TNO TOEGEPASTE CRYPTOGRAFIE EN QUANTUM-ALGORITMEN
CWI CRYPTOLOGIEGROEP
AIVD NATIONAAL BUREAU VOOR VERBINDINGSBEVEILIGING

Het PQC-migratie handboek

RICHTLIJNEN VOOR HET MIGREREN NAAR POST-QUANTUMCRYPTOGRAFIE

Maart 2023

TNO TOEGEPASTE CRYPTOGRAFIE EN QUANTUM-ALGORITMEN
CWI CRYPTOLOGIEGROEP
AIVD NATIONAAL BUREAU VOOR VERBINDINGSBEVEILIGING

Het PQC-migratie handboek

RICHTLIJNEN VOOR HET MIGREREN NAAR POST-QUANTUMCRYPTOGRAFIE

Maart 2023

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 migratie naar post-quantumcryptografie en het vergroten van de kennis van cryptografie als integraal onderdeel van informatiebeveiliging. 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 achterhaald blijken te zijn. AIVD, CWI en TNO zijn in géén geval aansprakelijk voor eventuele gevolgen van de in deze publicatie vermelde adviezen.

TNO innovation for life

CWI

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Auteurs Thomas Attema[1,2], João Diogo Duarte[1], Vincent Dunning[1], Matthieu Lequesne[2], Ward van der Schoot[1], Marc Stevens[2] en *AIVD-cryptologen en -adviseurs*[3]

Ontwerp Studio Oostrum in samenwerking met C10 Ontwerp

Contact thomas.attema@tno.nl

[1] TNO, Toegepaste cryptografie en quantumalgoritmen
[2] CWI, Cryptologiegroep
[3] AIVD, Nationaal Bureau voor Verbindingsbeveiliging

Samenvatting

Dit handboek ondersteunt organisaties met concrete stappen en advies om de dreiging van quantumcomputers voor cryptografie te beperken. Het moment waarop quantumcomputers een dreiging zullen vormen voor momenteel gebruikte cryptografie is onvoorspelbaar. Toch moeten bepaalde organisaties nu al aan oplossingen werken vanwege het risico dat quantumcomputers met zich meebrengen. Bijvoorbeeld organisaties die data verwerken die zelfs over 20 jaar nog vertrouwelijk moeten blijven of die systemen met een lange levensduur ontwikkelen. De meest veelbelovende oplossing is de zogenaamde *post-quantumcryptografie* (PQC). PQC kan draaien op nagenoeg dezelfde systemen die nu in gebruik zijn en is veilig tegen quantumcomputers. Migreren naar PQC kost echter bijzonder veel tijd en middelen. Afgaande op eerdere migraties kan dit ruim meer dan vijf jaar in beslag nemen.

Organisaties dienen daarom nu al te beginnen zich op de quantum-dreiging voor te bereiden. Als eerste *no-regret move* zou elke organisatie al een *PQC-diagnose* moeten uitvoeren. Deze eerste stap is bedoeld om te bepalen welke houding een organisatie moet aannemen op basis van het soort gegevens dat ze verwerkt en haar risico-oppervlak. Verder is het aan te raden een inventarisatie te maken van alle gebruikte cryptografische technieken, van de data die ze beschermen en van wie deze assets beheert. Alleen dan kan een organisatie de mate van urgentie correct inschatten. Deze inventarisatie verkleint later ook het risico op een overhaaste, foutgevoelige migratie die in de toekomst onnodige kosten en risico's met zich zou meebrengen. Het is voor elke organisatie nuttig om een dergelijke inventarisatie te maken en up-to-date te houden, aangezien elke organisatie vroeg of laat zal moeten migreren.

Na deze eerste stap richt het handboek zich tot de zogenaamde *urgente adopters*, organisaties die daadwerkelijk zo snel mogelijk met de migratie moeten starten omdat ze anders over twintig jaar onaanvaardbare risico's lopen. De volgende twee stappen van de migratie bestaan uit het *plannen* en het *uitvoeren* van de migratie. In de planningsfase is het belangrijk om een speciaal team te vormen om de migratie uit te voeren en ervoor te zorgen dat er bedrijfsprocessen actief zijn om de migratie soepel te laten verlopen. Vanuit technisch oogpunt kunnen organisaties PQC op verschillende manieren implementeren. Voor momenteel gebruikte systemen is mogelijk niet elke PQC-oplossing geschikt. Dit handboek geeft concrete handvatten voor het kiezen van een geschikte implementatiestrategie voor PQC, afhankelijk van de functionaliteiten die de organisatie levert of beheert. Dit kan betekenen dat een organisatie nieuwe hardware moet kopen of moet overstappen op nieuwe leveranciers die de juiste PQC-oplossingen ondersteunen.

Ten slotte moet de organisatie dit plan uitvoeren. Het is van groot belang daarbij voorzichtig te werk te gaan om geen nieuwe risico's te introduceren. Dit handboek bevat richtlijnen voor het migreren van verschillende soorten cryptografie op basis van de strategieën die in de planningsfase zijn gekozen. Bovendien is het niet onwaarschijnlijk dat er de komende jaren nieuwe kwetsbaarheden in de PQC-oplossingen worden ontdekt. Daarom is het belangrijk om *cryptographic agility* in gedachten te houden. Met cryptographic agility kan een organisatie gemakkelijk geïmplementeerde cryptografische primitieven aanpassen of vervangen zonder dat dit de processen van organisaties bovenmatig verstoort. Dit is vooral belangrijk wanneer wanneer er er nieuwe verbeteringen of kwetsbaarheden in protocollen worden ontdekt.

Dankbetuigingen

Wij danken Ronald Cramer (CWI en Universiteit Leiden) en Maran van Heesch (TNO) voor hun bijdragen aan de totstandkoming en afbakening van dit handboek. Daarnaast danken wij Itan Barmes (Deloitte), Shane Gibbons (CWI en Universiteit Leiden), Loulou Hanna (MinlenW), Erik Holkers (DICTU), Silke Knossen (KPN), Larissa Kalle (NCSC), Oscar Koeroo (MinVWS), Daan Planque, Eamonn Postlethwaite (CWI), Sterre Romkema (MinlenW), Robert Seepers (NCSC), Thijs Timmerman (KPMG), Daan van der Valk (Deloitte), Germain van der Velden (MinlenW), Anita Wehmann (MinBZK) en Daniël Worm (TNO) voor hun waardevolle opmerkingen en suggesties.

Dit handboek is ontwikkeld en gepubliceerd in het kader van de Nationale Cryptostrategie (NCS).

Inhoud

1 Inleiding

Dit handboek is bedoeld om organisaties te helpen bij het identificeren van de risico's van hun huidige cryptografische landschap met het oog op de komst van zogenoemde quantumcomputers. Er zijn al meerdere whitepapers en position papers gepubliceerd om organisaties voor deze risico's te waarschuwen en de urgentie van het plannen van deze onvermijdelijke migratie over te brengen. Dit handboek bouwt voort op deze adviezen en formuleert daarnaast concrete, uitvoerbare stappen om een migratiestrategie uit te werken. De belangrijkste doelgroep van de handleiding zijn organisaties die niet veel langer meer kunnen wachten, de zogenaamde *urgente adopters*. In dit verband dient te worden opgemerkt dat tegenwoordig bijna elke organisatie gebruik maakt van cryptografie en daardoor in zekere mate kwetsbaar is.
Cryptografie is uitermate belangrijk in de huidige digitale samenleving. Het vormt immers een essentieel onderdeel van de informatiebeveiliging van alle organisaties. Cryptografie is onontbeerlijk om diefstal van gevoelige data te voorkomen, te verifiëren of ontvangen data correct zijn en om ongeautoriseerde toegang tot systemen te voorkomen. Zwakke cryptografie kan enorme risico's met zich meebrengen zoals datalekken, ongeautoriseerde toegang, diefstal van bedrijfs- of staatsgeheimen en erger.
Een groot deel van de huidige cryptografie is echter verzwakt of zelfs volkomen onveilig door de opkomst van *quantumcomputers*. Hoewel op dit moment quantumcomputers nog niet krachtig genoeg zijn om cryptografische algoritmes te breken die momenteel in gebruik zijn, gaat de ontwikkeling van quantumcomputers almaar sneller. Vermoedelijk kunnen quantumcomputers over tien tot twintig jaar cryptografische standaarden breken. Met *klassieke cryptografie* bedoelen we cryptografische algoritmes die veilig zijn tegen klassieke computers, maar niet tegen quantumcomputers. Met *post-quantumcryptografie* (PQC) bedoelen we algoritmes die ook veilig zijn tegen quantum-aanvallers.
Er zijn al drie belangrijke redenen waarom organisaties nu al de migratie naar PQC moeten voorbereiden en aan de slag moeten:

1. Gevoelige informatie loopt het risico te worden onderschept en opgeslagen om in de toekomst te worden ontsleuteld met een quantumcomputer. Een dergelijke aanval noemen we ook wel een *store-now-decrypt-later* aanval. Er zijn ernstige vermoedens dat momenteel versleutelde data reeds worden verzameld. Zo lopen data die gedurende lange tijd beschermd moeten blijven nu al het risico om vóór het einde van deze vertrouwelijkheidsperiode te worden ontsleuteld.

2. Het is bijzonder moeilijk - zo niet onmogelijk - om systemen met een lange levensduur en kritieke infrastructuren die nu worden ontwikkeld en geïmplementeerd, later naar PQC te updaten. Zelfs als het mogelijk is om de software op deze systemen te upgraden, heeft PQC krachtige hardware nodig terwijl het mogelijk niet haalbaar is om de hardware van zulke geïmplementeerde systemen zomaar te vervangen.

3. Het updaten of vervangen van cryptografische infrastructuur door post-quantumalternatieven is een bijzonder omslachtige en tijdrovende taak. Afgaande op eerdere migraties verwachten we dat het updaten van legacy-systemen om heel wat planning en voorbereiding vraagt. Zo was er meer dan vijf jaar nodig voordat alle organisaties, leveranciers en andere partijen van SHA-1 naar SHA-256 waren gemigreerd, hoewel de specificaties en implementaties reeds beschikbaar waren.

PQC moet uitgroeien tot de nieuwe cryptografische standaard om de veiligheid van cryptografische algoritmes in de toekomst te waarborgen, ongeacht wanneer quantumcomputers voldoende krachtig zijn om de huidige cryptografie te breken. Daarom zullen alle organisaties uiteindelijk moeten migreren naar PQC. Het is nog niet precies bekend hoeveel de migratie naar PQC zal gaan kosten. Wel staat vast dat elke organisatie

voldoende middelen in de vorm van personeel, tijd en geld voor deze migratie zal moeten vrijmaken. Bovendien moeten apparaten mogelijk worden vervangen als ze PQC niet ondersteunen of als de leverancier niet van plan is om PQC te integreren. Ten slotte heeft PQC in vergelijking met traditionele algoritmen krachtigere hardware nodig om goed te functioneren, waardoor bepaalde hardware zal moeten worden vervangen.
Organisaties dienen hun cryptografische landschap in kaart te brengen om zo de urgentie van de migratie goed te kunnen beoordelen. Hoe eerder deze inventarisatie beschikbaar is, des te eerder een (eerste) migratieplan kan worden opgesteld. Met dit plan kunnen sommige assets al worden voorbereid op de migratie om het proces te vergemakkelijken en toekomstige kosten te beperken. Wanneer te lang wordt gewacht en onder druk een overhaaste migratie uitgevoerd moet worden, bestaat het risico dat fouten ontstaan die erg duur kunnen uitpakken. Het is mogelijk deze *agility* te vereisen voor systemen die momenteel door leveranciers worden beheerd of die nog moeten worden ingekocht.

1.1 Doel van deze handleiding

Dit document is bedoeld om beveiligingsarchitecten en het management binnen organisaties te helpen bij de migratie naar post-quantumcryptografie. Deze handleiding richt zich vooral tot organisaties die enige urgentie voelen (of zouden moeten voelen) om naar PQC te migreren. De migratie naar post-quantumcryptografie is urgent voor organisaties waarop de eerste twee hierboven benoemde redenen direct van toepassing zijn. Bovendien verkleint een vroege voorbereiding van de migratie de kans op tegenslagen en toekomstige risico's.
Dit document voorziet de betrokken doelgroep van informatie over de risico's, actiestappen, voor- en nadelen van migratie en praktische adviezen voor het opstellen van een migratieplan naar post-quantumcryptografie. Elke organisatie dient een plan op te stellen in overeenstemming met haar risicobereidheid. Voor CISO's en CIO's die een algemeen overzicht willen van de dreiging van quantumcomputers voor klassieke cryptografie, verwijzen we naar eerdere whitepapers van TNO [MvH20] en het NBV [NBV21]. Dit document biedt in aanvulling op bovengenoemde papers concrete stappen om te bepalen of quantumcomputing momenteel een bedreiging vormt voor een organisatie en welke stappen een organisatie moet ondernemen om deze risico's te beperken.
In Nederland bestaat een grote verscheidenheid aan organisaties, het is belangrijk op te merken dat elk van hen mogelijk een heel ander advies nodig heeft voor de migratie naar PQC. Daarom geven wij uiteenlopende adviezen voor verschillende organisatiegroepen, zodat deze zoveel mogelijk aansluiten. Het verdient opmerking dat zelfs binnen één organisatie verschillende afdelingen of teams een ander urgentieniveau kunnen hebben op basis van de data die ze verwerken of de systemen waarmee ze werken.

1.2 Bijbehorende risico's

Alle systemen die momenteel worden beschermd met behulp van klassieke cryptografie lopen het risico in zekere mate te worden aangevallen door quantumcomputers. Het is echter moeilijk dit risico te kwantificeren en nauwkeurige schattingen te maken. In deze paragraaf wordt dieper ingegaan op vier risico's die quantumcomputers met zich meebrengen.
Ten eerste is het onduidelijk of en wanneer quantumcomputers in staat zullen zijn cryptografie te breken. Volgens de huidige schattingen zal dit over 10 tot 20 jaar zijn, maar bij een onverwachte doorbraak kan dit veel sneller gaan. Over het algemeen is te stellen dat het risico toeneemt naarmate een organisatie de migratie langer uitstelt.
Ten tweede hangt het risico af van het soort systemen die beschermd moeten worden. Indien het een systeem of data betreft met een langere levensduur dan de komst van voldoende sterke quantumcomputers, is het risico nu al groot vanwege *store-now-decrypt-later* aanvallen en moet de migratie zo snel mogelijk

worden uitgevoerd. Indien het om andere functionaliteiten gaat, zoals authenticatie of systeembeschikbaarheid, is het risico iets lager. De systemen lopen dan immers alleen risico als een quantumcomputer ze *real-time* kan breken.
Ten derde worden de verschillende PQC-algoritmen tijdens het standaardisatieproces aan analyses en controles onderworpen, waardoor er regelmatig nieuwe kwetsbaarheden aan het licht komen. Daarom bestaat bij een te vroege migratie het risico dat een organisatie later opnieuw moet migreren als een nieuwe aanval wordt ontdekt. Aan de andere kant kan een te late migratie tot ernstige schade leiden, zoals gestolen informatie en reputatieschade als de systemen van een organisatie succesvol worden aangevallen. Een organisatie kan de migratie van een bepaald systeem uitstellen op basis van haar risicobereidheid. De kosten kunnen dus dalen of stijgen door te wachten. Daarom moeten organisaties een juiste balans zoeken tussen een vroege of late migratie van systemen.
Ten slotte is het niet bekend hoe lang het migratieproces van elk systeem precies in beslag neemt. Afgaande op eerdere (kleinere) migraties kan dit ruim 10 jaar duren. Daarom kunnen organisaties, afhankelijk van hun risicobereidheid, reeds deels met de voorbereiding van de migratie aan de slag. Organisaties kunnen de daadwerkelijke migratie nog even uitstellen, maar wel al kwetsbare systemen identificeren en prioriteren en een migratieplan opstellen. Zo beperken ze extra risico's door vertragingen en kosten door onverwachte tegenslagen tijdens de uiteindelijke migratie.

1.3 Documentstructuur en leeswijzer

Deze handleiding bestaat ruwweg uit een drieledige benadering, zoals ook beschreven in [ETS20]:

In Hoofdstuk 2 beschrijft de PQC-diagnose. Dit hoofdstuk is vooral interessant voor strategie- en beleidsmakers en moet mogelijk ook onder de aandacht worden gebracht van medewerkers met kennis van het type data/systemen dat in een organisatie aanwezig is. Eerst wordt de urgentie om te migreren voor een organisatie in kaart gebracht. Daartoe introduceert deze handleiding het concept van *PQC-persona's*. Deze persona's zijn bedoeld om organisaties te helpen bepalen welk standpunt ze ten opzichte van PQC-migratie moeten innemen. Met behulp van (visuele) beslisbomen en schema's kan een organisatie zich met één of meerdere persona's identificeren. Daarna dient de organisatie een inventarisatie te maken van alle cryptografische protocollen en van de systemen die deze protocollen gebruiken.

1

In Hoofdstuk 3 beschrijft de planning van het migratieproces op zowel technisch als organisatorisch vlak. Vooral urgente adopters dienen dit hoofdstuk goed te lezen, daarbij rekening houdend met de urgentie genoemd in het vorige hoofdstuk. Vervolgens wordt de urgentie vastgesteld en wordt bepaald welke systemen gemigreerd dienen te worden. Met behulp van deze kennis wordt in de volgende stap besloten welke mitigatiestrategieën voor de kwetsbare systemen geïmplementeerd worden. Bovendien wordt in deze stap de timing van het migratieproces voor de verschillende systemen bepaald. De doelgroep van dit hoofdstuk is wederom strategie- en beleidsmakers. Zij moeten het migratieproces plannen en prioriteren en het juiste team voor de migratie samenstellen. Verder is dit hoofdstuk interessant voor (beveiligings)architecten die het migratieproces vanuit technisch perspectief gaan leiden.

2

Hoofdstuk 4 is in de eerste plaats bedoeld voor een technisch publiek. Dit hoofdstuk beschrijft een aantal technische handvatten om te beslissen *hoe* de cryptografie moet worden gemigreerd. Eerst komen algemene strategieën en overwegingen voor het migreren van cryptografie aan bod. Daarna volgen strategieën voor specifieke cryptografische algoritmen en protocollen.

In Hoofdstuk 5 biedt tot slot diepgaande technische informatie voor verschillende populaire cryptografische constructies. Dit hoofdstuk dient vooral als naslagwerk om details op te zoeken van de cryptografie die door een organisatie wordt gebruikt. Het is niet nodig dit hoofdstuk in zijn geheel te lezen. De beoogde doelgroep van dit hoofdstuk zijn zowel technische leiders van het migratieproces als ontwikkelaars op het gebied van beveiliging en cryptografie die aan de migratie zullen werken.

1.4 Achtergrondinformatie over cryptografie

Deze paragraaf legt eerst enkele basisbeginselen van de cryptografie uit en gaat daarna in op de PQC-migratie zelf.

	Symmetrische sleutels	Asymmetrische sleutels
Versleuteling	Block Cipher / Stream Cipher	Public-key Encryption
Authenticatie	Message Authentication Code	Digital Signature
Sleutelgeneratie	Random Number Generator	Key Exchange

Tabel 1.1: Samenvatting van categorieën cryptografische primitieven.

Cryptografie is de studie van het waarborgen van veilige communicatie en opslag van data in aanwezigheid van vijandelijke actoren. Het doel van cryptografie is het beschermen van (een combinatie van) vier basisdoelen: vertrouwelijkheid, authenticiteit, integriteit en onweerlegbaarheid. *Vertrouwelijkheid* verwijst naar het beschermen van data zodat alleen de beoogde ontvanger de versleutelde data kan ontsleutelen. *Authenticiteit* betreft het kunnen verifiëren van de afzender van versleutelde data en/of het pad dat deze data hebben afgelegd. Het derde basisdoel is *integriteit*, teneinde een ontvanger in staat te stellen te verifiëren dat de data na het verzenden door niemand zijn gewijzigd. *Onweerlegbaarheid* betekent dat een partij die oorspronkelijk een bericht heeft verzonden later niet kan ontkennen dit bericht te hebben verzonden.
De bouwstenen van cryptografie worden cryptografische *primitieven* genoemd. Dit zijn low-level algoritmen waarmee gecompliceerde en ingewikkelde cryptografische *protocollen*, *algoritmen* 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.
Encryptie of *versleuteling* is veruit de bekendste cryptografische functionaliteit. Deze beschermt de vertrouwelijkheid van data en verhindert dat de data gelezen kan worden door onbevoegden. Hiertoe versleutelen encryptieprotocollen de data met een encryptiesleutel. Op die manier ontstaat een versleutelde cijfertekst die alleen kan worden ontsleuteld met de juiste decryptiesleutel.[1]

[1] Encryptieprotocollen kunnen ook bijdragen aan authenticiteit en onweerlegbaarheid, want in sommige gevallen kent alleen een bepaalde partij de encryptiesleutel en kan alleen die partij een geldige versleuteling uitvoeren.

Digitale handtekeningen vormen een andere veelgebruikte cryptografische functionaliteit. Deze 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 met behulp van een verificatiesleutel worden geverifieerd.
De derde toepassing die wordt besproken is *sleutelgeneratie*. Deze wordt gebruikt voor het genereren en afstemmen van sleutels die later kunnen worden gebruikt door andere cryptografische protocollen zodat alleen de bevoegde partijen toegang tot de sleutels hebben.
Voor al deze functionaliteiten kunnen de sleutels ofwel *symmetrisch* ofwel *asymmetrisch* zijn, hetgeen leidt tot symmetrische cryptografie of asymmetrische cryptografie. Bij symmetrische cryptografie zijn de encryptie- en decryptiesleutels identiek. Ze moeten vooraf door de betrokken partijen worden overeengekomen. AES is een voorbeeld van een encryptiemethode met symmetrische sleutels. Het behoort tot de algemene klasse van de blokvercijferingen. De zogenaamde hashfuncties vormen een speciale klasse van symmetrische cryptografie. Hashfuncties pseudonimiseren een bericht wat een op het oog random string van karakters is. Dit gebeurt zodanig dat het gemakkelijk is om te verifiëren of een bepaald pseudoniem overeenkomt met een bepaald bericht. Het is daarentegen moeilijk om het bericht op basis van alleen de pseudoniem te kunnen achterhalen. Message Authentication Codes (MAC's) ondersteunen de authenticiteit en integriteit door middel van symmetrische sleutels. Ze maken een *tag* van een bericht 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. Ten slotte kunnen symmetrische cryptografie en hashfuncties worden gebruikt bij het bouwen van (pseudo) Random Number Generators (RNG's) die willekeurige waarden genereren die als sleutels voor andere protocollen kunnen worden gebruikt.
Bij asymmetrische cryptografie zijn beide sleutels verschillend en worden ze vaak de *publieke* sleutel en de *geheime* sleutel genoemd. Eén partij kan daarbij een sleutelpaar genereren en de publieke sleutel publiekelijk bekendmaken, zodat iedereen berichten kan versleutelen. Alleen die ene partij kan het bericht ontsleutelen met zijn geheime sleutel. Symmetrische cryptografie is meestal sneller dan asymmetrische cryptografie, maar is moeilijker op te zetten omdat dezelfde geheime sleutel aan beide kanten bekend moet zijn. Daarom wordt asymmetrische cryptografie meestal gebruikt om een vertrouwelijke symmetrische sleutel te genereren om de rest van een gesprek te versleutelen, bijvoorbeeld met AES. Dit proces noemen we ook wel een sleuteluitwisselingsprotocol. Een voorbeeld hiervan is het Diffie-Hellman-sleuteluitwisselingsprotocol. Voor digitale-handtekeningschema's kan alleen de partij met de geheime sleutel de handtekeningen genereren, zodat er sprake is van authenticiteit en onweerlegbaarheid. De bijbehorende publieke sleutel kan dan weer worden gebruikt om de handtekening te verifiëren.

Dreiging van quantumcomputers

De mate waarin quantumcomputers een dreiging vormen voor bovenstaande protocollen en use cases verschilt. Aanvallen op symmetrische cryptografie worden kwadratisch sneller met het quantum-algoritme van Grover [Gro96]. Dit betekent dat het beveiligingsniveau dat wordt gegarandeerd door een bepaalde configuratie van een hash of door een symmetrisch encryptiesysteem afneemt. De algoritmen zelf kunnen echter nog steeds worden gebruikt indien de sleutel of de grootte van de output voldoende wordt opgeschaald. Voor hashfuncties betekent dit doorgaans dat de grootte van de output van de functie met een factor 3 wordt verhoogd om hetzelfde beveiligingsniveau te behouden. Bij versleuteling met symmetrische sleutels moeten de sleutelgroottes worden verdubbeld om hetzelfde beveiligingsniveau tegen quantumcomputers te behouden. Al met al is het relatief eenvoudig om het risico van quantumcomputers bij symmetrische cryptografie te verkleinen.
Aan de andere kant wordt veel van de momenteel gestandaardiseerde asymmetrische cryptografie volledig gebroken door het algoritme van Shor [Sho94]. Dit betekent dat momenteel gebruikte algoritmen niet meer veilig zijn als er voldoende krachtige quantumcomputers beschikbaar komen en deze dus door geschikte alternatieven moeten worden vervangen. Daarom is het beperken van quantum-risico's voor asymmetrische cryptografie veel omslachtiger.

Over Quantum key-distributie

In de praktijk wordt asymmetrische cryptografie meestal gebruikt voor het veilig genereren van een sleutel voor een symmetrisch schema voor elke nieuwe communicatieverbinding. Dit proces staat bekend als *key distributie*. Op internet moeten bijvoorbeeld veel verbindingen worden opgezet met onbekende systemen en voor elke verbinding is een nieuwe sleutel nodig.
Quantum key distributie (QKD) is onderzocht en uitgeroepen tot een quantum-veilige oplossing voor sleutelgeneratie. QKD verwijst naar een manier om sleutelovereenstemming te bereiken met behulp van quantum-communicatie tussen twee partijen. Dit mechanisme wordt aanbevolen omdat het resistent is tegen zowel klassieke als quantum-aanvallen. Hoewel dit een veelbelovend alternatief lijkt, is het om verschillende redenen geen praktisch alternatief voor klassieke cryptografie.
Ten eerste vormt het alleen een alternatief voor sleutelgeneratie, en de verbinding heeft zelf cryptografische authenticatie nodig. Bovendien moeten twee partijen worden verbonden door een quantum-communicatiekanaal om veilig te communiceren met behulp van QKD. Dit betekent concreet dat ze rechtstreeks verbonden moeten zijn via een glasvezel of een optisch (*free-space*) communicatiekanaal. Verder moet het quantum-communicatiekanaal een laag ruisniveau hebben. Dit beperkt de afstand waarover (quantum-)informatie kan worden overgedragen. Met versterkers kan deze afstandsbeperking worden ondervangen. Dit betekent echter dat een derde partij vertrouwd moet worden met de niet-versleutelde gevoelige informatie, hetgeen niet realistisch is als het gaat om beveiliging. Voor het gebruik van QKD zijn dus grote infrastructuurinvesteringen nodig terwijl het protocol slechts in bepaalde gevallen kan worden gebruikt. QKD kan geen beveiliging bieden tussen gevirtualiseerde omgevingen omdat het per definitie afhankelijk is van deze hardware-infrastructuur. Daarom is het niet geschikt als alternatief voor klassieke cryptografische algoritmen. Ten slotte biedt de specifieke voor QKD benodigde apparatuur nieuwe aanvalsvectoren. Er is een lange geschiedenis van voorbeelden die aantonen dat commerciële QKD-apparaten kwetsbaar zijn voor '*side-channel*'- of '*Denial-of-Service*'-aanvallen.
Al met al is post-quantumcryptografie goedkoper, flexibeler en beter ingeburgerd dan QKD. PQC kan klassieke cryptografie in alle contexten vervangen, aangezien het kan draaien op nagenoeg dezelfde systemen die nu in gebruik zijn.
Daarom raden belangrijke veiligheidsdiensten het gebruik van QKD af voor het beveiligen van communicatie. Ze zijn het erover eens dat post-quantumcryptografie de beste manier is om de quantum-dreiging te verminderen. Zie voor meer informatie over dit onderwerp de whitepaper van het NBV [NBV21] en de position papers van ANSSI (Frankrijk) [ANS20b], het NCSC (VK) [NCS20b] of de NSA (VS) [NSA21].

1.5) Bijbehorende werkzaamheden op het vlak van PQC-migratie

Nederlandse organisaties

In respectievelijk 2020 en 2021 waarschuwden de Nederlandse onderzoeksorganisatie TNO [MvH20] en het Nationaal Bureau voor Verbindingsbeveiliging (NBV) [NBV21] voor de risico's van quantumcomputers. Daarnaast presenteerden ze enkele overwegingen voor gevallen waarin de migratie onmiddellijk moet plaatsvinden. Beide publicaties adviseren het gebruik van symmetrische cryptografie met een voldoende grote sleutel en het gebruik van hybride oplossingen voor asymmetrische cryptografie. Deze handleiding houdt vast aan die adviezen en presenteert we daarnaast concrete actiestappen voor het implementeren van deze oplossingen, ook voor andere (minder urgente) gevallen.
In 2022 heeft het Nationaal Cyber Security Centrum (NCSC) richtlijnen voor quantumveilige transportlaagversleuteling gepubliceerd [NCS22]. Deze publicatie is specifiek gericht op urgente adopters die nu al een post-quantumalternatief moeten kiezen. De aanbevelingen in deze handleiding zijn afgestemd op de NCSC-richtlijnen.

Standaardisatieorganisaties

Van oudsher worden de standaardisatie en aanpassing van nieuwe cryptografische protocollen geïnitieerd en geleid door het National Institute of Technology and Standards (NIST, VS) en het European Telecommunications and Standardization Institute (ETSI). NIST is in 2016 begonnen met het aanvragen, evalueren en standaardiseren van tegen quantumcomputers beveiligde cryptografische protocollen. In juli 2022 werd de selectie van PQC voor standaardisatie aangekondigd [NIS22]. De daadwerkelijke standaarden worden in 2024 verwacht. De aanbevelingen voor post-quantumalgoritmen in dit document zijn afgestemd op deze geselecteerde kandidaatstandaarden.
Verder geven zowel NIST als ETSI advies over de daadwerkelijke migratie. In 2020 bracht ETSI 'Migration Strategies and Recommendations for Quantum-safe Schemes' uit [ETS20] waarin drie belangrijke stappen worden gedefinieerd die organisaties ten behoeve van de migratie moeten zetten:

1. het maken van een inventaris van systemen;
2. het opstellen van een migratieplan;
3. het uitvoeren van de migratie.

Dit document is goedgekeurd door de technische commissie voor informatiebeveiliging van ETSI, waarin experts uit het bedrijfsleven en overheidsorganisaties zijn samengebracht. Deze handleiding volgt dezelfde drieledige benadering. NIST is momenteel bezig met het opzetten van een projectconsortium [NN21] om onderzoek te doen naar deze benadering, waarbij het in eerste instantie de bedoeling is om ondersteunende tools voor de eerste stap te ontwikkelen. Het is op dit moment nog niet bekend wanneer dit project van start gaat en of de ontwikkelde tools en kennis beschikbaar worden voor het grote publiek.

Andere organisaties

In 2021 publiceerde het Europees Agentschap voor Cyber Security (ENISA) een technisch overzicht van de (algemene) wiskundige eigenschappen van de verschillende post-quantumalgoritmen, hun specifieke kenmerken en beschikbare implementaties [BDH+21]. Dit document bevat een overzicht van de stand van zaken wat betreft beschikbare algoritmen en hybride oplossingen, maar mist een opsomming van de concrete actiestappen.
Het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI) heeft ook een gids gepubliceerd waarin de interne werking van de algoritmen wordt uitgelegd, en waarin recente ontwikkelingen van PQC in de politiek, onderzoek en industrie worden beschreven [BSI22]. Ten slotte geven ze enkele basisaanbevelingen voor de te nemen stappen. De adviezen en stappen in deze handleiding komen grotendeels overeen met hun aanbevelingen, maar zijn minder gericht op de details van de algoritmen en meer op de strategie om naar deze algoritmen te migreren.
Het Britse National Cyber Security Centre (NCSC) heeft tot slot ook een whitepaper gepubliceerd over de noodzaak voor organisaties om zich voor te bereiden op post-quantumcryptografie in 2020 [NCS20a].

2 Diagnose

Overzicht

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 (sub)organisatie zich met ten minste één van deze persona's kan identificeren. Het tweede deel bevat concrete adviezen over het doen van een PQC-diagnose, een eerste stap die elke organisatie moet nemen in de PQC-migratie.

De 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 een meer reactieve houding ten aanzien van 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 beveiligingsarchitectuur 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 wachten met het uitvoeren van deze PQC-diagnose, hoewel het in sommige gevallen nuttig kan zijn om nu al met deze diagnose te beginnen.

In de latere hoofdstukken volgen adviezen in de vorm van concrete actiestappen voor urgente adopters. Daarom is het essentieel om de PQC-persona's nauwkeurig te bepalen, zodat alle organisaties die nu al stappen moeten zetten in de PQC-migratie dit ook daadwerkelijk doen.

2.1 PQC-persona's

Voordat organisaties zich in het avontuur van de PQC-migratie storten, moeten ze uitzoeken of ze nu al aan dit avontuur moeten beginnen, en zo niet nu, wanneer dan wel. Het landschap van organisaties is opgedeeld in een klein aantal categorieën, de zogenaamde PQC-persona's. Op die manier worden organisaties ondersteund bij hun beslissingen en wordt zo goed mogelijk tegemoetgekomen aan de verschillende behoeften

van organisaties bij de migratie naar PQC. Ten eerste is het op deze manier mogelijk in kaart te brengen welke organisaties zo snel mogelijk stappen in de migratie moeten zetten en welke organisaties nog even kunnen wachten. Ten tweede maakt dit het mogelijk om advies op maat te verstrekken aan verschillende organisaties met een vergelijkbare structuur.
Voor elk van de persona's zijn verschillende concrete actiestappen opgesteld, die onder andere variëren wat betreft urgentie, tijdlijn, risicoanalyse en aandachtspunten. Deze indeling is gebaseerd op de volgende kenmerken:

- **Aanvalsoppervlak:** welke infrastructuur biedt/heeft de organisatie die vatbaar is voor aanvallen met behulp van een quantumcomputer?
- **Soorten systemen:** welke soorten systemen worden gebruikt en wat is de impact van een gebrekkige werking van deze systemen?
- **Soorten data:** welke soort data en informatie wordt verwerkt in termen van gevoeligheid voor openbaarmaking en gevolgen van ongeoorloofde en onopgemerkte wijziging?
- **Tijdsdruk:** hoe snel moet de PQC-migratie plaatsvinden om de veiligheid van data en systemen te waarborgen, rekening houdend met store-now-decrypt-later-aanvallen?
- **Afhankelijkheid van andere organisaties:** in welke mate zijn verschillende organisaties van elkaar afhankelijk?
- **Dreigingsniveau:** hoe realistisch is het dat een kwaadwillende actor met een quantumcomputer ervoor kiest om deze organisatie aan te vallen?

De PQC-persona's zijn onder te verdelen in drie hoofdcategorieën:

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 geen gevoelige data verwerken en niet beschikken over kritieke of langlevende infrastructuren met een hoog risico om te worden aangevallen. Deze organisaties verwerken bijvoorbeeld wel gevoelige data, maar het is onwaarschijnlijk dat 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 cryptografie-kennis voor PQC-migratie al in huis. Daarnaast zijn ze ook verantwoordelijk voor cryptografische systemen van andere organisaties.

Deze handleiding is vooral gericht op advies en concrete stappen voor urgente adopters. Daarom is het belangrijkste doel van dit hoofdstuk om organisaties te helpen bepalen of ze een urgente of reguliere adopter zijn. In de latere hoofdstukken is een uitgebreid advies voor urgente adopters en voor de andere twee categorieën opgenomen.

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

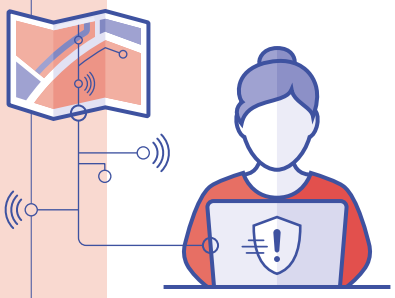
Organisaties die **persoonlijke informatie met een lange vertrouwelijkheidstermijn verwerken**. Deze organisaties zijn wettelijk verplicht om dergelijke persoonlijke informatie te beschermen. Store-now-decrypt-later-aanvallen vormen het belangrijkste risico waarmee deze organisaties worden geconfronteerd. 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. 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 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 kritieke infrastructuur

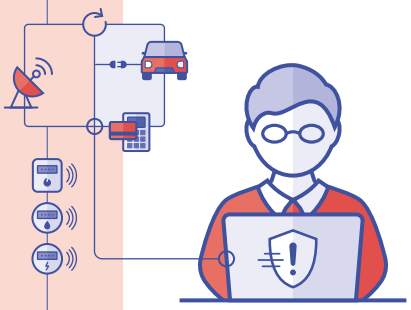


Organisaties die **systemen aanbieden die cruciaal zijn voor het functioneren van grote groepen mensen**, zoals dorpen, steden, provincies of zelfs landen. Er bestaan tal van dergelijke systemen; de meeste voorzien in basisbehoeften van grote groepen mensen, zoals water, elektriciteit, transport, communicatie 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].

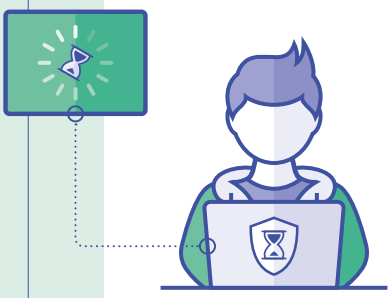
Het verschil met de eerste twee persona's is tweeledig. Enerzijds is beschikbaarheid bij deze organisaties van groter belang dan integriteit en betrouwbaarheid. Anderzijds is de risicobereidheid bij deze organisaties veel lager, aangezien defecten een veel grotere impact hebben. Om deze twee redenen 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.

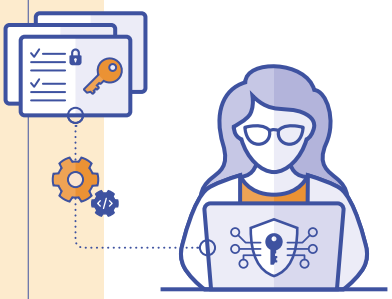
2.1.2 Reguliere adopters



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 vatbaar kunnen zijn voor aanvallen met behulp van een quantumcomputer, maar het voor deze organisaties vooralsnog gunstiger is om verdere standaardisatie van PQC af te wachten. 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.

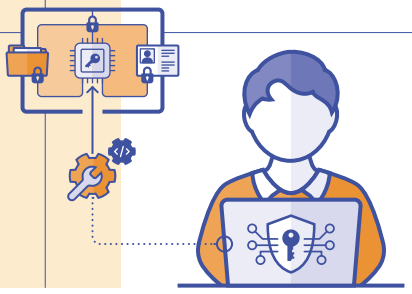
2.1.3 Cryptografie-experts

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.
Allereerst moet de belangrijkste groep van urgente adopters weten dat deze groep bestaat en wat ze van deze experts kunnen verwachten. De meeste urgente adopters nemen hun cryptografische systemen bij cryptografie-experts af. Urgente adopters die naar PQC willen migreren, moeten deze leveranciers vragen of hun producten quantumveilig zijn en, zo niet, wanneer hun producten naar verwachting wél quantumveilig zullen zijn. In sommige gevallen zullen deze urgente adopters moeten overstappen op een andere leverancier voor hun cryptografische systemen.
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 algoritmen ze van plan zijn te implementeren. Daarom moeten ze ook zo snel mogelijk beginnen met het migreren van hun producten naar PQC-standaarden.



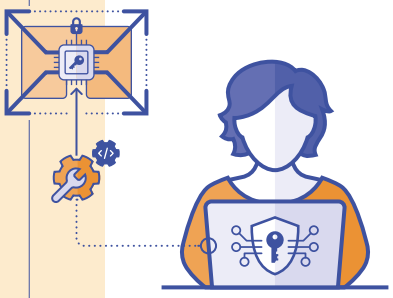
Standaardisatieorganisaties

Dit zijn organisaties die **cryptografische standaarden en/of protocollen** definieren. 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

Dit zijn 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 Fox Crypto, Logius, Compumatica, NXP, Brightsight, Technolution, Apache en MSSP's (Managed Security Service Providers) zoals Cipher en SecurityHQ.



Aanbieders van cryptografie die verder gaat dan veilige communicatie

Dit zijn organisaties die **infrastructuur ontwikkelen, implementeren of onderhouden op basis van cryptografische protocollen die worden gebruikt voor doeleinden die verder gaan dan veilige communicatie**. Van belang is dat dit soort cryptografie niet noodzakelijkerwijs hogere veiligheidsgaranties oplevert. De door deze organisaties ontwikkelde cryptografische protocollen worden voor verschillende doeleinden gebruikt en kunnen op verschillende principes zijn gebaseerd. Voorbeelden van dergelijke protocollen zijn blockchain, ZKP, MPC en Idemix. Deze persona wordt apart vermeld omdat de ontwikkelde cryptografie dermate kan verschillen dat deze organisaties andere maatregelen moeten nemen dan organisaties die meer standaard cryptografische functionaliteiten ontwikkelen. Het gaat bij deze organisaties veelal om start-ups die één van de genoemde technieken inzetten voor specifieke doeleinden, aangezien deze vormen van cryptografie in de praktijk relatief jong zijn. Voorbeelden zijn Roseman Labs, Linksight, Cosmian (allen MPC) en IRMA.

2.1.4 Uw persona bepalen

Niveaus van cryptografie

Over het algemeen zijn er drie niveaus van cryptografie waarvoor een organisatie verantwoordelijk is, namelijk:

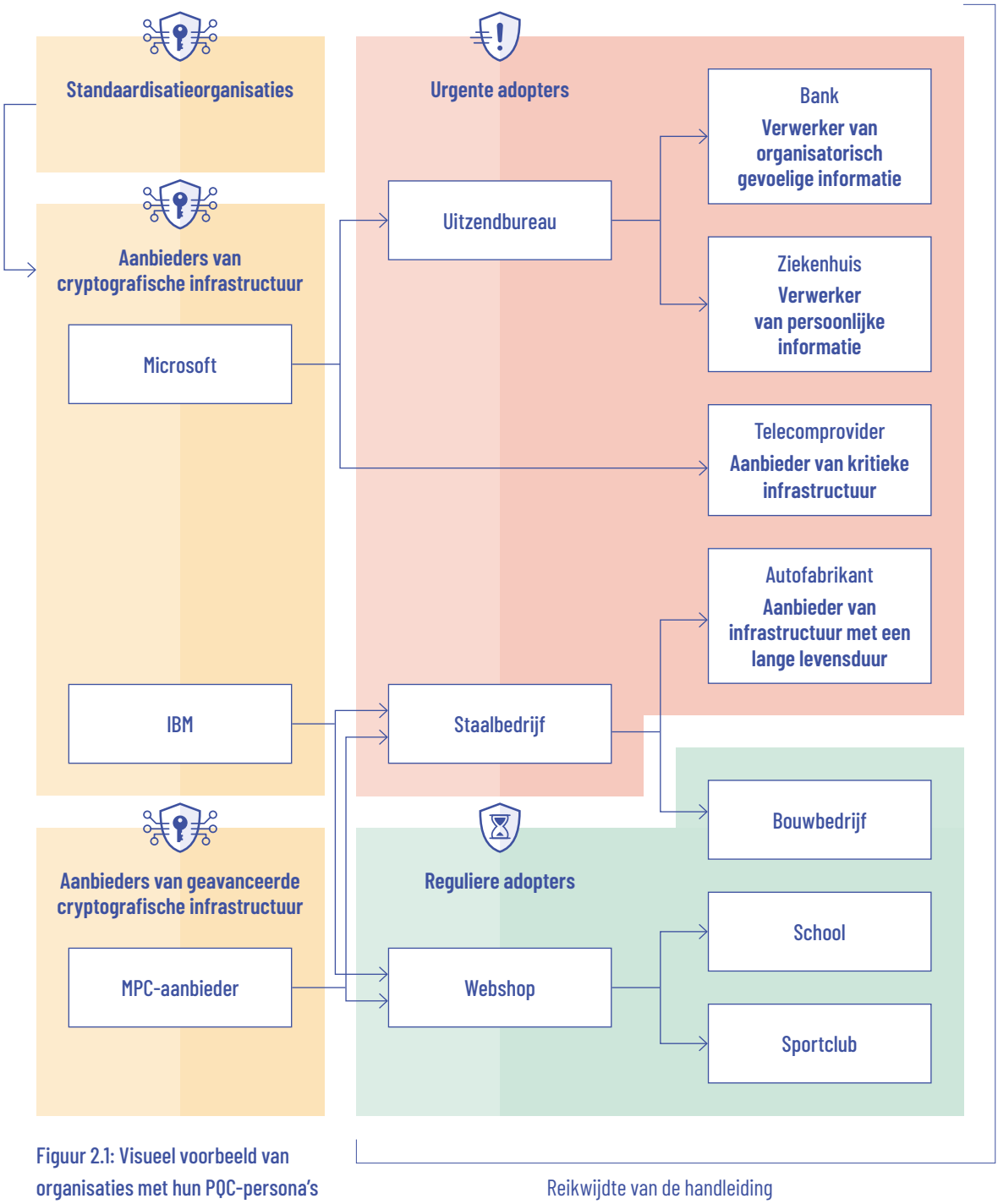
1. haar eigen cryptografische infrastructuur;
2. haar cryptografische kennis;
3. cryptografische infrastructuur voor het leveren van diensten of producten aan andere organisaties.

Er dient rekening te worden gehouden met elk van deze drie niveaus bij het migreren naar PQC en dus bij het bepalen van uw persona. Niveau 3 wordt apart vermeld a, want als een organisatie die levert aan andere organisaties wordt aangevallen, dan kunnen die andere organisaties aan zogenaamde supply-chain aanvallen worden blootgesteld. Een supply chain is een keten van organisaties waarbij elke organisatie aan de volgende organisatie in de keten levert. Een voorbeeld van een supply chain met verschillende organisaties vindt u in Figuur 2.1. In dit diagram geven de pijlen aan dat organisaties aan elkaar leveren (bijvoorbeeld Microsoft levert aan het uitzendbureau en de telecomaanbieder). Aanvallen op organisaties hoger in de supply chain kunnen ook een risico vormen voor organisaties lager in de supply chain.
Een voorbeeld van een supply chain-aanval is de SolarWinds-hack in 2020. Bij deze aanval plaatsten hackers een kwaadaardig stukje code in één van de producten van softwarebedrijf SolarWinds. Hierna verzond SolarWinds deze aanpassing (zonder het te weten) als update naar duizenden organisaties, waaronder grote multinationals en de Amerikaanse overheid, zodat de hackers vervolgens toegang kregen tot data, netwerken en systemen.
Voorbeelden van persona's die (cryptografische) systemen aan andere partijen leveren, 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 bovengenoemde niveaus. Ten eerste moet de organisatie haar eigen infrastructuur bekijken om één (of meer) geschikte persona('s) te bepalen. Ten tweede kan een organisatie tot bepaalde persona's behoren vanwege de cryptografische kennis die zij bezit. Ze behoort dan tot de persona 'cryptografie-expert'. Ten slotte erft een organisatie dezelfde persona als alle organisaties aan wie ze levert, omdat ze hetzelfde advies moet volgen als de organisaties aan wie ze levert. Anders vormt ze een te groot risico voor de andere organisaties in de supply chain.

Dit overnemen van persona's werkt zelfs nog verder door in de supply chain. Dat betekent dat een organisatie alle persona's erft van organisaties die zich op een lager niveau in de supply chain bevinden. Dit betekent bijvoorbeeld dat in Figuur 2.1 het uitzendbureau een verwerker van zowel organisatorisch gevoelige informatie als persoonlijke informatie is, het staalbedrijf ook een aanbieder van infrastructuur met een lange levensduur is, en Microsoft een verwerker van zowel organisatorisch gevoelige als persoonlijke informatie én een aanbieder van kritieke infrastructuur is.
Als we al deze persona's samenvoegen, zou elke organisatie kunnen behoren tot de urgente of reguliere adopters, en mogelijk zelfs tot de cryptografie-experts. Een organisatie die een urgente adopter is, kan behoren tot meer dan één van de subpersona's.



Figuur 2.1: Visueel voorbeeld van organisaties met hun PQC-persona's

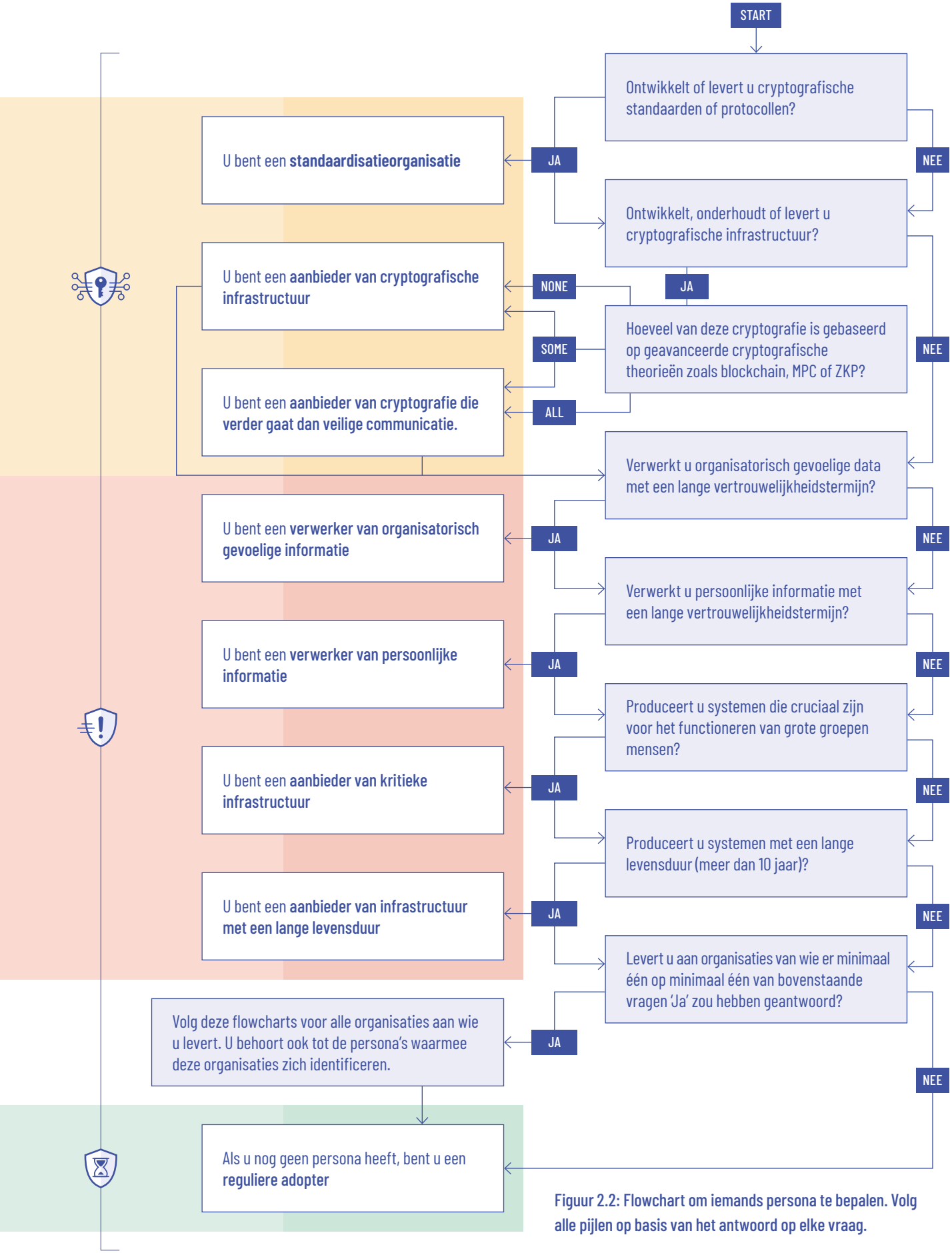
Bovendien is van belang dat de persona('s) van een organisatie in de loop van de tijd kunnen veranderen, omdat ook de risico's waaraan zij worden blootgesteld in de loop van de tijd kunnen veranderen. Het advies is om zorgvuldig te beoordelen tot welke persona een organisatie behoort telkens wanneer deze organisatie nieuwe stappen in PQC-migratie zet. In dit verband wordt benadrukt dat sommige organisaties mogelijk denken dat ze reguliere adopters zijn, terwijl ze in de praktijk een urgente adopter zijn vanwege hun eigen cryptografische infrastructuur of de infrastructuur van één van de organisaties aan wie ze leveren. Daarom luidt het advies aan deze organisaties om conservatief te zijn bij het bepalen van hun PQC-persona. Op het grensvlak tussen een urgente en reguliere adopter is het raadzaam om het advies in Hoofdstuk 3.2 te volgen. Daar staan verdere richtlijnen over het tijdstip waarop een organisatie moet beginnen met het migreren van bepaalde systemen.
Het is het eenvoudigst de persona('s) van een organisatie vast te stellen door de beschrijvingen van alle bovenstaande persona's te lezen en te kijken welke beschrijving(en) van toepassing zijn op de desbetreffende organisaties. Daarnaast vormt de flowchart in Figuur 2.2 een visueel hulpmiddel om de PQC-persona('s) van een organisatie te bepalen.

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 PQC-diagnose 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 PQC-migratie

PQC-migratie is vaak niet een proces dat door organisaties individueel kan worden uitgevoerd vanwege afhankelijkheden tussen verschillende organisaties. Deze afhankelijkheid kan zowel op organisatorisch als op technisch niveau voorkomen. Coördinatie tussen deze organisaties tijdens PQC-migratie is vereist om interoperabiliteit tussen verschillende organisaties te behouden.
Dit kan op verschillende manieren gebeuren. Als een organisatie A lineair afhankelijk is van een organisatie B, moet organisatie B migreren naar PQC-standaarden vóórdat organisatie A dit kan doen. Vaak zijn dergelijke 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.



Figuur 2.2: Flowchart om iemands persona te bepalen. Volg alle pijlen op basis van het antwoord op elke vraag.

2.2 PQC-diagnose

Nu een organisatie haar persona heeft vastgesteld, kan zij vaststellen of zij moet doorgaan met de migratie, met als eerste stap de PQC-diagnose.

Urgente adopters

Tot urgente adopters behorende organisaties 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 op de quantum-dreiging te reageren. 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, bijvoorbeeld via (toekomstige) aanbestedingen. Voor meer informatie over crypto-agility, zie 'Cryptographic Agility' in Hoofdstuk 4.1. Ze moeten er daarnaast rekening mee houden dat toekomstige updates een impact zullen hebben op de prestaties van cryptografische algoritmen. Deze organisaties kunnen al beginnen een risicobeoordeling te maken en de diagnosestappen uit te voeren van het in Hoofdstuk 2.2.1 beschreven migratieplan.

Daarnaast moeten deze organisaties goed geïnformeerd blijven en standaardisatieontwikkelingen in de gaten blijven houden. Binnen vijf tot tien jaar, ná de publicatie van de post-quantum standaarden, zullen nieuwe aanbevelingen specifiek voor deze organisaties worden aangekondigd, rekening houdend met de ontwikkelingen en de lessen van urgente adopters.

Ten slotte willen sommige tot de reguliere adopters behorende organisaties wellicht proactief handelen en het in deze handleiding beschreven migratieplan uitvoeren, met als eerste stap de PQC-diagnose. Er zijn verschillende redenen om dit te doen, zoals: een organisatie staat op het punt grote infrastructuurinvesteringen te doen; een organisatie verandert van activiteit of een organisatie heeft nieuwe klanten waardoor de risicobeoordeling verandert. Hoe dan ook zullen deze stappen op een gegeven moment noodzakelijk zijn, dus het is nooit verspilde moeite om nu de eerste migratiestappen te zetten.

Cryptografie-experts

De tot de cryptografie-experts behorende organisaties dienen ook te beginnen de migratieaanbevelingen op hun eigen infrastructuur toe te passen. Bovendien vertrouwen alle andere actoren in de supply chain op deze organisaties, de leveranciers van cryptografische systemen. Daarom moeten ze gereed zijn voor het implementeren van quantumveilige algoritmen zodra de standaarden beschikbaar zijn.

Cryptografie-experts dienen duidelijk met hun klanten te communiceren om de migratieplanning te vergemakkelijken voor organisaties aan wie 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. Voor aanbieders van cryptografie die verder gaan dan alleen veilige communicatie wordt benadrukt dat sommige veelgebruikte geavanceerde cryptografische protocollen niet quantumveilig zijn.

2.2.1 De PQC-diagnose uitvoeren

Nadat een organisatie heeft besloten om met de PQC-migratie aan de slag te gaan, moet allereerst een diagnose worden uitgevoerd om de huidige situatie met betrekking tot de informatiebeveiliging 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. Over het algemeen dient een organisatie te beschikken over de volgende informatie voor het opstellen van een geschikt migratieplan:

- risicobeoordeling;
- inventaris van alle cryptografische systemen die in de organisatie worden gebruikt;
- inventaris van alle data waarover de organisatie beschikt;
- inventaris van de leveranciers van cryptografische systemen.

Risicobeoordeling

Elke organisatie beoordeelt regelmatig het risico van aanvallen op haar IT-infrastructuur en de mogelijke gevolgen (financieel, reputatiegebonden, juridisch, enz.). Het risico wordt beoordeeld aan de hand van verschillende parameters: de waarde van de informatie, de kwetsbaarheid en de dreiging.
De eerste fase van de risicobeoordeling bestaat uit het beoordelen van het risico van de huidige IT-infrastructuur in een nieuw scenario waarin de aanvaller toegang heeft tot een grootschalige quantumcomputer. De quantumdreiging heeft geen invloed op de waarde van de informatie: de waardevolle systemen blijven identiek. Maar er ontstaan nieuwe kwetsbaarheden: bepaalde informatie die werd beschermd door cryptografische algoritmen die volgens een klassiek model veilig zijn, wordt nu niet meer beschermd. Bovendien moet de organisatie anticiperen op nieuwe dreigingen: aanvallers die zich richten op de nieuwe kwetsbaarheden die door deze situatie ontstaan. Daarom moet de organisatie het risico opnieuw beoordelen. Een goede risicobeoordeling is essentieel om te beslissen welke systemen als eerste moeten worden gemigreerd.

Inventaris van cryptografische systemen

Voor het uitvoeren van de migratie dient een organisatie alle cryptografische systemen te identificeren, waaronder systemen die binnenkort in de organisatie zullen worden geïntroduceerd. Dit is een belangrijke stap om ervoor te zorgen dat alle systemen correct worden gemigreerd. Als er één algoritme overblijft dat kwetsbaar is voor een quantumaanval, kan dit leiden tot een grotere aanval op het volledige systeem.
Daarom dient men te streven naar een volledige lijst van alle toepassingen van cryptografie binnen een organisatie, zowel software- als hardwarematig. De verzamelde informatie moet zo gedetailleerd mogelijk zijn, waaronder de aard van het algoritme, de grootte van de sleutel, de toepassing, enz. Deze informatie zal worden gebruikt om te bepalen of een cryptografisch systeem kwetsbaar is voor quantumaanvallen en welke quantumveilige oplossing in plaats daarvan kan worden gebruikt. Organisaties dienen de leverancier te informeren over systemen waarover zijzelf geen controle hebben. De inventaris kan de vorm aannemen van een Configuration Management Database (CMDB). Eerdere cryptografische migraties hebben aangetoond dat het inventariseren van cryptografische systemen het belangrijkste en moeilijkste onderdeel van de diagnose is. Organisaties dienen er dan ook rekening mee te houden dat deze stap veel tijd in beslag zal nemen.
Er bestaan geautomatiseerde tools die helpen identificeren waar en hoe cryptografische algoritmen binnen een infrastructuur worden gebruikt. NIST werkt momenteel aan de ontwikkeling van een dergelijke tool [NN21]. Er kunnen ook andere tools worden gebruikt voor het identificeren van cryptografische systemen, zoals *testssl.sh* [Wet].
Bovendien moet de organisatie er rekening mee houden dat een dergelijke inventaris ook nuttig is buiten de scope van dit migratieproject. Een volledig beeld van de gebruikte cryptografische algoritmen kan immers helpen bij het identificeren van kwetsbaarheden in het huidige systeem. Dergelijke kwetsbaarheden zijn

verre van ongewoon en moeten worden verholpen. Een goede inventaris van alle gebruikte cryptografische systemen kan daarom organisatie helpen bij het beperken van dreigingen, waaronder de dreiging die uitgaat van quantumcomputers. Deze inventaris kan ook worden gebruikt om compliancevraagstukken te vereenvoudigen. Verder moet de inventaris voortdurend worden bijgewerkt vanwege de continue ontwikkelingen in de cryptografie.
Daarbij dient opgemerkt te worden dat een dergelijk overzicht bijzonder gevoelig van aard is omdat het alle kwetsbaarheden van een organisatie bevat. Daarom is het van het allergrootste belang om deze inventaris goed te beveiligen en af te schermen.

Inventaris van data

Een lijst van de door uw organisatie gebruikte data is een goed hulpmiddel om de juiste beslissingen te nemen bij het plannen van uw migratie. U heeft daarbij in principe geen volledige lijst van alle data nodig, maar een lijst met alle soorten data gebaseerd op verschillende factoren zoals:

- type data (data in rust, data in transit of data in gebruik);
- locatie van de data;
- waarde van de data (vertrouwelijkheid, beschikbaarheid);
- classificatie van de data;
- risicobeoordeling voor elke dataverzameling.

Inventaris van cryptografische afhankelijkheden

Bij de meeste organisaties wordt een aanzienlijk deel van de cryptografische systemen (hardware en software) door externe leveranciers geleverd. Een groot deel van de migratie bestaat er dan ook uit om ervoor te zorgen dat leveranciers migreren en nieuwe quantumveilige oplossingen aanbieden, of anders om nieuwe leveranciers te vinden. Het doel van deze inventaris is om de cryptografische supply chain in kaart te brengen. Het is raadzaam voor elke leverancier alle gebruikte producten in kaart te brengen, vast te stellen of er sprake is van een doorlopend contract en de wijze van het opnemen van contact vast te leggen. Deze lijst moet ook certificeringsinstanties bevatten. Naast de officiële leveranciers van cryptografische systemen, moet een organisatie ook rekening houden met interne communicatiemiddelen (instant messaging, samenwerkingsplatforms) en schaduw-IT.
Dit geldt ook andersom, als een organisatie oplossingen met behulp van cryptografie aanlevert. De organisaties waaraan geleverd wordt, zullen een vergelijkbare beoordeling van hun afhankelijkheden maken en kunnen verlangen dat een leverancier zijn intenties met betrekking tot PQC correct communiceert. Het is voor leveranciers niet noodzakelijk dit voor al hun klanten bij te houden, maar het is raadzaam hier rekening mee te houden het bepalen van een geschikte strategie.

3 Migratieplanning

Overzicht

Dit hoofdstuk bevat een beschrijving van de actiestappen die nodig zijn voor een post-quantummigratie. Het is vooral bedoeld voor organisaties die zich identificeren als urgente adopters of reguliere adopters die proactief willen handelen.
In dit hoofdstuk wordt ervan uitgegaan dat een organisatie de diagnosestap zoals beschreven in Hoofdstuk 2 al heeft doorlopen. Voordat de beslissing kan worden genomen welke systemen als eerste moeten worden gemigreerd, wordt aangeraden om eerst de informatie door te nemen die wordt beschreven in Hoofdstuk 2.2.1. Aan de hand van deze informatie helpt dit hoofdstuk bij het bepalen van twee aspecten:
Het eerste deel van dit hoofdstuk geeft handvatten voor het bepalen wanneer de migratie dient plaats te vinden. Over een paar jaar zullen gecertificeerde post-quantum cryptografische standaarden en library's worden vrijgegeven. Sommige organisaties kunnen het zich veroorloven te wachten tot deze beschikbaar zijn, terwijl andere zo snel mogelijk moeten beginnen met migreren. Dit heeft invloed op het migratiebeleid. Het eerste deel van dit hoofdstuk bevat alle benodigde informatie om te beslissen welk migratiescenario bij een organisatie past.
Het tweede deel van dit hoofdstuk bevat adviezen voor het plannen van de migratie. Hier wordt bepaald welke cryptografische systemen moeten worden vervangen, waardoor ze moeten worden vervangen en in welke volgorde dat dient te gebeuren. Hiertoe dienen prioriteiten gesteld te worden, afhankelijkheden geïdentificeerd te worden en geanticipeerd te worden op enkele gevolgen van de migratie, zoals de noodzaak om bepaalde data systemen tijdelijk te isoleren.

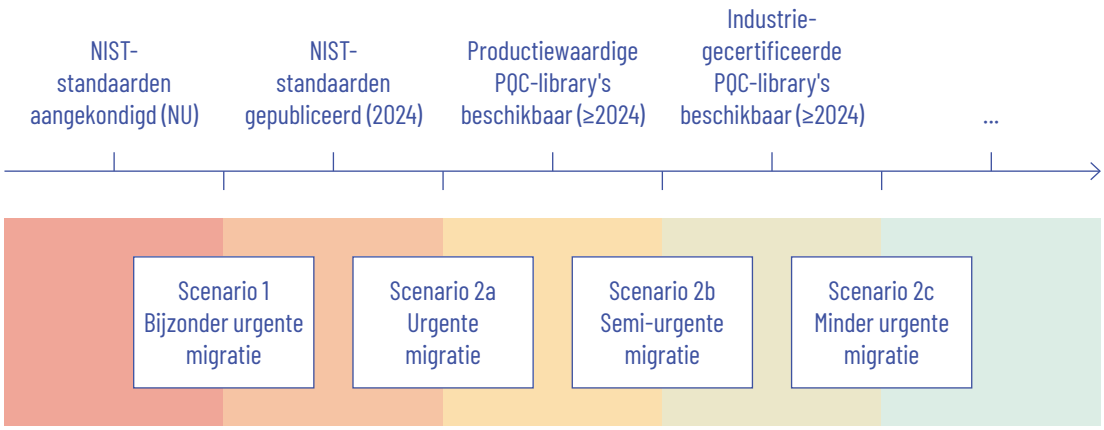
Zodra de migratie zorgvuldig is gepland, leidt de daaropvolgende paragraaf de lezer door de uitvoering van de migratie. Hoewel in dit document de migratiestappen (diagnose-planning-uitvoering) achtereenvolgens worden beschreven, hoeven organisaties in de praktijk niet te wachten om met de volgende stap te beginnen totdat de vorige stap volledig is afgerond. Organisaties moeten beginnen met het identificeren van hun meest kritieke systemen, het plannen van een eerste migratiefase voor deze kritieke systemen en deze migratie uitvoeren. Tegelijkertijd moeten ze 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 Wanneer te beginnen met migreren?

3.1.1 Verschillende migratiescenario's

Indien systemen op korte termijn moeten worden gemigreerd, is het nu tijd om te beslissen *wanneer* dat gebeurt.. Dit is afhankelijk van drie variabelen, namelijk de tijd X gedurende welke het systeem veilig moet blijven, de migratietijd Y, en de tijd Z totdat een quantumcomputer cryptografie kan breken. Er moet op tijd gemigreerd worden zodat $X + Y < Z$, ook wel de ongelijkheid van Mosca genoemd [MP21]. Hoe dichter $X + Y$ bij Z ligt, des te urgenter is de migratie. Het is belangrijk op te merken dat al deze variabelen slechts schattingen zijn en mogelijk niet volledig met de werkelijkheid stroken. Ze zijn slechts een indicatie voor of het al tijd is om te migreren.

Terwijl een organisatie *X* zelf moet kunnen inschatten op basis van haar bedrijfsprocessen, is de waarde van *Y* moeilijker te bepalen. Hieronder staat advies voor het inschatten van deze waarde. Hierbij moet rekening worden houden met het traject voor door de industrie gecertificeerde implementaties van NIST post-quantum-cryptografiestandaarden en de mijlpalen ervan. Dit traject bestaat uit drie vermoedelijke mijlpalen, waaruit vier verschillende momenten volgen waarop een cryptografische systeem kan worden gemigreerd, zoals te zien is in de onderstaande figuur. Dit hoofdstuk is bedoeld om een keuze te maken per cryptografische systeem.



Figuur 3.1: Tijdlijn van verschillende migratiescenario's.

De totale migratietijd $X + Y$ bij het migreren vanuit scenario *i* kan met het bovenstaande worden geherformuleerd als $X + W_i + Y_i$, waarbij

- X de geschatte tijd is dat de data geheim moeten blijven;
- W_i de geschatte wachttijd is tot de mijlpaal gekoppeld aan scenario *i*;
- Y_i de benodigde geschatte tijd is om de migratie vanuit scenario *i* uit te voeren.

Elk systemm moet worden gemigreerd vanuit scenario *i* zodat de migratietijd $X + W_i + Y_i$ kleiner is dan Z. De scenario's in Figuur 3.1 geven ook een indicatie van de bijbehorende mate van urgentie. Merk op dat W_i en Y_i niet relevant zijn als $X > Z$ en dat de migratie dan hoogst urgent moet plaatsvinden.
Men dient er rekening mee te houden dat voor elke optie de tijd voor het daadwerkelijk uitvoeren van de migratie per organisatie of zelfs per systeem kan verschillen, omdat library-documentatie, commerciële ondersteuning en algemene kennis van PQC hoogstwaarschijnlijk volledieger zullen zijn als de migratie later gestart wordt. Daarom is het absoluut noodzakelijk dat elk systeem wordt gemigreerd naar productiewaardige of gecertificeerde implementaties van NIST PQC-standaarden, als de situatie dit toelaat. Op dit punt dient nogmaals benadrukt te worden dat de exacte timing van de migratie sterk afhankelijk is van de risicobereidheid van de organisatie. Dit komt later nog verder aan bod.
De verschillen tussen de opties lijken misschien slechts kleine details, maar door te focussen op deze details kan ervoor worden gezorgd dat belangrijke informatie van de organisatie adequaat wordt beschermd. Een adequate beveiliging van deze informatie kan het verschil maken tussen het welslagen of het falen van een organisatie.

Opmerking over gecertificeerde library's

Voor sommige organisaties is het van essentieel belang om te migreren vanuit scenario 1, 2a of 2b, wat betekent dat er gemigreerd moet worden naar PQC-standaarden zonder dat er gecertificeerde library's beschikbaar zijn. Hier dient opgemerkt te worden dat dit een extra nadeel met zich meebrengt. Het gebruik van niet-gecertificeerde library's kan immers leiden tot certificeringsproblemen en het gebruik van code die niet klaar voor een productieomgeving is, kan leiden tot een hele reeks beveiligingsproblemen. De organisatie

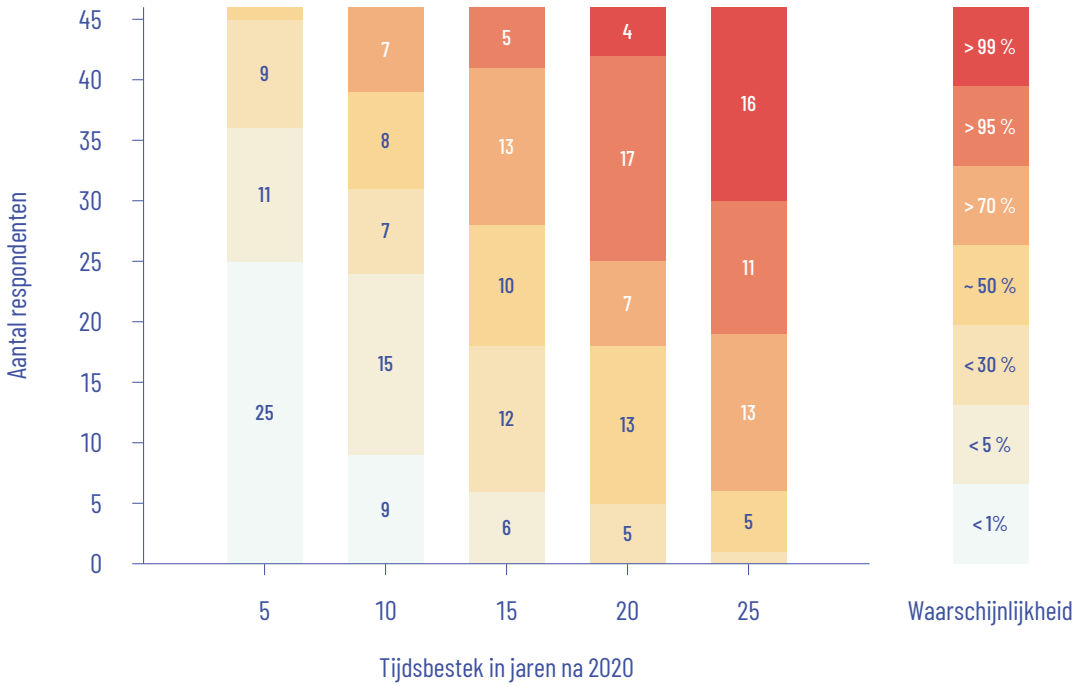
moet rekening houden met dit nadeel bij het besluit vanuit welk scenario ze wil migreren. De huidige meest gangbare standaard voor cryptografie, FIPS 140-2, staat echter al hybride schema's toe. Dit betekent dat via de hybride benadering minimaal de certificering van het klassieke algoritme kan worden behaald. Voor meer informatie over de hybride benadering, zie 'Hybride oplossingen' in Hoofdstuk 4.1.

3.1.2 Stapsgewijs proces

Stap 1: W_i, Y_i en Z inschatten

W_i en Y_i inschatten. Het is moeilijk te bepalen wanneer PQC-library's op productiewaardig niveau zullen zijn en/of industrie-gecertificeerde PQC-library's beschikbaar zullen zijn voor algemeen gebruik. Dit komt met name doordat elke PQC-library gericht zal zijn op het optimaliseren van andere algoritmen, elk voor andere use cases, zoals smartcards of IoT-apparaten. Daarom is ervaring met vergelijkbare situaties een nuttige manier om dit tijdsbestek te bepalen.
Bovendien kunnen eindgebruikers zelf invloed hebben op deze tijdlijnen. In deze periode moeten leveranciers beginnen met het ontwikkelen van library's op productiewaardig niveau. De publicatie van library's kan mogelijk versneld worden door contact op te nemen met deze leveranciers of door wensen voor PQC-library's op feedback en community fora duidelijk te maken.

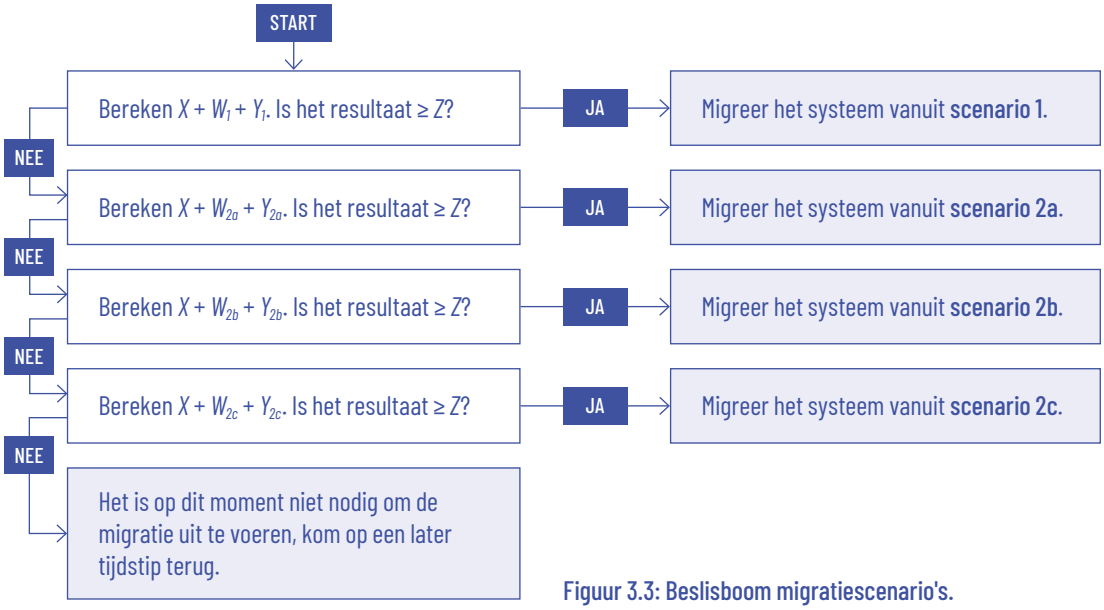
Z *inschatten.* Het valt moeilijk in te schatten wanneer een quantumcomputer in staat is om asymmetrische cryptografie te breken. Experts zijn nog altijd verwikkeld in discussies hierover. Om dit proces te vereenvoudigen, toont Figuur 3.2 de mening van experts over de waarschijnlijkheid dat een quantumcomputer RSA-2048 over 5, 10, 15, 20 en 30 jaar zal weten te breken [MP21]. Hieruit volgt een conservatieve schatting dat quantumcomputers asymmetrische cryptografie in het jaar 2040 zullen weten te breken, terwijl dit volgens een minder conservatieve schatting al in 2030 mogelijk is. Daarbij dient vermeld te worden dat dit onderzoek al bijna twee jaar oud is ten tijde van deze publicatie. Nieuwe onderzoeken met nieuwe schattingen van *Z* zullen waarschijnlijk in de komende jaren worden vrijgegeven.



Figuur 3.2: Meningen van experts over het breken van RSA-2048 met een quantumcomputer [MP21].

Stap 2: Het migratiescenario bepalen

Nu een ruwe schets van de tijdlijn voor elke mijlpaal is opgesteld, kan met behulp van de volgende beslisboom voor elk systeem worden besloten vanuit welk scenario dit dient te migreren:



Figuur 3.3: Beslisboom migratiescenario's.

Hoofdstuk 4 bevat, afhankelijk van het scenario, advies over het migreren van asymmetrische primitieven. In de rest van het document zijn scenario 2a, 2b en 2c samengenomen onder de naam scenario 2, omdat het algemene advies voor deze drie scenario's identiek is. Houd er echter rekening mee dat dit advies kan veranderen zodra de bovenstaande mijlpalen zijn bereikt.

Stap 3: Algemene strategie

Aangezien het onmogelijk is alles in één keer te migreren, is een algemene strategie nodig. In zo'n strategie is het aan te raden om verouderde protocollen eerst te migreren naar protocollen die op dit moment door het NCSC worden aanbevolen. Hierdoor zullen het beheer van de systemen en de algemene flexibiliteit van zowel de cryptografie als de organisatie in haar geheel op de proef worden gesteld. Pas als dit is gebeurd, wordt aanbevolen om met de migratie naar PQC te beginnen. Op deze manier kan een organisatie haar migratieproces reeds moderniseren om zo de uiteindelijke transitie soepel te laten verlopen.

3.2 Advies over migratieplanning

Het tweede deel van dit hoofdstuk bevat adviezen voor het plannen van de migratie. Het hoofddoel van deze stap is tweeledig, namelijk:

1. Voor elk cryptografisch systeem beslissen of dit moet worden vervangen, en zo ja, vaststellen waardoor het moet worden vervangen.
2. De volgorde bepalen waarin de verschillende cryptografische systemen moeten worden gemigreerd.

Dit hoofdstuk bevat nuttige informatiebronnen met richtlijnen voor welke cryptografische elementen moeten worden vervangen en met welke oplossingen ze vervangen kunnen worden (zie Hoofdstuk 4). De prioritering hangt af van de risicobeoordeling die in het vorige hoofdstuk is vastgesteld. Er moet echter ook rekening worden gehouden met de afhankelijkheden en de gevolgen van de migratie voor de organisatie.

3.2.1 Bedrijfsprocesplanning

Omdat bij een migratie bedrijfsprocessen een wezenlijk onderdeel zijn, 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 onderdelen van de organisatie. De migratiemanager moet alle betrokken medewerkers van het bedrijf instrueren over de verschillende stappen van de migratie en de tijdlijnen hiervoor. Ten tweede moeten voldoende middelen worden vrijgemaakt voor de noodzakelijke migratiestappen, 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 zie ook het technisch rapport [ETS20] van ETSI.

Kosten

Hoewel het moeilijk is een inschatting te maken van de exacte kosten van een migratie naar PQC, staat vast dat dit een bijzonder kostbaar proces is waarvoor een goede planning en budgettering nodig is. Er moet een team worden opgezet dat bestaat uit onder meer een migratiemanager en vijf tot tien andere personen, afhankelijk van de grootte van de organisatie. Dit team moet de in de organisatie aanwezige cryptografie in kaart brengen, de systemen die eerst moeten worden vervangen prioriteren en een migratieplan voor die systemen opstellen. Dit proces kan tot wel twee jaar in beslag nemen afhankelijk van wat reeds is verwezenlijkt en de grootte van de organisatie [ETS20].
Bovendien moeten apparaten mogelijk worden vervangen als ze PQC niet ondersteunen of als de leverancier niet van plan is om PQC te integreren. Ook heeft PQC krachtigere hardware nodig dan traditionele algoritmen. Als blijkt dat de huidige hardware niet meer voldoet, moet deze worden vervangen.
Ten slotte kunnen er potentiële kosten zijn door de risico's die de migratie met zich meebrengt. Zoals vermeld in de inleiding, brengt zowel te vroeg als te laat migreren risico's met zich mee, hetgeen tot extra kosten kan leiden. Daarnaast bestaat het risico dat huidige leveranciers niet snel genoeg naar PQC-standaarden migreren. In dat geval zullen er ook extra kosten ontstaan. Er dient daarom rekening te worden gehouden met beide vormen van potentiële kosten.

3.2.2 Technische planning

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

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.

Vervanging 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. Hoofdstuk 4 stelt vervangende oplossingen voor, afhankelijk van het cryptografisch systeem en de use case. Het wordt aangeraden om een *crypto-agile* cryptografische oplossing te gebruiken, zodat de implementatie snel kan worden bijgewerkt zodra er in de toekomst nieuwe standaarden of regels uitkomen. Voor meer informatie over crypto-agility, zie het Hoofdstuk 'Cryptographic Agility' in Hoofdstuk 4.1.
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 klassieke 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/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 in transit, 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. Echter, het is belangrijk zich te realiseren dat isolatie een enorme impact heeft op de functionaliteit en beschikbaarheid van de data. Zolang een systeem is geïsoleerd, kan deze 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.

Vervanging van hardware

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 oplossingen op zowel hardware- als softwareniveau moeten een testfase doorlopen, bijvoorbeeld in een *sandbox* omgeving. Deze testfase is bijzonder belangrijk en moet goed worden voorbereid. De testen zullen uitwijzen of de nieuwe algoritmen compatibel zijn met de overige infrastructuur en daadwerkelijk de beloofde beveiliging bieden.

4 Uitvoering

Overzicht

Dit hoofdstuk biedt meer informatie en richtlijnen voor het uitvoeren van de migratie. Het bevat richtlijnen voor het migreren van onveilige cryptografie en protocollen. Deze richtlijnen bevatten zowel algemene als gespecialiseerde stappen om succesvol naar een quantumveilige omgeving te migreren. Veel stappen zijn afhankelijk van wanneer de organisatie de migratie daadwerkelijk uitvoert. Het is dan ook raadzaam om eerst uw migratiescenario te bepalen aan de hand van het vorige hoofdstuk. Verder is het belangrijk om al te werken aan de cryptographic agility van de systemen. De belangrijkste aanbeveling voor bijna alle protocollen is om een hybride benadering te gebruiken.

4.1 Algemene strategieën

De beschrijving van de laatste fase van de migratie is voorlopig vrij algemeen. De lezer moet er rekening mee houden dat de migratie een lang proces is. Verschillende instellingen werken momenteel aan gedetailleerde richtlijnen voor deze fase. Meer gedetailleerde informatie zal over enkele jaren beschikbaar zijn. Dit mag organisaties er niet van weerhouden om nu al aan de eerste fasen van de migratie te beginnen.

De laatste fase van de migratie bestaat uit de uitvoering van het plan dat in het vorige hoofdstuk is opgesteld. Idealiter is op dit moment een volledig overzicht van cryptografische systemen beschikbaar en is er een plan opgesteld naar welke PQC-alternatieven de kwetsbare systemen moeten worden gemigreerd. Een organisatie kan ook besluiten om systemen met hoge prioriteit al te migreren voordat het plan is voltooid en om vervolgens de laatste fase parallel aan de andere fasen uit te voeren. Houd er rekening mee dat IT-omgevingen voortdurend veranderen. Een inventaris van twee jaar geleden zal hoogstwaarschijnlijk niet meer overeenkomen met het huidige cryptografische landschap van een organisatie. Daarom is het belangrijk om deze inventaris voortdurend up-to-date te houden.
Het eerste deel van dit hoofdstuk bevat enkele algemene strategieën die kunnen worden toegepast bij de PQC-migratie. In de volgende twee hoofdstukken bespreken we in detail hoe cryptografische primitieven en protocollen kunnen worden gemigreerd.

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 van elke vervangende oplossing te begrijpen. We moeten ook meegeven dat post-quantum asymmetrische cryptografie minder goed is ingeburgerd dan klassieke asymmetrische cryptografie. Er moet nog jarenlang grondig crypto-analytisch werk worden verricht om hetzelfde niveau van vertrouwen te bereiken. Toch mag dit geen argument zijn om de migratie uit te stellen. Hybride schema's bieden immers een beveiligingsniveau dat ten minste overeenstemt met het beveiligingsniveau van het gebruikte klassieke algoritme , waarmee de dreiging van quantumcomputers strikt minder is.

Cryptographic Agility

Organisaties wordt aangeraden om alle systemen die ze zelf beheren *crypto-agile* maken.
De term *crypto-agile* betekent dat cryptografische protocollen, producten en systemen zodanig worden geïmplementeerd dat de betrokken cryptografische algoritmen met minimale inspanning kunnen worden gewijzigd en zonder dat er significante wijzigingen in de overige architectuur nodig zijn. Merk op dat crypto-agility niet iets is wat een organisatie zomaar kan kopen. Hiervoor is een herstructurering van personen, processen en technologie nodig. Door het toepassen van crypto-agility is het veel gemakkelijker om van cryptografisch systeem te wisselen zodra er nieuwe best practices of standaarden ontstaan.
Post-quantumcryptografie is nog relatief jong, hetgeen betekent dat de bijbehorende parameters kunnen variëren en in de loop van de tijd nieuwe kwetsbaarheden zullen worden ontdekt. Volgens deze nieuwe inzichten zullen protocolparameters moeten worden gewijzigd, terwijl verschillende protocollen worden gestandaardiseerd. Het is belangrijk dat organisaties al beginnen met de voorbereiding zodat parameters en protocollen snel kunnen worden gewisseld met minimale inspanning voor de organisatie. Een organisatie moet voorbereid zijn om gemakkelijk cryptografische algoritmen te wisselen zodra de relevante standaarden beschikbaar zijn of een nieuwe implementatie wordt aanbevolen. Vooral wanneer ze ervoor kiest om bepaalde systemen gedeeltelijk te migreren *voordat* standaarden en gevalideerde implementaties beschikbaar zijn. Dit is duidelijk anders dan bij de huidige klassieke cryptografie waar standaarden en goede parameterkeuzes al stevig zijn ingeburgerd. Het is belangrijk om te beoordelen of de huidige hardware geschikt is voor PQC omdat deze laatste meer capaciteit van de hardware vraagt. Het is belangrijk om alvast na te denken over alternatieven als dit niet het geval is. Meer informatie over de vereisten voor verschillende PQC-alternatieven staan in Hoofdstuk 5.
Organisaties kunnen de crypto-agility verbeteren door deze af te dwingen voor nieuwe of bijgewerkte systemen en crypto-agility scans te integreren in oplossingen met *continuous integration/continuous delivery* (CI/CD). Om nieuwe systemen of systemen die worden geüpdatet inherent crypto-agile te maken, wordt geadviseerd de cryptografie zoveel mogelijk te abstraheren van de eigenlijke code. Dit kan bijvoorbeeld door middel van abstracte oproepen naar (high-level) library's of cloudservices voor het uitvoeren van cryptografische bewerkingen en/of extern sleutelbeheer [Saf21]. Door het afdwingen van deze principes wordt de uiteindelijke migratie van deze systemen veel eenvoudiger. Voor meer informatie over deze taken op het gebied van crypto-agility wordt de whitepaper van Cryptosense aangeraden [Cry21]. Het bedrijf werkt ook aan tools om bepaalde delen van deze taken te automatiseren.

Migratie van primitieven versus protocollen

Alvorens de migratie van primitieven of protocollen te bespreken, moet eerst een belangrijk onderscheid worden gemaakt. Cryptografische primitieven staan over het algemeen niet op zich, maar vormen een stukje van een groter protocol. Dit betekent dat de meeste organisaties eigenlijk nooit direct in aanraking komen met de echte details van cryptografische algoritmen. Ze komen in aanraking met en maken gebruik van library's met veelgebruikte protocollen op basis van deze cryptografische primitieven, zoals TLS. Via deze library's kunnen verschillende cryptografische keuzes worden gemaakt, zoals welke primitieve of sleutelgrootte moet worden gebruikt. Het is normaliter niet de verantwoordelijkheid van de organisatie om zelf cryptografische algoritmen in library's te implementeren.
Over het algemeen is het direct migreren van primitieven in plaats van protocollen voorbehouden voor de zeldzame gevallen waarin een organisatie direct met zuiver cryptografische library's communiceert en zelf protocollen implementeert. Het eerste deel van Hoofdstuk 5 bevat een lijst met de belangrijkste klassieke primitieven, hun basiskenmerken en of ze al dan niet quantumveilig zijn. Dit hoofdstuk bevat ook de belangrijkste post-quantum primitieven.

Migratie van symmetrische cryptografie en hashfuncties

Quantumcomputers zullen in staat zijn het beveiligingsniveau van klassieke symmetrische cryptografie of hashfuncties te verlagen. Voor symmetrische cryptografie betekent dit dat een bericht kan worden ontsleuteld door iemand die de geheime sleutel niet kent, waardoor de vertrouwelijkheid van het bericht in gevaar komt. Hashfuncties worden niet gebruikt om vertrouwelijkheid te beschermen, maar wel om de integriteit te beschermen. Bij het migreren van symmetrische cryptografie naar post-quantumstandaarden moet de sleutellengte van het gebruikte algoritme verdubbeld worden om zo een voldoende beveiligingsniveau te garanderen. Dit moet reeds worden gedaan voor documenten die zijn versleuteld met behulp van een symmetrische sleutel en die voor een langere periode vertrouwelijk moeten blijven om store-now-decrypt-later aanvallen te voorkomen. Hash-functies zijn niet gevoelig voor deze store-now-decrypt-later aanvallen.
Een andere categorie betreft systemen met een lange levensduur die afhankelijk zijn van symmetrische cryptografie of hashfuncties zoals simkaarten, satellieten of operationele technologie. Systemen met een lange levensduur zijn in de toekomst mogelijk moeilijk of niet te updaten en moeten daarom reeds worden bijgewerkt met algoritmen die langere symmetrische sleutels of een grotere hashuitvoer gebruiken. Organisaties moeten er rekening mee houden dat deze langere sleutelgroottes leiden tot grotere opslagvereisten en langzamere algoritmen.

Migratie van asymmetrische cryptografie met behulp van hybride oplossingen

Quantumcomputers zullen in staat zijn om klassieke asymmetrische cryptografie te breken en daarmee dus alle garanties die worden geboden door protocollen op basis van deze algoritmen te ondergraven. Net als bij symmetrische cryptografie zijn de belangrijkste zorgen die nu moeten worden aangepakt de vertrouwelijkheid van data gedurende een lange periode en de veiligheid van systemen met een lange levensduur.

Hybride oplossingen

Hybride oplossingen verwijst naar het gelijktijdige gebruik van zowel klassieke als post-quantumcryptografie binnen één enkel protocol. Om het schema te breken, zou een aanvaller zowel het klassieke als het post-quantum algoritme moeten breken. Daarom is de beveiliging van het volledige schema minimaal zo goed als de beveiliging van elk algoritme afzonderlijk.
Dit is gericht op het verminderen van de beveiligingsrisico's als gevolg van de beperkte volwassenheid van de nieuwe post-quantum algoritmen. Bovendien krijgen we zo de extra beveiliging van het post-quantumalgoritme.
Hybride oplossingen worden met name aanbevolen voor organisaties die quantumveilige cryptografie moeten inzetten vóórdat referentie-implementaties van de nieuwe gestandaardiseerde algoritmen beschikbaar zijn, bijvoorbeeld als uw data vandaag al gevoelig zijn voor store-now-decrypt-later aanvallen.
Het belangrijkste nadeel is dat deze techniek tot overhead (in tijd en/of geheugen) kan leiden aangezien er nu twee cryptografische algoritmen voor een enkele versleuteling moeten worden uitgevoerd. Deze extra kosten zullen normaliter meevallen ten opzichte van de PQC-implementatie, aangezien de meeste post-quantumschema's al een grotere berichtgrootte met zich meebrengen.

Waarschuwing | Wanneer producten beweren gebruik te maken van hybride versleuteling, zorg er dan voor dat u zich houdt aan de bovenstaande beschrijving, dat wil zeggen dat u tegelijkertijd klassieke EN post-quantumalgoritmen voor versleuteling gebruikt. Dit mag niet verward worden met de keuze tussen het gebruik van een klassiek OF post-quantumalgoritme voor versleuteling (zie hieronder).

Downgrade Attacks

Sommige hybride benaderingen zijn onderhevig aan *downgrade attacks*. Dit gebeurt wanneer een systeem *hybrid OR* implementeert in plaats van *hybrid AND* zoals hierboven uitgelegd. Hybrid OR, of *optioneel post-quantum*, beschrijft een situatie waarin zowel het klassieke als het post-quantumalgoritme op de server zijn geïmplementeerd. Voor communicatie met de server kan een client dan kiezen om het klassieke of

het quantumveilige protocol te gebruiken en is hij niet verplicht beide te gebruiken. Een dergelijke configuratie is gunstig voor *backward compatibility*. Deze compatibiliteit is bijzonder handig om tijdens de test- en vroege ontwikkelingsfase interoperabiliteit te bieden.
Een dergelijke oplossing vormt echter een belangrijk risico: een tegenstander kan doen alsof hij geen post-quantum protocollen ondersteunt en zo de server dwingen te communiceren met behulp van het klassieke algoritme. Dit staat bekend als een *downgrade attack*. Zelfs als de kwaadwillende actor de gebruikte klassieke primitieve niet kan breken, kan hij nog altijd store-now-decrypt-later aanvallen uitvoeren.
Daarom is het advies over het algemeen om voor interne systemen hybride oplossingen van het type hybrid AND te gebruiken. Voor naar buiten gerichte systemen kan dit echter omslachtiger zijn en is hybrid OR misschien wel de enige optie. Beleidslijnen en strategieën moeten worden ontwikkeld voor wanneer en hoe dergelijke systemen hybride schema's correct ingezet kunnen worden.

Migratie van asymmetrische cryptografie met behulp van vooraf gedeelde sleutels

Asymmetrische cryptografie kan ook quantumveilig worden gemaakt door middel van klassieke symmetrische cryptografie met vooraf gedeelde sleutels. Deze methode is bedoeld om communicatie tot stand te brengen zonder cryptografie met publieke sleutel. Voor deze methode moeten vooraf gedeelde sleutels op een fysieke manier worden gedeeld, bijvoorbeeld via een USB-stick. De distributie van dergelijke sleutels is meestal een vrij omslachtig proces, waardoor de oplossingen met name in één-op-veel-infrastructuren niet schaalbaar zijn. Bovendien kunnen certificaten niet worden gevalideerd aangezien asymmetrische cryptografie wordt vermeden. Dit is echter een bijzonder veilige en efficiënte benadering nadat dergelijke vooraf gedeelde sleutels eenmaal zijn ingesteld.
Het advies is daarom om de hybride benadering te volgen, tenzij het systeem aan *alle* 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 Primitieven migreren

Dit hoofdstuk is bedoeld voor library-ontwikkelaars en beveiligingsarchitecten en geeft een overzicht van gangbare klassieke en post-quantumcryptografie. Voor elke functionaliteit waarvoor cryptografie wordt gebruikt, worden aanbevolen, acceptabele en te vermijden primitieven vermeld. Dit hoofdstuk gaat uit van een redelijk inzicht in cryptografie.

Hoewel er voor elke functionaliteit een aanbevolen keuze is, worden ook acceptabele alternatieven vermeld om organisaties enige flexibiliteit te bieden. Dat gebeurt vooral omdat er een grote verscheidenheid aan use cases is waarvoor een bepaalde functionaliteit kan worden gebruikt. Ook wordt vermeld welke primitieven niet mogen worden gebruikt.

Een overzicht van alle aanbevolen, acceptabele en te vermijden cryptografieën staat in Tabel 4.1. Een gedetailleerde beschrijving van elke primitieve staat in Hoofdstuk 5. De rest van dit hoofdstuk bevat meer informatie over elk van de bovenstaande functionaliteiten. Bovendien wordt verduidelijkt welke primitieve wordt aanbevolen, afhankelijk van het scenario waaruit wordt gemigreerd.
Post-quantumprimitieven kunnen worden geconfigureerd met beveiligingsniveaus tussen 1 (laagste beveiliging) en 5 (hoogste beveiliging). De afweging daarbij is dat hoe hoger het beveiligingsniveau, des te slechter de prestaties. Het advies voor **alle post-quantumprimitieven ten minste beveiligingsniveau 3 en hoger**. Beveiligingsniveau 1 en 2 zijn acceptabel.

Type	Functionaliteit	Aanbevolen	Acceptabel	Niet gebruiken
Symmetrisch	*Block Cipher*	AES-256	Camellia-256	AES-128, AES-192 (T)DES, IDEA, en Blowfish
Symmetrisch	*Stream Cipher*	ChaCha20 met 256-bits sleutel	-	RC4
Asymmetrisch (Alle scenario's)	*Public-Key Encryption/KEMs*	CRYSTALS-KYBER	Classic McEliece, FrodoKEM	Elke klassieke PKC
Asymmetrisch (scenario 1 met stateful hash-based handtekeningen)	*Digital Signatures*	XMSS, XMSS^{MT} LMS, HSS	Alle (ontwerp)standaarden van NIST	Elke klassieke PKC
Asymmetrisch (scenario 1 zonder stateful hash-based handtekeningen)	*Digital Signatures*	Alle (ontwerp)standaarden van NIST	-	Elke klassieke PKC
Asymmetrisch (Scenario 2)	*Digital Signatures*	Alle (ontwerp)standaarden van NIST	XMSS, XMSS^{MT} LMS, HSS	Elke klassieke PKC
Hash	*Hashing*	Ten minste SHA3-256 of SHA-256	BLAKE2, SHAKE256	SHA1, MD5, SHAKE128, SHA3-224, SHA-224
MAC's	*Block Cipher Construction*	CMAC-AES-256	CMAC-Camellia	CBC-MAC
MAC's	*Hash Constructions*	HMAC met ten minste SHA-256 of SHA3-256	BLAKE2-MAC	HMAC-MD5
MAC's	*Universal Hashing*	Poly1305	-	-

Tabel 4.1: Aanbevolen, acceptabele en te vermijden cryptografische primitieven per functionaliteit.

4.2.1 Symmetrische cryptografie

Migratie van symmetrische cryptografie

Scenario 1 en 2 | Voor symmetrische cryptografie zijn de opties aanbevolen, acceptabel en niet gebruiken identiek voor beide migratiescenario's. Zie hiervoor Tabel 4.1.

Het verdient opmerking dat AES de aanbevolen keuze is omdat het door NIST is gestandaardiseerd en stevig is ingeburgerd. Camellia is gestandaardiseerd in verschillende protocollen zoals TLS 1.2 [KK10], IPSec [AMK05] en S/MIME [Mor04], en wordt daarom ook als een acceptabele keuze beschouwd. Houd er bovendien rekening mee dat sleutellengtes van minder dan 256 bits te laag zijn om veiligheid te garanderen.
Organisaties die met veel legacysystemen werken, zoals banken, merken waarschijnlijk dat TDES vaak in hun systemen wordt gebruikt. Door diens kleine blok- en sleutelgrootte zal TDES volledig verouderd zijn tegen de tijd dat quantumcomputers voldoende groot zijn om asymmetrische cryptografie te breken.

4.2.2 Asymmetrische cryptografie: Mechanismen voor asymmetrische versleuteling en sleutelincapsulatie

PKE- en KEM-migratie

Scenario 1 en 2 | Voor mechanismen voor asymmetrische versleuteling en key encapsulation zijn de opties aanbevolen, acceptabel en niet gebruiken identiek voor beide migratiescenario's. Zie hiervoor Tabel 4.1.

Er zijn geen quantumveilige klassieke primitieven voor deze twee functionaliteiten. Daarom zijn post-quantumprimitieven de enige aanbevolen en aanvaardbare optie. Ook nu dient opgemerkt te worden dat geen van deze schema's in dezelfde mate is gestandaardiseerd of getest als hun klassieke tegenhangers. Zie voor meer informatie over deze PQC-primitieven Hoofdstuk 5.3.

4.2.3 Asymmetrische cryptografie: Digitale handtekeningen

Migratie van digitale handtekeningen

Stateful hash-based handtekeningschema's (HBS) zijn handtekeningschema's op basis van hashes die slechts een vast aantal handtekeningen kunnen produceren. Dit komt omdat een handtekening wordt gemaakt met een eenmalige sleutel die niet opnieuw mag worden gebruikt. Daarom is zorgvuldig beheer van deze sleutels essentieel. Het is belangrijk om een duidelijk onderscheid te maken tussen systemen die deze handtekeningen wél en niet moeten implementeren, aangezien stateful hash-based handtekeningen niet bedoeld zijn voor algemeen gebruik. Kies daarom **scenario 1: HBS** als en alleen als het systeem dat momenteel wordt gemigreerd voldoet aan alle van de volgende vereisten [SP 20]:

1. U heeft uw migratiescenario geïdentificeerd als 1.
2. De implementatie van stateful hash-based handtekeningen zal een lange levensduur hebben.
3. Omschakelen naar een ander handtekeningschema in de nabije toekomst is niet praktisch.

4. U bent in staat om eenmalig gebruikte paren van publieke/private sleutel effectief en correct bij te houden (en dus de status te beheren).
5. HBS hebben over het algemeen een (desalniettemin grote) limiet voor het aantal berichten dat ze kunnen ondertekenen. Er moet dus voor worden gezorgd dat een systeem slechts een beperkt aantal berichten hoeft te ondertekenen.

Dit komt omdat stateful hash-based handtekeningen een bijzonder zorgvuldig statusbeheer vereisen, hetgeen de algemene toepasbaarheid beperkt.
Als het systeem niet voldoet aan de bovengenoemde vereisten, kies dan **scenario 1: Niet-HBS**.

Asymmetrische cryptografie: Scenario 1

Scenario 1: HBS | Voor asymmetrische cryptografie toont Tabel 4.1 de aanbeveling voor systemen met scenario 1 met HBS. Er is gekozen voor deze opties omdat Classic McEliece een conservatief en grondig bestudeerd algoritme is, ondanks de keerzijde van grote sleutelgroottes. Het is ook finalist in ronde 4 van het standaardisatieproces van NIST. Bovendien is FrodoKEM, een meer conservatieve beveiligingsoptie, ook een acceptabel alternatief. Van belang is dat FrodoKEM niet door NIST zal worden gestandaardiseerd.

Scenario 1: niet-HBS | Voor asymmetrische cryptografie toont Tabel 4.1 de aanbeveling voor systemen met scenario 1. Het is natuurlijk belangrijk om op de nieuwe standaarden over te stappen zodra NIST haar standaarden aankondigt en de juiste productiewaardige of gecertificeerde implementaties beschikbaar zijn.

Asymmetrische cryptografie: Scenario 2

Voor scenario 2 wordt met klem geadviseerd om te wachten op de PQC-standaarden van NIST. Van belang is dat HBS hier ook een acceptabele keuze is. Het is wederom belangrijk om de implicaties van het gebruik van HBS'en volledig te begrijpen alvorens deze te gebruiken. Zie Tabel 4.1 voor de lijst met primitieven.

Er bestaan verschillende soorten asymmetrische primitieven. Daarom is het ook belangrijk om use cases te overwegen, samen met de voor- en nadelen van elke primitieve. Zie hiervoor Hoofdstuk 5.

4.2.4 Hash

Hash-migratie

Scenario 1 en 2 | Voor hashes zijn de opties aanbevolen, acceptabel en niet gebruiken identiek voor alle migratiescenario's. Zie hiervoor Tabel 4.1.

Doordat de SHA-familie gestandaardiseerd is door NIST, wordt deze verkozen boven BLAKE2.

4.2.5 MAC's

MAC-migratie

Scenario 1 en 2 | Voor MAC's zijn de opties aanbevolen, acceptabel en niet gebruiken identiek voor alle migratiescenario's. Zie hiervoor Tabel 4.1.

Doordat AES gestandaardiseerd is door NIST, wordt CMAC-AES-256 verkozen boven CMAC-Camellia. Bovendien is HMAC door NIST gestandaardiseerd en kan het worden gecombineerd met andere gestandaardiseerde hashes, in tegenstelling tot BLAKE2-MAC. Het advies is daarom HMAC. Zie hiervoor Tabel 4.1.

4.3) Protocollen migreren

Dit hoofdstuk beschrijft hoe protocollen naar een quantumveilige versie worden gemigreerd. Het behandelt veelgebruikte protocollen en vermeldt voor elk protocol ten minste één oplossing om naar PQC te migreren. Voor elk van deze oplossingen worden actiestappen vermeld voor zowel systeembeheerders, library-ontwikkelaars, als personeel dat verantwoordelijk is voor het beveiligingsbeleid in de organisatie. Deze informatie blijft vrij algemeen van aard, maar bevat wel al advies voor een aantal relevante partijen.
Dit hoofdstuk presenteert alleen zeer gangbare protocollen, namelijk TLS, SSH, S/MIME, PGP, IPSec en X.509. Veel van de bovengenoemde protocollen zijn gedefinieerd in een type document dat ook wel een RFC (Request for Comments) wordt genoemd. Het gaat hier om standaardisatiedocumenten opgesteld door de *Internet Engineering Task Force* (IETF). Ontwerpstandaarden 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 datavercijferingen.

TLS-optie 1: Vooraf 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 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.

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.

Library-ontwikkelaars | Een gedetailleerd technisch overzicht voor het implementeren van vooraf gedeelde sleutels in TLS is gedefinieerd in RFC 4279 [ET05] en RFC 5487 [Bad09]. Library-ontwikkelaars moeten ervoor zorgen dat hun TLS-implementatie voldoet aan deze standaarden.

TLS-optie 2: Hybride benadering

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 [SFG22].

Te implementeren beleid | Cruciaal beleid is een gesprek met de systeembeheerder en eventueel cryptografische experts over de toegestane versleutelingssuites die kunnen worden gebruikt om quantumbeveiliging 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.

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.

Library-ontwikkelaars | Library-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 [LY06c].

Standaardisatiedocumenten | RFC 8446 [LY06c].

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 [KSF+20].

Te implementeren beleid | Cruciaal is een gesprek met de systeembeheerder en eventueel cryptografische experts over de toegestane vercijferingen die kunnen worden gebruikt om quantumbeveiliging 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.

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.

Library-ontwikkelaars | Library-ontwikkelaars 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] en 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. Ze stellen echter dat hun 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.

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 quantumbeveiliging te informeren.

Library-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 [FDC+07] en GnuPGP [MJ21].

Standaardisatiedocumenten | RFC 4880 [FDC+07].

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

Op dit moment is er weinig tot geen onderzoek naar post-quantum PGP. Daarom is het belangrijk 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.

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

Library-ontwikkelaars | Het monitoren 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 VPN's.

Er zijn twee opties om IPSec naar quantumveilig te migreren: het gebruik van vooraf gedeelde sleutels (optie 1) en de hybride benadering (optie 2).

IPSec-optie 1: Vooraf 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 bitsleutel 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.

Systeembeheerders | Uiteraard moet de systeembeheerder IPSec configureren om vooraf 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.

Library-ontwikkelaars | Een gedetailleerd technisch overzicht van dit proces is gedefinieerd in RFC 7296 [KHN+14]. Library-ontwikkelaars 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 benadering

ETSI TR 103 617 is een nuttig technisch hulpmiddel om quantumbeveiliging in IPSec te realiseren [EST18].

Te implementeren beleid | Belangrijk is een gesprek met de systeembeheerder en eventueel cryptografische experts over de toegestane versleutelingssuites die kunnen worden gebruikt om quantumbeveiliging 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.

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.

Library-ontwikkelaars | Library-ontwikkelaars kunnen deze functie implementeren op basis van het technische rapport van ETSI [EST18]. 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 [X5019].

Standaardisatiedocumenten | RFC 5280 en ITU-T X.509 [X5019].

Normaal gebruik | X.509 wordt vaak gebruikt in HTTPS om websites te verifiëren.

De organisatie moet voor alle scenario's de hybride benadering overwegen aangezien het X.509-protocol geen vooraf gedeelde sleutels accepteert.
De ITU-T heeft al hybride certificaten (meerdere algoritmen) gestandaardiseerd in hoofdstuk 9.8 van [X5019]. Het is gebaseerd op de verouderde Internet Draft van Truskovsky et al. [TGF+18]. Root-CA's en CA's accepteren dit soort certificaten nog niet en geven ze ook nog niet uit. De kans bestaat dus dat deze voorlopig allemaal zelf ondertekend moeten zijn. Uiteraard zullen op een gegeven moment meer root-CA's en CA's post-quantumcertificaten gaan aanbieden. Daarom is het belangrijk om op de hoogte te blijven van de technologieonwikkelingen.

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-library's dan compatibel moeten worden gemaakt met de nieuwe certificaten.

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. Communicatie en planning met de CA of root-CA is essentieel om dit alles te realiseren.

Systeembeheerders | De systeembeheerder moet X.509-certificaten zodanig configureren dat ze compatibel zijn met de hybride benadering.

Library-ontwikkelaars | Library-ontwikkelaars kunnen deze experimentele functie implementeren op basis van de RFC en het artikel van Bindel et al. 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.

5 Achtergrondinformatie over primitieven

Overzicht

Dit hoofdstuk is bedoeld om library-ontwikkelaars te helpen bij het selecteren van verschillende primitieven voor hun library's, en om organisaties te helpen om te begrijpen welke er gekozen moet worden en hoe de systemen naar een quantumveilige versie van het protocol gemigreerd moeten worden. Het is ook bedoeld om te helpen bij het identificeren van systemen en risico's. Rekening houdend met de doelgroep en de te behandelen informatie wordt er aanzienlijke kennis van het cryptografische landschap verwacht.
Hiertoe bevat dit hoofdstuk een lijst met de belangrijkste cryptografische primitieven die momenteel worden gebruikt. Van belang is dat het woord 'primitieve' in een ruimere betekenis dan de gebruikelijke betekenis wordt gebruikt. Het overzicht bevat voor elk van de primitieven de belangrijkste kenmerken en geeft aan of ze al dan niet quantumveilig zijn.
Tabel 5.1 bevat de lijst met veelgebruikte klassieke primitieven. Dit is geen uitputtende lijst en het is absoluut noodzakelijk om alle andere in de organisatie gebruikte vercijferingen en cryptografische algoritmen op de juiste manier te vermelden.

Symmetrisch	Asymmetrisch	Hash	MAC	HBS
AES	RSA	SHA-familie	HMAC-constructies	XMSS
(T)DES	ElGamal	MD5	BLAKE2-MAC	$XMSS^{MT}$
ChaCha20	ECDSA	BLAKE2	CMAC-constructies	LMS
Blowfish	EdDSA		CBC-MAC-constructies	HSS
RC4	ECDH		Poly1305	
Camellia				
IDEA				

Tabel 5.1: Veelgebruikte primitieven

5.1) Klassieke primitieven

5.1.1 Symmetrische versleutelingen

AES

Beschrijving | AES is een blokvercijfering die door NIST is gestandaardiseerd [FIP01] en is bovendien de de facto standaard voor symmetrische versleuteling.

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

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

Verdere opmerkingen | AES is de facto standaard voor symmetrische vercijferingen.

Standaardisatiedocumenten | FIPS 197 [FIP01], ISO/IEC 180330-3:2010 [IS010b].

Quantumveilig? | Ja, mits er een 256-bits sleutel gebruikt wordt.

(T)DES

Beschrijving | DES is een blokvercijfering die eerder door NIST als de facto standaard voor symmetrische versleuteling werd gestandaardiseerd [FIP99]. Tegenwoordig wordt meestal de Triple DES (TDES)-variant gebruikt, die twee of drie DES-sleutels combineert om de totale sleutellengte te vergroten.

Ondersteunde sleutellengtes (bits) | 56 (DES), 112 (TDES), 168 (TDES).

Toepassingen | (T)DES wordt gebruikt in een breed scala van legacy software- en hardwaredomeinen.

Verdere opmerkingen | (T)DES is gebruikelijk in de bank- en betalingssector. Het is al achterhaald voor nieuwe systemen en in 2024 voor alle systemen.

Standaardisatiedocumenten | NIST SP 80067 Rev. 2 [SP 17], ISO/IEC 18033-3:2010 [IS010b].

Quantumveilig? | Nee, de veiligheid wordt verlaagd tot 56- of 84-bits quantumveiligheid?

ChaCha20

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

Ondersteunde sleutellengtes (bits) | 128, 256.

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

Verdere opmerkingen | ChaCha20 is bekend om zijn snelheid en eenvoudige implementatie.

Standaardisatiedocumenten | RFC 8439 [NL18].

Quantumveilig? | Ja, mits er een 256-bits sleutel wordt gebruikt.

Blowfish

Beschrijving | Blowfish is een oudere symmetrische blokvercijfering voor algemeen gebruik die als alternatief voor DES werd uitgebracht [Sch94].

Ondersteunde sleutellengtes (bits) | 32-448.

Toepassingen | Blowfish wordt meestal gebruikt in legacy systemen.

Verdere opmerkingen | Blowfish is gevoelig voor *verjaardagsaanvallen* (Birthday Attacks) vanwege de 64-bits blokgrootte.

Standaardisatiedocumenten | Originele publicatie [Sch94].

Quantumveilig? | Blowfish wordt niet aanbevolen voor moderne toepassingen vanwege kleine blokgroottes.

RC4

Beschrijving | RC4 is een populaire stream cipher die bekend staat om zijn eenvoud en snelheid [Pop15].

Ondersteunde sleutellengtes (bits) | 40-2048.

Toepassingen | RC4 wordt beschouwd als onveilig en dus als legacy.

Verdere opmerkingen | -

Standaardisatiedocumenten | RC4 is achterhaald.

Quantumveilig? | RC4 wordt al als onveilig beschouwd in een klassieke setting.

Camellia

Beschrijving | Camellia is een vercijfering van Mitsubishi die min of meer dezelfde beveiliging als AES biedt [NTT05].

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

Toepassingen | Camellia is bedoeld voor gebruik in verschillende omgevingen, van systemen met laag vermogen tot systemen met hoge doorvoer.

Verdere opmerkingen | Camellia is onderdeel van de TLS 1.2-versleutelingssuites.

Standaardisatiedocumenten | ISO/IEC 18033-3:2010 [ISO10b], PKCS #11 [OAS20], RFC 3713 [MMN04].

Quantumveilig? | Ja, mits een 256-bits sleutel wordt gebruikt.

5.1.2 Asymmetrische versleutelingen

RSA

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

Grootte van publieke sleutels (bits) | ≥ 1024.

Grootte van geheime sleutels (bits) | Ongeveer *n*.

Grootte van het versleutelde bericht (bits) | Ten hoogste *n*.

Complexiteit | Het ontbinden in factoren van gehele getallen.

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

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

Verdere opmerkingen | -

Standaardisatiedocumenten | FIPS 186-4 [FIP13], NIST-SP 800-56B [SP 19] rev. 2, RFC 8017 [MKJR16], ANSI X9.44 [ANS17a], PKCS #1 [MKJR16], ISO/IEC 14888-2:2008 [IS008], ISO/IEC 11770-3:2021 [IS010a], ISO/IEC 9796-2:2010 [IS010c], ISO/IEC 18033-2 [IS010c].

Quantumveilig? | Nee, RSA is niet quantumveilig.

ElGamal

Beschrijving | ElGamal is een populair asymmetrische vercijfering op basis van het discrete logaritme probleem [IS010a].

Grootte van publieke sleutels (bits) | Ten hoogste ≈ 3*p*, waardoor *p* de volgorde van de gekozen cyclische groep G is. Gewoonlijk is *p* ten minste 2048.

Grootte van geheime sleutels (bits) | Ten hoogste *p*.

Grootte van het versleutelde bericht (bits) | ≈ 2*p*, dus ≥ 4098.

Complexiteit | Discrete logaritme.

Crypto-functionaliteit | ElGamal is een algoritme voor sleutelencapsulatie en digitale handtekening.

Toepassingen | ElGamal wordt gebruikt in het softwaredomein.

Verdere opmerkingen | ElGamal is één van de beschikbare cryptosystemen voor gebruik in GnuPGP.

Standaardisatiedocumenten | ISO/IEC 11770-3:2021 [IS010a].

Quantumveilig? | Nee, ElGamal is niet quantumveilig.

ECDSA

Beschrijving | ECDSA is een lliptische curve-variant van het door NIST gestandaardiseerde Digital Signature Algorithm [FIP13].

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

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

Grootte van het versleutelde bericht (bits) | Het dubbele van de lengte van de geheime sleutel.

Complexiteit | 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.

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

Standaardisatiedocumenten | FIPS 186-4 [FIP13], ANSI X9.63 [ANS17b], ANSI X9.142 [ANS20a], ISO/IEC 14888-3:2018 [ISO18b], SECG SEC-1 [Bro09].

Quantumveilig? | Nee, ECDSA is niet quantum-veilig.

EdDSA

Beschrijving | EdDSA is een elliptische curve-variant van het door NIST gestandaardiseerde Digital Signature Algorithm. In EdDSA worden gedraaide Edwards-curven gebruikt, zoals Curve25519 [JL17].

Grootte van publieke sleutels (bits) | 512 (niet-gecomprimeerd).

Grootte van geheime sleutels (bits) | 256.

Grootte van het versleutelde bericht (bits) | 512.

Complexiteit | EdDSA is een algoritme voor het maken van discrete logaritme.

Crypto-functionaliteit | Digitale handtekeningen.

Toepassingen | EdDSA is geschikt voor algemeen gebruik.

Verdere opmerkingen | EdDSA is gebaseerd op de handtekeningen van Schnorr.

Standaardisatiedocumenten | FIPS 186-4 [FIP13], RFC 8032 [JL17].

Quantumveilig? | Nee, EdDSA is niet quantumveilig.

ECDH

Beschrijving | ECDH is een elliptische curve-variant van de Diffie-Hellman-sleuteluitwisseling [SP 19].

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

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

Grootte van het versleutelde bericht (bits) | Het dubbele van de lengte van de geheime sleutel.

Complexiteit | Discrete logaritme.

Crypto-functionaliteit | ECDH wordt gebruikt voor sleuteluitwisseling.

Toepassingen | ECDH is geïntegreerd in protocollen die sleuteluitwisseling vereisen.

Verdere opmerkingen | ECDH wordt gebruikt in het signal protocol.

Standaardisatiedocumenten | NIST SP 800-56A Rev. 3 [SP 19], ANSI X9.63 [ANS17b], SECG SEC-1 [Bro09]

Quantumveilig? | Nee, ECDH is niet quantumveilig.

5.1.3 Hash

SHA

Beschrijving | SHA is een verzameling hashes ontworpen door het NSA [FIP02] (SHA2) en op basis van Keccak [FIP15b] (SHA3) die worden beschouwd als de de facto standaard voor hash-algoritmen. Van belang is dat SHA1 achterhaald is en niet zal worden besproken.

Hash-uitvoergroottes (bits) | 224, 256, 384, 512.

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

Verdere opmerkingen | SHA is de de facto standaard voor hashes.

Standaardisatiedocumenten | FIPS 180-4 [FIP15a], NIST SP 800 107 Rev. 1 [SP 12], RFC 6234 [Hr11], ISO/IEC 10118-3:2018 [IS011b] (SHA2), FIPS 180-4 [FIP15a], FIPS 202 [FIP15b], NIST SP 800 107 Rev. 1 [SP 12], ISO/IEC 10118-3:2018 [IS011b] (SHA3).

Quantumveilig? | Ja, mits er gebruikt wordt gemaakt van een hash digest van ten minste 256 bits.

MD5

Beschrijving | MD5 is een onveilige hashfunctie [Tur11] die nog altijd veelvuldig wordt gebruikt.

Hash-uitvoergroottes (bits) | 128.

Toepassingen | MD5 wordt gebruikt als een niet-cryptografische hashfunctie in verschillende domeinen.

Verdere opmerkingen | MD5 wordt als onveilig beschouwd als cryptografische hashfunctie.

Standaardisatiedocumenten | RFC 1321 [Riv92].

Quantumveilig? | MD5 wordt al als onveilig beschouwd in een klassieke setting.

BLAKE2

Beschrijving | BLAKE2 is een hashfunctie met betere softwareprestaties dan SHA3 [BLA17]. Beschikbaar in twee 'varianten', BLAKE2b en BLAKE2s.

Hash-uitvoergroottes (bits) | ≤ 256 (BLAKE2b), ≤ 128 (BLAKE2s).

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

Verdere opmerkingen | -

Standaardisatiedocumenten | RFC 7693 [SA15].

Quantumveilig? | Ja, mits er gebruik wordt gemaakt van BLAKE2b.

5.1.4 MAC's

HMAC

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

MAC-sleutelgroottes (bits) | Willekeurig.

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

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

Verdere opmerkingen | HMAC is gevoelig voor performance-problemen.

Standaardisatiedocumenten | FIPS 198-1 [FIP08], RFC 2104 [KBC97].

Quantumveilig? | Ja, mits de onderliggende hash 128-bits quantumveilig is.

BLAKE2-MAC

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

MAC-sleutelgroottes (bits) | Willekeurig.

MAC-uitvoerformaten (bits) | ≤ 256 (BLAKE2b), ≤ 128 (BLAKE2s).

Toepassingen | BLAKE2-MAC wordt gebruikt in het softwaredomein.

Verdere opmerkingen | BLAKE2-MAC is sneller dan HMAC dankzij het geïntegreerde versleutelingsmechanisme.

Standaardisatiedocumenten | RFC 7693 [SA15].

Quantumveilig? | Ja, mits er gebruikt wordt gemaakt van BLAKE2b.

CBC-MAC

Beschrijving | CBC-MAC is een manier om op basis van een blokvercijfering een MAC te construeren [IS011b].

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

MAC-uitvoerformaten (bits) | Dit is afhankelijk van de gekozen blokvercijfering.

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

Verdere opmerkingen | CBC-MAC is opgevolgd door CMAC.

Standaardisatiedocumenten | ISO/IEC 9797-1 [IS011b].

Quantumveilig? | Ja, mits de onderliggende blokvercijfering 128 bits quantumveiligheid heeft. Echter, er wordt aanbevolen om in plaats daarvan HMAC of CMAC te gebruiken.

CMAC

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

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

MAC-uitvoerformaten (bits) | Dit is afhankelijk van de gekozen blokvercijfering.

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

Verdere opmerkingen | CMAC wordt aanbevolen door NIST in plaats van CBC-MAC.

Standaardisatiedocumenten | NIST SP 800-38B [SP 16], RFC 4493 [ISLP06], ISO/IEC 9797-1:2011 [IS018a].

Quantumveilig? | Ja, mits de onderliggende hash 128-bits quantumveilig is.

Poly1305

Beschrijving | Poly1305 is een hoge-snelheid MAC die volledig losstaat van andere blokvercijferingen of hashes.

MAC-sleutelgroottes (bits) | 256.

MAC-uitvoerformaten (bits) | 128.

Toepassingen | Poly1305 kan worden gebruikt in domeinen die snel verkeer vereisen of die geen hardware-versnelling voor AES hebben.

Verdere opmerkingen | Poly1305 wordt vaak gebruikt in combinatie met ChaCha20 voor geverifieerde versleuteling.

Standaardisatiedocumenten | RFC 8439 [NL18], ISO/IEC 9797-3:2011 [IS011a].

Quantumveilig? | Ja.

5.2) Stateful hash-based handtekeningen

XMSS en XMSSMT

Beschrijving | Het eXtended Merkle Signature Scheme (XMSS) is een stateful hash-based handtekeningschema dat WOTS+ gebruikt voor eenmalige handtekeningen en is gebaseerd op Merkle hashbomen. XMSSMT is een variant met meerdere hashbomen [SP 20].

Grootte van publieke sleutels (bits) | 416-544.

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

Grootte van het versleutelde bericht (bits) | 11936-221504.

Complexiteit | Bestand tegen collisions.

Verdere opmerkingen | Zorgvuldig beheer van de state is essentieel en het belangrijkste probleem in het algoritme.

Standaardisatiedocumenten | [SP 20].

Quantumveilig? | Ja.

LMS en HSS

Beschrijving | Leighton-Micali Signatures is een stateful hash-based handtekeningschema dat LM-OTS gebruikt voor eenmalige handtekeningen en is gebaseerd op Merkle hashbomen. HSS is een variant met meerdere hashbomen [SP 20].

Grootte van publieke sleutels (bits) | 384-448 (alleen voor LMS, geen gestandaardiseerde parameter voor het aantal hashbomen in HSS).

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

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

Complexiteit | Bestand tegen collisions.

Verdere opmerkingen | Zorgvuldig beheer van de state is essentieel en het belangrijkste probleem in het algoritme.

Standaardisatiedocumenten | [SP 20].

Quantumveilig? | Ja.

5.3) Post-quantum primitieven

Tabel 5.2 toont de sterke en zwakke punten van elke post-quantum primitieve. Donkergroen betekent zeer sterk, lichtgroen op licht sterk, oranje op licht zwak en rood op zeer zwak.

	Kenmerken			Snelheid			Geheugen		
	QUANTUM-VEILIG?	VOLWASSEN-HEID	VEELZIJDIG-HEID	SLEUTELGE-NERATIE	VERSLEUTE-LING	ONTSLEUTE-LING	PUBLIEKE SLEUTEL	GEHEIME SLEUTEL	VERSLEU-TELDE TEKST
RSA									
Elliptische curve									
CRYSTALS-DILITHIUM									
CRYSTALS-KYBER									
FrodoKEM									
FALCON									
BIKE									
Classic McEliece									
HQC									
SPHINCS+									

Tabel 5.2: Sterke en zwakke punten van verschillende post-quantum primitieven.

5.3.1 Digitale handtekening

CRYSTALS-DILITHIUM

Beschrijving | CRYSTALS-DILITHIUM is een roostergebaseerd handtekeningschema dat deel uitmaakt van de NIST-finalisten voor standaardisatie [BLK+21a].

Grootte van publieke sleutels (bits) | 10496-20736.

Grootte van geheime sleutels (bits) | 20224-38912.

Grootte van het versleutelde bericht (bits) | 19360-36760.

Complexiteit | Module Small Integer Problem (MSIS) en Module Learning with Errors (MSIS).

Verdere opmerkingen | CRYSTALS-KYBER, een tegenhanger van versleuteling met publieke sleutel, is ook een door NIST geselecteerd algoritme.

Ondersteunde beveiligingsniveaus | 1, 3, 5 [ABB+21b].

Standaardisatiedocumenten | Officiële website [ABB+21b].

Quantumveilig? | Ja.

FALCON

Beschrijving | FALCON is een roostergebaseerd handtekeningschema dat deel uitmaakt van de NIST-finalisten voor standaardisatie [FHK+21].

Grootte van publieke sleutels (bits) | 7176-14264.

Grootte van geheime sleutels (bits) | 10248-18440.

Grootte van het versleutelde bericht (bits) | 5328-10240.

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

Verdere opmerkingen | FALCON maakt gebruik van floating-point berekeningen, hetgeen niet erg gebruikelijk is in cryptografie.

Ondersteunde beveiligingsniveaus | 1, 3, 5 [FHK+21].

Standaardisatiedocumenten | Officiële website [FHK+21].

Quantumveilig? Ja.

SPHINCS+

Beschrijving | SPHINCS+ is een stateless hash-based handtekeningschema dat is gebaseerd op het eerdere handtekeningschema SPHINCS. Volgens de ontwerpers is de kleinere handtekeninggrootte een verbetering ten opzichte van SPHINCS [HBD+21].

Grootte van publieke sleutels (bits) | 32-64.

Grootte van geheime sleutels (bits) | 64-128.

Grootte van het versleutelde bericht (bits) | 7856-49856.

Complexiteit | Bestand tegen collisions.

Verdere opmerkingen | SPHINCS+ wordt geselecteerd als NIST-ontwerpstandaard.

Ondersteunde beveiligingsniveaus | 1, 3, 5 [HBD+21].

Standaardisatiedocumenten | Officiële website [HBD+21].

Quantumveilig? | Ja.

5.3.2 Versleuteling met publieke sleutel en sleutelvorming

BIKE

Beschrijving | BIKE is een code-based KEM waarvan de hardheid is gebaseerd op Quasi-Cyclic Moderate Density Parity-Check codes. Het werd ingediend bij NIST en is momenteel een kandidaat in ronde 4 [ABB+21a].

Grootte van publieke sleutels (bits) | 12320-40792.

Grootte van geheime sleutels (bits) | 2244-4640.

Grootte van het versleutelde bericht (bits) | 12579-41229.

Complexiteit | Quasi-Cyclic Moderate Density Parity-Check codes.

Verdere opmerkingen | BIKE is kandidaat in ronde 4 van het standaardisatieproces van NIST

Ondersteunde beveiligingsniveaus | 1, 3, 5 [ABB+21a].

Standaardisatiedocumenten | Officiële website [ABB+21a].

Quantumveilig? | Ja.

Classic McEliece

Beschrijving | Classic McEliece is een conservatieve, code-based KEM op basis van het originele McEliece-cryptosysteem uit 1978 [ABC+20]. Kandidaat in ronde 4 van het standaardisatieproces van NIST.

Grootte van publieke sleutels (bits) | 2088960-10862592.

Grootte van geheime sleutels (bits) 51936-112960.

Grootte van het versleutelde bericht (bits) 1024-1920.

Complexiteit | Syndrome Decoding Problem (SDP).

Verdere opmerkingen | Classic McEliece gebruikt zeer grote sleutelgroottes maar kleine versleutelde berichten, dus waarschijnlijk niet bruikbaar voor systemen met beperkte opslag zoals smartcards of IoT.

Ondersteunde beveiligingsniveaus | 1, 3, 5 [ABC+20].

Standaardisatiedocumenten | Officiële website [ABC+20].

Quantumveilig? | Ja.

CRYSTALS-KYBER

Beschrijving | CRYSTALS-KYBER is een roostergebaseerde KEM die deel uitmaakt van de NIST-finalisten voor standaardisatie [BLK+21b].

Grootte van publieke sleutels (bits) | 13056-25344.

Grootte van geheime sleutels (bits) | 6400-12544.

Grootte van het versleutelde bericht (bits) | 6144-12544.

Complexiteit | Modular Learning with Errors (MLWE).

Verdere opmerkingen | CRYSTALS-DILITHIUM, een tegenhanger van de digitale handtekening, is ook een door NIST geselecteerd algoritme.

Ondersteunde beveiligingsniveaus | 1, 3, 5 [ABB+21b].

Standaardisatiedocumenten | Officiële website [ABB+21b].

Quantumveilig? | Ja.

FrodoKEM

Beschrijving | FrodoKEM is een roostergebaseerde KEM die conservatieve, maar toch praktische constructies ondersteunt. Het zal niet door NIST worden gestandaardiseerd. [ABD+21].

Grootte van publieke sleutels (bits) | 76928-172160.

Grootte van geheime sleutels (bits) | 159104-344704.

Grootte van het versleutelde bericht (bits) | 77760-173056.

Complexiteit | Learning with Errors (LWE).

Verdere opmerkingen | Momenteel zal FrodoKEM niet door NIST worden gestandaardiseerd.

Ondersteunde beveiligingsniveaus | 1, 3, 5 [ABD+21].

Standaardisatiedocumenten | Officiële website [ABD+21].

Quantumveilig? | Ja.

HQC

Beschrijving | HQC is een codegebaseerde KEM die is ingediend bij NIST en is momenteel een kandidaat in ronde 4 [MAB+21].

Grootte van publieke sleutels (bits) | 17992-57960.

Grootte van geheime sleutels (bits) | 320.

Grootte van het versleutelde bericht (bits) | 35848-115752.

Complexiteit | Decisional Syndrome Decoding Problem.

Verdere opmerkingen | HQC is kandidaat in ronde 4 van het standaardisatieproces van NIST

Ondersteunde beveiligingsniveaus | 1, 3, 5 [MAB+21].

Standaardisatiedocumenten | Officiële website [MAB+21].

Quantumveilig? | Ja.

Bibliografie

[ABB+21a] 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/, 2021. [Accessed: 22/08/2022].

[ABB+21b] Roberto Avanzi, Shi Bai, Ducas Lé Bos, Joppe, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Stehlé. CRYSTALS Website. https://classic.mceliece.org/index.html, 2021. [Accessed: 23/05/2022].

[ABC+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, 2020. [Accessed: 23/05/2022].

[ABD+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/, 2021. [Accessed: 23/05/2022].

[AMK05] Kato Akihiro, Shiho Moriai, and Masayuki Kanda. The Camellia Cipher Algorithm and Its Use With IPsec. RFC 4312, December 2005.

[ANS17a] Key Establishment Using Integer Factorization Cryptography. Standard, ANSI, November 2017.

[ANS17b] Key Agreement and Key Transport Using Elliptic Curve Cryptography. Standard, ANSI, February 2017.

[ANS20a] Financial services - Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm - ECDSA. Standard, ANSI, September 2020.

[ANS20b] 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.

[Bad09] Mohamad Badra. Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode. RFC 5487, March 2009.

[BDH+21] Ward Beullens, Jan-Pieter D'Anvers, Andreas T Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, and Nigel P Smart. Post-quantum cryptography: Current state and quantum mitigation. 2021.

[BLA17] BLAKE2 – fast secure hashing. https://www.blake2.net/, 2017. [Accessed on 24-03-2022].

[BLK+21a] Shi Bai, Ducas Lé, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (Version 3.1). https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf, 2021. [Accessed: 23/05/2022].

[BLK+21b] Shi Bai, Ducas Lé, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation (Version 3.02). https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf, 2021. [Accessed: 22/08/2022].

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

[BSI22] BSI. Quantum-safe cryptography – fundamentals, current developments and recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html, 2022.

[Cry21] Building a Crypto-agile Organization? https://cryptosense.com/whitepapers/crypto-agility-whitepaper, 2021.

[EST18] ESTI. Quantum-Safe Virtual Private Networks. Standard, ETSI, Valbonne, FR, September 2018.

[ET05] Pasi Eronen and Hannes Tschofenig. Pre-shared key ciphersuites for transport layer security (TLS). RFC 4279, 2005.

[ETS20] 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.

[FDC+07] Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney L. Thayer, and David Shaw. OpenPGP Message Format. RFC 4880, November 2007.

[FHK+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/, 2021. [Accessed: 23/05/2022].

[FIP99] Data encryption standard (DES). Standard, NIST, Gaithersburg, MD, October 1999.

[FIP01] Advanced encryption standard (AES). Standard, NIST, Gaithersburg, MD, November 2001.

[FIP02] Announcing Approval of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard; a Revision of FIPS 180-1. Notice, NIST, August 2002.

[FIP08] The Keyed-Hash Message Authentication Code (HMAC). Standard, NIST, Gaithersburg, MD, July 2008.

[FIP13] Digital Signature Standard (DSS). Standard, NIST, Gaithersburg, MD, June 2013.

[FIP15a] Secure Hash Standard (SHS). Standard, NIST, Gaithersburg, MD, August 2015.

[FIP15b] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Standard, NIST, Gaithersburg, MD, August 2015.

[FK11] Sheila Frankel and Suresh Krishnan. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071, February 2011.

[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.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In STOC, pages 212–219. ACM, 1996.

[HBD+21] Andreas Hüsling, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS+ Website. http://sphincs.org/index.html, 2021. [Accessed: 22/08/2022]

[Hou02] Russ Housley. Cryptographic Message Syntax (CMS). RFC 3369, September 2002.

[Hr11] Tony Hansen and Donald E. Eastlake 3rd. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234, May 2011.

[ISLP06] Tetsu Iwata, Junhyuk Song, Jicheol Lee, and Radha Poovendran. The AES-CMAC Algorithm. RFC 4493, June 2006.

[ISO08] Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms. Standard, International Organization for Standardization, Geneva, CH, April 2008.

[ISO10a] Information technology – Security techniques – Key management – Part 1: Framework. Standard, International Organization for Standardization, Geneva, CH, April 2010.

[ISO10b] Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. Standard, International Organization for Standardization, Geneva, CH, December 2010.

[ISO10c] Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms. Standard, International Organization for Standardization, Geneva, CH, December 2010.

[ISO11a] Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function. Standard, International Organization for Standardization, Geneva, CH, November 2011.

[ISO11b] IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions. Standard, International Organization for Standardization, Geneva, CH, March 2011.

[ISO18a] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher. Standard, International Organization for Standardization, Geneva, CH, October 2018.

[ISO18b] T Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. Standard, International Organization for Standardization, Geneva, CH, November 2018.

[JL17] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, January 2017.

[KBC97] Dr. Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.

[KHN+14] Charlie Kaufman, Paul E. Hoffman, Yoav Nir, Pasi Eronen, and Tero Kivinen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296, October 2014.

[KK10] Masayuki Kanda and Satoru Kanno. Camellia Cipher Suites for TLS. RFC 5932, June 2010.

[KSF+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, Internet Engineering Task Force, October 2020. Work in Progress.

[LY06c] Chris M. Lonvick and Tatu Ylonen. The Secure Shell (SSH) Protocol Architecture. RFC 4251, January 2006.

[MAB+21] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Bidoux. Löıc, 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/, 2021. [Accessed: 22/08/2022].

[MJ21] Nikos Mavrogiannopoulos and Simon Josefsson, 2021. [Accessed: 22/02/2022].

[MKJR16] Kathleen Moriarty, Burt Kaliski, Jakob Jonsson, and Andreas Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017, November 2016.

[MMN04] Mitsuru Matsui, Shiho Moriai, and Junko Nakajima. A Description of the Camellia Encryption Algorithm. RFC 3713, April 2004.

[Mor04] Shiho Moriai. Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS). RFC 3657, January 2004.

[MP21] Michele Mosca and Marco Piani. 2021 quantum threat timeline report. https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/, 2021.

[MvH20] Frank Muller and Maran van Heesch. Migration to Quantum-safe Cryptography. https://www.tno.nl/en/digital/digital-innovations/trusted-ict/cyber-security-through-quantum-safe/, 2020.

[NBV21] NBV. 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.

[NCS20a] NCSC. Whitepaper: Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography, 2020.

[NCS20b] NCSC. Whitepaper: Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, 2020.

[NCS22] NCSC. Guidelines for quantum-safe transport-layer encryption. https://www.ncsc.nl/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption, 2022.

[NIS22] NIST. Post-Quantum Cryptography - Selected Algorithms 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022, 2022.

[NL18] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439, June 2018.

[NN21] NIST and NCCoE. Migration to Post-Quantum Cryptography. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms, 2021.

[NSA21] NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/, 2021.

[NTT05] NTT. Japan's First 128-bit Block Cipher "Camellia" Approved as a New Standard Encryption Algorithm in the Internet. 2005. [Accessed on 23-05-2022].

[OAS20] OASIS. OASIS PKCS 11 TC. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11, 2020. [Accessed on 23-05-2022].

[Pop15] Andrei Popov. Prohibiting RC4 Cipher Suites. RFC 7465, February 2015.

[Res18] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.

[Riv92] Ronald L. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, April 1992.

[SA15] Markku-Juhani O. Saarinen and Jean-Philippe Aumasson. The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). RFC 7693, November 2015.

[Saf21] How Agile Is Your Cryptographic Strategy? https://safecode.org/blog/how-agile-is-your-cryptographic-strategy/, 2021.

[Sch94] Bruce Schneier. Academic: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) – Schneier on Security. https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html, 1994. [Accessed on 24-03-2022].

[SFG22] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-04, Internet Engineering Task Force, January 2022. Work in Progress.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In FOCS, pages 124–134. IEEE Computer Society, 1994.

[SP 12] Recommendation for Applications Using Approved Hash Algorithms. Special publication, NIST, Gaithersburg, MD, August 2012.

[SP 16] Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication. Special publication, NIST, Gaithersburg, MD, June 2016.

[SP 17] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. Special publication, NIST, Gaithersburg, MD, November 2017.

[SP 19] Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. Special publication, NIST, Gaithersburg, MD, March 2019.

[SP 20] Recommendation for Stateful Hash-Based Signature Schemes. Special publication, NIST, Gaithersburg, MD, October 2020.

[TGF+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, Internet Engineering Task Force, August 2018. Work in Progress.

[Tur11] Sean Turner. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. RFC 6151, March 2011.

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

[Wet] Dirk Wetter. testssl.sh. https://testssl.sh/.

[X5019] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. Standard, ITU-T, Geneva, Switzerland, October 2019.

Het PQC-migratiehandboek

RICHTLIJNEN VOOR HET MIGREREN NAAR POST-QUANTUMCRYPTOGRAFIE

TNO TOEGEPASTE CRYPTOGRAFIE EN QUANTUM-ALGORITMEN
CWI CRYPTOLOGIEGROEP
AIVD NATIONAAL BUREAU VOOR VERBINDINGSBEVEILIGING