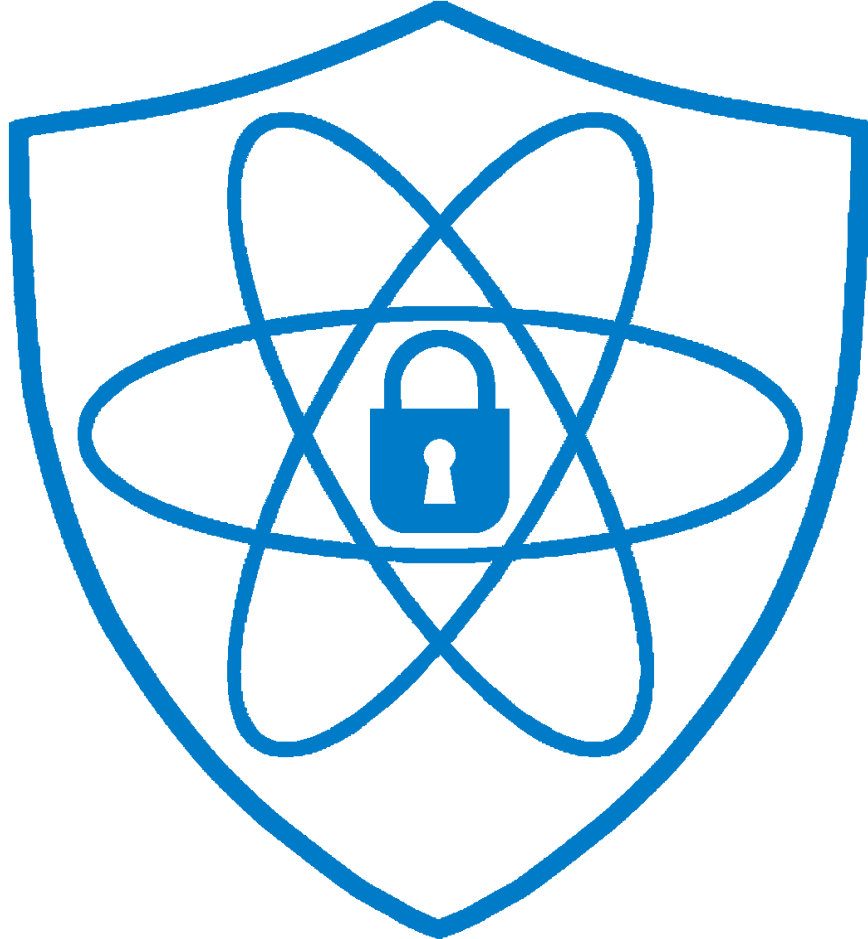


Quantumveilige Cryptografie



NORA, Open huis van de architectuur
5 september 2024



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties



Anita Wehmann BZK

Germain van der Velden IenW



Larissa Kalle NCSC

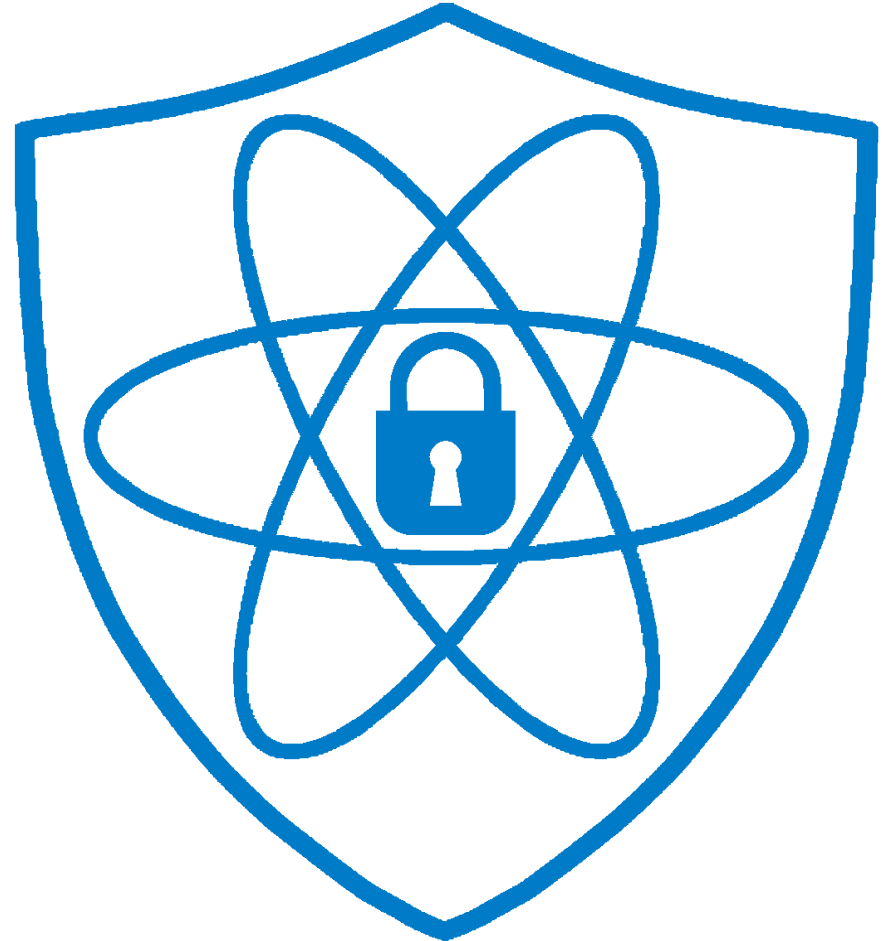
Oscar Koeroo VWS



Agenda



- Wat is er aan de hand: Quantumtechnologie, impact op cryptografie
- Actualiteit, Aanbeveling EU Commissie
- De aanpak: Quantumveilige Cryptografie Rijk
- Interactief: rol van en samenwerking met architectuur





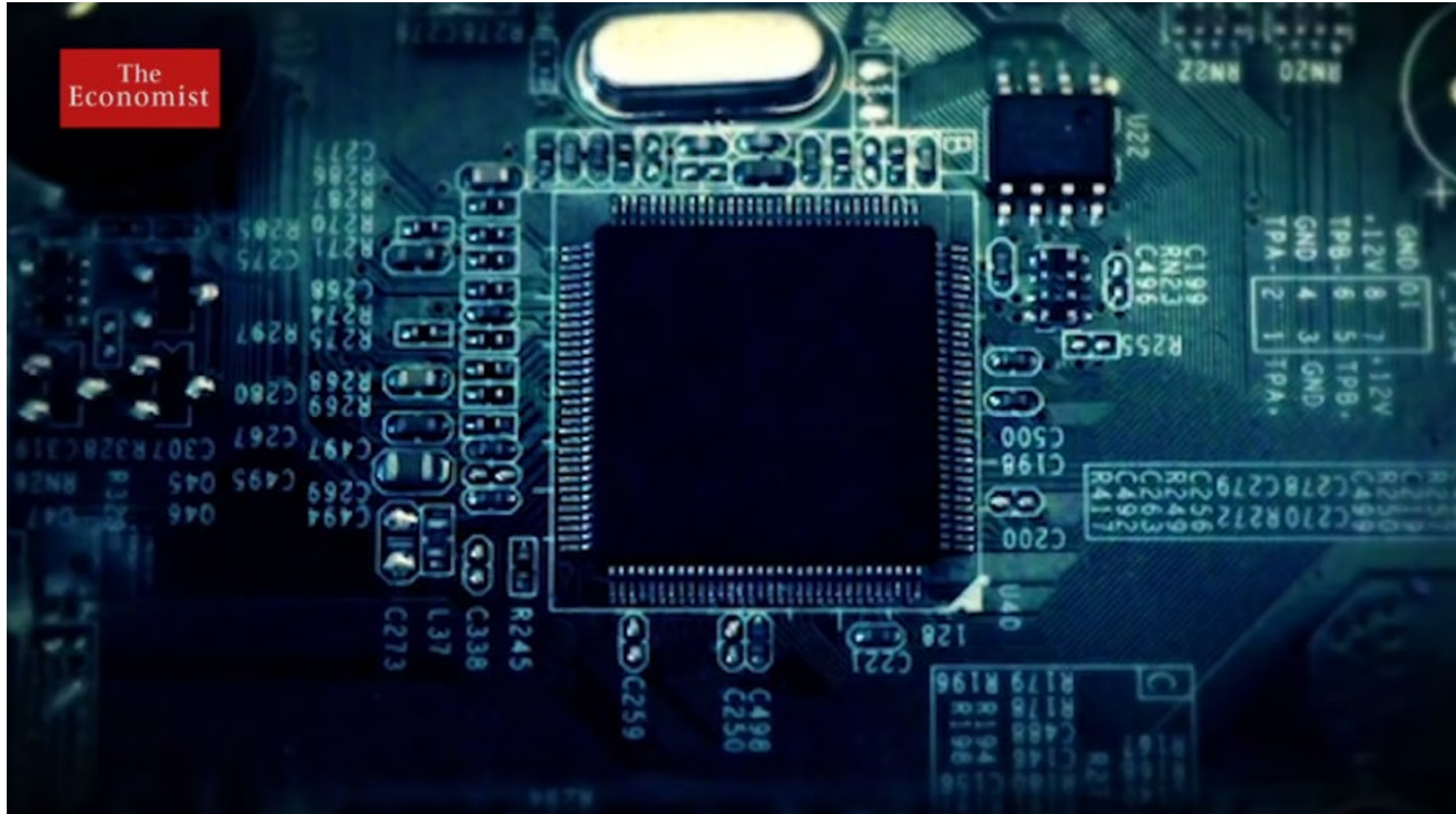
Quantumtechnologie



Kansen en dreiging

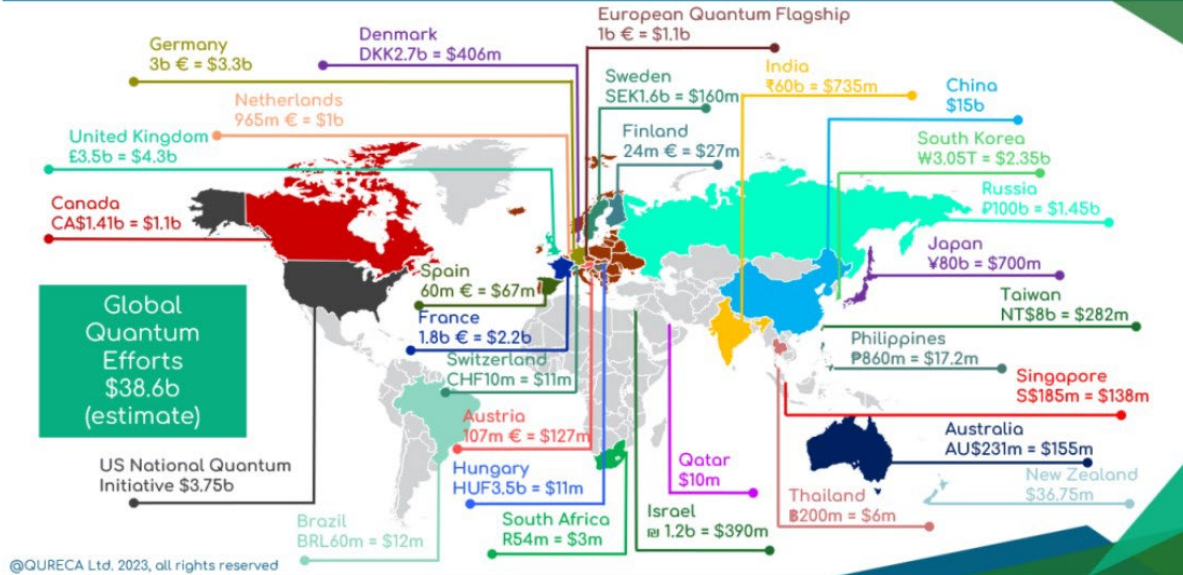
Quantum computer

introductie



> https://www.youtube.com/watch?v=dDOn_n7tNyo

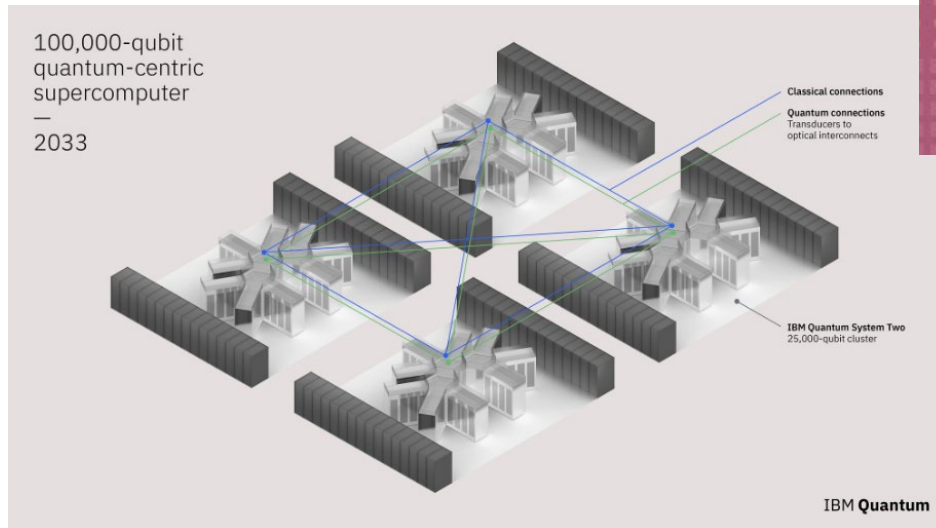
Quantum effort worldwide



Ontwikkelingen gaan snel

QUANTUM EUROPE
Unlocking Innovation Through a Quantum-Enabled Europe
Nov 2024 BRUSSELS

Overview of Quantum Initiatives Worldwide 2023 - Qureca



[IBM Launches \\$100 Million Partnership with Global Universities to Develop Novel Technologies Towards a 100,000-Qubit Quantum-Centric Supercomputer](#)



Asymmetrische cryptografie

Symmetrische cryptografie

**Sleutel
uitwisseling**

ECDHE

Authenticatie

RSA

**Vertrouwelijk-
heid**

AES

Integriteit

SHA256

Uitwisseling van
een sleutel

Bewijst identiteit
met PKI

Versleutelt de
getransporteerde
data

Borgt data
integriteit

Gebroken

Gebroken

50%

?



Impact op cryptografie

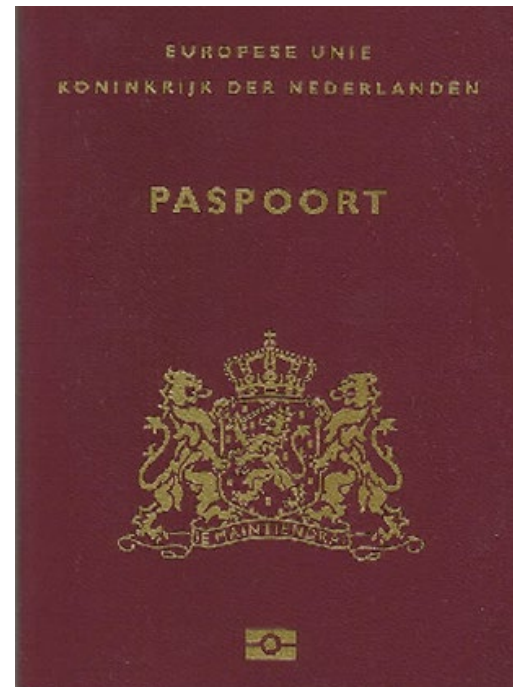
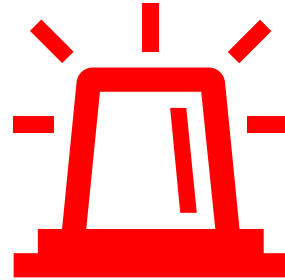
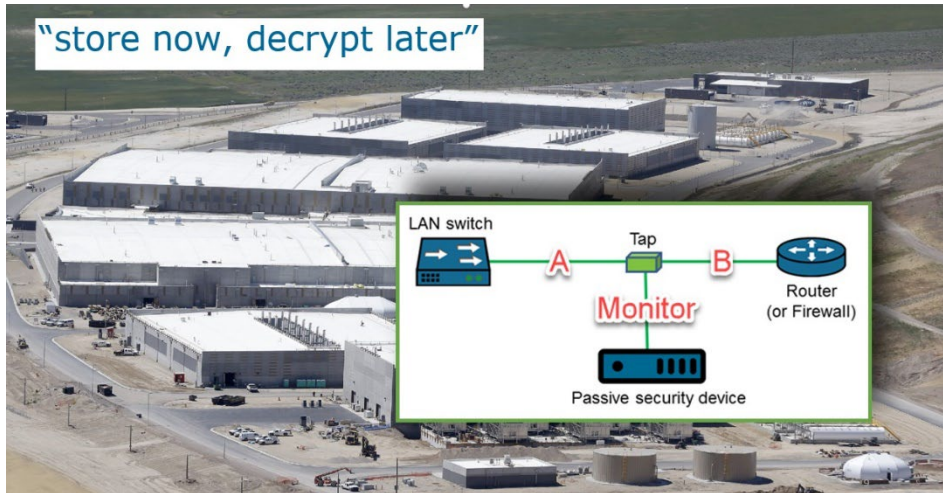


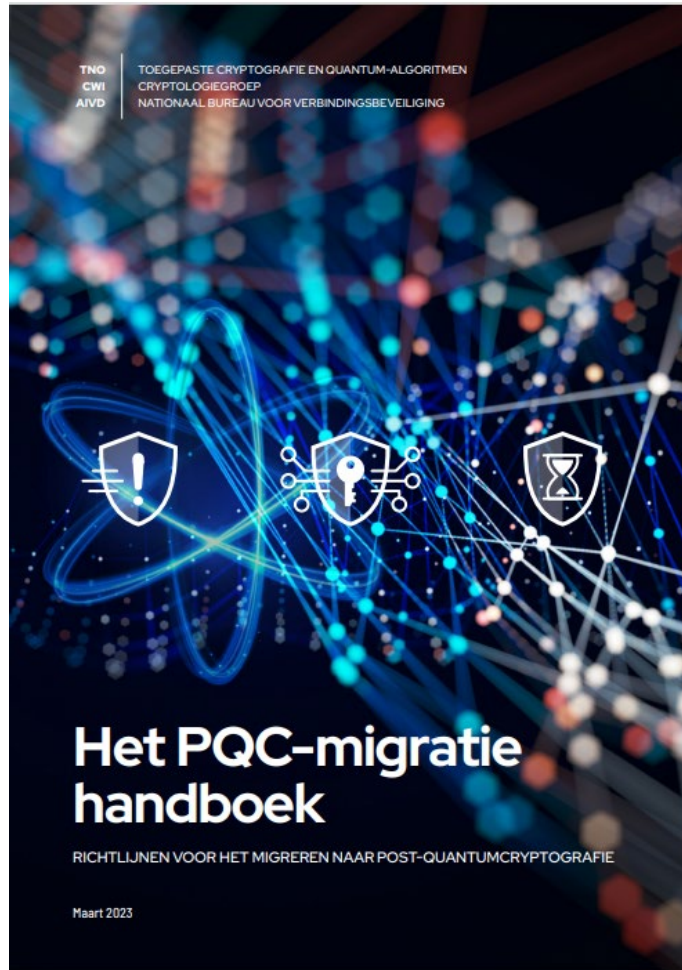
Wat is de betekenis van de impact

De impact van



gebroken cryptografie





[Het PQC-migratie handboek | Publicatie | AIVD](#)

URGENTE ADOPTERS MOETEN NU BEGINNEN:

- > Gevoelige informatie van de organisatie met een lange vertrouwelijkheids-termijn ("store now decrypt later")
- > Persoonlijke informatie met een lange vertrouwelijkheidstermijn: paspoorten
- > Aanbieden van systemen voor de kritieke infrastructuur: betalingsverkeer, energie, transport
- > Aanbieden van systemen met een lange levensduur: waterbeheer, chemische industrie, drinkwater, spoor

Conclusie: de Rijksoverheid is een urgente adopter

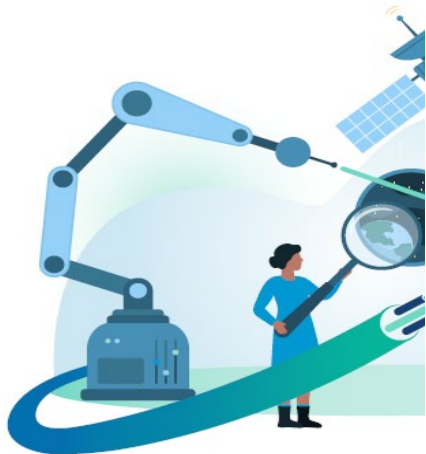
Actualiteiten



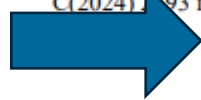
Ministerie van Economische Zaken
en Klimaat



De Nationale Technolo
Bouwstenen voor strategisch technolog



Brussel, 11.4.2024
C(2024) 193 final



AANBEVELING VAN DE COMMISSIE

van 11.4.2024

over een routekaart voor een gecoördineerde uitvoering van de transitie naar post-
kwantumcryptografie

- EU workstream om de doelen van de aanbeveling te realiseren
- Looptijd gepland: sept '24 – april '25
- DE, FR, IT, ES, NL voorzitter
- NL rouwdeur
- routekaart





Doel: transitie naar PQC 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. TOEPASSINGSGEBIED EN DOELSTELLINGEN

- Een routekaart voor gecoördineerde uitvoering van post-kwantumcryptografie vast te stellen - nationale transitieplannen te synchroniseren en waarborgen van grensoverschrijdende interoperabiliteit.
- Vaststelling van PQC algoritmen als Unienormen als onderdeel van de routekaart.
- Maatregelen te nemen om zich op deze transitie voor te bereiden.

2. ROUTEKAART VOOR EEN GECOÖRDINEERDE UITVOERING VAN DE TRANSITIE NAAR POST-KWANTUMCRYPTOGRAFIE

- Aanmoedigen dat de lidstaten hun maatregelen op Eu-niveau via een subgroep coördineren.
- Afstemmen met andere instanties, zoals Europol en de NAVO, om dubbel werk te voorkomen en een samenhangende aanpak van nieuwe uitdagingen te waarborgen.
- De subgroep moet snel worden opgericht en deskundige vertegenwoordigers aan te wijzen die nauw met de Commissie moeten samenwerken voor ontwikkelen en bepalen van de routekaart.
- De routekaart moet over april 2026 beschikbaar zijn, gevolgd door ontwikkeling en aanpassing van de plannen voor de transitie naar post-kwantumcryptografie van de afzonderlijke lidstaten.



3. MAATREGELEN OP UNIENIVEAU

- Periodieke monitoring en beoordeling van de werkzaamheden door de CIE, in samenwerking met de deskundige vertegenwoordigers van de lidstaten.
- Landen leveren op verzoek van de CIE voldoende informatie over de voortgang.
- Op basis van deze informatie en alle andere beschikbare informatie beoordeelt de CIE de geplande maatregelen en de werking van het netwerk van vertegenwoordigers van de lidstaten en bepaalt zij of er aanvullende maatregelen nodig zijn, zoals voorstellen voor bindende handelingen van het Unierecht.

4. EVALUATIE

- Uiterlijk april 2027 moeten de lidstaten met de CIE samenwerken om de gevolgen ervan te beoordelen en passende volgende stappen te bepalen. Bij deze beoordeling moeten de resultaten van de werkzaamheden van de nationale deskundigen in de subgroep postkwantumcryptografie in acht worden genomen.

Link: [Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography | Shaping Europe's digital future \(europa.eu\)](#)

Op 17 mei jl. heeft het Kabinet het NL standpunt hierover gepubliceerd: [Fiche: Aanbeveling Routekaart Post-Quantumcryptografie | Tweede Kamer der Staten-Generaal.](#)

Aspecten uit het fiche Kabinetsinzet

Nederlandse positie ten aanzien van het voorstel; essentie Nederlands beleid:

- Het programma QvC Rijk werkt het beleid op de transitie naar post-quantum cryptografie uit
- AIVD en NCSC hebben een handleiding en aanvullende handreiking gepubliceerd in 2023 (PQC-migratiehandboek)
- Transitie naar PQC is onderdeel NLCS en Dcypher voert hierbinnen de routekaart crypto-communicatie uit
- Post-quantum cryptografie is een van de prioritaire onderwerpen in de agenda voor Cybersecurity Technologies onder de Nationale Technologiestrategie (NTS)
- Afwijking ten opzichte van *Quantum Key Distribution* – momenteel geen rol voor QKD

Inzet van het Kabinet:

- Het kabinet zet zich ervoor in dat de aanbeveling, met uitzondering van het gedeelte over constructies met QKD van de Commissie uitgevoerd zal worden
- De overheid werkt hiervoor samen met andere lidstaten, o.a. via het voorgestelde lidstatenforum. 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



Quantumveilige Cryptografie Rijk



Update programma en
voortgang



Quantumveilige Cryptografie RIJK (QvC Rijk)



Doel:

We richten een programma in om de Rijksoverheid te helpen de risico's van quantumtechnologie op cryptografie op tijd te beheersen

QvC Rijk ondersteunt en stimuleert door:



bewustwording, kennis en communicatie te leveren i.s.m. onderzoek en wetenschap en uitwisseling daarvan stimuleren voor alle doelgroepen binnen het Rijk



adequaat beleid, kaders en richtlijnen beschikbaar te stellen en daarmee departementen in hun verantwoordelijkheid te ondersteunen



handreikingen en een expertisecentrum te bieden en daarmee de (voorbereiding van) veilige en tijdige mitigatie van de risico's faciliteren.



STUURGROEP (ROADMAP DIGITALE WEERBAARHEID)

- Gekoppeld aan de I-strategie Rijk (deelnemers CIO's)

PROGRAMMAMANAGER EN KERNTTEAM

- Aantal trekkers
- Verschillende departementen/organisaties

KLANKBORDGROEP

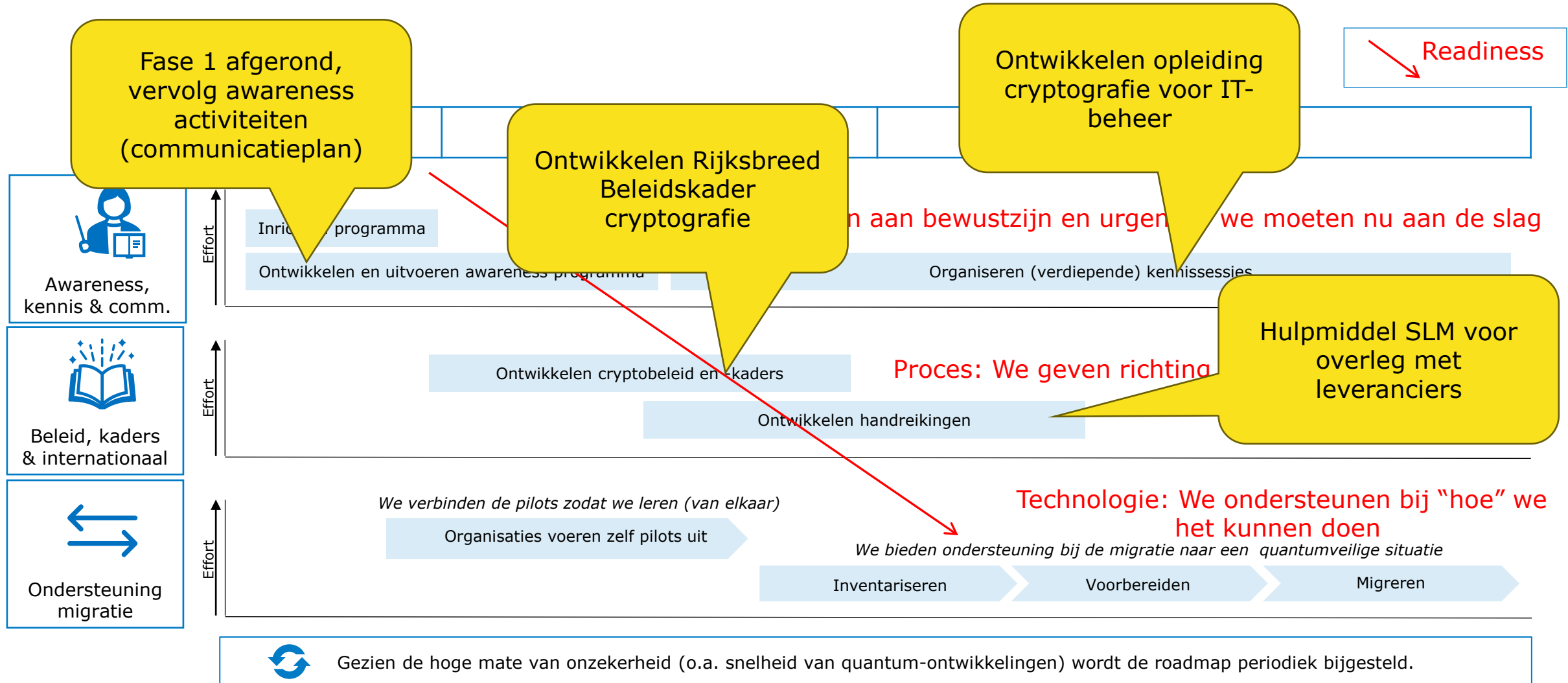
- Externen: onderzoek en wetenschap
- Internen: CTO's CISO en CIO

WERKGROEPEN EN EXPERTISECENTRUM,

- Uit verschillende onderdelen van de Rijksoverheid
- Departementen, uitvoeringsorganisaties
- IT-dienstverleners en toezichthouders/controleurs
- *Samenwerking publiek-privaat-onderzoek*



Roadmap Quantumveilige Cryptografie Rijk



QvC Rijk

eenvoudig model

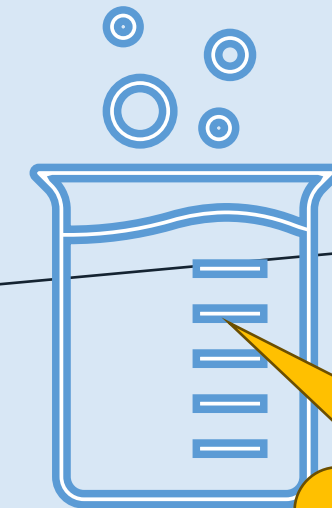
Awareness, kennis en communicatie

Onderzoek automatisering
cryptografisch
assetmanagement

van

A

Huidige cryptografie



Expertisecentr

Verkennen / realiseren van
een expertisecentrum
cryptografie (Δ)

Verkennen / realiseren van
standaardisatie van
quantumveilige cryptografie

naar

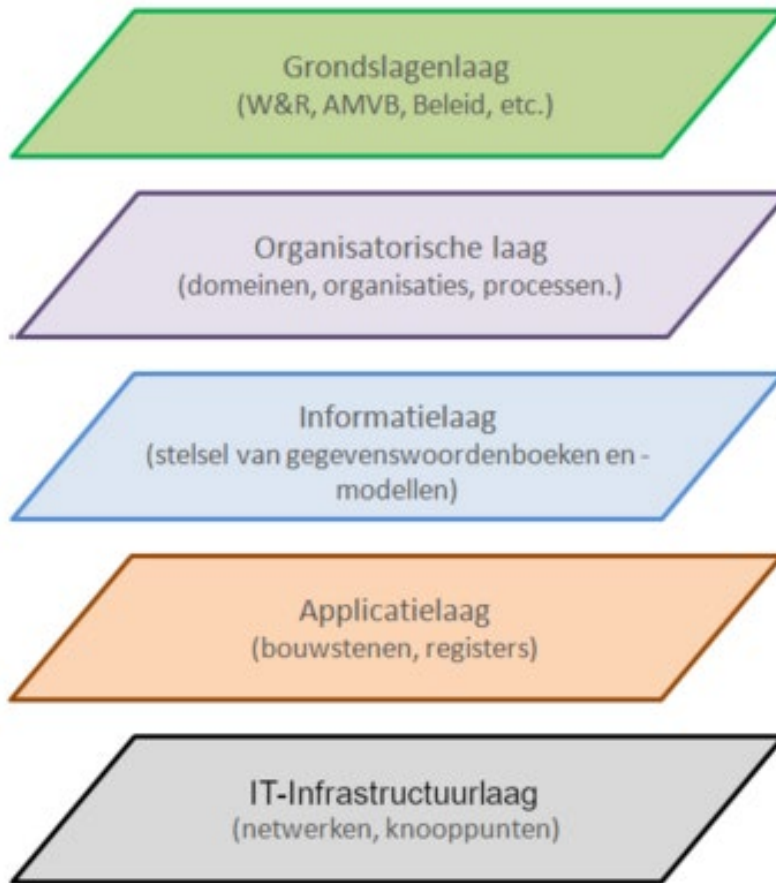
B

Q-veilige cryptografie

Beleid, kaders, hulpmiddelen



Vijf-laagsmodel



- > **Wet & regelgeving: NIS2, CRA, Aanbeveling EU-CIE, EU routekaart transitie naar PQC, BIO etc**
Beleid: Rijksbreed beleidskader cryptografie
- > **(Cryptografie in) Ontwerp en ontwikkelprocessen (crypto agility); IT-asset management, Lifecycle-management, Inkoop- en leveranciersmanagement, Kwetsbaarheden management, Changemanagement etc.**
- > **Afspraken metadata cryptografie (ihkv SBOM) – gerelateerd aan bv assetmanagement en kwetsbaarheden management**
- > **Toepassing van cryptografie op de applicatie laag tbv verschillende functies waar cryptografie voor wordt ingezet**
- > **Toepassing van cryptografie op de IT-infrastructuur laag voor versleuteling**



Interactief: rol van en samenwerking met architectuur



1. Welke rol heb jij als architect bij deze transitie?
2. Waar zie je de belangrijkste uitdagingen binnen jouw werkgebied?
3. Wat heb je, of heeft jouw organisatie nodig?



Vragen en opmerkingen ?





Appendix



Wijzigingen die je nu al kunt/moet doen:

- Bescherm nu je informatie die langdurig geheim moet blijven; ken je TBB.
- Neem de quantumdreiging op in je risicomangementproces.
- Symmetrische cryptografie: Verleng de sleutels.
- Voeg eisen voor (toekomstige) cryptografie toe in aanbestedingen.

Vorbereidingen nu voor wijzigingen later:

- Weet waar je welke cryptografie gebruikt (borg het in assetmanagement).
- Zorg dat je voorbereidende wijzigingen doorvoert (bv TLS 1.3).
- Ga met je leveranciers in gesprek over cryptografie in hun producten.



Meer weten?



- Lees (de eerste pagina's van): [Het PQC-migratie handboek | Publicatie | AIVD](#)
- Lees de NCSC Handreiking: [Maak je organisatie quantumveilig | Publicatie | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)
- Bezoek onze webpagina's op: [Quantumveilige cryptografie Quantumveilige cryptografie - Digitale Overheid](#)
- Contactadres: QvC-Rijk@rijksoverheid.nl