Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3945 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 mei 2024

Overeenkomstig de bestaande afspraken ontvangt u hierbij 2 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Aanbeveling Routekaart Post-Quantumcryptografie
Fiche: Mededeling biotechnologie en biofabricage (Kamerstuk 22 112, nr. 3946)

De Minister van Buitenlandse Zaken,
H.G.J. Bruins Slot

kst-22112-3945
ISSN 0921 - 7371
's-Gravenhage 2024

Fiche: Aanbeveling Routekaart Post-Quantumcryptografie

1. Algemene gegevens

a) *Titel voorstel*
Aanbeveling van de Commissie over een routekaart voor een gecoördineerde uitvoering van de transitie naar post-quantumcryptografie
b) *Datum ontvangst Commissiedocument*
11 april 2024
c) *Nr. Commissiedocument*
C(2024)2393
d) *EUR-Lex*
https://eur-lex.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401101&qid=1713797897850
e) *Nr. impact assessment Commissie en Opinie*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad Vervoer, Telecommunicatie en Energie (Telecommunicatie)
g) *Eerstverantwoordelijk ministerie*
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

2. Essentie voorstel

De Europese Commissie (hierna: Commissie) herkent de dreiging die een toekomstige quantumcomputer met zich meebrengt ten aanzien van de cyberveiligheid en de huidige versleutelingsmethoden (cryptografie). De Commissie houdt er rekening mee dat quantumcomputers in de toekomst de huidige versleutelingstechnologieën (mogelijk) kunnen kraken. Hierbij ziet de Commissie urgentie om oplossingen te vinden die de vertrouwelijkheid en integriteit van informatie en de bescherming van gevoelige communicatie op de lange termijn kunnen waarborgen. De Commissie adviseert dit te bereiken door middel van een spoedige transitie naar post-quantumcryptografie: nieuwe soorten cryptografie die niet kwetsbaar zijn voor aanvallers die over een quantumcomputer beschikken.

De Commissie moedigt in de aanbeveling de lidstaten aan om in onderlinge samenwerking een strategie, welke leidt tot een routekaart, te ontwikkelen ten behoeve van de transitie naar post-quantumcryptografie voor een gecoördineerde en gesynchroniseerde transitie onder de lidstaten. De routekaart moet als blauwdruk dienen voor de bepaling van de nationale plannen voor de transitie naar post-quantumcryptografie, of indien die plannen reeds bestaan, voor de afstemming ervan op de routekaart. Twee jaar na de publicatie van deze aanbeveling van de Commissie dient de routekaart beschikbaar te zijn en moet deze worden gevolgd. De lidstaten zouden echter nu al moeten beginnen met passende en evenredige maatregelen om zich voor te bereiden.

Daarnaast worden lidstaten aangemoedigd om hun acties te coördineren via een op te richten toegewijd lidstatenforum. Dit forum kan vertegenwoordigers bevatten van nationale (cyber)beveiligingsautoriteiten en cybersecurityexperts van nationale cybersecurityautoriteiten en het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA).

Tegelijkertijd adviseert de Commissie om gemeenschappelijke Europese standaarden[1] te ontwikkelen en een kader om post-quantumcryptografie-algoritmen binnen de Europese Unie vast te stellen en te selecteren.

[1] Met «standaarden» wordt hier bedoeld: regels waaraan een bepaalde technologie of product moet voldoen.

Ook op Unieniveau worden maatregelen getroffen. De Commissie zal de werkzaamheden omtrent post-quantumcryptografie in het kader van haar aanbeveling periodiek monitoren en beoordelen. Daartoe kan zij informatie opvragen bij de lidstaten en indien nodig aanvullende maatregelen voorstellen aan de lidstaten, zoals voorstellen van bindende handelingen van het Unierecht. Tot slot beoordeelt de Commissie uiterlijk drie jaar na publicatie van deze aanbeveling de gevolgen van haar aanbeveling, in samenwerking met de lidstaten.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Digitale weerbaarheid heeft de aandacht van het kabinet, om digitale dreigingen nu en in de toekomst het hoofd te kunnen bieden. Het kabinet ziet quantumveilige cryptografie als belangrijk element van digitale weerbaarheid omdat het de vertrouwelijkheid en integriteit van informatie beschermt tegen kwaadwillenden. Daarom werkt het kabinet op dit moment aan een visie en bijbehorend beleid op het gebied van post-quantumcryptografie voor informatiebeveiliging. De uitwerking hiervan valt binnen de I-Strategie Rijk. Een van de thema's daarin is digitale weerbaarheid.[2] Binnen het thema digitale weerbaarheid wordt een routekaart met een aantal projecten en programma's gevolgd. De stuurgroep Digitale Weerbaarheid stuurt op (de uitvoering van) deze routekaart. Een van de programma's binnen de routekaart is Quantumveilige Cryptografie Rijksoverheid. Dit programma werkt het beleid op de transitie naar post-quantumcryptografie uit.[3]

In 2021 is in Nederland het Rijksbrede programma Quantumveilige Cryptografie Rijk opgestart om daarmee een Rijksbrede transitie naar quantumveilige cryptografie te faciliteren en aan te jagen. Dit samenwerkingsprogramma valt onder Chief Information Office Rijk (CIO Rijk). Het doel van dit programma is om de Rijksoverheid te helpen om risico's van quantumtechnologie op cryptografie op tijd beheersbaar te maken en coördinatie te faciliteren. Ook treedt dit programma naar buiten, onder andere richting medeoverheden en vitale partijen.
Binnen dit programma houden een kernteam en werkgroepen met brede samenstelling zich bezig met de verschillende aspecten van de transitie zoals bewustwording en kennisopbouw, ondersteuning met behulp van beleid, kaders en handreikingen.

Daarnaast is er binnen de Rijksoverheid sinds 2014 al aandacht voor de dreiging van de quantumcomputer en is door de jaren heen een aantal brochures gepubliceerd over het onderwerp. In 2023 is een handleiding[4] gepubliceerd met daarin de te nemen stappen in de transitie naar een quantumveilige organisatie op basis van post-quantumcryptografie. Op basis daarvan hebben NCSC en AIVD ook een handreiking gepubliceerd.[5]

Het voorbereiden op quantumveilige cryptografie maakt inherent deel uit van de Nederlandse Cybersecuritystrategie 2022–2028 (NLCS[6]). De NLCS stelt dat cybersecuritykennis en -kunde moet worden versterkt om de digitale veiligheid van Nederland nu en in de toekomst te kunnen

---

[2] Thema 2, https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/i-strategie-rijk-2021-2025/digitale-weerbaarheid/

[3] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/

[4] PQC Migratiehandboek (https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-transitie-handboek)

[5] https://www.aivd.nl/documenten/publicaties/2023/09/18/jenv-maak-je-organisatie-quantumveilig

[6] Nederlandse Cybersecuritystrategie 2022–2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

beschermen. Intensieve innovatiesamenwerking tussen overheid, bedrijfsleven en kennisinstellingen is hiervoor essentieel. Het door het kabinet opgerichte samenwerkingsplatform dcypher speelt hier een rol in en legt de basis voor publiek-private onderzoeks- en innovatietrajecten. Dit platform voert een routekaart cryptocommunicatie uit waarin transitie naar post-quantumcryptografie veel aandacht krijgt en publicaties oplevert.

Tevens vormt post-quantumcryptografie een van de prioritaire onderwerpen in de agenda voor *Cybersecurity Technologies* onder de Nationale Technologiestrategie (NTS) die op dit moment voorbereid wordt voor publicatie aan de Tweede Kamer.

De transitie naar post-quantumcryptografie is niet alleen voor de Rijksoverheid en andere overheden van belang, maar ook voor organisaties in de vitale sectoren. Het kabinet acht het van belang om de transitie ook aan te jagen bij deze sectoren. Ook werkt de crypto-industrie actief aan kennisopbouw en voorbereidingen op de transitie naar post-quantumcryptografie.

Op dit moment werkt Nederland al met andere lidstaten samen in de transitie naar quantumveilige cryptografie op basis van post-quantumcryptografie. Dit gebeurt zowel door langlopende samenwerkingen vanuit organisaties zoals het Ministerie van Economische Zaken en Klimaat, het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD en het NCSC, alsook vanuit het programma Quantumveilige Cryptografie Rijk.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet staat positief tegenover de meerderheid van de voorgestelde acties uit de aanbeveling van de Commissie om de transitie EU-breed aan te pakken. Dit is mede doordat de aanbeveling in feite een uitbreiding is van de Rijksbrede transitie waar Nederland nu al op inzet. Wanneer dit niet EU-breed gedaan wordt, zal dit leiden tot een ongelijke transitie, met het risico dat er zwakke plekken in de EU ontstaan ten aanzien van de digitale veiligheid. Het initiatief van de Commissie komt overeen met de aanpak van het kabinet op coördinatie, inzet van expertisecentra en het gebruik van EU-breed gesteunde standaarden. Daarom omarmt het kabinet het voorstel van de Commissie om de transitie gezamenlijk vorm te geven.

Het kabinet is op dit moment ook al bezig met de voorbereidende werkzaamheden voor de transitie, zoals de Commissie vraagt.[7] Het kabinet is zich ervan bewust dat Nederland een vliegende start heeft ten aanzien van de plannen van de Commissie en wil deze voorsprong ook behouden.

Er zijn twee belangrijke verschillen van inzicht tussen het kabinet en de Commissie. Het eerste verschil van inzicht is de inhoudelijke betekenis van hybride cryptografische constructies. De Commissie verstaat onder hybride constructies de combinatie van post-quantumcryptografie met de huidige cryptografie of post-quantumcryptografie met *Quantum Key Distribution*. Dit is een methode die gebruikmaakt van quantumtechnologie om cryptografische sleutels te genereren en uit te wisselen. Het kabinet is negatief over dit onderdeel van de aanbeveling. Het kabinet verstaat onder hybride cryptografische constructies alleen de combinatie

[7] PQC Migratiehandboek (https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-transitie-handboek)

van post-quantumcryptografie met de huidige cryptografie.[8] Hybride cryptografische constructies zijn een belangrijke bouwsteen voor de transitie naar quantumveilige cryptografie.

Ten tweede ziet het kabinet geen rol voor *Quantum Key Distribution* (QKD) in hybride cryptografische constructies.[9] *Quantum Key Distribution* kan naar het oordeel van het kabinet geen onderdeel zijn van de routekaart, omdat er nog te veel open onderzoeksvragen zijn die nog niet in de komende twee jaar beantwoord zullen zijn. Ook zal er binnen twee jaar nog geen standaardisatie plaatsvinden van *Quantum Key Distribution* omdat daarvoor de technologie nog niet volwassen genoeg is en een dergelijk standaardisatieproces jaren zal gaan duren. Het kabinet zal dit aankaarten bij de Commissie.

Naast de twee verschillen van inzicht ziet het kabinet ook nog ruimte voor vijf aanvullingen voor de aanbeveling. Ten eerste volgt het kabinet op dit moment de bestaande initiatieven met betrekking tot post-quantum-cryptografie van standaardisatieorganisaties, zoals ISO, NIST en IETF. Het kabinet adviseert om de standaarden van deze organisaties leidend te laten zijn voor de EU-breed gesteunde standaarden. In overleg met andere Europese verbindingsbeveiligingsautoriteiten, waaronder de *Appropriately Qualified Authorities* (AQUA)[10] en andere samenwerkingspartners dient een breed draagvlak gecreëerd te worden voor de standaarden van ISO, NIST en IETF.

Ten tweede is het voor het kabinet belangrijk dat de routekaart naar post-quantumcryptografie aanpasbaar is, onder andere omdat de technologie nog volop in beweging is en er dus ook nog geen definitieve EU-breed gedeelde post-quantumcryptografie standaarden zijn. Deze worden naar verwachting gefinaliseerd in 2024. Het kabinet raadt de Commissie aan om aanpassingen aan de routekaart te laten geschieden op basis van verzoeken van het lidstatenforum en met instemming van de daartoe nationaal aangewezen autoriteiten (de hiervoor genoemde AQUA's).

Ten derde acht het kabinet het belangrijk dat de Europese routekaart in lijn is met de Nederlandse risico-gebaseerde aanpak van de transitie naar post-quantumcryptografie, zodat het Nederlands en Europese beleid elkaar versterken in plaats van tegenwerken. Het kabinet zal zich er daarom voor inzetten dat de routekaart hierbij aansluit.

Ten vierde wordt in de aanbeveling van de Commissie het belang van investeringen in onderzoek en innovatie nog onvoldoende belicht. Kennis en capaciteit voor de transitie naar quantumveilige cryptografie is schaars. Daarom moet de routekaart die de Commissie voorstelt zich ook richten op het ontwikkelen van capaciteit en competenties in de arbeidsmarkt om de transitie praktisch mogelijk te maken. De ontwikkeling van meer kennis en innovatie rondom dit onderwerp is essentieel om voorbereid te zijn op toekomstige dreigingen. Dit is ook nodig om de concurrentiepositie van de EU, en daarmee van Nederland, op dit onderwerp te verbeteren en afhankelijkheden van buitenlandse partijen te voorkomen. Om die reden zal kennis en innovatie een belangrijk

---

[8] Zoals benoemd in de antwoorden op Kamervragen (Aanhangsel Handelingen II 2021/22, nr. 4064), pagina 4.

[9] *Quantum Key Distribution* is een nieuwe technologie waar nog veel onderzoek naar verricht moet worden. Op dit moment biedt het echter onvoldoende beveiligingswaarde en kan het niet worden ingezet voor informatiebeveiliging, met het oog op de urgente quantumdreiging. Zie ook de recente publicatie «*Position Paper on Quantum Key Distribution*».

[10] *Appropriately Qualified Authorities* zijn de landen die cryptoproducten voor EU-gerubriceerde informatie kunnen goedkeuren voor gebruik binnen de EU.

onderwerp zijn in de ontwikkeling van de routekaart en is financiering hiervoor nodig vanuit programma's zoals de Digital Europe Programma (DEP) en Horizon Europe. Het kabinet zal zich hiervoor inzetten.

Ten vijfde erkent het kabinet dat nieuwe cryptografische inzichten kunnen resulteren in kwetsbaarheden in bepaalde cryptografische systemen. Het is daarom van belang om mogelijke risico's te blijven identificeren en in te zetten op wendbaarheid van cryptografie, ook wel *crypto-agility* genoemd. Hierdoor blijven systemen functioneren als de onderliggende cryptografie wordt vervangen.[11]

Al met al zal het kabinet zich ervoor inzetten dat de aanbeveling, met uitzondering van het gedeelte over constructies met *Quantum Key Distribution*, van de Commissie uitgevoerd zal worden. Dit zal gebeuren door de overheid in samenwerking met andere lidstaten, onder andere door middel van het voorgestelde lidstatenforum. Daarnaast zal het kabinet zorgen voor een afvaardiging in dit lidstatenforum, waarin zij onder andere kennis zal delen. Ook zal personele inzet geborgd worden, zowel voor coördinatie binnen Europa, als ook voor de vormgeving van de transitie in Nederland, en het bijdragen aan standaardisatie-initiatieven.

c) Eerste inschatting van krachtenveld

Het Nederlandse standpunt met betrekking tot noodzaak en urgentie van de transitie wordt door andere lidstaten gedeeld met als doel een gecoördineerde transitie. De samenwerkingen met andere lidstaten hebben ook al geleid tot gezamenlijke en overeenkomende onderzoeken[12] en publicaties[13] en gedeelde standpunten.

De Duitse, Franse, Zweedse en Nederlandse verbindingsbeveiligingsautoriteiten hebben een gezamenlijk visie op de inzet van transitie naar post-quantumcryptografie gepubliceerd in een *position paper.*[14] In dit paper wordt geadviseerd om hybride cryptografische constructies te gebruiken, waarin huidige cryptografie gecombineerd wordt met post-quantumcryptografie, en voorlopig nog geen gebruik te maken van *Quantum Key Distribution*. Voor zover bekend is er geen Europese verbindingsbeveiligingsautoriteit met een andere visie.

De positie van het Europees Parlement is nog niet duidelijk. Wel heeft een aantal Europarlementariërs een brandbrief gestuurd naar de Commissie met een oproep om de transitie naar post-quantumcryptografie te starten.[15]

---

[11] Expertblog *crypto-agility* (https://www.ncsc.nl/actueel/weblog/weblog/2024/het-crypto-agilitymonster)

[12] HAPKIDO (https://hapkido.tno.nl)

[13] Position Paper on Quantum Key Distribution (https://www.aivd.nl/documenten/publicaties/2024/01/26/position-paper-on-quantum-key-distribution)

[14] https://www.aivd.nl/onderwerpen/informatiebeveiliging/documenten/publicaties/2024/01/26/position-paper-on-quantum-key-distribution

[15] https://www.computable.nl/wp-content/uploads/2024/03/Letter-MEPs-Post-Quantum-Encryption.pdf

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Bevoegdheid

De grondhouding van het kabinet is positief. De aanbeveling maakt zelf niet expliciet duidelijk op welke bevoegdheidsgrond zij gebaseerd is, anders dan artikel 292 VWEU. Op grond van artikel 292 VWEU is de Commissie bevoegd om aanbevelingen vast te stellen op de gebieden waarvoor de EU bevoegd is. Uit de overwegingen kan worden afgeleid dat de aanbeveling met name ziet op de ruimte van vrijheid, veiligheid en recht, en trans-Europese (communicatie)netwerken. Op deze terreinen is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, lid 2, onder h en j, VWEU). Gezien de brede strekking van de aanbeveling alsook het niet-bindende karakter meent het kabinet dat deze aanbeveling de uitsluitende verantwoordelijkheid van elke lidstaat voor de nationale veiligheid, zoals vastgelegd in artikel 4, lid 2 VEU, niet aantast. De Commissie is zodoende bevoegd deze aanbeveling uit te vaardigen.

b) Subsidiariteit

De grondhouding van het kabinet is positief. De aanbeveling van de Commissie heeft tot doel om een routekaart voor een gecoördineerde uitvoering van de transitie naar post-quantumcryptografie vast te stellen. De routekaart beoogt de inzet van lidstaten voor transitie naar post-quantumcryptografie te synchroniseren. Aangezien organisaties meer en meer internationaal opereren en digitaal nauw met elkaar verbonden zijn, kan deze transitie onvoldoende worden verwezenlijkt wanneer deze op lokaal, regionaal en zelfs op nationaal niveau zou worden uitgevoerd. Het kabinet ziet geen minder ingrijpende mogelijke oplossing om hetzelfde resultaat te bereiken; een gezamenlijke EU-aanpak is noodzakelijk. Wanneer dit niet EU-breed gedaan wordt, zal dit leiden tot een ongelijke transitie, met het risico dat er zwakke plekken in de EU ontstaan ten aanzien van de digitale veiligheid. Daarnaast zou het ontbreken van Europees ondersteunde standaarden kunnen leiden tot problemen met interoperabiliteit. Bovendien moet EU-breed worden afgesproken om hybride oplossingen al dan niet te verplichten.

c) Proportionaliteit

De grondhouding van het kabinet is positief. De aanbeveling heeft tot doel om een routekaart voor een gecoördineerde uitvoering van de transitie naar post-quantumcryptografie vast te stellen. Het voorgestelde optreden is geschikt om deze doelstelling te bereiken, mede omdat er aanbevolen wordt om op vrijwillige basis deel te nemen in een op te richten subgroep van de NIS-samenwerkingsgroep. De lidstaten dienen de resulterende routekaart als blauwdruk te gebruiken voor de bepaling van nationale plannen dan wel af te stemmen op de gemeenschappelijke routekaart. De aanbeveling gaat niet verder dan noodzakelijk, omdat een Europese routekaart als blauwdruk voor nationale plannen zorgt voor een gesynchroniseerde Europese aanpak en voldoende ruimte laat voor de lidstaten om een snellere transitie te doorlopen dan vereist volgens de blauwdruk.

d) Financiële gevolgen

De aanbeveling kent geen directe financiële gevolgen anders dan personele deelname van lidstaten aan het voorgestelde lidstatenforum. Mogelijk dient hier extra capaciteit voor geworven te worden. Eventuele

budgettaire gevolgen worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

De Raadsaanbevelingen heeft vooralsnog geen consequenties voor de EU-begroting. Het kabinet is van mening dat, indien nodig, de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Het kabinet wil daarnaast niet vooruitlopen op de integrale afweging van middelen na 2027.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

De aanbeveling bevat geen bindende maatregelen die de regeldruk voor bedrijfsleven, burgers en overheden vergroten. Wel is het kabinet van plan om een of meerdere vertegenwoordigers af te vaardigen naar het lidstatenforum. Ook zal de Commissie toezicht houden op de opvolging van deze aanbeveling. In dat kader kan de Commissie de vertegenwoordigers van de lidstaten verzoeken informatie te verstrekken. Op basis van deze informatie en alle andere beschikbare informatie beoordeelt de Commissie de gevolgen van deze aanbeveling en bepaalt zij of er aanvullende stappen nodig zijn, zoals voorstellen voor bindende handelingen van het Unierecht.

Ook moeten lidstaten uiterlijk drie jaar na bekendmaking van deze aanbeveling samenwerken met de Commissie om de gevolgen van de aanbeveling te beoordelen en de volgende stappen te bepalen.

Het beoogde effect van de aanbeveling op de concurrentiekracht is positief. De aanbeveling draagt bij aan de verdere harmonisering van post-quantumcryptografie in de EU. Daarbij stelt de aanbeveling dat ook samenwerking gezocht moet worden met internationale strategische partners bij de ontwikkelingen van internationale normen om de interoperabiliteit van communicatie ook buiten de EU in de toekomst te waarborgen.

De aanbeveling kent geopolitieke aspecten gezien de dreiging, vanuit statelijke actoren, waaraan de EU en de lidstaten worden blootgesteld wanneer zij onvoldoende zijn voorbereid op de komst van een voldoende krachtige quantumcomputer. In dit kader beoogt de aanbeveling een positieve bijdrage te leveren aan de veiligheid en de open strategische autonomie van de EU.