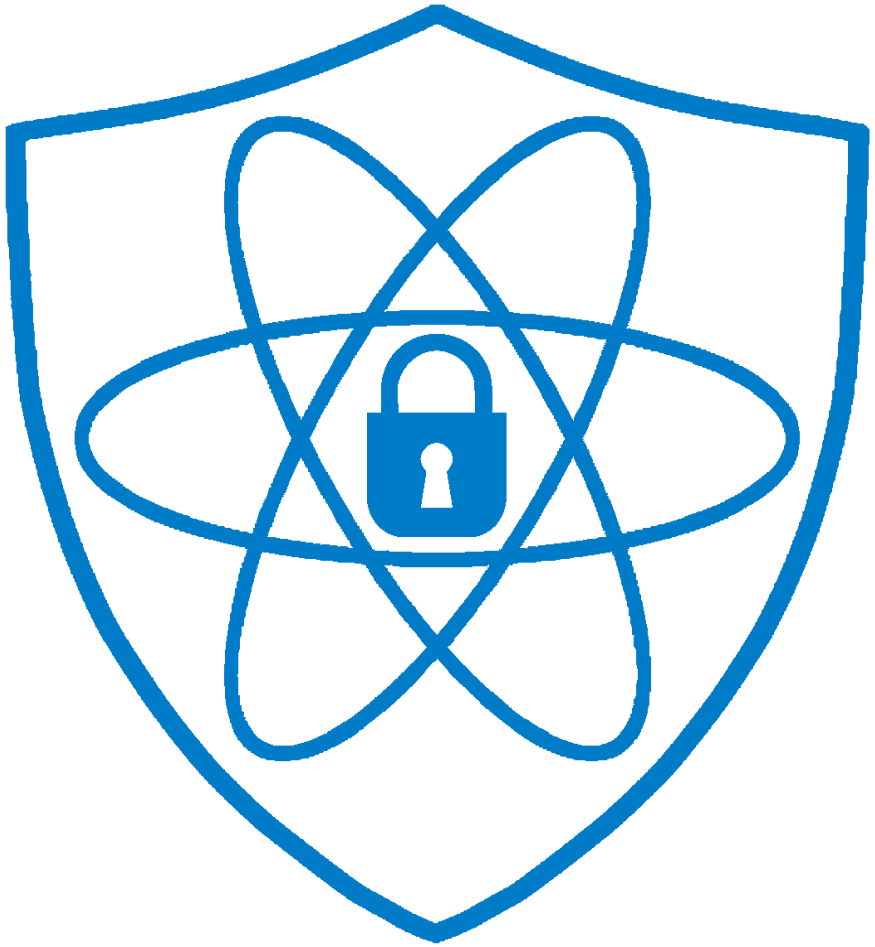
Post-Quantum

Cryptography Conference

Unlocking the Quantum-Resilient Cryptography Strategy for the Dutch central government

Anita Wehmann
Senior Advisor Information Security at the Ministry of the Interior and Kingdom Relations (BZK) of the Netherlands

Germain van der Velden
Senior Information Advisor at the Ministry of Infrastructure and Water Management of the Netherlands



Ministry of the Interior and
Kingdom Relations

Quantum secure Cryptography

Support program of the Dutch Central Government

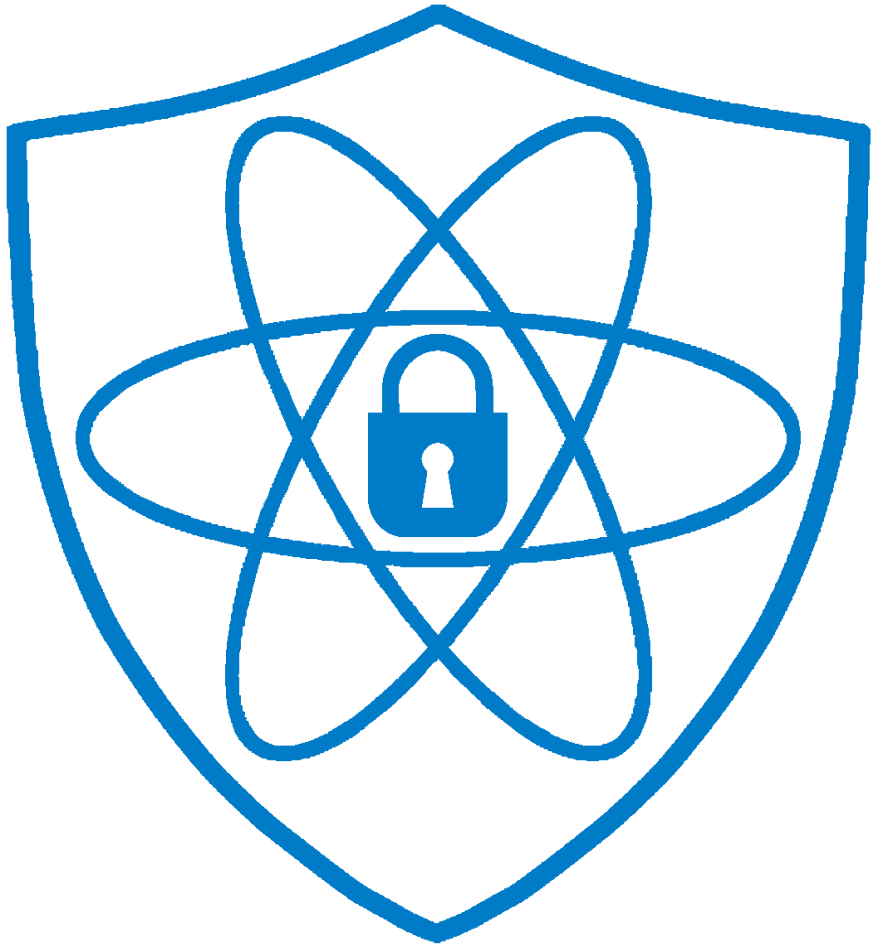
Anita Wehmann

Germain van der Velden

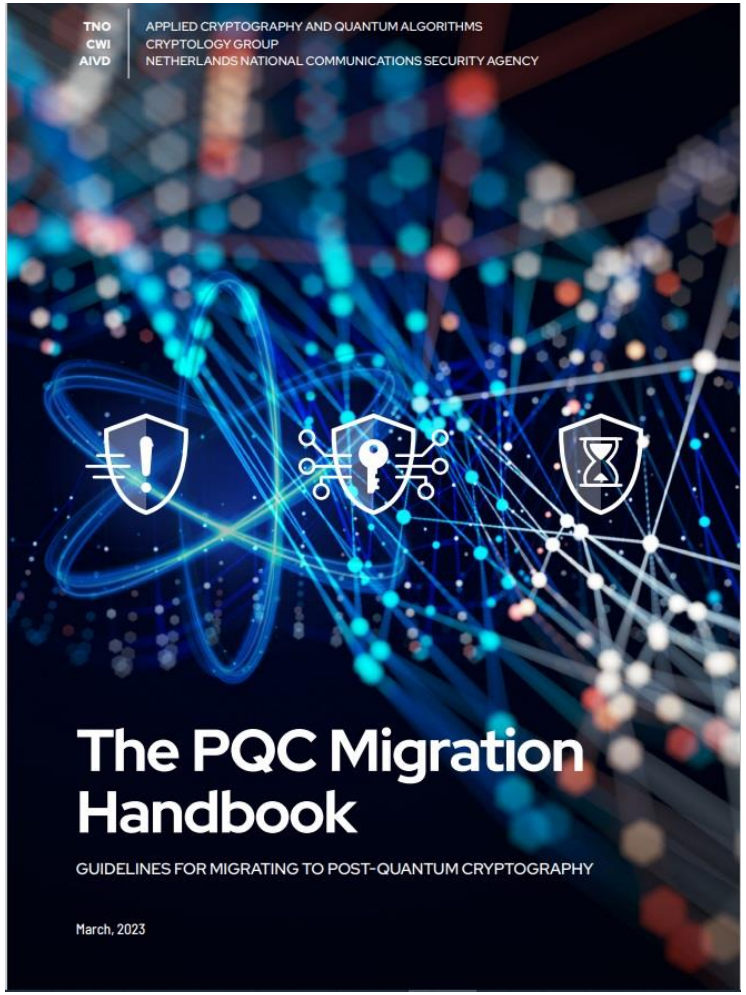
Agenda

Introduction

Program for Quantum secure Cryptography
- Purpose
- Steering model
- Roadmap



PQC Migration



The PQC Migration Handbook | Publication | AIVD

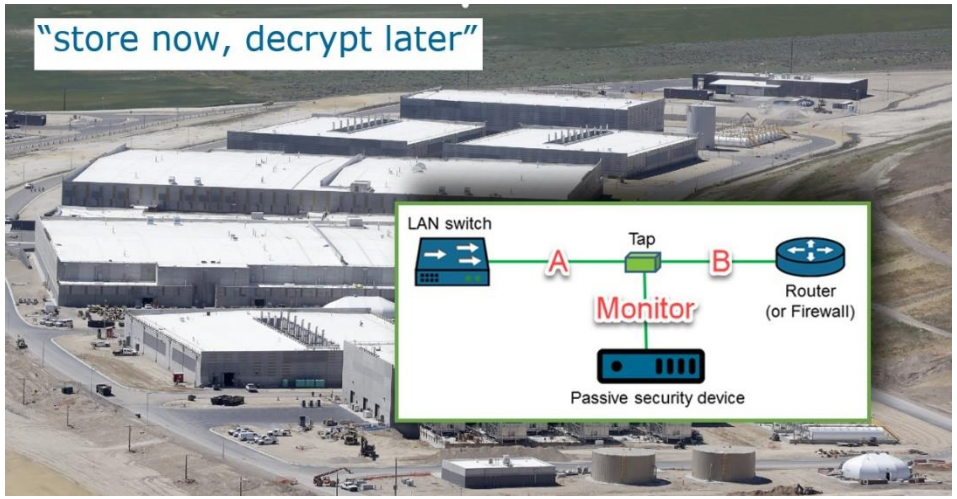
Handbook

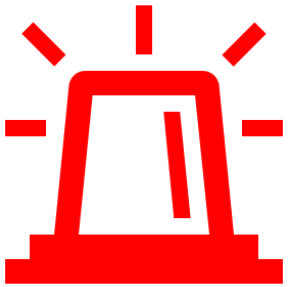
URGENT ADOPTERS SHOULD START NOW

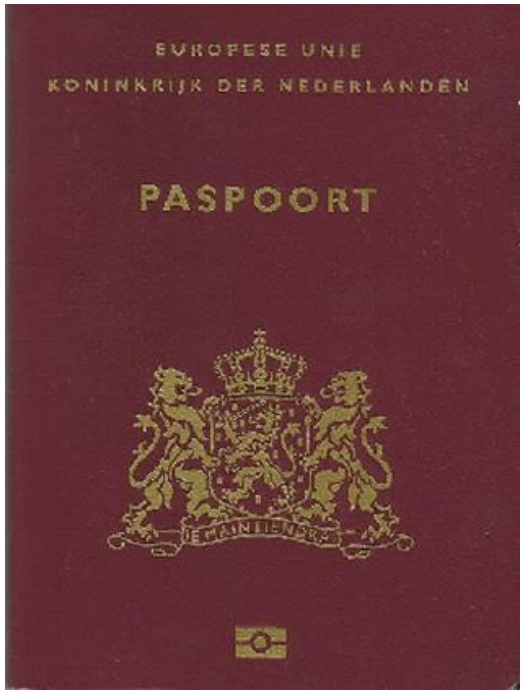
- Sensitive information with a long confidentiality span ("store now decrypt later")
- Personal Data with a long confidentiality span: passports
- Provide systems of critical infrastructure: payment transactions, energy, transportation
- Provide systems which are built to have a long life-span: water management, chemical industry, drinking water, railroads

Conclusion: Central Dutch government is an urgent adopter

The impact of broken cryptography







Quantum secure Cryptography Dutch Central Government (QsC Gov)

Purpose:
The Dutch Central Government aims to control the risks of quantum technology on cryptography in time

QsC Gov supports and stimulates through:

Creating awareness, knowledge and communication in collaboration with science and research and stimulating its exchange for all target audiences within the Dutch Central Government

Creating adequate policy, frameworks and guidelines to support the Dutch ministries in their responsibility

Offering guidance and a centre of expertise in order to facilitate and support (the preparation) of secure and timely mitigation of these risks

Collaboration realisation

Steering

implementation

STEERING BOARD (ROADMAP DIGITAL RESILIENCE)

- part of I-strategy Dutch Central Government (CIO's)

PROGRAM MANAGER & CENTRAL TEAM

- Program Members
- various ministries/ government organisations

ADVISORY BOARD

- External: Science and research
- Internal: CTO's CISO en CIO

WORK GROUP AND CENTRE OF EXPERTISE

- From different parts of the central government
- Ministries and its various departments
- Internal IT-service providers and auditors/supervisors
- collaboration public-private-research

Roadmap Quantum secure Cryptography Gov

readiness

2023	2024	2025	2026 and beyond

Awareness, knowl. & comm.

Effort

Establish program

Develop and execute awareness program

Organise knowledge sharing sessions

People: We work on awareness and urgency: we have to act now!

Policy,guidelines & international

Effort

Develop crypto policy and -frameworks

Develop guidelines

Proces: We give direction to "what" we must do

Supporting migration

Effort

We connect pilots in order to learn (from each other)

Organisations execute pilots themselves

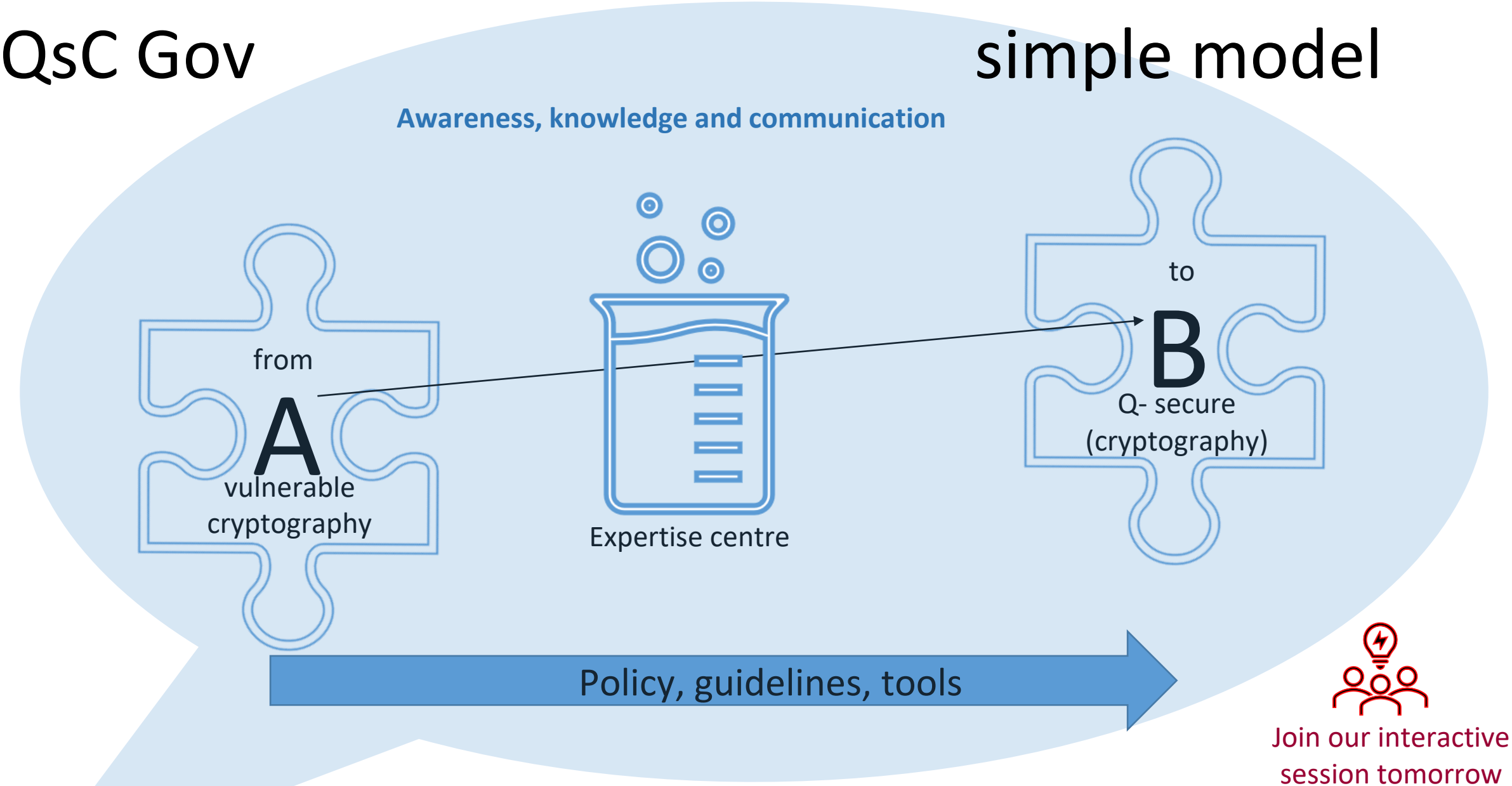
Technology: We support "how" we can do it

We offer support at the migration to a quantum secure status

Inventarisation → Preparation → Migration

Because of the high rate of uncertainty (f.i. speed of quantum tech. developments) the roadmap will be updated frequently.

QsC Gov simple model



Questions?

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia