Belgisch Instituut voor postdiensten en telecommunicatie

Raadpleging over een ontwerpvoorstel van het BIPT waarin vereisten en een routekaart voor de post-kwantumtransitie in de telecommunicatiesector worden vastgelegd

Hoe kunt u reageren op dit document?

Tot 03/11/2025
Enkel via e-mail naar consultation.sg@ibpt.be
Met de referentie CONSULT-2025-C3

Aanspreekpunt: Reda Meftah, ingenieur-adviseur (+32 2 226 87 75)

Antwoorden dienen elektronisch te worden verzonden naar het opgegeven adres.

Voeg dit formulier als eerste blad bij uw antwoord a.u.b.

Uw opmerkingen zouden moeten verwijzen naar de paragrafen en/of tekstgedeelten waarop ze betrekking hebben en duidelijk aangeven wat vertrouwelijk is.

Belgisch Instituut voor postdiensten en telecommunicatie
Koning Albert II-laan 32 bus 10 | 1000 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

1. Inleiding

1. Gegevensbescherming en beveiliging van gevoelige communicatie staan centraal op de Europese agenda.

2. In de gezamenlijke **mededeling** aan het Europees Parlement en de Raad van 16 december 2020[1] over "*De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk*" werd al aangegeven dat cyberbeveiliging van strategisch belang is voor de opbouw van een veerkrachtig digitaal Europa.

3. Het **Besluit** (EU) 2022/2481[2] van het Europees Parlement en de Raad van 14 december 2022 *tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030* verwijst in artikel 4, lid 1, 2° naar de "digitale streefcijfers" die tegen 2030 worden nagestreefd, namelijk *"beveiligde, veerkrachtige, goed presterende en duurzame digitale infrastructuurvoorzieningen* (…)".

4. Met de aanneming van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/11481, hierna de "NIS 2-richtlijn", werd een nieuwe stap gezet op het stuk van cyberbeveiliging.

5. Deze richtlijn werd gedeeltelijk omgezet bij de wet van 26 april 2024[3] *tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid*, die onder meer de bevoegde autoriteiten en onderlinge samenwerking op nationaal niveau bepaalt.

6. Artikel 21 bevat de volgende maatregelen voor het beheer van cyberbeveiligingsrisico's:

   De lidstaten zien erop toe dat: "1. De essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen [nemen] om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun activiteiten of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.
   Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in paragraaf 1 bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen. (...)".

[1] Gezamenlijke mededeling van 16 december 2020 (JOIN (2020) 18 final)
[2] BESLUIT (EU) 2022/2481
[3] Wet van 26 april 2024

7. Tot slot, na de goedkeuring van een witboek met als thema "Tegemoetkomen aan de digitale-infrastructuurbehoeften van Europa"[4], waarin ze het doel aanhaalt van leiderschap te verwerven bij de ontwikkeling van nieuwe capaciteiten op gebieden zoals kwantumcommunicatie en kwantumbestendige versleuteling, heeft de Commissie op 11 april 2024 een aanbeveling over een **routekaart** voor een gecoördineerde uitvoering van de transitie naar post-kwantumcryptografie[5] aangenomen.

8. *Het doel van deze aanbeveling is de transitie naar post-kwantumcryptografie voor de bescherming van digitale infrastructuren en diensten voor overheidsdiensten en andere kritieke infrastructuren in de Unie te bevorderen door de lidstaten de mogelijkheid te geven om*:

1. een routekaart voor een gecoördineerde uitvoering van post-kwantumcryptografie vast te stellen die erop is gericht om de inspanningen van de lidstaten voor het ontwerp en de uitvoering van nationale transitieplannen te synchroniseren, en om grensoverschrijdende interoperabiliteit te waarborgen;

2. met de hulp van cyberbeveiligingsdeskundigen de evaluatie en de selectie van toepasselijke post-kwantumcryptografiealgoritmen van de EU te ondersteunen, evenals de verdere vaststelling van dergelijke algoritmen als Unienormen die in de Unie als onderdeel van de routekaart voor een gecoördineerde uitvoering van post-kwantumcryptografie moeten worden toegepast;

3. passende en evenredige maatregelen te nemen om zich op deze transitie voor te bereiden."

2. Intern wettelijk kader

9. Dit document vertaalt de Europese verwachtingen die in punt 1 op nationaal niveau zijn geformuleerd door de minimumvereisten voor kwantumrisicobeheer en de transitie naar post-kwantumcryptografie te definiëren, en een sectoraal tijdschema te bepalen voor de doelstellingen voor de Belgische telecomoperatoren.

10. Na de goedkeuring van de wet van 26 april 2024 *tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid* heeft het BIPT de reikwijdte van zijn bevoegdheden zien uitbreiden aangezien artikel 14, § 1, laatste lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector *(*hierna *"wet met betrekking tot het statuut")* werd gewijzigd.

11. Het BIPT werd derhalve aangewezen als sectorale autoriteit, maar ook als sectorale inspectiedienst voor de digitale-infrastructuursector[6], met uitzondering van de aanbieders van vertrouwensdiensten in de zin van artikel 8, 24°, van de bovengenoemde wet van 26 april 2024.

[4] Witboek
[5] Aanbeveling 2014 1101 routekaart
[6] Voor de volledigheid moet worden opgemerkt dat het BIPT in deze hoedanigheid ook is aangewezen voor de sector van de post- en koerierdiensten.

12. In deze hoedanigheid lanceert het BIPT deze raadpleging, met name op basis van de werkzaamheden van verschillende instanties en van de richtsnoeren[7] voor het beheer van kwantumrisico's in de telecommunicatiesector die door de GSMA werden uitgegeven.

13. In het kader van de uitoefening van zijn bevoegdheden beschikt het BIPT over verschillende in artikel 14, § 2, van de wet met betrekking tot het statuut genoemde actiemiddelen, met name de mogelijkheid om op niet-discriminerende wijze elke vorm van onderzoek en openbare raadpleging te organiseren.

14. Deze raadpleging kadert daarin en beoogt ervoor te zorgen dat rekening wordt gehouden met de standpunten van de belanghebbenden die betrokken zijn bij de post-kwantumtransitie in de elektronische-communicatiesector.

3. Voorstel tot vaststelling van de vereisten en een routekaart voor de post-kwantumtransitie in de telecommunicatiesector

15. Het voorstel tot vaststelling van de vereisten en een routekaart voor de post-kwantumtransitie voor de telecommunicatiesector werd als bijlage toegevoegd.

16. In de voorgestelde tekst wordt aanvullende contextuele informatie verstrekt.

Bernardo Herman
Lid van de Raad

Peggy Valcke
Lid van de Raad

Stefaan Vyverman
Lid van de Raad

Michel Van Bellinghen
Voorzitter van de Raad

[7] "Guidelines for quantum risk management for telco v1.0", 2023, te vinden via deze rechtstreekse link.

Bijlage: voorstel tot vaststelling van de vereisten en een routekaart voor de post-kwantumtransitie in de telecommunicatiesector

INHOUDSOPGAVE

SAMENVATTING

De ontwikkeling van kwantumcomputers dreigt een aantal cryptografische algoritmen die worden gebruikt om telecommunicatienetwerken te beveiligen, achterhaald te maken.

In het licht van de risico's van retroactieve compromissen via "store now, decrypt later"-aanvallen en de mogelijk ernstige gevolgen voor de vertrouwelijkheid van de klanten en de continuïteit van diensten, teneinde de naleving van de aanbeveling van 11 april 2024 te waarborgen, werken de EU-lidstaten aan een gecoördineerde transitie naar post-kwantumcryptografie.

Dit document vertaalt de Europese verwachtingen op nationaal niveau door de minimumvereisten voor kwantumrisicobeheer en de transitie naar post-kwantumcryptografie te definiëren, alsook door het sectorale tijdschema van streefcijfers voor Belgische telecommunicatieoperatoren vast te stellen.

De gekozen referentieaanpak is opgebouwd uit drie fasen.

Deze omvat:

- de inventarisatie van de cryptografische activa en kwantumrisicoanalyse;
- de migratieplanning met de aanwijzing van een specifieke verantwoordelijke en ecosysteemcoördinatie;
- de uitvoering van de progressieve uitrol van de oplossingen.

Het sectorale tijdschema stelt doelstellingen vast die variëren van de voltooiing van de inventarisaties zodra het document is gepubliceerd tot de voltooiing van de migratie tegen 2030 voor de meest kritieke systemen, met een monitoringmechanisme vastgelegd in de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook in de "NIS 2-richtlijn" en "CER-richtlijn" (Richtlijn (EU) 2022/2557 van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten), teneinde de doelstellingen van de Europese kwantumveerkracht tegen 2035 te bereiken.

1. Inleiding

1. De ontwikkeling van kwantumcomputers dreigt tal van huidige cryptografische algoritmen achterhaald te maken, met name de asymmetrische algoritmen (ongeacht of het gaat over "RSA"[1] of elliptische curven) die worden gebruikt om de telecommunicatienetwerken te beveiligen. (GSMA, 2023)

2. Kwaadwillende actoren zouden deze dreiging nu al kunnen uitbuiten via aanvallen van het type "store now, decrypt later", waarbij ze versleutelde communicatie onderscheppen en opslaan om deze te ontcijferen zodra er een voldoende krachtige kwantumcomputer beschikbaar is. (GSMA, 2023) (NIS Cooperation Group, 2025) Ook de integriteit en authenticiteit van de gegevens staan op het spel, omdat het kraken van digitale handtekeningen het mogelijk zou maken om software-updates of kritieke registraties te vervalsen. (GSMA, 2023)

3. Gezien deze risico's met mogelijk ernstige gevolgen (schending van de vertrouwelijkheid van klanten, onderbreking van diensten, financiële verliezen) (GSMA, 2023) is een gecoördineerde transitie naar post-kwantumcryptografie (hierna "PQC" voor "Post Quantum Cryptography") noodzakelijk. (NIS Cooperation Group, 2025)

4. Al enkele jaren worden er grote inspanningen gedaan voor PQC-standaardisering. Het National Institute of Standards and Technology (hierna "NIST"[2]) in de Verenigde Staten heeft nieuwe algoritmen geselecteerd die resistent zijn tegen kwantumcomputers (bijv. CRYSTALS-Kyber voor sleutelgeneratie, CRYSTALS-Dilithium voor de handtekeningen) en heeft de eerste officiële post-kwantumcryptografiestandaarden gepubliceerd in 2024. (AIVD-CWI-TNO, 2024)

5. De vooruitgang op het gebied van standaardisering en ontwikkeling van oplossingen leggen de technische grondslag die nodig is voor de transitie. Het is ook zaak van de sector om de nodige inspanningen te leveren om deze dynamiek te ondersteunen en zich voor te bereiden op de kwantumdreiging en om innovatieve technologische oplossingen te bieden om zich te wapenen tegen deze dreiging. De tijdelijke immaturiteit van de oplossingen mag geen reden zijn om niks te ondernemen.

1.1 Doel en reikwijdte van het document

6. In dit document wordt een normatief kader voorgesteld voor de begeleiding, het kader en de beoordeling van de post-kwantumtransitie hierna "PQC" (afkorting van het Engels Post Quantum Cryptography), van de Belgische telecommunicatieoperatoren die als kritieke infrastructuur zijn aangewezen. Het biedt een referentiebasis voor de toekomstige controles en beoogt een consistent minimumniveau van kwantumbeveiliging in de sector te waarborgen.

7. Dit document komt tegemoet aan de Europese verwachtingen door de minimumvereisten vast te stellen voor de beoordeling, planning en uitvoering van de transitie, de criteria voor het

[1] RSA is een afkorting voor "Rivest–Shamir–Adleman". Dit is de naam van het cryptografische algoritme.
[2] "NIST" is de Engelse afkorting die wordt gebruikt om te verwijzen naar het "National Institute of Standards and Technology"

kwantumrisicobeheer en afstemming op het Europese tijdschema voor kwantumveerkracht (deadlines 2026, 2030, 2035).

8. **Uitgesloten van de scope:**
De kwantumsleuteldistributietechnologieën ("QKD" in het Engels voor "Quantum Key Distribution") en andere kwantumcryptografieoplossingen vallen buiten de scope van dit document, dat zich uitsluitend richt op de migratie naar gestandaardiseerde post-kwantumcryptografiealgoritmen.

2. Telecomkader

9. De Belgische operatoren van elektronische-communicatienetwerken stemmen overeen met de persona's[3] van de urgente adopters volgens de taxonomie die is vastgesteld in het PQC Migration Handbook. (AIVD-CWI-TNO, 2024) Dit is het gevolg van de kritikaliteit van hun infrastructuur, de operationele levensduur van hun apparatuur en hun systemische blootstelling aan kwantumbedreigingen.

10. Dit houdt in dat de operatoren:

- onmiddellijk de post-kwantummigratieprocessen initiëren;
- een governance invoeren, gericht op kwantumrisico's;
- een bindend transitieschema opstellen;
- periodiek verslag uitbrengen over de voortgang van de migratie.

2.1 Kwantumkwetsbaarheid in de huidige telecommunicatienetwerken

11. De cryptografische architectuur van telecommunicatienetwerken vertoont een gelaagde kwetsbaarheid voor kwantumdreigingen. Zoals weergegeven in afbeelding 1, maken de onderste lagen van de netwerkstack hoofdzakelijk gebruik van symmetrische versleuteling via statische verbindingen (bijvoorbeeld AES), terwijl de bovenste lagen vaker gebruik maken van asymmetrische versleuteling via dynamische verbindingen voor sleuteluitwisseling en/of authenticatie (bijvoorbeeld TLS). De symmetrische cryptografie die in de onderste lagen wordt toegepast voor de versleuteling van statische verbindingen vereist een beoordeling van de sleutelgroottes en distributiemechanismen. Asymmetrische versleuteling, die vooral in de bovenste lagen (transport, toepassing) wordt gebruikt voor sleutelgeneratie en authenticatie, vormt een kritieke kwetsbaarheid die prioritair moet worden gemigreerd naar post-kwantumstandaarden. (Coomans, et al., 2025)

[3] Een "persona" stemt overeen met een categorie van organisaties gedefinieerd op basis van hun specifieke behoeften voor post-kwantummigratie. (AIVD-CWI-TNO, 2024)

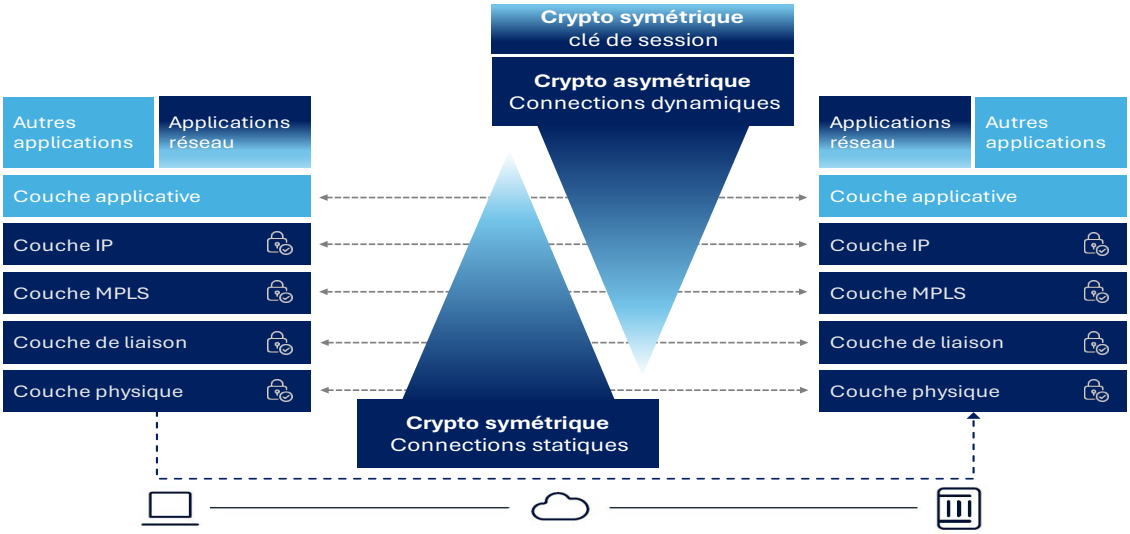
12. De operatoren moeten de kwantumkwetsbaarheid van elk beveiligingsdomein van hun infrastructuur beoordelen:

12.1. **Daniveau:**
Transport van de gebruikerscommunicatie met end-to-end cryptografische bescherming. Risico van retroactieve compromittering van gevoelige gegevens.

12.2. **Besturingsniveau:**
Netwerksignalering en verkeersroutering. Kritieke kwetsbaarheid die de algehele operationele integriteit van het netwerk in gevaar kan brengen.

12.3. **Beheerniveau:**
Netwerkmiddelen configureren en bewaken. Blootstelling van beheersystemen via onbeveiligde beheerprotocollen aan risico's als gevolg van kwantumtechnologieën.

12.4. **Interfaces voor netwerkblootstelling:**
API's voor programmeerbaarheid van het netwerk die nieuwe aanvalsoppervlakken introduceren. Met deze API's kunnen externe toepassingen bepaalde functies van het netwerk van de operator besturen (toewijzing van bandbreedte, servicekwaliteit, routering). Deze interfaces maken gebruik van cryptografische authenticatiemechanismen die kwetsbaar zijn voor kwantumaanvallen, risico's die worden versterkt door de toenemende openheid van netwerkarchitecturen.

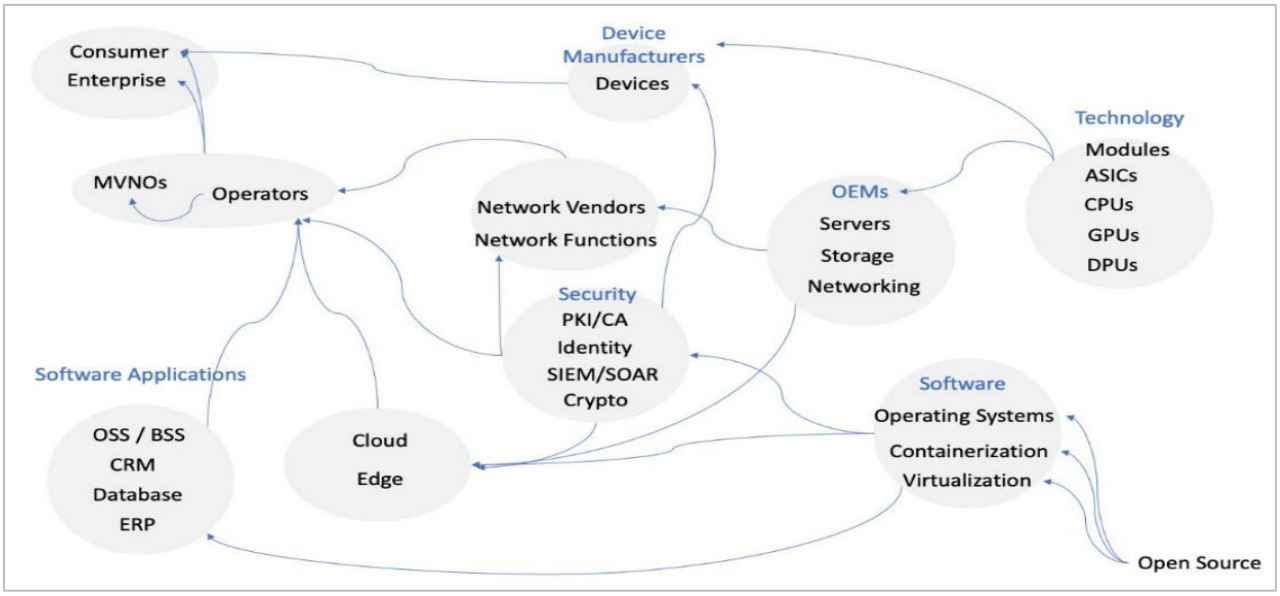


Figuur 1. SYMMETRISCHE EN ASYMMETRISCHE CRYPTOGRAFIE IN DE VERSCHILLENDE LAGEN VAN HET NETWERK (Coomans, et al., 2025)

2.2 Overzicht van het post-kwantumtelecomecosysteem

13. De post-kwantumtransitie van de telecomoperatoren kan niet afzonderlijk worden bekeken. De genoemde kwetsbaarheden, en dus de PQC-transitie, maken deel uit van een complex ecosysteem van cryptografische onderlinge afhankelijkheden die de risico's van verspreiding van kwantumkwetsbaarheden versterkt. De onderstaande mapping (GSMA, 2023) illustreert deze afhankelijkheidsstromen die bepalend zijn voor het welslagen van de post-kwantummigratie.

14. De operatoren moeten hun cryptografische afhankelijkheidsketens zo volledig mogelijk in kaart brengen, de risico's van kettingreacties beoordelen en hun migratieplannen afstemmen met alle belanghebbenden in hun technologisch ecosysteem.



Figuur 2. VOORBEELD VAN EEN AFHANKELIJKHEIDSSTRUCTUUR VAN HET POST-KWANTUMECOSYSTEEM [2]

3. PQC-migratie

15. De operatoren worden aangemoedigd om in drie fasen een gestructureerde migratieaanpak te hanteren die in overeenstemming is met de beste praktijken van ETSI " (ETSI, 2020)" en het TNO[4] Migration Handbook (AIVD-CWI-TNO, 2024). Deze aanpak vergemakkelijkt een gecontroleerde en controleerbare transitie naar post-kwantumcryptosystemen.

Figuur 3. MIGRATIE GESTRUCTUREERD IN 3 FASEN

[4] "TNO" is de afkorting van "Toegepast Natuurwetenschappelijk Onderzoek".

16. Fase 1: Beoordeling en diagnose van de kwantumkwetsbaarheden

- Inventaris van de cryptografische activa Uitgebreide inventarisatie van alle uitgerolde cryptografische elementen, protocollen en implementaties;
- Analyse van de kwantumrisico's: Beoordeling van de blootstelling van elk actief aan de kwantumdreiging met classificatie op basis van operationele kritikaliteit.

17. Operatoren moeten hun cryptografische inventaris en kwantumrisicoanalyse regelmatig updaten. Deze verplichte periodieke herziening is noodzakelijk gezien de voortdurend veranderende computeromgevingen en de mogelijke opkomst van nieuwe kwantumkwetsbaarheden. Deze aanpak vormt overigens ook een goede praktijk op het stuk van computerbeveiliging die verder gaat dan alleen kwantumvraagstukken.

18. Fase 2: Planning van de migratie

- Opstellen van een migratieplan met deadlines en controlemijlpalen;
- Prioritering van migratie op basis van risicoanalyse;
- Coördinatie met het ecosysteem van technologieaanbieders en -partners.

19. Fase 3: De migratie uitvoeren;

- Gefaseerde uitrol van post-kwantumoplossingen overeenkomstig het vastgestelde plan;
- Conformiteitsvalidering en interoperabiliteitstests;
- De bedrijfscontinuïteit tijdens de transitie handhaven.

20. Hoewel de migratie naar postkwantumalgoritmen een noodzakelijk antwoord vormt op de kwantumdreiging, garandeert deze transitie geen absolute zekerheid. Post-kwantumimplementaties in reële omstandigheden zullen waarschijnlijk intrinsieke kwetsbaarheden vertonen, waaronder algoritmische fouten, suboptimale keuzes van domeinparameters, het genereren van zwakke sleutels, implementatiefouten en kwetsbaarheden voor aanvallen via hulpkanalen. Deze beperkingen onderstrepen het cruciale belang van cryptografische[5] flexibiliteit als veerkrachtmechanisme.

21. Dankzij cryptografische flexibiliteit zouden operatoren snel moeten kunnen reageren op vastgestelde kwetsbaarheden, veranderingen in beveiligingsaanbevelingen en ontwikkelingen op het gebied van cryptanalyse. Dit aanpassingsvermogen is een essentieel onderdeel van de post-kwantumveiligheidsstrategie, waardoor deze migratie een continu proces van verbetering wordt.

22. Het succes van post-kwantummigratie hangt daarom af van de organisatorische capaciteit om de technische en strategische uitdagingen van deze transitie te begrijpen en te beheren.

[5] Cryptografische flexibiliteit of cryptoflexibiliteit verwijst naar de organisatorische en technische capaciteit om cryptografische algoritmen binnen bestaande systemen (protocollen, toepassingen, apparatuur, infrastructuren) snel te vervangen zonder dat alle systemen systematisch opnieuw moeten worden geconfigureerd of vervangen, terwijl de beveiliging en operationele continuïteit tijdens de transitie behouden worden. (Elaine Barker (NIST), Lily Chen (NIST), David Cooper (NIST), Dustin Moody (NIST), Andrew Regenscheid (NIST), Murugiah Souppaya (NIST), William Newhouse (NIST), Russ Housley (Vigil Security), Sean Turner (sn3rd), 2025)

23. Operatoren moeten ervoor zorgen dat hun teams over de nodige kennis beschikken om de migratie aan te sturen en voortdurend technologisch toezicht houden op veranderingen in postkwantumstandaarden en opkomende kwetsbaarheden.

3.1 Fase 1: stand van zaken en diagnostiek bij kwantumbedreigingen

24. De beoordelings- en diagnostiekfase vormt een essentiële voorwaarde voor elke postkwantummigratie. Deze stap heeft tot doel een nauwkeurige kennis van de blootstelling aan kwantumrisico's vast te stellen en het transitieproces te structureren. Deze fase beoogt de volgende doelstellingen:

- Bepalen welke middelen met prioriteit moeten worden gemigreerd op basis van hun operationele kritikaliteit en kwantumkwetsbaarheid;
- De bestaande afhankelijkheden in kaart brengen binnen het technologisch ecosysteem van de operator;
- Anticiperen op de mogelijke gevolgen van de migratie voor de continuïteit van de diensten en prestaties.

25. De operatoren kunnen de volgorde en de gedetailleerdheid van de beoordelingsactiviteiten aanpassen aan hun operationele beperkingen. In de praktijk kunnen verschillende beoordelings- of informatievergaringsactiviteiten gelijktijdig worden uitgevoerd. Een gefaseerde aanpak, te beginnen met de analyse van de meest kritieke systemen, is een aanvaardbare strategie om het proces in gang te zetten en tegelijkertijd snel waarde te genereren.

3.1.1 Inventaris van de cryptografische activa

26. Een doeltreffende inventarisatieaanpak is gebaseerd op een gestructureerde strategie voor het ontdekken/verkennen van de activa, die alle contexten van cryptografisch gebruik omvat: de broncode en geïntegreerde bibliotheken, de operationele systemen en geïmplementeerde applicaties, evenals het netwerkverkeer en de communicatieprotocollen.

27. De formalisering van de resultaten in een gestandaardiseerd formaat zoals de Cryptographic Bill of Materials (afgekort als "CBOM") vergemakkelijkt de analyse, het delen en het bijhouden van de inventaris. Automatisering van de ontdekking, waar technisch mogelijk, verbetert de betrouwbaarheid en volledigheid van het proces en vermindert de operationele belasting.

28. Voor de telecomoperatoren maakt een geprioriteerde aanpak het mogelijk om zich te concentreren op de meest kritieke elementen: corenetwerkinfrastructuren, signaalprotocollen, toegangsnetwerkinterfaces en beheersystemen die risico lopen.

29. De operatoren moeten:

- Beschikken over een geformaliseerd cryptografisch beleid waarin de regels voor het beheer van cryptografische activa zijn vastgelegd;
- Een volledige en actuele inventaris bijhouden van hun cryptografische activa die hun gehele infrastructuur bestrijkt;
- De cryptografische afhankelijkheden met hun technologische leveranciers en partners documenteren;
- Deze inventaris regelmatig herzien om de ontwikkelingen in hun omgeving weer te geven.

3.1.2 Kwantumrisicoanalyse

30. Een gestructureerde analyse van kwantumrisico's is gebaseerd op de beoordeling van verschillende dimensies: de intrinsieke kwetsbaarheid van cryptografische primitieven ten opzichte van kwantumalgoritmen, de potentiële impact van een operationele inbreuk, en de complexiteit van migratie naar post-kwantumalternatieven.

31. Methodologieën zoals deze ontwikkeld door het TNO (TNO, Manon de Vries, Sven Bootsma, Vincent Dunning, and Marc van Vliet., 2024) of de sectorale richtlijnen van de GSMA (GSMA, 2023) bieden beoordelingscriteria en beslissingsondersteunende instrumenten voor een beter beheer van kwantumrisico's. Het gebruik van deze gestructureerde benaderingen maakt het mogelijk de analyse te systematiseren en te zorgen voor de consistentie van de beoordelingen bij de prioritering van migratieacties.

32. De samenwerking met experts op het gebied van kwantumcryptografie en het raadplegen van de aanbevelingen van normalisatie-instellingen versterken de kwaliteit en relevantie van de analyse.

33. De operatoren moeten:

- Een kwantumrisicoanalyse uitvoeren voor al hun geïnventariseerde cryptografische activa;
- De kritikaliteiten rangschikken om prioriteiten te stellen voor de migratieacties;
- De redenen en criteria voor de genomen besluiten vastleggen;
- Deze analyse bijwerken naarmate de kwantumdreiging evolueert en de infrastructuur verandert.

3.2 Fase 2: planning van de migratie

34. De migratieplanning structureert de transitie naar post-kwantumcryptografiesystemen door de prioriteiten, middelen en deadlines te definiëren. In deze fase worden de juiste migratiestrategieën voor elke activaklasse vastgesteld en wordt de noodzakelijke coördinatie met het technologische ecosysteem tot stand gebracht.

35. Een doeltreffende planning is afhankelijk van de oprichting van een speciaal team met een geïdentificeerde migratiebeheerder, de toewijzing van de nodige budgettaire en technische middelen en de vaststelling van een schema dat rekening houdt met systeemeigen afhankelijkheden (AIVD-CWI-TNO, 2024). De definitie van migratiestrategieën aangepast aan de specifieke kenmerken van elk element (hybride aanpak, tijdelijke isolatie, vervanging van hardware) optimaliseert de efficiëntie van het proces.

36. De operatoren moeten:

- Officieel een post-kwantummigratieverantwoordelijke aanwijzen, die een multidisciplinair overzicht heeft op de organisatie;
- Een gedocumenteerd migratieplan opstellen met prioriteiten op basis van de analyse van kwantumrisico's van fase 1;
- Voor elk kritiek actief een migratiestrategie definiëren (hybride[6], directe vervanging, isolatie).

3.3 Fase 3: de migratie uitvoeren

37. Bij de uitvoering van de migratie worden de strategieën toegepast die tijdens de planning werden gedefinieerd, waarbij de nadruk ligt op benaderingen die operationele risico's tot een minimum beperken. In deze fase dient bijzondere aandacht besteed te worden aan de validering van de uitgerolde oplossingen en aan het behoud van de continuïteit van de dienstverlening.

38. Het post-kwantummigratieproces moet de cryptografische veerkracht gedurende de ganse transitiefase handhaven en versterken. Deze veerkracht is gebaseerd op een diepgaande verdediging, langetermijnbeveiliging (anticipatie op cryptanalytische ontwikkelingen) en cryptografische flexibiliteit (snelle vervanging van de primitieven volgens de beveiligingsaanbevelingen).

39. De operatoren moeten:

- De volgorde van prioriteit die tijdens de kwantumrisicoanalyse is vastgesteld, in acht nemen;
- Een traceerbaarheidsregister bijhouden waarin elke migratie met data en versies wordt gedocumenteerd;
- De conformiteit en interoperabiliteit valideren voorafgaand aan de inproductiename van elke post-kwantumoplossing.

[6] Hybridisatie: een aanpak die tegelijkertijd post-kwantumalgoritmen combineert met bewezen klassieke cryptografische algoritmen om de risico's die verbonden zijn aan de relatieve nieuwigheid van de nieuwe cryptografische primitieven, te beperken en tegelijk bescherming te bieden tegen de kwantumdreiging. Met name aanbevolen door het ANSSI en BSI.

3.4 In kaart brengen van de GSMA-aanbevelingen en vereisten vastgesteld door het BIPT

40. In dit hoofdstuk worden de aanbevelingen die de GSMA in het kader van haar richtlijnen doet, gekoppeld aan de minimumvereisten die het BIPT in dit document heeft vastgesteld.

	AANBEVELINGEN VAN DE GSMA (GSMA, 2023)	BIPT-VEREISTEN
GOVERNANCE	Bewustmaking op besluitvormingsniveau: bewustwording van de kwantumdreiging creëren bij het algemene management en de raad van bestuur	De operatoren moeten: ▪ Het migratieproces onmiddellijk initiëren. Elke vertraging bij het nemen van deze maatregel vormt een schending van de veiligheidsverplichtingen, ▪ Een governance invoeren die is gericht op de kwantumrisico's, ▪ De rollen en verantwoordelijkheden met betrekking tot de PQC-migratie en de voorbereiding ervan definiëren.
	Organisatorisch governanceproces: een transversaal governanceproces invoeren voor het kwantumrisicobeheer.	
	Uitvoerende verantwoordelijkheid: officieel een post-kwantummigratieverantwoordelijke aanwijzen, die een multidisciplinair overzicht heeft op de organisatie;	

	AANBEVELINGEN VAN DE GSMA (GSMA, 2023)	BIPT-VEREISTEN
ORGANISATORISCHE CAPACITEIT	Ontwikkeling van de competenties: de organisatorische capaciteiten ontwikkelen om kwantumrisico's en post-kwantumtransitie te beheren	De operatoren moeten: ▪ Ervoor zorgen dat hun teams over de nodige kennis beschikken om de migratie aan te sturen en continu technologisch toezicht houden op ontwikkelingen in post-kwantumstandaarden en opkomende kwetsbaarheden.
	Opleiding en bewustmaking: de opleidingsprogramma's bijwerken om het inzicht in de kwantumuitdagingen in de telecomcontext te verbeteren	
	Technologisch toezicht: follow-up van de ontwikkeling van tools die de transitie vergemakkelijken, met name hybride oplossingen en standaarden.	

	AANBEVELINGEN VAN DE GSMA (GSMA, 2023)	BIPT-VEREISTEN
RISICOBEHEER	Risicobeheerkader: de bestaande risicobeheermethodologie aanpassen om specifiek de kwantumrisico's te integreren Analyse van de kwantumrisico's: een uitgebreide en uiterst nauwkeurige kwantumrisicoanalyse uitvoeren voor alle geïnventariseerde cryptografische middelen Beheer van de restrisico's: de restrisico's identificeren en beheren tijdens en na de transitie	De operatoren moeten: ▪ Beschikken over een geformaliseerd cryptografisch beleid dat de governanceregels voor cryptografische activa definieert, ▪ Een kwantumrisicoanalyse uitvoeren voor al hun geïnventariseerde cryptografische activa; ▪ Deze inventaris periodiek evalueren om de ontwikkelingen in hun omgeving te weerspiegelen, ▪ Deze analyse bijwerken naarmate de kwantumdreiging evolueert en de infrastructuur verandert.

	AANBEVELINGEN VAN DE GSMA (GSMA, 2023)	BIPT-VEREISTEN
TRANSITIEPLANNING	Cryptografische inventaris: een volledige en actuele inventaris bijhouden van de cryptografische middelen die de gehele infrastructuur bestrijkt Gegevensclassificatie: de cryptografische afhankelijkheden met de leveranciers en technologiepartners documenteren door de beveiligingsvereisten en de levensduur van gegevens te identificeren Prioritering: een kritikaliteitsindeling maken zodat de migratiemaatregelen kunnen worden geprioriteerd op basis van de kwantitatieve risicoanalyse. Transitieplan: een gedocumenteerd migratieplan opstellen waarin de prioriteiten en migratiestrategieën voor elk kritiek actief worden gedefinieerd, met inachtneming van de vastgelegde sectorale tijdschema's	De operatoren moeten: ▪ Een volledige en actuele inventaris bijhouden van hun cryptografische activa die hun gehele infrastructuur bestrijkt; ▪ Deze inventaris periodiek herzien om rekening te houden met de ontwikkelingen in hun omgeving; ▪ De cryptografische afhankelijkheden met hun technologische leveranciers en partners documenteren; ▪ De kritikaliteiten rangschikken om prioriteiten te stellen voor de migratieacties; ▪ De analyses en indien nodig het migratieplan actualiseren naarmate de kwantumdreiging zich ontwikkelt en de infrastructuur verandert; ▪ De redenen en criteria voor de genomen besluiten documenteren.

4. Timeline

41. De post-kwantumtransitie kadert binnen een gecoördineerd Europese tijdschema.

42. Aanbeveling (EU) 2024/1101 (Commission Européenne) en de werkzaamheden van de EU PQC Workstream (NIS Cooperation Group, 2025) bieden een tijdskader voor het structureren van deze transitie op Europees niveau, met als doelstellingen de uitwerking van nationale routekaarten tegen 2026.

43. De Europese tijdlijn die door de EU PQC Workstream werd uitgewerkt (NIS Cooperation Group, 2025), beschrijft een driestappenplan om kwantumveerkracht te bereiken.

    De initiatiefase, die reeds in gang is gezet overeenkomstig de gezamenlijke verklaring van 18 lidstaten "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography", markeert de gecoördineerde start van de transitie.

    Tegen 2026 moeten de PQC-transitieplanning en de pilotprojecten voor de gebruikssituaties met een hoog en middelhoog risico worden gestart.

    De cruciale stap in 2030 bestaat in de voltooiing van de PQC-transitie voor gebruikssituaties met een hoog risico, waarbij standaard software- en firmware-updates met kwantumbeveiliging worden geactiveerd. Dit proces eindigt in 2035 met als doelstelling een volledig kwantumveerkrachtige Europese infrastructuur.

44. Op basis van dit Europese tijdschema werden voor de Belgische telecommunicatiesector de volgende doelstellingen en termijnen vastgesteld:

    - Deadline 1 - Evaluatie (vandaag): voltooiing van de cryptografische inventarisatie en de kwantumrisicoanalyse ;
    - Deadline 2 - Planning (2026-2027): ontwikkeling en validering van de post-kwantummigratieplannen;
    - Deadline 3 - Tenuitvoerbrenging (2027- 2030): progressieve uitrol van de post-kwantumoplossingen volgens de vastgestelde prioriteiten.

45. Dit sectorale tijdschema vormt de vertaling van de Europese doelstellingen voor de kritieke telecommunicatie-infrastructuur en garandeert een gecoördineerde en geharmoniseerde transitie.

4.1 Monitoringtijdlijn

46. Om ervoor te zorgen dat deze doelstellingen worden bereikt, wordt voorzien in een monitoringmechanisme. Dit monitoringtijdschema zorgt ervoor dat de nationale inspanningen worden gebundeld om tegen 2035 het gemeenschappelijke doel van kwantumveerkracht te bereiken.

47. 2026 - 2027 -- Verificatie van de grondslag:

- De inventaris van de cryptografische activa controleren;
- Validering van de kwaliteit van de kwantumrisicoanalyses;
- Evaluatie van de vastgelegde migratieplannen.

48. 2028 - 2030 – Controle van de kwantumrisicobeheersystemen:

- Controle van de tenuitvoerbrenging van de kwantumrisicobeheersystemen;
- Toezicht houden op de voortgang van de kritieke migraties;
- Evaluatie van de post-kwantumgovernance.

49. 2031 - 2035 -- Inspectie van de systemen met hoog risico:

- Gerichte controle: "Quantum-Secure or not?";
- Verificatie van de migratie van de prioritaire activa.

Figuur 4. MONITORINGTIJDLIJN

Referenties

AIVD-CWI-TNO. (2024). *The PQC Migration Handbook - guidelines for migrating to post-quantum cryptography.* Url: TNO-2024-pqc-en.pdf

Commission Européenne. (n.d.). RECOMMANDATION (UE) 2024/1101 DE LA COMMISSION du 11 avril . Url: Recommandation 2014 1101 feuille de route

Coomans, W., Schoinianakis, D., Sohn, R., Chenard, S., Banerjee, A., & Charbonneau, M. (2025). The road to quantum-safe networks. Nokia Bell Labs. Url: Nokia: The road to quantum-safe networks

Elaine Barker (NIST), Lily Chen (NIST), David Cooper (NIST), Dustin Moody (NIST), Andrew Regenscheid (NIST), Murugiah Souppaya (NIST), William Newhouse (NIST), Russ Housley (Vigil Security), Sean Turner (sn3rd). (2025). Considerations for Achieving Cryptographic Agility: Strategies and Practices. Url: NIST CSWP 39 second public draft, Considerations for Achieving Crypto Agility: Strategies and Practices

ETSI. (2020). Migration strategies and recommendations to Quantum Safe schemes. Url: TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes

GSMA. (2023). *Guidelines for quantum risk management for telco v1.0.* Url: Guidelines for Quantum Risk Management for Telco

GSMA. (2023). *Post quantum Telco Network Impact Assessment - Whitepaper Version 1.0.* Url: PQTN_1_Doc_006 PQTN White Paper

NIS Cooperation Group. (2025). *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.* Url: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future

TNO, Manon de Vries, Sven Bootsma, Vincent Dunning, and Marc van Vliet. (2024). *Quantum risicomethodologie.* TNO. Retrieved from Url: Quantum risicomethodologie voor cryptografie