de belangrijkste kenmerken en of ze quantumveiligheid bieden.

Tabel 6.1 toont een lijst van cryptografische primitieven die vaak gebruikt worden. Dit is geen volledige lijst en het is noodzakelijk dat alle andere versleutelingen en cryptografische algoritmes die in de organisatie worden gebruikt op de juiste manier worden vermeld.

Symmetrisch	Asymmetrisch	Hashfuncties	MAC	Stateful HBS
AES	RSA	SHA-2	HMAC	XMSS
ChaCha20	ECDH	SHA-3	CMAC	XMSS^{MT}
	ECDSA	Blake	BLAKE2-MAC	LMS
	EdDSA		CBC-MAC	HSS

Tabel 6.1 | Veelgebruikte cryptografische primitieven.

6.1 Quantumkwetsbare asymmetrische cryptografie

In deze sectie geven we een lijst van asymmetrische cryptografie die veel gebruikt wordt, maar kwetsbaar is voor een quantumcomputer.

ECDH

Beschrijving | ECDH is een elliptische kromme-variant van Diffie-Hellman-sleuteluitwisseling [NIST19a].

Grootte publieke sleutel (bits) | Dit is afhankelijk van de gebruikte kromme. Het gebruik van NIST P-256P resulteert bijvoorbeeld in een niet gecomprimeerde publieke sleutel van 512 bits.

Grootte geheime sleutel (bits) | Dit is afhankelijk van de gebruikte kromme. Het gebruik van NIST P-256P resulteert bijvoorbeeld in een geheime sleutel van 256 bits.

Grootte ciphertext (bits) | Het dubbele van de lengte van de geheime sleutel.

Veiligheidsaanname | Decisional Diffie-Hellman.

Crypto-functionaliteit | ECDH wordt gebruikt voor sleuteluitwisseling.

Toepassingen | ECDH is geïntegreerd in protocollen die sleuteluitwisseling vereisen.

Andere opmerkingen | ECDH wordt gebruikt in het Signal-protocol.

Standaardisatiedocumenten | NIST, SP, 800-56A [NIST19a] rev. 3, ANSI X9.63 [ANSI17a], SECG SEC-1 [Bro09].

Quantumveilig? | Nee.

ECDSA

Beschrijving | ECDSA is een elliptische kromme-variant van het door NIST gestandaardiseerde algoritme voor digitale handtekeningen [NIST23].

Grootte publieke sleutel (bits) | Dit is afhankelijk van de gebruikte kromme. Het gebruik van NIST P-256P resulteert bijvoorbeeld in een niet gecomprimeerde publieke sleutel van 512 bits.

Grootte geheime sleutel (bits) | Dit is afhankelijk van de gebruikte kromme. Het gebruik van NIST P-256P resulteert bijvoorbeeld in een geheime sleutel van 256 bits.

Grootte van handtekening (bits) | Het dubbele van de lengte van de geheime sleutel.

Veiligheidsaanname | Discrete Logaritme.

Crypto-functionaliteit | ECDSA is een algoritme voor het maken van digitale handtekeningen.

Toepassingen | ECDSA wordt gebruikt in een breed scala van zowel software- als hardwaredomeinen.

Andere opmerkingen | ECDSA is één van de de facto standaarden voor digitale handtekeningen.

Standaardisatiedocumenten | FIPS 186-5 [NIST23], ANSI X9.63 [ANSI17a], ANSI X9.142 [ANSI20], ISO/IEC 14888-32018 [ISO18b], SECG SEC-1 [Bro09].

Quantumveilig? | Nee.

EdDSA

Beschrijving | EdDSA is een elliptische kromme-variant van het door NIST gestandaardiseerde algoritme voor digitale handtekeningen. In EdDSA worden gedraaide Edwards-krommen gebruikt, zoals Curve25519 [JL17].

Grootte publieke sleutel (bits) | Dit is afhankelijk van de gebruikte kromme. Het gebruik van Curve25519 resulteert bijvoorbeeld in een publieke sleutel van 512 bits (zonder compressie).

Grootte geheime sleutel (bits) | Dit is afhankelijk van de gebruikte kromme. Het gebruik van Curve25519 resulteert bijvoorbeeld in een geheime sleutel van 256 bits (zonder compressie).

Grootte van handtekening (bits) | Het dubbele van de lengte van de geheime sleutel.

Veiligheidsaanname | Discrete Logaritme.

Crypto-functionaliteit | EdDSA is een algoritme voor het maken van digitale handtekeningen.

Toepassingen | EdDSA is geschikt voor algemeen gebruik.

Andere opmerkingen | EdDSA is gebaseerd op Schnorr-handtekeningen en wordt gebruikt in bijv. GnuPG en OpenSSH.

Standaardisatiedocumenten | FIPS 186-5 [NIST23], RFC 8032 [JL17].

Quantumveilig? | Nee.

RSA

Beschrijving | RSA is een erg populair asymmetrische encryptiealgoritme voor algemene toepassingen, gebaseerd op de moeilijkheid om een getal in twee priemgetallen te ontbinden [MKJR16].

Grootte publieke sleutel (bits) | ≥2048.

Grootte geheime sleutel (bits) | Ongeveer de grootte van de publieke sleutel.

Grootte ciphertext (bits) | Maximaal de grootte van de publieke sleutel.

Veiligheidsaanname | Integer Factorisatie.

Crypto-functionaliteit | RSA is een algoritme voor sleutelinkapseling en digitale handtekeningen.

Toepassingen | RSA wordt gebruikt in een breed scala van zowel software- als hardwaredomeinen.

Andere opmerkingen | -

Standaardisatiedocumenten | FIPS 186-5 [NIST23], NIST SP 800-56B [NIST19a] rev 2, RFC 8017 [MKJR16], ANSI X9.44 [ANSI17b], PKCS #1 [MKJR16], ISO/IEC 14888-2:2008 [IS008], ISO/IEC 11770-3:2021 [IS010c], ISO/IEC 9796-2:2010 [IS010a], ISO/IEC 18033-2 [IS010a].

Quantumveilig? | Nee.

6.2) Quantumveilige asymmetrische cryptografie

In deze sectie geven we een overzicht van enige quantumveilige asymmetrische cryptografie,

6.2.1 Mechanismen voor sleutelinkapseling en -uitwisseling

Er is een subtiel verschil in de functionaliteit van sleuteluitwisselingen en sleutelinkapselingsmechanismen. Dit verschil valt buiten de scope van dit document en daarom worden deze primitieven gegroepeerd. Merk ook op dat in dit hoofdstuk de voormalige NIST-kandidaat SIKE niet wordt behandeld, omdat deze is gebroken [CD23].

ML-KEM (CRYSTALS-Kyber)

Beschrijving | ML-KEM, ook bekend als CRYSTALS-KYBER, is op roosters gebaseerd en de primaire KEM die door NIST is gestandaardiseerd [NIST24a].

Parameters | Groottes (in bits) van de sleutels en ciphertexten van ML-KEM:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
1	ML-KEM-512	6,400	13,056	6,144
3	ML-KEM-768	9,472	19,200	8,704
5	ML-KEM-1024	12,544	25,344	12,544

Veiligheidsaanname | Module Learning with Errors (MLWE).

Andere opmerkingen | NIST raadt ML-KEM-768 (niveau 3) als standaard aan. Europese veiligheidsinstanties raden ook *minstens* niveau 3 aan.

Standaardisatiedocumenten | [NIST24a].

Quantumveilig? | Ja.

BIKE

Beschrijving | BIKE [ABBB+21] is een KEM die op foutcorrigerende codes is gebaseerd. Het is momenteel een kandidaat in Ronde 4 van de NIST-procedure.

Parameters | Groottes (in bits) van de sleutels en ciphertexten van BIKE:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
1	BIKE-L1	12,323	2,244	12,579
3	BIKE-L3	24,659	3,346	24,915
5	BIKE-L5	40,973	4,640	41,229

Veiligheidsaanname | Quasi-Cyclic Syndrome Decoding probleem.

Andere opmerkingen | Kandidaat in Ronde 4 bij NIST.

Standaardisatiedocumenten | BIKE website [ABBB+21].

Quantumveilig? | Ja.

Classic McEliece

Beschrijving | Classic McEliece [ABCC+20] is een conservative KEM die op foutcorrigerende codes is gebaseerd. Classic McEliece is gebaseerd op het originele McEliece cryptosysteem uit 1978 [McE78]. Het is een kandidaat in Ronde 4 bij NIST en wordt door ISO als potentiële standaard overwogen.

Parameters | Groottes (in bits) van de sleutels en ciphertexten van Classic McEliece:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
1	Classic-McEliece-348864	2,088,960	51,936	768
3	Classic-McEliece-460896	4,193,280	108,864	1,248
5	Classic-McEliece-6688128 Classic-McEliece-6960119 Classic-McEliece-8192128	8,359,936 8,378,552 10,862,592	111,456 111,584 112,960	1,664 1,552 1,664

Veiligheidsaannames | Syndrome Decoding Probleem (*message security*) en Goppa code recovery (*key security*).

Andere opmerkingen | Kandidaat in Ronde 4 bij NIST. Classic McEliece heeft zeer grote sleutels, maar kleine ciphertexten. Het is waarschijnlijk niet bruikbaar door systemen met kleine opslag, zoals smartcards of IoT, Het heeft echter wel aandachtige cryptoanalyse doorstaan en Europese veiligheidsinstanties hebben vertrouwen in de veiligheid.

Standaardisatiedocumenten | Officiële website [ABCC+20].

Quantumveilig? | Ja.

FrodoKEM

Beschrijving | FrodoKEM is een KEM die op roosters gebaseerd is. FrodoKEM ondersteunt conservatieve doch praktische constructies. Het wordt niet door NIST gestandaardiseerd [ABDL+21].

Parameters | Groottes (in bits) van de sleutels en ciphertexten van FrodoKEM:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
1	FrodoKEM-640-AES	76,928	159,104	78,016
3	FrodoKEM-976-AES	125,056	250,368	126,336
5	FrodoKEM-1344-AES	172,160	344,704	173,568

Veiligheidsaanname | (Normale) Learning with Errors (LWE).

Andere opmerkingen | FrodoKEM wordt momenteel niet gestandaardiseerd door NIST, maar wordt wel door ISO overwogen en wordt door Europese veiligheidsinstanties aangeraden.

Standaardisatiedocumenten | Officiële website [ABDL+21].

Quantumveilig? | Ja.

HQC

Beschrijving | HQC [MABL+21] is een KEM die op foutcorrigerende codes is gebaseerd. Het is momenteel een kandidaat in Ronde 4 van de NIST-procedure.

Parameters | Groottes (in bits) van de sleutels en ciphertexten van HQC:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
1	HQC-L1	17,992	448	35,976
3	HQC-L2	36,176	512	72,336
5	HQC-L3	57,960	576	115,880

Veiligheidsaanname | Decisional Quasi-Cyclic Syndrome Decoding Probleem.

Andere opmerkingen | Kandidaat in Ronde 4 bij NIST. HQC kan worden gezien als het analoog van ML-KEM, maar dan gebaseerd op codes.

Standaardisatiedocumenten | Officiële website [MABL+21].

Quantumveilig? | Ja.

6.2.2 Algoritmes voor digitale handtekeningen met interne toestand

LMS en HSS

Beschrijving | Leighton-Micali Signatures (LMS) is een handtekeningalgoritme gebaseerd op hashfuncties, met een interne toestand (het is *stateful*). LMS gebruikt LM-OTS voor eenmalige handtekeningen en is gebaseerd op Merkle-hashbomen. HSS is een variant met meerdere hashbomen [NIST20a].

Grootte publieke sleutel (bits) | 384-448 (alleen voor LMS; er is geen gestandaardiseerde parameter voor het aantal hashbomen in HSS).

Grootte geheime sleutel (bits) | Meerdere eenmalige geheime sleutels die afhankelijk zijn van veel variabelen en aannames, moeilijk in te schatten.

Grootte van handtekening (bits) | 6240-74592 (alleen voor LMS, geen gestandaardiseerde parameter voor aantal hashbomen in HSS).

Veiligheidsaanname | Collision Resistance.

Andere opmerkingen | Zorgvuldig beheer van de toestand (state) is essentieel en het belangrijkste nadeel van het algoritme.

Standaardisatiedocumenten | SP800-208 [NIST20a], RFC 8554 [IETF19].

Quantumveilig? | Ja.

XMSS and XMSS^{MT}

Beschrijving | Het eXtended Merkle Signature Scheme (XMSS) is een handtekeningalgoritme gebaseerd op hashfuncties, met een interne toestand (het is *stateful*). XMSS gebruikt WOTS+ voor eenmalige handtekeningen en is gebaseerd op Merkle-hashbomen. XMSS^MT is een variant met meerdere hashbomen [NIST20a].

Grootte publieke sleutel (bits) | 384-1024.

Grootte geheime sleutel (bits) | Meerdere eenmalige geheime sleutels die afhankelijk zijn van veel variabelen en aannames.

Grootte van handtekening (bits) | 11936-221504.

Veiligheidsaanname | Collision Resistance.

Andere opmerkingen | Zorgvuldig beheer van de toestand (state) is essentieel en het belangrijkste nadeel van het algoritme.

Standaardisatiedocumenten | SP800-208 [NIST20a], RFC 8391 [IETF18].

Quantumveilig? | Ja.

6.2.3 Algoritmes voor digitale handtekeningen zonder interne toestand

ML-DSA (CRYSTALS-Dilithium)

Beschrijving | ML-DSA, ook bekend als CRYSTALS-Dilithium, is gebaseerd op roosters en het primaire handtekeningalgoritme dat gestandaardiseerd is door NIST [NIST24b].

Parameters | Groottes (in bits) van de sleutels en ciphertexten van ML-DSA:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
2	ML-DSA-44	10,496	20,480	19,360
3	ML-DSA-65	15,616	32,256	26,472
5	ML-DSA-87	20,736	39,168	37,016

Veiligheidsaanname | Module Small Integer Solution (MSIS) en Module Learning with Errors (MLWE).

Andere opmerkingen | ML-DSA is het als handtekeningschema de tegenhanger van ML-KEM, dat ook door NIST gestandaardiseerd is. Europese veiligheidsinstanties raden aan om parameters te gebruiken die corresponderen met *minstens* veiligheidsniveau 3

Standaardisatiedocumenten | FIPS 204 [NIST24b].

Quantumveilig? | Ja.

FN-DSA (Falcon)

Beschrijving | FN-DSA, ook bekend als] [FHKP+21], is een op roosters gebaseerd handtekeningalgoritme en is door NIST geselecteerd voor standaardisatie.

Parameters | Groottes (in bits) van de sleutels en ciphertexten van FN-DSA:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
1	Falcon-padded-512	7,176	10,248	5,328
5	Falcon-padded-1024	14,344	18,440	10,240

Veiligheidsaanname | Short Integer Solution (SIS) over NTRU-roosters.

Andere opmerkingen | Het primaire handtekeningalgoritme van NIST is ML-DSA. FN-DSA gebruikt *floating point arithmetic*, wat niet erg gebruikelijk is binnen de cryptografie. Dat is namelijk lastig om op een veilige manier te implementeren zodat het robuust is tegen *side-channel*-aanvallen. Hetwordt niet aangeraden door Europese veiligheidsinstanties.

Standaardisatiedocumenten | Officiële website [FHKP+21].

Quantumveilig? | Ja.

SLH-DSA (SPHINCS+)

Beschrijving | SLH-DSA, ook bekend als SPHINCS+, is een handtekeningalgoritme gebaseerd op hashfuncties, zonder een interne toestand (het is *stateless*). SLH-DSA is gestandaardiseerd door NIST [NIST24c].

Parameters | Groottes (in bits) van de sleutels en ciphertexten van SLH-DSA:

Veiligheidsniveau	Parameterset	Publieke sleutel	Geheime sleutel	Ciphertext
2	SLH-DSA-SHA2-128s	256	512	62,848
3	SLH-DSA-SHA2-192s	384	768	129,792
5	SLH-DSA-SHA2-256s	512	1,024	238,336

Veiligheidsaanname | Second-Preimage Resistance.

Andere opmerkingen | Het primaire handtekeningalgoritme van NIST is ML-DSA.

Standaardisatiedocumenten | FIPS 205 [NIST24c].

Quantumveilig? | Ja.

6.3) Symmetrische cryptografie

In deze sectie beschrijven we enige symmetrische cryptografie waarvan er quantumveilige versies bestaan.

6.3.1 Ciphers

AES

Beschrijving | AES is een block cipher die is gestandaardiseerd door NIST [NIST01b].

Ondersteunde sleutelgroottes (bits) | 128, 192, 256.

Toepassingen | AES wordt gebruikt in een breed scala van zowel software- als hardware-implementaties.

Andere opmerkingen | AES is *de facto* de standaard voor symmetrische ciphers.

Standaardisatiedocumenten | FIPS 197 [NIST01b], ISO/IEC 180330-3:2010 [IS010b].

Quantumveilig? | Ja.

ChaCha20

Beschrijving | ChaCha20 is een stream cipher die normaal gesproken met Poly1305 [NL18] wordt gecombineerd bij gebruik in TLS.

Ondersteunde sleutelgroottes (bits) | 128, 256.

Toepassingen | ChaCha20 wordt gebruikt in verschillende protocollen zoals TLS en S/MIME (meestal in het softwaredomein).

Andere opmerkingen | ChaCha20 staat bekend om zijn snelheid en eenvoudige implementatie.

Standaardisatiedocumenten | RFC 8439 [NL18].

Quantumveilig? | Ja.

6.3.2 Hashfuncties

SHA-3 (Keccak)

Beschrijving | SHA-3, ook bekend als Keccak, is een verzameling hashfuncties die gestandaariseerd is door NIST.

Outputgroottes (bits) | 224, 256, 384, 512.

Toepassingen | SHA-3 wordt gebruikt in een breed scala van zowel software- als hardwaredomeinen.

Andere opmerkingen | SHA-3 is *de facto* de standaard voor hashfuncties. SHA-3 is de opvolger van SHA-2 en SHA-1. Zowel SHA-3 als SHA-2 worden aangeraden, terwijl SHA-1 onveilig en uitgefaseerd is.

Standaardisatiedocumenten | FIPS 180-4 [NIST15a], NIST SP 800 107 Rev. 1 [NIST12], RFC 6234 [HE11], ISO/IEC 10118-3:2018 [IS011] (SHA2), FIPS 180-4 [NIST15a], FIPS 202 [NIST15b], NIST SP 800 107 Rev. 1 [NIST12], ISO/IEC 10118-3:2018 [IS011] (SHA3).

Quantumveilig? | Ja.

SHA-2

Beschrijving | SHA-2 is een verzameling hashfuncties die gestandaardiseerd is door NIST en oorspronkelijk ontworpen is door het NSA [NIST02]. SHA-2 is de opvolger/vervanger van SHA-1.

Outputgroottes(bits) | 224, 256, 384, 512.

Toepassingen | SHA-2 wordt gebruikt in een breed scala van zowel software- als hardwaredomeinen.

Andere opmerkingen | SHA-3 is de opvolger van SHA-2 en SHA-1. Zowel SHA-3 als SHA-2 worden aangeraden, terwijl SHA-1 onveilig en uitgefaseerd is.

Standaardisatiedocumenten | FIPS 180-4 [NIST15a], NIST SP 800 107 Rev. 1 [NIST12], RFC 6234 [HE11], ISO/IEC 10118-3:2018 [IS011] (SHA2), FIPS 180-4 [NIST15a], FIPS 202 [NIST15b], NIST SP 800 107 Rev. 1 [NIST12], ISO/IEC 10118-3:2018 [IS011] (SHA3).

Quantumveilig? | Ja.

BLAKE2

Beschrijving | BLAKE2 is een hashfunctie met betere softwareprestaties dan SHA-3 [BLAKE217]. Het komt in twee "smaken": BLAKE2b and BLAKE2s.

Outputgroottes (bits) | ≤ 512 (BLAKE2b), ≤ 256 (BLAKE2s).

Toepassingen | BLAKE2 wordt gebruikt in zowel cryptografische als niet-cryptografische settings.

Andere opmerkingen | SHA-3 en SHA-2 worden aangeraden. BLAKE2 is aanzienlijk minder nauw geanalyseerd dan SHA-3 and SHA-2.

Standaardisatiedocumenten | RFC 7693 [SA15].

Quantumveilig? | Ja, als BLAKE2b wordt gebruikt.

6.3.3 Message Authentication Codes (MACs)

CMAC

Beschrijving | CMAC is een andere manier om op basis van een block cipher een MAC te construeren [ISLP06].

MAC-sleutelgroottes (bits) | Dit is afhankelijk van de gekozen block cipher.

MAC-outputgroottes (bits) | Dit is afhankelijk van de gekozen block cipher.

Toepassingen | CMAC wordt niet zo veel gebruikt als CBC-MAC.

Andere opmerkingen | Aanbevolen om te gebruiken met AES. CMAC wordt aanbevolen door NIST in plaats van CBC-MAC.

Standaardisatiedocumenten | NIST SP 800-38B [NIST16a], RFC 4493 [ISLP06], ISO/IEC 9797-1:2011 [IS018a].

Quantumveilig? | Ja, mits de onderliggende block cipher quantumveilig is.

HMAC

Beschrijving | MAC is een manier om op basis van cryptografische hashfuncties een MAC op te bouwen [KBC97].

MAC-sleutelgroottes (bits) | Arbitrair.

MAC-outputgroottes (bits) | Dit is afhankelijk van de gekozen hash.

Toepassingen | HMAC wordt gebruikt in IPSec-, SSH- en TLS-protocollen.

Andere opmerkingen | HMAC is gevoelig voor performance-problemen.

Standaardisatiedocumenten | FIPS 198-1 [NIST08], RFC 2104 [KBC97].

Quantumveilig? | Ja, mits de onderliggende hashfunctie quantumveilig is.

KMAC

Beschrijving | KMAC is-een MAC gebaseerd op SHA-3, waarvan de outputgroottes variabel zijn [NIST16b].

MAC-sleutelgroottes (bits) | ≥ 128.

MAC-outputgroottes (bits) | Variabel.

Toepassingen | Symmetrische authenticatie.

Andere opmerkingen | -

Standaardisatiedocumenten | NIST SP 800-185 [NIST16b].

Quantumveilig? | Ja.

BLAKE2-MAC

Beschrijving | BLAKE2 hoeft de HMAC-transformatie niet te gebruiken als MAC aangezien er al een versleutelingsmechanisme is voorzien [SA15].

MAC-sleutelgroottes (bits) | Arbitrair.

MAC-outputgroottes (bits) | ≤ 512 (BLAKE2b), ≤ 256 (BLAKE2s).

Toepassingen | BLAKE2-MAC wordt gebruikt in het softwaredomein.

Andere opmerkingen | HMAC-SHA-2 en KMAC worden aanbevolen. BLAKE2-MAC is sneller dan HMAC dankzij het ingebouwde *keying*-mechanisme.

Standaardisatiedocumenten | RFC 7693 [SA15].

Quantumveilig? | Ja, mits er gebruik wordt gemaakt van Blake2b.

CBC-MAC

Beschrijving | CBC-MAC is een manier om op basis van een block cipher een MAC te construeren [ISO11].

MAC-sleutelgroottes (bits) | Dit is afhankelijk van de gekozen block cipher.

MAC-outputgroottes (bits) | Dit is afhankelijk van de gekozen block cipher.

Toepassingen | CBC-MAC wordt normaal gesproken gebruikt voor berichten met vaste lengte.

Andere opmerkingen | CBC-MAC is opgevolgd door CMAC.

Standaardisatiedocumenten | ISO/IEC 9797-1 [ISO11].

Quantumveilig? | Ja, als de onderliggende block cipher quantumveilig is, maar overweeg om in plaats hiervan HMAC of CMAC te gebruiken.

6.4) Vergelijking van PQC

In deze sectie vergelijken we verschillende PQC-schema's, zowel in prestatie als onderliggende wiskundige problemen.

Tabel 6.2 toont de sterke en zwakke punten van bepaalde algoritmes voor sleuteluitwisseling en – inkapseling. Op eenzelfde manier toont tabel 6.3 de sterke en zwakke punten van bepaalde algoritmes voor digitale handtekeningen. Donkergroen geeft een positieve eigenschap aan, lichtgroen een enigszins positieve, oranje een enigszins negatieve en rood geeft een negatieve eigenschap aan. We vergelijken de PQC-schema's op NIST-veiligheidsniveau 5. Voor RSA gebruiken we de variant met 3072 bits en voor EdDSA gebruiken we Curve25519.
De kolom 'standaard' is donkergroen voor schema's die door NIST zijn gestandaardiseerd, lichtgroen voor schema's die in het proces zitten voor standaardisatie door NIST of ISO en oranje voor schema's waarvan het onzeker is of ze gestandaardiseerd zullen worden. De kolom 'vertrouwen' weerspiegelt het niveau van vertrouwen dat de wetenschappelijke gemeenschap heeft in het cryptografische schema. Sommige schema's zijn bijvoorbeeld gebaseerd op conservatievere aannames en andere hebben een uitgebreidere controle ondergaan. Dit kan allebei het vertrouwensniveau verhogen.
De snelheidsbenchmarks zijn geproduceerd met behulp van de Open Quantum Safe benchmarking suite [OQS23] en Botan [BSI24a]. Ze zijn uitgevoerd op een server met een Intel® Xeon® Gold 6248 CPU en onze resultaten en code zijn beschikbaar op [Ste]. Er zijn ook verschillende openbaar beschikbare benchmarks van cryptografische implementaties, bijvoorbeeld bij eBACS [BL] of OQS [OQS23]. De relatieve prestaties van de schema's kunnen verschillen tussen machines en implementaties. Bovendien kunnen toekomstige implementaties van sommige schema's een grotere snelheidsverbetering ondergaan door optimalisatie dan andere. Afhankelijk van hoe kritiek snelheid is voor een toepassing, raden we aan om benchmarks te maken die specifiek voor een toepassing zijn gedaan.

		Kenmerken		Snelheid			Grootte		
QUANTUMVEILIG		STANDAARD	VERTROUWEN	SLEUTEL-GENERATIE	ENCRYPTIE	DECRYPTIE	PUB. SLEUTEL	GEHEIME SLEUTEL	CIPHERTEXT
	X25519								
	RSA								
	BIKE								
	Classic McEliece (s)								
	Classic McEliece (f)								
	FrodoKEM-AES								
	FrodoKEM-SHAKE								
	HQC								
	ML-KEM								

Tabel 6.2 | Sterke en zwakke punten van enkele mechanismen voor sleuteluitwisseling en -inkapseling.

		Kenmerken		Snelheid			Grootte		
QUANTUMVEILIG		STANDAARD	VERTROUWEN	SLEUTEL-GENERATIE	ONDERTEKENEN	VERIFIËREN	PUB. SLEUTEL	GEHEIME SLEUTEL	HANDTEKENING
	EdDSA								
	RSA								
	FN-DSA								
	ML-DSA								
	SLH-DSA-SHA (s)								
	SLH-DSA-SHA (f)								
	LMS*								
	XMSS*								

Tabel 6.3 | Sterke en zwakke punten van enkele schema's voor digitale handtekeningen. *Schema met een interne toestand.

De bronnen voor de grootte van de sleutels, handtekeningen en ciphertexten zijn te vinden in de vorige secties van dit hoofdstuk. Deze tabellen houden geen rekening met methoden om de geheime sleutel te comprimeren. (Zo is het soms bijvoorbeeld mogelijk om de seed van een deterministische random number generator op te slaan in plaats van de geheime sleutel zelf. Zie bijvoorbeeld Sectie A.2.3 in [NIST23] voor EdDSA.) Om te helpen begrijpen welk PQC-schema het best bij een gegeven use-case past, verwijzen we naar de PQChoiceAssistant[TC24]. Deze tool biedt een interactieve vragenlijst die gebruikers door een reeks vragen leidt over eisen rondom performance en veiligheid. De beoogde doelgroep voor dit hulpmiddel zijn mensen

met algemene kennis van security en (abstract) overzicht van hun use-cases. Voor gebruikers met cryptografische kennis zijn er gedetailleerdere vragen. Op basis van de antwoorden stelt de tool geschikte PQC-algoritmes voor, waarbij scores en gedetailleerde uitleg worden gegeven over de overeenkomst tussen de use-case en de algoritmes. De PQChoiceAssistant ondersteunt momenteel de algoritmes ML-KEM, FrodoKEM, Classic McEliece, HQC en BIKE voor sleutelinkapseling en ML-DSA, FN-DSA, SLH-DSA en XMSS voor digitale handtekeningen.

6.4.1 Overzicht van PQC

In de afgelopen decennia heeft academisch onderzoek vijf algemene families van wiskundige domeinen geïdentificeerd die geschikt zijn om post-quantumcryptografie op te bouwen.

Roosters | Het belangrijkste probleem bij cryptografie gebaseerd op roosters is het *Learning With Errors*-probleem (LWE). Het gaat hier om het oplossen van een lineair stelsel van vergelijkingen over een eindig lichaam, maar met toegevoegde ruis. Er is de bijkomende beperking dat alle coëfficiënten van de oplossingen klein moeten zijn. Voor geschikte parameters kan worden aangetoond dat LWE net zo moeilijk is als het vinden van een korte vector in een (of eigenlijk: elk) Euclidisch rooster. Dit laatste probleem staat bekend als het *Shortest Vector Problem* (SVP) en wordt al decennia bestudeerd. De complexiteit wordt daarom goed begrepen en er is veel vertrouwen dat het probleem moeilijk blijft, zelfs voor cryptografisch relevante quantumcomputers. Een ander goed begrepen probleem in de roostertheorie dat wordt gebruikt om cryptografische primitieven te construeren is het *NTRU-probleem*. Benaderingen gebaseerd op roosters bieden zeer goede prestaties in termen van bandbreedte en efficiëntie.

Foutcorrigerende codes | Cryptografie gebaseerd op codes is gebaseerd op een probleem dat in zekere zin lijkt op het probleem bij roosters. Het belangrijkste verschil is dat de oplossingsvector nu een specifiek *Hamming-gewicht* moet hebben. Over het algemeen wordt bovendien geëist dat oplossing een klein Hamming-gewicht heeft. Dit probleem is equivalent aan het decoderen van een willekeurige lineaire code, een probleem dat in het begin van de telecommunicatie in de jaren 1950 is geïntroduceerd en sindsdien is bestudeerd. Classic McEliece is een cryptosysteem dat gebaseerd is op een originele constructie door McEliece in 1978 [McE78]. Het is het oudste cryptosysteem dat nog steeds ongebroken is (en zelfs quantumveilig is) en daarom profiteert het van veel vertrouwen in de veiligheid. Aan de andere kant komt deze sterke veiligheid ten koste van een grote publieke sleutel.

Systemen van multivariabele polynomen | De vorige twee families zijn gebaseerd op de moeilijkheid van het oplossen van beperkte, maar lineaire, systemen over een eindig lichaam. *Multivariate Quadratic*-cryptografie (MQ) is gebaseerd op de moeilijkheid van het oplossen van een systeem van polynoomvergelijkingen van graad twee over een eindig lichaam. Eén van de belangrijkste MQ-constructies staat bekend als *Oil and Vinegar* (soms aangeduid als *unbalanced Oil and Vinegar* en afgekort tot UOV) dat in 1999 werd geïntroduceerd [KPG99]. MQ-benaderingen zijn vooral geschikt voor digitale handtekeningen en produceren doorgaans zeer kleine handtekeningen. MQ-schema's lijden echter meestal aan grotere sleutellengtes en verschillende pogingen om dit te verbeteren hebben geleid tot zwakkere schema's dan verwacht. Dit blijkt ook uit de aanvallen die bepaalde NIST-kandidaten hebben gebroken [Beu22].

Isogenieën | Traditionele cryptografie met elliptische krommen is gebaseerd op het zogenaamde *Discrete Logaritme Problem*, wat kwetsbaar is voor quantumaanvallen. Er wordt echter vermoed dat het berekenen van bepaalde speciale afbeeldingen tussen elliptische krommen, bekend als *isogenieën*, moeilijk blijft zelfs met de hulp van quantumcomputers. Cryptografie op basis van isogenieën is verreweg het jongste ontwerpprincipe voor PQC. Dergelijke cryptografie lijdt meestal aan dure operaties die resulteren in langzame schema's. Bovendien heeft een recente doorbraak in cryptoanalyse de voormalige NIST-finalist SIKE gebroken [CD23].

Omdat SIKE op isogenieën is gebaseerd, is het vertrouwen in de veiligheid van zulke schema's verder verminderd. Wel is er na de doorbraak een nieuw onderzoekslijn ontdekt, gericht op de zogenaamde *hogerdimensionale isogenieën*. Gezien zo'n turbulente recente geschiedenis is de overheersende mening van de cryptografische gemeenschap dat verder onderzoek nodig is voordat schema's op basis van isogenieën kunnen worden gestandaardiseerd. Desalniettemin erkent de gemeenschap de toegevoegde waarde van verder onderzoek naar deze schema's, vanwege hun intrinsieke verschil met de eerder genoemde problemen.

Hashfuncties | Cryptografische hashfuncties worden sinds het einde van de jaren 70 gebruikt om handtekeningalgoritme's te bouwen. Dit gebeurt met behulp van de basisconcepten van *hashbomen* en het selectief openen van *pre-images* van hashes. Hun veiligheid is goed begrepen en gebaseerd op de moeilijkheid van het vinden van (tweede) *pre-images*: het vinden van een (tweede) bericht dat hasht naar een gegeven digest. Er zijn verschillende op hashing gebaseerde handtekeningalgoritme's met een *interne toestand*, waarbij het erg belangrijk is om bij te houden welke delen van de geheime sleutel zijn gebruikt, d.w.z. om de *toestand* (state) bij te houden. Als twee handtekeningen worden gegenereerd vanuit hetzelfde deel van de geheime sleutel, kan dit namelijk vervalsingen vergemakkelijken. In veel toepassingsscenario's is zorvuldig beheer van de toestand moeilijk, zo niet onmogelijk. Recentelijk zijn er ook op hashing gebaseerde handtekeningalgoritme's geïntroduceerd die niet met een dergelijke toestand te kampen hebben, waardoor het belangrijkste nadeel wordt geëlimineerd. Schema's met toestand kunnen echter nog steeds de voorkeur hebben boven schema's zonder toestand vanwege hun snellere handtekeninggeneratie.

Gestructureerd en ongestructureerd | Cryptografie op basis van roosters en codes draait om het oplossen van lineaire systemen over eindige lichamen, met toegevoegde niet-lineaire beperkingen. Dit leidt echter meestal tot schema's met lage efficiëntie. Om dit gebrek aan efficiëntie te compenseren kan men die problemen beperken tot lineaire systemen waarvan de onderliggende matrix een speciale structuur heeft, bijvoorbeeld gevormd door meerdere *circulante* (of *anti-circulante*) submatrices. In de context van roostercryptografie staat deze variant bekend als *Module Learning With Errors* en vormt het de kern van zowel ML-KEM (Kyber) als ML-DSA (Dilithium). De andere op roosters gebaseerde digitale handtekening die door NIST is geselecteerd voor standaardisatie, namelijk FN-DSA (Falcon), maakt ook gebruik van een gestructureerd rooster dat bekend staat als een *NTRU-rooster*. Analoge gestructureerde problemen worden ook gebruikt in cryptografie op basis van codes. Dan gaat dat onder de naam *Quasi-Cyclic Syndrome Decoding* (QCSD), wat de kern vormt van zowel BIKE als HQC – twee algoritmes die beide nog meedingen in de vierde ronde van de NIST-competitie. Het voordeel van het gebruik van dergelijke gestructureerde varianten is dat ze resulteren in efficiëntere cryptografische schema's met kortere sleutels, ciphertexten en handtekeningen. Aan de andere kant kan deze extra structuur de moeilijkheid van het onderliggende wiskundige probleem verminderen, waardoor de cryptografische primitieve zwakker wordt. Om deze reden pleiten sommige instanties, zoals het Nederlandse NLNCSA, het Duitse BSI en het Franse ANSSI voor de standaardisatie van ongestructureerde schema's zoals Classic McEliece (met codes) en FrodoKEM (met roosters) in plaats van uitsluitend te vertrouwen op gestructureerde varianten.

6.5) Veiligheid van implementaties

Om cryptografische primitieven in de praktijk in gebruik te nemen is een implementatie nodig. In deze sectie willen we herhalen dat onzorgvuldige implementatie kan leiden tot veel zwakheden, zelfs als het ontwerp van een primitieve theoretisch zeer veilig is. We geven hiervan ook enkele voorbeelden. Specifieke veiligheidseisen voor implementatie kunnen onder andere bescherming tegen *Side-Channel Analysis* (SCA), *Fault Injection* (FI) en *Differential Fault Analysis* (DFA) omvatten. Voor een diepgaander overzicht van SCA en FI op roostergebaseerde schema's, zie [RCDB24].

Side-Channel Analysis | *Side-Channel Analysis* (SCA) is een aanval op cryptografische implementaties die geheime informatie onttrekt door meer te observeren dan alleen de invoer- en uitvoergegevens tijdens de uitvoering van een programma. Dit geldt voor cryptografische primitieven, maar ook voor andere beveiligingsgevoelige operaties, zoals het transporteren van een sleutel naar een cryptografische coprocessor. Een voorbeeld van een side-channel-zwakte die kan worden uitgebuit is een loop waarvan het aantal iteraties afhangt van een geheime waarde. Door naar de responstijd van het programma te kijken, kan een aanvaller met een *timing-aanval* het aantal iteraties schatten en zo informatie over het geheim verkrijgen. Als er relevante informatie wordt gevonden in een side-channel, wordt dit vaak aangeduid als een *lek*. Om timing-aanvallen te voorkomen, moeten cryptografische implementaties in constante tijd worden uitgevoerd of moet de uitvoeringstijd volledig onafhankelijk zijn van geheime waarden. Naast tijd zijn andere bekende side-channels stroomverbruik en elektromagnetische straling. In sommige gevallen kunnen temperatuur, geluid of licht ook informatie lekken over processen die op een apparaat worden uitgevoerd. In de meeste gevallen moet een side-channel gemeten worden in de nabijheid van het apparaat dat de geheime gegevens verwerkt. Een timing-aanval kan echter op afstand worden uitgevoerd, bijvoorbeeld vanaf het apparaat van de andere partij in de communicatie. In de meeste SCA-aanvallen zal de aanvaller de side-channel tijdens meerdere uitvoeringen van het algoritme monitoren. Door vervolgens statistische analyses toe te passen op de geregistreerde gegevens, kan er zo informatie over de gebruikte geheime sleutel worden geëxtraheerd. In sommige gevallen kan zelfs gedeeltelijke informatie over de sleutel al genoeg zijn om een haalbare aanval uit te voeren om de gehele sleutel te reconstrueren. Er zijn ook SCA-aanvallen die alleen observatie van een enkele uitvoering van een algoritme vereisen, of gebruik maken van machine learning om geheime gegevens te extraheren. Het voorkomen van SCA-aanvallen kan zeer uitdagend zijn.

Zelfs als een cryptografisch algoritme is ontworpen om in constante tijd te draaien, kan de compiler zwakheden introduceren door optimalisatie. Een recent ontdekte kwetsbaarheid in de referentie-implementatie van ML-KEM [BBBC+24], die ook in veel andere implementaties voor kwam, toont dit probleem aan: operaties die afhangen van geheime waarden veroorzaakten een lek van de geheime sleutel die binnen enkele minuten werd gereconstrueerd. Aangezien dit een software-implementatie betrof, is de kwetsbaarheid snel verholpen met een patch. Hoewel dit niet het belangrijkste of meest relevante werk is op het gebied van SCA voor PQC, onderstreept het wel het belang van geïnformeerd en waakzaam blijven over de dreiging van implementatiekwetsbaarheden. Dit is in het bijzonder zo omdat deze kwetsbaarheid pas zo laat in het standaardisatieproces werd ontdekt
Standaardtechnieken om SCA te voorkomen zijn niet altijd compatibel met het ontwerp van PQC-algoritmes. Het digitale handtekeningalgoritme FN-DSA gebruikt bijvoorbeeld *floating point arithmetic*, wat zeer uitdagend is om te beschermen tegen side-channel aanvallen. Deze complexiteit vertraagde de standaardisatie [Moo24].

Fault Injection | Een *Fault Injection* (FI) is een implementatie-aanval die erop gericht is om fouten in de normale werking van het apparaat te introduceren. Een voorbeeld van een dergelijke aanval is een safe-error aanval, waarbij de aanvaller een fout injecteert die een bit van de geheime sleutel instelt die door het doelwit wordt beheerd. Door te verifiëren of het resultaat van de berekening is gewijzigd, is het mogelijk om de waarde van de gerichte bit van de geheime sleutel te bepalen, wat resulteert in lekkage. Bekende fault injection-technieken zijn: *clock* en *reset glitching*, *voltage fault injection* (manipulatie van de spanning van de voeding van het apparaat of *Body Bias Injection*), *laser fault injection* (voor het aanvallen van halfgeleiders), en blootstelling aan elektromagnetische straling. Deze technieken kunnen worden toegepast op het volledige apparaat, of specifiek gericht zijn op een *Integrated Circuit* (chip) in het apparaat.

Differential Fault Analysis | *Differential Fault Analysis* (DFA) is een type implementatie-aanval waarbij beschadigde (*corrupted*) berekeningen van een algoritme worden geanalyseerd om geheime gegevens te extraheren. Er is eerst een FI nodig om de beschadigingen in de berekening te introduceren.

Voor sommige DFA-aanvallen zijn meerdere fouten nodig voor de analyse (dit is het geval in de meeste aanvallen op symmetrische algoritmes) en andere aanvallen vereisen slechts één foutief antwoord, zoals de bekende Bellcore-aanval op RSA-CRT [SvdBFG+12]. DFA-aanvallen werken niet op alle cryptografische algoritmes, maar er bestaan publicaties met betrekking tot DFA-aanvallen op post-quantumcryptografie, zoals op FN-DSA [BD23] en ML-DSA [CBH24].
Het is cruciaal om te bepalen in welke mate een toepassing moet worden beschermd tegen SCA, FI en DFA. Weerstand tegen timing-aanvallen is essentieel, maar het is belangrijk op te merken dat het nemen van maatregelen tegen SCA, FI en DFA de grootte en prestaties van de implementatie zal beïnvloeden. Het is van essentieel belang dat beschermde implementaties passen bij de toepassing zonder problemen of knelpunten te veroorzaken. Vanwege de vele zwakheden die in een implementatie van een cryptografisch algoritme kunnen worden geïntroduceerd, wordt sterk aangeraden om de implementatie aan experts over te laten. Het is daarom essentieel om alleen productieklare implementaties in gebruik te nemen die een grondige beveiligingsevaluatie zijn ondergaan, zoals die gecertificeerd onder FIPS 140 [NIST01a; NIST19c] of ISO/IEC 19790 [ISO12] (voor cryptogragische modules) of ISO/IEC 15408 [ISO22b], ook bekend als de Common Criteria (CC), en de Nederlandse Baseline Security Product Assessment (BSPA) [BSPA20] voor generieke implementaties van cryptografie en security-maatregelen. Veiligheidsevaluaties moeten worden uitgevoerd door geaccrediteerde *security evaluation labs* die certificeringsdiensten verlenen. Deze labs kunnen ook trainingen en tools bieden om interne veiligheidsevaluaties uit te voeren.

6.6 PQC-implementaties

Het doel van deze sectie is om de stand van zaken te schetsen rondom beschikbare cryptografische softwarelibraries voor PQC. Daartoe geven we een overzicht van verschillende libraries die post-quantum primitieven bevatten. Let op: niet elke library bevat een implementatie van elke cryptografische primitieve.
Hoewel bijvoorbeeld alle KEMs functioneel equivalent zijn, kunnen andere factoren zoals snelheid en geheugengebruik relevant zijn. Een library kan eventueel ook een interface bieden naar de programmeertaal of het framework waarop het project is gebouwd, of kan bedoeld zijn voor gespecialiseerde use-cases, zoals embedded systems.

Voortgang van software-ontwikkeling | Alle inzendingen voor de NIST PQC-standaardisatiecompetitie in 2016 bevatten al referentie-implementaties. Later werden er geoptimaliseerde implementaties beschikbaar gesteld. Veel inzendingen werden uiteindelijk gebroken, waarvan de opvallendste de kandidaat SIKE in 2023 was, die het tot de vierde ronde had geschopt [CD23]. Het is niet ondenkbaar dat andere kandidaten alsnog worden gebroken, wat voor nu een argument is om hybride cryptografie te gebruiken, zie sectie 4.1. De referentie-implementaties zijn te vinden in de standaardisatiedocumenten die in de vorige secties zijn vermeld. Ze zijn echter niet bedoeld voor gebruik in een productieomgeving. Er is bijvoorbeeld onlangs een aanval geweest op de referentie-implementatie van ML-KEM, die ook verschillende andere implementaties raakt [BBBC+24].
Referentie-implementaties kunnen tijdens de migratie worden gebruikt als tijdelijke oplossing totdat betrouwbaardere implementaties beschikbaar worden. Dit vereist ook enige mate van crypto-agility. Binnen een enkele library wordt dit over het algemeen bereikt door een 'universele' interface naar de cryptografie. Voor bijvoorbeeld OpenSSL kan het vervangen van de DES-cijfer door de AES-cijfer worden gedaan door de functieaanroep EVP_CIPHER_fetch(0,"DES-CBC",0) te vervangen door EVP_CIPHER_fetch(0,"AES-256-CBC",0). Om de migratie te vergemakkelijken, biedt Open Quantum Safe (OQS) PQC-implementaties die op vergelijkbare wijze binnen OpenSSL kunnen worden gebruikt. Merk op dat, net als bij de referentie-implementaties, OQS momenteel niet aanbeveelt om de library in een productieomgeving te gebruiken. Er zijn libraries die PQC bieden die ISO- of FIPS-gecertificeerd zijn, wat een vereiste kan zijn bijvoorbeeld wan-

neer een van de eindgebruikers een overheidsorganisatie is. De nieuwe PQC-schema's die door NIST zijn goedgekeurd, zullen hoogstwaarschijnlijk de certificering FIPS 140-3 krijgen, aangezien er geen nieuwe certificeringen voor FIPS 140-2 meer worden verleend.

Hardware-implementaties | Over het algemeen zijn hardware-implementaties ontworpen om parallelliteit te gebruiken om zo de performance te verbeteren. In tegenstelling tot software-oplossingen die doorgaans op een enkele *core* draaien, kan hardware meerdere bewerkingen tegelijkertijd uitvoeren.
Deze parallelliteit wordt bereikt door verschillende mechanismen, zoals *dedicated processing units*, pipeline-architectuur en aangepaste circuits. Een nadeel is dat extra hardware duur kan zijn. Een *dedicated coprocessor* geïmplementeerd in hardware zal een software-implementatie overtreffen, maar kan (meestal) niet worden bijgewerkt in geval van een probleem dat na ingebruikname pas wordt ontdekt. Hardwareversnelling kan een oplossing bieden tussen een volledige software- en hardware-implementatie. In dit geval heeft een CPU ofwel toegewijde instructies, óf wordt een coprocessor gebruikt om delen van de berekening uit te voeren die tijdrovend zijn in een pure software-implementatie.

Software-implementaties | Tabel 6.4 geeft een overzicht van verschillende veelgebruikte cryptografische libraries met enkele aanvullende informatie over compatibiliteit en veiligheid. Deze lijst is niet bedoeld om volledig te zijn, noch als een aanbeveling voor een specifieke library. Bovendien kan deze lijst snel verouderd raken, en daarom moet de huidige versie van deze tabel alleen worden geraadpleegd door degenen die op korte termijn migreren. Het PKI Consortium houdt een vergelijkbare tabel bij op https://pkic.org/pqccm.

De kolommen 'stateful DSA', 'stateless DSA' en 'KE(M)' bevatten een vinkje als de library ten minste één PQC-algoritme met die eigenschap bevat.

Advies voor integratie | We sommen kort enkele praktische adviezen op voor degenen die post-quantumcryptografie integreren:

- Blijf op de hoogte van de ontwikkelingen van standaarden: nu de standaarden voor ML-KEM [NIST24a], ML-DSA [NIST24b] en SLH-DSA [NIST24c] zijn gepubliceerd, worden binnenkort veilige implementaties verwacht;
- Blijf op de hoogte van de ontwikkelingen van certificeringen als deze relevant zijn voor specifieke toepassingen;
- Blijf op de hoogte van publicaties met betrekking tot SCA, FI, DFA en andere kwetsbaarheden tijdens alle fasen van de levenscyclus van het product. Zie bijvoorbeeld een Common Vulnerabilities and Exposure database zoals https://nvd.nist.gov/;
- Overweeg een combinatie van software- en hardwareoplossingen te gebruiken;
- Onderzoek het gebruik van (her)configureerbare hardware (bijv. FPGA of IC met een gedeeltelijk configureerbaar logica-gedeelte) als de toepassing update-mogelijkheden na ingebruikname vereist.

Organisatie	Git-repository	*Stateful* DSA	*Stateless* DSA	KE(M)	Hybride constructies	Certificering	Interfaces met talen
Botan	[BSI24a]	✓	✓	✓	✓	–	C, C++, D, Python, Rust, Ruby, Haskell
Bouncy Castle	[BC24b]	✓	✓	✓	✓	FIPS 140-3	C#, Java, Kotlin
Crypto++	[Dai23]				–	–	C++
FoxCrypto	[Fox23]	✓			–	CC	C
GnuTLS	[GnuTLS24]				–	FIPS 140-2	C
KyberLib	[Rou24]			✓	–	–	Rust
LibreSSL	[LibreSSL24]				–	–	C
Libsodium (NaCl)	[Libsodium13]				–	–	C, C++
Nettle	[Nettle24]				–	–	C
OpenSSL	[OpenSSL03]				–	FIPS 140-2	C
OpenSSL-OQS	[OQSprovider24]		✓	✓	–	–	C
OQS	[OQS24]	✓	✓	✓	–	–	C, Python, Rust, Java
PQM4	[KPRS+22]		✓	✓	–	–	C (ARM MCU)
PQClean	[PQClean23]		✓	✓	–	–	C
RustTLS	[Rust24]	✓	✓	✓	–	–	Rust
WolfSSL	[Wol24a]		✓	✓	–	FIPS 140-3	C (Embedded systems)

Tabel 6.4 | Enkele bekende cryptografische softwarelibraries (9 oktober, 2024).

Bibliografie

[ABBB+21] Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor, Vasseur. Valentin, Santosh Ghosh, and Jan Richter-Brokmann. BIKE Website. https://bikesuite.org/. [Bezocht 22/08/2022]. 2021.

[ABCC+20] Martin Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece Website. https://classic.mceliece.org/index.html. [Bezocht 23/05/2022]. 2020.

[ABDL+21] Erdem Alkim, Joppe Bos, Léo Ducas, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, Douglas Stebila, Karen Easterbrook, and Brian LaMacchia. FrodoKEM Website. https://frodokem.org/. [Bezocht 23/05/2022]. 2021.

[ABNS24] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), and Swedish Armed Forces Swedish National Communications Security Authority. Position Paper on Quantum Key Distribution. Bezocht 2024-07-16. 2024. url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4.

[AIVD23] AIVD. AIVD-jaarverslag 2023. https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2024/04/22/jaarverslag-2023. 2023.

[ANSI10] American National Standards Institute (ANSI). ANSI X9.98-2010 Lattice-Based Polynomial Public Key Establishment Algorithm For The Financial Services Industry. ANSI X9.98-2010. American National Standards Institute, 2010. url: https://webstore.ansi.org/standards/ascx9/ansix9982010.

[ANSI17a] American National Standards Institute. Key Agreement and Key Transport Using Elliptic Curve Cryptography. Standard. ANSI, Feb. 2017.

[ANSI17b] American National Standards Institute. Key Establishment Using Integer Factorization Cryptography. Standard. ANSI, Nov. 2017.

[ANSI20] American National Standards Institute. Financial services - Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm - ECDSA. Standard. ANSI, Sept. 2020.

[ANSSI20] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Technical Position Paper QKD v2.1 - Should Quantum Key Distribution be Used for Secure Communications? https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/. 2020.

[ANSSI23] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Migration to Post-Quantum Cryptography Recommendations and Guidelines. https://www.ssi.gouv.fr/en/guide/migration-to-post-quantum-cryptography/. Jan. 2023.

[Apple24] Apple. iMessage PQ3 Quantum-Secure Messaging at Scale. https://security.apple.com/blog/imessage-pq3/. Bezocht 2024-07-31. 2024.

[ASWH+23] Nouri Alnahawi, Nicolai Schmitt, Alexander Wiesmaier, Andreas Heinemann, and Tobias Grasmeyer. "On the State of Crypto-Agility". In Cryptology ePrint Archive (2023).

[AVW23] Suleman Ahmad, Luke Valenta, and Bas Westerbaan. Cloudflare now uses post-quantum cryptography to talk to your origin server. 2023. url: https://blog.cloudflare.com/post-quantum-to-origins.

[BBBC+24] Daniel J. Bernstein, Karthikeyan Bhargavan, Shivam Bhasin, Anupam Chattopadhyay, Tee Kiah Chia, Matthias J. Kannwischer, Franziskus Kiefer, Thales Paiva, Prasanna Ravi, and Goutam Tamvada. KyberSlash Exploiting secret-dependent division timings in Kyber implementations. Cryptology ePrint Archive, Paper 2024/1049. url: https://eprint.iacr.org/2024/1049. 2024.

[BC24a] Legion of the Bouncy Castle Inc. Bouncy Castle Cryptography APIs. 2024. url: https://bouncycastle.org.

[BC24b] The Legion of the Bouncy Castle. The Bouncy Castle for Java. https://github.com/bcgit/bc-java. Tag r1rv78v1. Apr. 2024.

[BD23] Sven Bauer and Fabrizio De Santis. "A differential fault attack against deterministic falcon signatures". In International Conference on Smart Card Research and Advanced Applications. Springer. 2023, pp. 43–61.

[Beu22] Ward Beullens. "Breaking Rainbow Takes a Weekend on a Laptop". In Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. Lecture Notes in Computer Science. Springer, 2022, pp. 464–479.

[BJKS24] Karthikeyan Bhargavan, Charlie Jacomme, Franziskus Kiefer, and Rolfe Schmidt. "Formal Verification of the PQXDH Post-Quantum Key Agreement Protocol for End-to-End Secure Messaging". In USENIX Security Symposium 2024. 2024.

[BL] Daniel J. Bernstein and Tanja Lange, eds. eBACS: ECRYPT Benchmarking of Cryptographic Systems. Bezocht: 14 October 2024. url: https://bench.cr.yp.to.

[BLAKE217] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. BLAKE2 – fast secure hashing. https://www.BLAKE2.net/. [Bezocht op 24-03-2022]. 2017.

[BLS24] David Basin, Felix Linker, and Ralf Sasse. A Formal Analysis of the iMessage PQ3 Messaging Protocol. Technical Report. 2024. url: https://security.apple.com/assets/files/A_Formal_Analysis_of_the_iMessage_PQ3_Messaging_Protocol_Basin_et_al.pdf.

[Bro09] Daniel Brown. Elliptic Curve Cryptography. Standard. SEC 1. Standards for Efficient Cryptography Group, May 2009.

[BSI22] Bundesamt für Sicherheit in der Informationstechnik (BSI). Quantum-safe Cryptography - fundamentals, current developments and recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html. May 2022.

[BSI24a] Bundesamt für Sicherheit in der Informationstechnik (BSI). Botan Crypto and TLS for modern C++. https://botan.randombit.net/. Version 3.5.0. 2024.

[BSI24b] Bundesamt für Sicherheit in der Informationstechnik (BSI). Cryptographic Mechanisms Recommendations and Key Lengths. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?blob=publicationFile&v=7. Feb. 2024.

[BSPA20] AIVD. Baseline Security Product Assessment (BSPA. https://www.aivd.nl/onderwerpen/informatiebeveiliging/certificeringen/baseline-security-product-assessment. Assessed: 2024-10-11. 2020.

[CBH24] Andersson Calle Viera, Alexandre Berzati, and Karine Heydemann. "Fault Attacks Sensitivity of Public Parameters in the Dilithium Verification". In: Smart Card Research and Advanced Applications. Cham: Springer Nature Switzerland, 2024, pp. 62–83.

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 423–447. doi: 10.1007/978-3-031-30589-4_15. url: https://doi.org/10.1007/978-3-031-30589-4_15.

[Cha23] Walker Chablott. Addressing post-quantum cryptography with CodeQL. https://github.blog/2023-12-05-addressing-post-quantum-cryptography-with-codeql/. Bezocht 2024-06-11. 2023.

[CISA23] Cybersecurity and Infrastructure Security Agency (CISA). Quantum-readiness Migration to Post-Quantum Cryptography. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography. Bezocht 2024-06-17. Aug. 2023.

[CW21] Sofía Celi and Thom Wiggers. KEMTLS Post-Quantum TLS Without Signatures. 2021. url: https://blog.cloudflare.com/kemtls-post-quantum-tls-without-signatures.

[Cyc24] CycloneDX Project. CycloneDX A Standard for Bill of Materials. Bezocht 2024-07-03. 2024. url: https://cyclonedx.org/.

[Dai23] Wei Dai. Crypto++ Library. https://github.com/weidai11/cryptopp. v8.9. Oct. 2023.

[dVBDvV24] Manon de Vries, Sven Bootsma, Vincent Dunning, and Marc van Vliet. Quantum risicomethodologie voor cryptografie. https://publications.tno.nl/publication/34642390/EUY5Mh/TNO-2024-R10707.pdf. 2024.

[EMVW22] Andre Esser, Alexander May, Javier Verbel, and Weiqiang Wen. "Partial Key Exposure Attacks on BIKE, Rainbow and NTRU". In Advances in Cryptology – CRYPTO 2022. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Cham Springer Nature Switzerland, 2022, pp. 346–375. isbn 978-3-031-15982-4.

[ET05] Pasi Eronen and Hannes Tschofenig. Pre-shared key ciphersuites for transport layer security (TLS). RFC 4279. Dec. 2005. doi: 10.17487/RFC4279. url: https://www.rfc-editor.org/info/rfc4279.

[ETSI18] ETSI. Quantum-Safe Virtual Private Networks. Standard. TR 103 617. Valbonne, FR ETSI, Sept. 2018.

[ETSI20a] ETSI. Migration strategies and recommendations to Quantum Safe schemes. https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes. 2020.

[ETSI20b] European Telecommunications Standards Institute. CYBER; Quantum-safe Hybrid Key Exchanges. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Dec. 2020.

[ETSI20c] European Telecommunications Standards Institute. Migration strategies and recommendations to Quantum Safe schemes. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Aug. 2020.

[ETSI21a] European Telecommunications Standards Institute. CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Oct. 2021.

[ETSI21b] European Telecommunications Standards Institute. CYBER; Quantum-Safe Signatures. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Sept. 2021.

[EU16a] European Parliament and Council of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union L 194, 19 July 2016, pages 1-30. 2016. url: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[EU16b] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union L 119, 4 May 2016, pages 1-88. 2016. url: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[EU18] European Parliament. Directive (EU) 2018/1972 of the European Parliamentand of the council of 11 December 2018 establishing the European Electronic Communications Code. 2018. url: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX32018L1972.

[EU22a] European Parliament and Council of the European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union L 333, 27 December 2022, pages 80-152. 2022. url: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[EU22b] European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union L 333, 27 December 2022, pages 1-79. 2022. url: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

[EU24] European Commission. Commission Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJL_202401101. Official Journal of the European Union, L 1101, 12 April 2024. Apr. 2024.

[FHKP+21] Pierre-Alain Fouque, Jeffrey Hoffstein, Vadim Kirchner Paul Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON Website. https://falcon-sign.info/. [Bezocht 23/05/2022]. 2021.

[Fiche24] Dutch Ministry of the Interior and Kingdom Relations. Fiche 1 Aanbeveling Routekaart Post-Quantumcryptografie. 2024. url: https://www.rijksoverheid.nl/documenten/publicaties/2024/04/11/fiche-1-aanbeveling-routekaart-post-quantumcryptografie.

[FK11] Sheila Frankel and Suresh Krishnan. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071. Feb. 2011. doi: 10.17487/RFC6071. url: https://www.rfc-editor.org/info/rfc6071.

[FKMS20] Scott Fluhrer, Panos Kampanakis, David McGrew, and Valery Smyslov. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security. RFC 8784. June 2020. doi: 10.17487/RFC8784. url: https://www.rfc-editor.org/info/rfc8784.

[Fox23] Fox Crypto. XMSS C Library. https://github.com/FoxCryptoNL/xmss. Version 1.0.0. Apr. 2023.

[GLRS16] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. "Applying Grover's Algorithm to AES: Quantum Resource Estimates". In: PQCrypto. Vol. 9606. Lecture Notes in Computer Science. Springer, 2016, pp. 29–43.

[GnuTLS24] GnuTLS. https://gitlab.com/gnutls/gnutls. v3.8. Oct. 2024.

[Google17] Google. Application Layer Transport Security. 2017. url: https://cloud.google.com/docs/security/encryption-in-transit/application-layer-transport-security.

[Google22a] Google. Messages End-to-End Encryption Overview (Technical Paper). Feb. 2022. url: https://www.gstatic.com/messages/papers/messages_e2ee.pdf.

[Google22b] Google. Securing tomorrow today Why Google now protects its internal communications from quantum threats. Nov. 2022. url: https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms.

[Gro24] The Tcpdump Group. TCPDUMP & LIBPCAP. 2024. url: https://www.tcpdump.org/.

[Gro96] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In STOC. ACM, 1996, pp. 212–219.

[GSMA24] GSM Association. Post Quantum Cryptography – Guidelines for Telecom Use Cases. https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf. Bezocht 2024-06-19. Feb. 2024.

[HE11] Tony Hansen and Donald E. Eastlake 3rd. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234. May 2011. doi: 10.17487/RFC6234. url: https://www.rfc-editor.org/info/rfc6234.

[Hou02] Russ Housley. Cryptographic Message Syntax (CMS). RFC 3369. Sept. 2002. doi: 10.17487/RFC3369. url: https://www.rfc-editor.org/info/rfc3369.

[HRSS17] Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. NTRU-HRSS-KEM-Submission to the NIST post-quantum cryptography project. 2017. url: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/NTRU_HRSS_KEM.zip.

[IBM24] IBM. Examples from CBOM repository. https://github.com/IBM/CBOM/blob/main/EXAMPLES.md. Bezocht 2024-07-04. 2024.

[IETF07] Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney L. Thayer, and David Shaw. OpenPGP Message Format. RFC 4880. Nov. 2007. doi: 10.17487/RFC4880. url: https://www.rfc-editor.org/info/rfc4880.

[IETF09] Mohamad Badra. Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode. RFC 5487. Mar. 2009. doi: 10.17487/RFC5487. url: https://www.rfc-editor.org/info/rfc5487.

[IETF18] Andreas Huelsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen. XMSS eXtended Merkle Signature Scheme. RFC 8391. May 2018. doi: 10.17487/RFC8391. url: https://www.rfc-editor.org/info/rfc8391.

[IETF19] David McGrew, Michael Curcio, and Scott Fluhrer. Leighton-Micali Hash-Based Signatures. RFC 8554. Apr. 2019. doi: 10.17487/RFC8554. url: https://www.rfc-editor.org/info/rfc8554.

[IETF24] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-10. Internet Engineering Task Force, Apr. 2024. url: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/.

[ISLP06] Tetsu Iwata, Junhyuk Song, Jicheol Lee, and Radha Poovendran. The AES-CMAC Algorithm. RFC 4493. June 2006. doi: 10.17487/RFC4493. url: https://www.rfc-editor.org/info/rfc4493.

[ISO06] International Electrotechnical Commission International Organization for Standardization. Information technology – Security techniques – Encryption algorithms – Part 2 Asymmetric ciphers. ISO/IEC 18033-2. 2006. url: https://www.iso.org/standard/38788.html.

[ISO08] International Organization for Standardization. Information Technology – Security Techniques – Digital Signatures with Appendix – Part 2 Integer Factorization Based Mechanisms. Standard. Geneva, CH, Apr. 2008.

[ISO10a] International Organization for Standardization. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2 Integer factorization based mechanisms. Standard. ISO/IEC 9796-22010. Geneva, CH International Organization for Standardization, Dec. 2010.

[ISO10b] International Organization for Standardization. Information technology – Security techniques – Encryption algorithms – Part 3 Block ciphers. Standard. ISO/IEC 29167-212018. Geneva, CH International Organization for Standardization, Dec. 2010.

[ISO10c] International Organization for Standardization. Information technology – Security techniques – Key management – Part 1 Framework. Standard. Geneva, CH International Organization for Standardization, Apr. 2010.

[ISO11] International Organization for Standardization. IT Security techniques – Hash-functions - Part 3: Dedicated hash-functions. Standard. Geneva, CH: International Organization for Standardization, Mar. 2011.

[ISO12] International Electrotechnical Commission International Organization for Standardization. Information technology – Security techniques – Security requirements for cryptographic modules. ISO/IEC 19790. 2012. url: https://www.iso.org/standard/52906.html.

[ISO18a] International Organization for Standardization. Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1 Mechanisms using a block cipher. Standard. ISO/IEC 10118-32018. Geneva, CH International Organization for Standardization, Oct. 2018.

[ISO18b] International Organization for Standardization. Information Technology – Security Techniques – Digital signatures with Appendix – Part 3 Discrete Logaritme Based Mechanisms. Standard. Geneva, CH, Nov. 2018.

[ISO22a] International Organization for Standardisation. Information technology – Security techniques – Information security management systems – Requirements. Standard. ISO/IEC 270012022. Geneva, CH International Organization for Standardisation, Oct. 2022.

[ISO22b] International Electrotechnical Commission International Organization for Standardization. Information security, cybersecurity and privacy protection - Evaluation criteria for IT security. ISO/IEC 15408-1. 2022. url: https://www.iso.org/standard/72891.html.

[ISO24] International Electrotechnical Commission International Organization for Standardization. Information Security - Digital Signatures with Appendix. ISO/IEC 14888. 2024. url: https://www.iso.org/standard/80492.html.

[ITU19] International Telecommunication Union (ITU). Information technology - Open Systems Interconnection - The Directory Public-key and attribute certificate frameworks. Standard. Geneva, Switzerland ITU-T, Oct. 2019.

[Jac24] Frederic Jacobs. "Designing iMessage PQ3 Quantum-Secure Messaging at Scale". In Real World Crypto Symposium 2024. Toronto, Canada, Mar. 2024.

[JACC+21] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. SIKE Website https://sike.org/. [Bezocht 22/08/2022]. 2021.

[JL17] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032. Jan. 2017. doi: 10.17487/RFC8032. url: https://www.rfc-editor.org/info/rfc8032.

[JNRV20] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC". In EUROCRYPT (2). Vol. 12106. Lecture Notes in Computer Science. Springer, 2020, pp. 280–310.

[KBC97] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC Keyed-Hashing for Message Authentication. RFC 2104. Feb. 1997. doi: 10.17487/RFC2104. url: https://www.rfc-editor.org/info/rfc2104.

[KHNE+14] Charlie Kaufman, Paul E. Hoffman, Yoav Nir, Pasi Eronen, and Tero Kivinen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296. Oct. 2014. doi: 10.17487/RFC7296. url: https://www.rfc-editor.org/info/rfc7296.

[KJB24] Ini Kong, Marijn Janssen, and Nitesh Bharosa. Organizational Readiness Model for Quantum-safe Transition. https://hapkido.tno.nl/deliverables/organizational-readiness-model-quantum/. Bezocht 2024-7-16. 2024.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. "Unbalanced Oil and Vinegar Signature Schemes". In Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Ed. by Jacques Stern. Vol. 1592. Lecture Notes in Computer Science. Springer, 1999, pp. 206–222. doi: 10.1007/3-540-48910-X_15. url: https://doi.org/10.1007/3-540-48910-X_15.

[KPMS23] Stefan Kölbl, Anvita Pandit, Rafael Misoczki, and Sophie Schmieg. "Crypto Agility and Post-Quantum Cryptography @ Google". In Real World Crypto Conference 2023. Tokyo, Japan, Mar. 2023. url: https://rwc.iacr.org/2023/.

[KPRS+22] Matthias J. Kannwischer, Richard Petri, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. PQM4 Post-quantum crypto library for the ARM Cortex-M4. https://github.com/mupq/pqm4. Round3. July 2022.

[KSFH+20] Panos Kampanakis, Douglas Stebila, Markus Friedl, Torben Hansen, and Dimitrios Sikeridis. Post-quantum public key algorithms for the Secure Shell (SSH) protocol. Internet-Draft draft-kampanakis-curdle-pq-ssh-00. Work in Progress. Internet Engineering Task Force, Oct. 2020. 13 pp. url: https://datatracker.ietf.org/doc/html/draft-kampanakis-curdle-pq-ssh-00.

[LibreSSL24] LibreSSL. https://github.com/libressl/portable. v4.0.0. Oct. 2024.

[Libsodium13] Frank Denis. The Sodium cryptography library. June 2013. url: https://download.libsodium.org/doc/.

[LTAN+24] Sheran Lin, Jolene Tan, Ajanthan Asogamoorthy, Kyle Nekritz, Rafael Misoczki, and Sotirios Delimanolis. Post-quantum readiness for TLS at Meta. https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/. 2024.

[LY06] Chris M. Lonvick and Tatu Ylonen. The Secure Shell (SSH) Protocol Architecture. RFC 4251. Jan. 2006. doi: 10.17487/RFC4251. url: https://www.rfc-editor.org/info/rfc4251.

[Lyo24] Gordon Lyon. Nmap Network Mapper. 2024. url: https://nmap.org/.

[MABL+21] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Bidoux. Loïc, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Lacan. Jerome, Robert. Jean-Marc, and Pascal Veron. HQC Website. http//pqc-hqc.org/. [Bezocht 22/08/2022]. 2021.

[Mar13] Moxie Marlinspike. Advanced Cryptographic Ratcheting. Signal Blog. Technical Whitepaper. Nov. 2013. url: https://signal.org/blog/advanced-ratcheting/.

[McE78] Robert J. McEliece. "A Public-Key System Based on Algebraic Coding Theory". In DSN Progress Report 44. Jet Propulsion Lab, 1978, pp. 114–116.

[Meta24] Meta. Fizz a TLS 1.3 Implementation. https://github.com/facebookincubator/fizz. v2024.08.19.00. Aug. 2024.

[Mil24] Jon Millican. "Shipping End-to-End Encryption to Billions". In Real World Crypto Symposium 2024. Contributed Talk. International Association for Cryptologic Research (IACR). Toronto, Canada, Mar. 2024.

[MJ21] Nikos Mavrogiannopoulos and Simon Josefsson. [Bezocht 22/02/2022]. 2021. url: https://www.gnupg.org/index.html.

[MKJR16] Kathleen Moriarty, Burt Kaliski, Jakob Jonsson, and Andreas Rusch. PKCS #1 RSA Cryptography Specifications Version 2.2. RFC 8017. Nov. 2016. doi: 10.17487/RFC8017. url: https://www.rfc-editor.org/info/rfc8017.

[Moo24] Dustin Moody. Are We There Yet? An Update on the NIST PQC Standardization Project. https://csrc.nist.gov/csrc/media/Presentations/2024/update-on-the-nist-pqc-standardization-project/images-media/moody-are-we-there-yet-pqc-pqc2024.pdf. Bezocht 2024-07-05. 2024.

[MP16] Moxie Marlinspike and Trevor Perrin. The X3DH Key Agreement Protocol. Signal Blog. Technical Wihtepaper. 2016. url: https://signal.org/docs/specifications/x3dh/.

[MP23] Michele Mosca and Marco Piani. 2023 Quantum Threat Timeline Report. https://globalriskinstitute.org/publications/2023-quantum-threat-timeline-report/. 2023.

[MvH20] Frank Muller and Maran van Heesch. Migration to Quantum-safe Cryptography. https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/trusted-ict/quantum/quantum-safe-crypto/. 2020.

[NCCoE23] National Cybersecurity Center of Excellence. Migration to Post-Quantum Cryptography. Quantum Readiness Cryptographic Discovery. Tech. rep. NIST SP 1800-38B. U.S. Department of Commerce, Dec. 2023. url: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

[NCSC-NL23] Dutch National Cyber Security Centre. Maak je organisatie quantumveilig. https://www.ncsc.nl/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig. 2023.

[NCSC-NL24] Dutch National Cyber Security Centre. Het crypto-agilitymonster op een bierviltje. https://www.ncsc.nl/actueel/weblog/weblog/2024/het-crypto-agilitymonster. Bezocht: 20-06-2024. 2024.

[NCSC-UK20a] National Cyber Security Centre (NCSC-UK). Whitepaper: Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography. 2020.

[NCSC-UK20b] National Cyber Security Centre (NCSC-UK). Whitepaper: Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies. 2020.

[NCSC-UK22] National Cyber Security Centre (NCSC-UK). Government Cyber Security Strategy: 2022 to 2030. Bezocht: 2024-07-08. 2022. url: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

[NCSC-UK23] National Cyber Security Centre (NCSC-UK). Next Steps in Preparing for Post-Quantum Cryptography. Bezocht: 2024-07-08. 2023. url: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography.

[NCTV22] AIVD, MIVD, and NCTV. Dreigingsbeeld Statelijke Actoren 2. https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2. 2022.

[Nettle24] Nettle. https://git.lysator.liu.se/nettle/nettle. v3.10. June 2024.

[NIST01a] National Institute of Standards and Technology. FIPS 197 Advanced encryption standard (AES). Standard. FIPS 197. Gaithersburg, MD: NIST, Nov. 2001.

[NIST01b] National Institute of Standards and Technology. FIPS 197: Advanced encryption standard (AES). Standard. FIPS 197. Gaithersburg, MD: NIST, Nov. 2001.

[NIST02] National Institute of Standards and Technology. Announcing Approval of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard; a Revision of FIPS 180-1. Notice. NIST, Aug. 2002.

[NIST08] National Institute of Standards and Technology. FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC). Standard. Gaithersburg, MD: NIST, July 2008.

[NIST12] Quynh Dang. Recommendation for Applications Using Approved Hash Algorithms. Special Publication. SP 800-107 Rev. 1. Gaithersburg, MD: NIST, Aug. 2012.

[NIST15a] National Institute of Standards and Technology. FIPS 180-4 Secure Hash Standard (SHS). Standard. FIPS 180-4. Gaithersburg, MD: NIST, Aug. 2015.

[NIST15b] National Institute of Standards and Technology. FIPS 202 SHA-3 Standard Permutation-Based Hash and Extendable-Output Functions. Standard. Gaithersburg, MD: NIST, Aug. 2015.

[NIST16a] Morris Dworkin. Recommendation for Block Cipher Modes of Operation the CMAC Mode for Authentication. Special Publication. SP 800-38B. Gaithersburg, MD: NIST, June 2016.

[NIST16b] National Institute of Standards and Technology. Report on Post-Quantum Cryptography. Tech. rep. National Institute of Standards and Technology Internal Report 8105 15 pages (April 2016). Washington, D.C.: U.S. Department of Commerce, 2016. doi: 10.6028/NIST.IR.8105.

[NIST16c] National Institute of Standards and Technology. IR8105: Report on Post-Quantum Cryptography. Tech. rep. National Institute of Standards and Technology Internal Report 8105 15 pages (April 2016). Washington, D.C.: U.S. Department of Commerce, 2016. doi: 10.6028/NIST.IR.8105.

[NIST19a] Elaine Barker, Lily Chen, Allen Roginsky, Apostol Vassilev, Richard Davis, and Scott Simon. Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. Special Publication. SP 800-56B. Gaithersburg, MD: NIST, Mar. 2019.

[NIST19b] National Institute of Standards and Technology. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Tech. rep. National Institute of Standards and Technology Internal Report 8240, 27 pages (January 2019). Washington, D.C.: U.S. Department of Commerce, 2019. doi: 10.6028/NIST.IR.8240.

[NIST19c] National Institute of Standards and Technology. FIPS 140-3: Security Requirements for Cryptographic Modules. Standard. FIPS 140-3. Gaithersburg, MD: NIST, Mar. 2019.

[NIST20a] David Cooper, Daniel Apon, Quynh Dang, Michael Davidson, Morris Dworkin, and Carl Miller. Recommendation for Stateful Hash-Based Signature Schemes. Special Publication. Gaithersburg, MD: NIST, Oct. 2020.

[NIST20b] National Institute of Standards and Technology. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Tech. rep. National Institute of Standards and Technology Interagency or Internal Report 8309, 39 pages (July 2020). Washington, D.C.: U.S. Department of Commerce, 2020. doi: 10.6028/NIST.IR.8309.

[NIST21] National Institute of Standards and Technology. Getting Ready for Post-Quantum Cryptography Exploring Challenges associated with Adopting and Using Post-quantum Cryptographic Algorithms. Tech. rep. Washington, D.C.: U.S. Department of Commerce, 2021. doi: 10.6028/NIST.CSWP.04282021.

[NIST22] National Institute of Standards and Technology. IR8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Proces. Tech. rep. National Institute of Standards and Technology Interagency or Internal Report NIST IR 8413-upd1, 102 pages (July 2022). Washington, D.C.: U.S.

[NIST23] National Institute of Standards and Technology. FIPS 186-5: Digital Signature Standard (DSS). Standard. FIPS 186-5. Gaithersburg, MD: NIST, Feb. 2023.

[NIST24a] National Institute of Standards and Technology. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard. Standard. Gaithersburg, MD: NIST, Aug. 2024. url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf.

[NIST24b] National Institute of Standards and Technology. FIPS204 Module-Lattice-Based Digital Signature Standard. Standard. Gaithersburg, MD: NIST, Aug. 2024. url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf.

[NIST24c] National Institute of Standards and Technology. FIPS205 Stateless Hash-Based Digital Signature Standard. Standard. Gaithersburg, MD: NIST, Aug. 2024. url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf.

[NL18] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. June 2018. doi: 10.17487/RFC8439. url: https://www.rfc-editor.org/info/rfc8439.

[NLNCSA21] Netherlands National Communications Security Agency (NLNCSA). Bereid je voor op de dreiging van quantumcomputers. https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers. 2021.

[NSA21a] National Security Agency (NSA). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). NSA Announcement, 19 July 2021. 2021. url: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.

[NSA21b] NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. 2021.

[OBr23] Devon O'Brien. Protecting Chrome Traffic with Hybrid Kyber KEM. 2023. url: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.

[OGPK+24a] Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, and Scott Fluhrer. Composite ML-DSA for use in Internet PKI. Internet-Draft draft-ietf-lamps-pq-composite-sigs-02. Work in Progress. Internet Engineering Task Force, July 2024. 51 pp. url: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/02/.

[OGPK+24b] Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, and Scott Fluhrer. Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS. Internet-Draft draft-ietf-lamps-pq-composite-kem-04. Work in Progress. Internet Engineering Task Force, July 2024. 42 pp. url: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/04/.

[OPAB+19] David Ott, Christopher Peikert, Reza Azarderakhsh, Shannon Beck, Andy Bernat, Matt Campagna, Khari Douglas, Ann Drobnis, Roberta Faux, Shay Gueron, Shai Halevi, Peter Harsha, Mark Hill, Jeff Hoffstein, David Jao, Sandip Kundu, Hugo Krawczyk, Brian LaMacchia, Susan Landau, David McGrew, Ilya Mironov, Rafael Misoczki, Dustin Moody, Kenny Paterson, Radia Perlman, Tom Ristenpart, Vladimir Soukharev, Helen Wright, and Rebecca Wright. "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility". In CoRR abs/1909.07353 (2019).

[OpenSSL03] The OpenSSL Project. OpenSSL The Open Source toolkit for SSL/TLS. Apr. 2003. url: https://www.openssl.org/.

[OQS S/MIME24] OQS S/MIME. Open Quantum Safe CMS and S/MIME Fork. https://openquantumsafe.org/applications/smime.html. Oct. 2024.

[OQS23] Open Quantum Safe (OQS). OQS algorithm performance visualizations. https://openquantumsafe.org/benchmarking/. 2023.

[OQS24] Open Quantum Safe. liboqs v0.11.0. https://github.com/open-quantum-safe/liboqs. Sept. 2024.

[OQSprovider24] OQSProvider. Open Quantum Safe provider for OpenSSL - v0.7.0. https://github.com/open-quantum-safe/oqs-provider. Oct. 2024.

[OWA24] OWASP. OWASP CycloneDX Authoritative Guide to CBOM. Bezocht 2024-07-01. 2024. url: https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf.

[PCI22] PCI Security Standards Council. Payment Card Industry Data Security Standard (PCI DSS) Version 4.0. url: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf. Bezocht 2024-06-19. Mar. 2022.

[PQClean23] Matthias J. Kannwischer, Peter Schwabe, Douglas Stebila, and Thom Wiggers. PQClean. https://github.com/PQClean/PQClean. Apr. 2023.

[RCDB24] Prasanna Ravi, Anupam Chattopadhyay, Jan Pieter D'Anvers, and Anubhab Baksi. "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results". In: 23.2 (Mar. 2024). doi: 10.1145/3603170. url: https://doi.org/10.1145/3603170.

[Res18] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Aug. 2018. doi: 10.17487/RFC8446. url: https://www.rfc-editor.org/info/rfc8446.

[Res24] Santander Security Research. CryptoBOM Forge. Bezocht 2024-07-02. 2024. url: https://github.com/Santandersecurityresearch/cryptobom-forge.

[Rou24] Sebastien Rousseau. KyberLib. https://github.com/sebastienrousseau/kyberlib. v0.0.6. May 2024.

[Rust24] Joseph Birr-Pixton. RustTLS. https://github.com/rustls/rustls. v0.23.12. July 2024.

[SA15] Markku-Juhani O. Saarinen and Jean-Philippe Aumasson. The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). RFC 7693. Nov. 2015. doi: 10.17487/RFC7693. url: https://www.rfc-editor.org/info/rfc7693.

[Sho94] Peter W. Shor. "Algorithms for Quantum Computation Discrete Logaritmes and Factoring". In FOCS. IEEE Computer Society, 1994, pp. 124–134.

[Signal24a] Signal. Quantum Resistance and the Signal Protocol. Signal Blog. 2024. url: https://signal.org/blog/pqxdh/.

[Signal24b] Signal. The PQXDH Key Agreement Protocol. Jan. 2024. url: https://signal.org/docs/specifications/pqxdh/.

[SM16] Douglas Stebila and Michele Mosca. "Post-quantum key exchange for the internet and the open quantum safe project". In International Conference on Selected Areas in Cryptography. Springer. 2016, pp. 14–37.

[SRT19] Jim Schaad, Blake C. Ramsdell, and Sean Turner. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. RFC 8551. Apr. 2019. doi: 10.17487/RFC8551. url: https://www.rfc-editor.org/info/rfc8551.

[SSW20] Peter Schwabe, Douglas Stebila, and Thom Wiggers. "Post-Quantum TLS Without Handshake Signatures". In CCS '20 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM, 2020, pp. 1461–1480. doi: 10.1145/3372297.3423350. url: https://doi.org/10.1145/3372297.3423350.

[Ste] Marc Stevens. pqc benchmarking. Bezocht: 14 October 2024. url: https://github.com/cr-marcstevens/pqc_benchmarking.

[SvdBFG+12] Andrey Sidorenko, Joachim van den Berg, Remko Foekema, Michiel Grashuis, and Jaap de Vos. Bellcore attack in practice. Cryptology ePrint Archive, Paper 2012/553. 2012. url: https://eprint.iacr.org/2012/553.

[TC24] TNO and CWI. PQChoiceAssistant. https://tno.github.io/PQChoiceAssistant/. Bezocht 2024-07-18. 2024.

[TGFK+18] Alexander Truskovsky, Daniel Van Geest, Scott Fluhrer, Panos Kampanakis, Mike Ounsworth, and Serge Mister. Multiple Public-Key Algorithm X.509 Certificates. Internet-Draft draft-truskovsky-lamps-pq-hybrid-x509-01. Work in Progress. Internet Engineering Task Force, Aug. 2018. 24 pp. url: https://datatracker.ietf.org/doc/draft-truskovsky-lamps-pq-hybrid-x509/01/.

[Uni02] United States Congress. Federal Information Security Management Act of 2002 (FISMA). Public Law 107-347, 107th Congress. 2002. url: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma.

[US22] US White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. 2022. url: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[US24] Executive Office of the President of the United States. Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No 117-260. 2024. url: https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

[US96] United States Congress. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191, 104th Congress. 1996. url: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

[VK19] Luke Valenta and Kris Kwiatkowski. The TLS Post-Quantum Experiment. 2019. url: https://blog.cloudflare.com/the-tls-post-quantum-experiment.

[WBKG+24] Thom Wiggers, Kaveh Bashiri, Stefan Kölbl, Jim Goodman, and Stavros Kousidis. Hash-based Signatures State and Backup Management. Internet-Draft draftwiggers-hbs-state-00. Work in Progress. Internet Engineering Task Force, Feb. 2024. 20 pp. url: https://datatracker.ietf.org/doc/draft-wiggers-hbs-state/00/.

[Wei21] Adam Weinberg. Analysis of top 11 cyber attacks on critical infrastructure. https://www.first-point-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/. [Bezocht 05/04/2022]. 2021.

[Wes21] Bas Westerbaan. Sizing Up Post-Quantum Signatures. 2021. url: https://blog.cloudflare.com/sizing-up-post-quantum-signatures.

[Wet24] Dirk Wetter. testssl.sh. https://testssl.sh/. v3.0.9. June 2024.

[Wha16] WhatsApp. WhatsApp Encryption Overview. Technical Whitepaper. Apr. 2016. url: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

[Wir24] Wireshark Foundation. Wireshark Network Protocol Analyzer. 2024. url: https://www.wireshark.org/.

[Wol24a] WolfSSL. Embedded SSL/TLS Library. https://github.com/wolfSSL/wolfssl. v5.7.2. July 2024.

[Wol24b] Inc. WolfSSL. wolfCrypt Embedded Crypto Engine. 2024. url: https://www.wolfssl.com/wolfcrypt/.

Het PQC-migratie handboek

RICHTLIJNEN VOOR HET MIGREREREN NAAR POST-QUANTUMCRYPTOGRAFIE

Herziene en uitgebreide tweede editie

AIVD | CWI | TNO