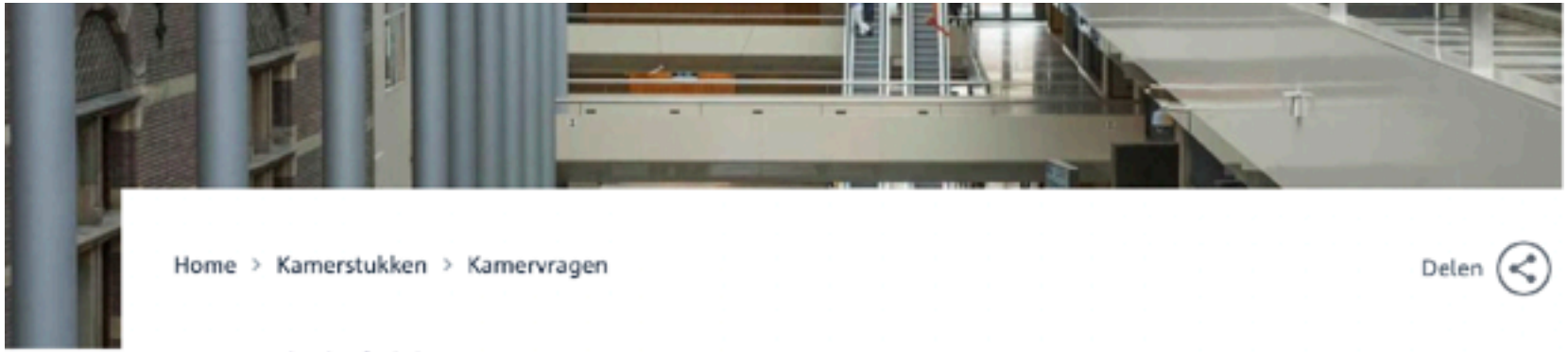
How do you upgrade a government to become post quantum crypto secure?

Oscar Koeroo

CISO Concern van het Ministerie van Volksgezondheid, Welzijn en Sport

Parlement taking quantum computer risk seriously



Home > Kamerstukken > Kamervragen

Delen

Antwoord schriftelijke vragen

Antwoord op vragen van het lid Rajkowski over het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'

Download

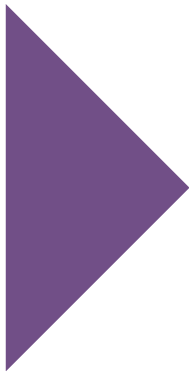
Ondertekenaars

Eerste ondertekenaar
A.C. van Huffelen, staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Mede namens
E. van der Burg, staatssecretaris van Justitie en Veiligheid

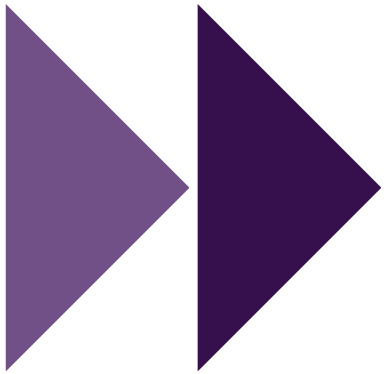
What are some our challenges?

What are some our challenges?



Cryptography choice needs to stabilised

What are some our challenges?



Cryptography choice needs to stabilised

Protocol standards adapted and published

What are some our challenges?

Cryptography choice needs to stabilised

Protocol standards adapted and published

Hardware and software needs to be made capable

What are some our challenges?

Cryptography choice needs to stabilised

Protocol standards adapted and published

Hardware and software needs to be made capable

Certification scheme must be finished

What are some our challenges?

Cryptography choice needs to stabilised

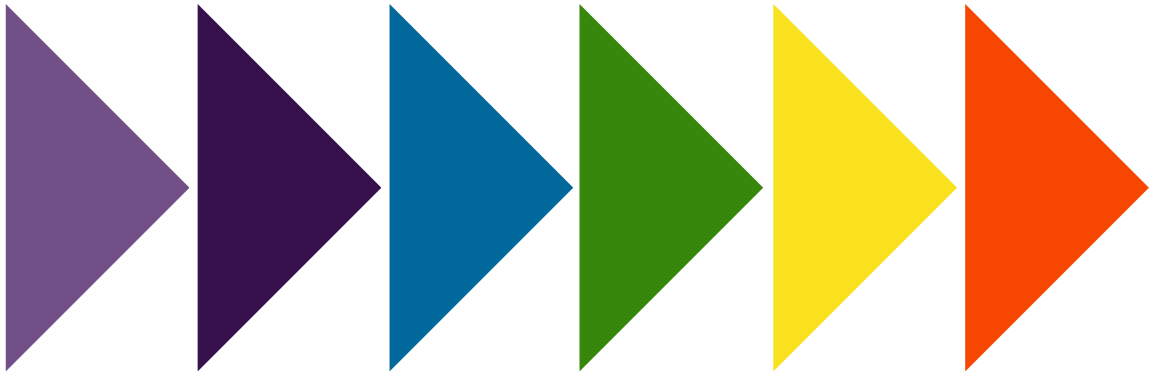
Protocol standards adapted and published

Hardware and software needs to be made capable

Certification scheme must be finished

Protocols Q-risk mitigating by config evolutions (e.g. dnssec)

What are some our challenges?



Cryptography choice needs to stabilised

Protocol standards adapted and published

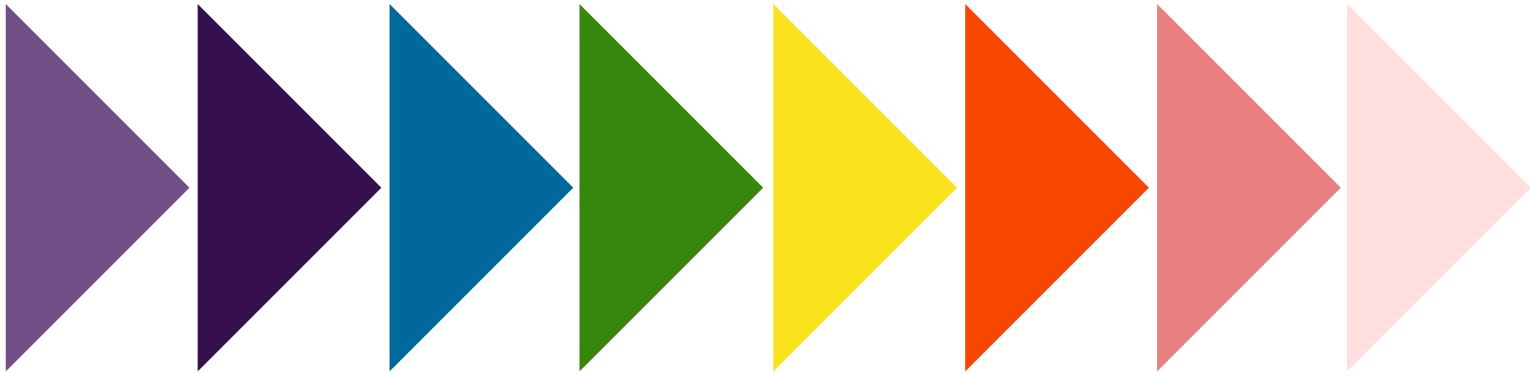
Hardware and software needs to be made capable

Certification scheme must be finished

Protocols Q-risk mitigating by config evolutions (e.g. dnssec)

Global PKI evolution must become commercially viable

What are some our challenges?



Cryptography choice needs to stabilised

Protocol standards adapted and published

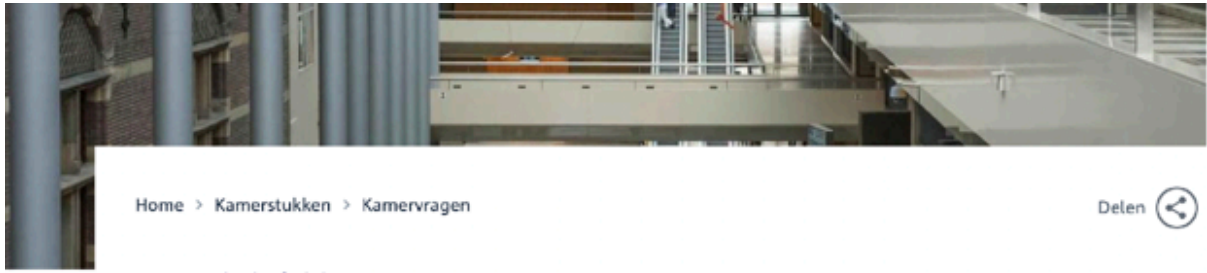
Hardware and software needs to be made capable

Certification scheme must be finished

Protocols Q-risk mitigating by config evolutions (e.g. dnssec)

Global PKI evolution must become commercially viable

Government is planning to address the quantum computer risks



Home > Kamerstukken > Kamervragen

Delen

Antwoord schriftelijke vragen

Antwoord op vragen van het lid Rajkowski over het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'

Download

Ondertekenaars

Eerste ondertekenaar
A.C. van Huffelen, staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Mede namens
E. van der Burg, staatssecretaris van Justitie en Veiligheid

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z15348&did=2022D36371

Government is planning to address the quantum computer risks

- National Crypto Strategy

Home › Kamerstukken › Kamervragen

Delen

Antwoord schriftelijke vragen

Antwoord op vragen van het lid Rajkowski over het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'

Download

Ondertekenaars

Eerste ondertekenaar
A.C. van Huffelen, staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Mede namens
E. van der Burg, staatssecretaris van Justitie en Veiligheid

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z15348&did=2022D36371

Government is planning to address the quantum computer risks

- National Crypto Strategy
- Invest in scientific research and the development of secure products

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z15348&did=2022D36371

Government is planning to address the quantum computer risks

- National Crypto Strategy
- Invest in scientific research and the development of secure products
- 2023: publication of the Quantum Migration Guide

Home › Kamerstukken › Kamervragen

Delen

Antwoord schriftelijke vragen

Antwoord op vragen van het lid Rajkowski over het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'

Download

Ondertekenaars

Eerste ondertekenaar
A.C. van Huffelen, staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Mede namens
E. van der Burg, staatssecretaris van Justitie en Veiligheid

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z15348&did=2022D36371

Government is planning to address the quantum computer risks

- National Crypto Strategy
- Invest in scientific research and the development of secure products
- 2023: publication of the Quantum Migration Guide
- Develop a Quantum Impact Assessment

Home › Kamerstukken › Kamervragen

Delen

Antwoord schriftelijke vragen

Antwoord op vragen van het lid Rajkowski over het bericht 'NIST kiest wapens tegen kwantumcomputer als cryptokraker'

Download

Ondertekenaars

Eerste ondertekenaar
A.C. van Huffelen, staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Mede namens
E. van der Burg, staatssecretaris van Justitie en Veiligheid

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z15348&did=2022D36371

Government is planning to address the quantum computer risks

- National Crypto Strategy
- Invest in scientific research and the development of secure products
- 2023: publication of the Quantum Migration Guide
- Develop a Quantum Impact Assessment
- **Create a plan to make the government quantum resistant**

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z15348&did=2022D36371

Workgroup: Quantum Safe Crypto

Mission from CIO council beraad with advice from CISO council

Mission fase 1 (CIO-council)

Create a **plan** en request approval by the CIO council

OBJECTIVES

1. **Increasing awareness and knowledge** among administrators and employee groups involved in cryptography.
2. Develop and determine **government-wide crypto policy** in close collaboration with the NBV.
3. **Connecting with other crypto initiatives** and ensuring that knowledge (building) is bundled and secured and becomes and remains available.
4. Ensuring that the use of cryptography in **new applications and systems is as secure** as possible “by design” quantum by embedding in design and development processes.
5. **Migrating current applications** via the recommended approach TNO and IenW.

Mission in perspective

PHASES

TIMELINE

The approach 3 tracks

THE TRACKS

1. **Awareness and (project) communication** (including ensuring connections with other initiatives)

2. **Policies and quantum secure by design processes** (including the threat: “store now decrypt later”)

3. **Migration current applications**

Collaboration

Realisation

Steering

Execution

STEERING GROUP (ROADMAP DIGITAL RESILIENCE)

- Tied to the “I-strategie Rijk”

CORE TEAM

- 3 x 2 leads
- Various departements and organisations

SOUNDING BOARD GROUP

- To be created (experts)

WORKING GROUPS

- From different parts of the government
- Different type of organisations
- IT-service provider and dienstverleners en supervisors

Governance

- To be implemented PQC standards and protocols
- Guard for interoperability
- Centrally managed aspects of supplier management
- Develop a risk management approach that assists prioritising

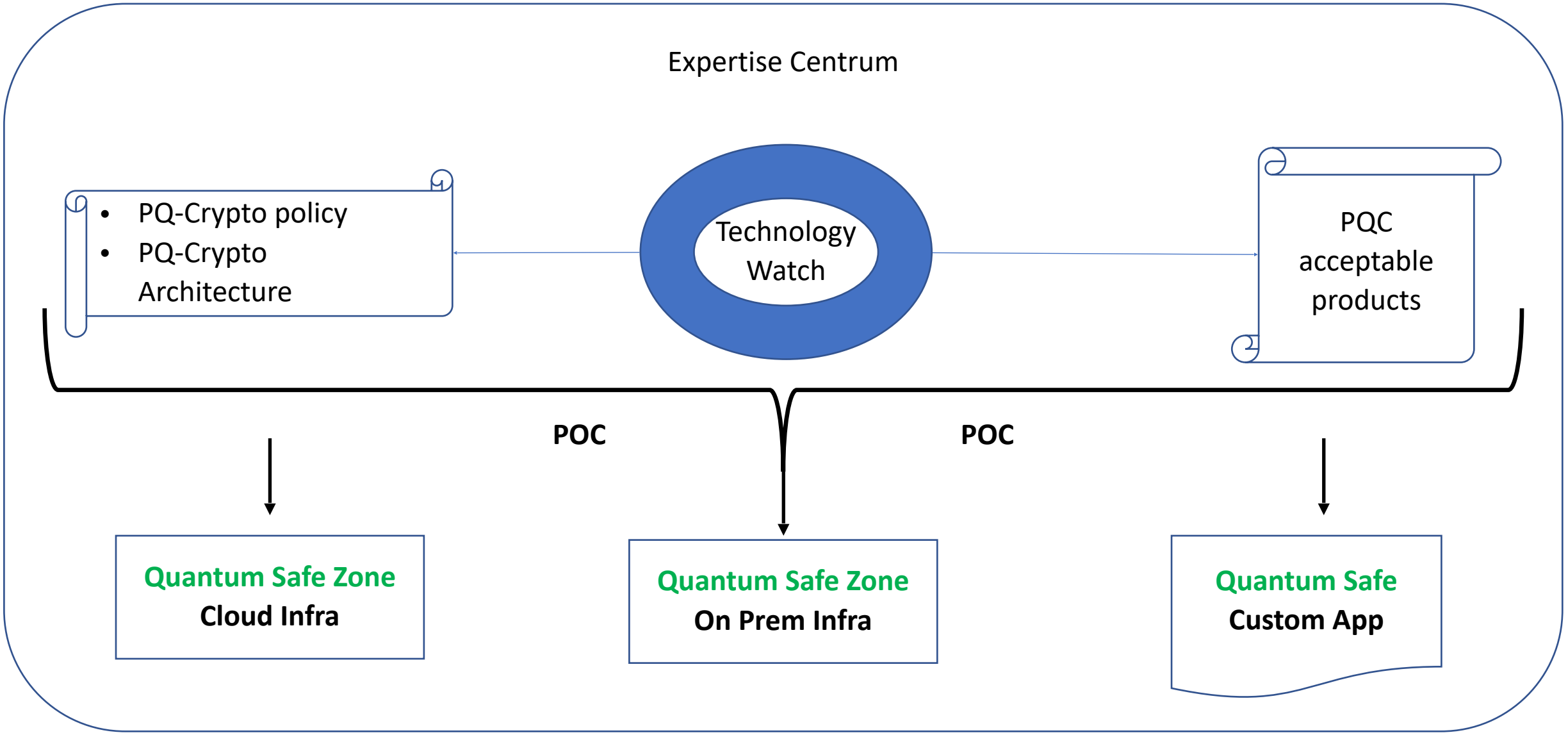
Disclaimer: this is an early concept! Feedback and management decision to be taken!

Interdepartmental collaboration

- Develop interoperability studies
  - Non-technical and technical.
- Create an expertise center
  - With trend-watch for new tech, standards, protocol development and products.
- Provide an interoperability lab

Disclaimer: this is an early concept! Feedback and management decision to be taken!

From Pre to Post Quantum Cryptography



Disclaimer: this is an early concept! Feedback and management decision to be taken!

Strategic/tactical procedures

- Supplier management
  - Post-quantum “ready” solutions as a qualifier.
- Development guidelines
  - e.g. instructions for documentation and CI/CD
- Extend inventory management with new guidelines
  - What products contain what crypto-technology?
  - Which cryptographic assets are there, and which technology is in use?

Disclaimer: this is an early concept! Feedback and management decision to be taken!

How do you upgrade a government to become post quantum crypto secure?

You do it together.