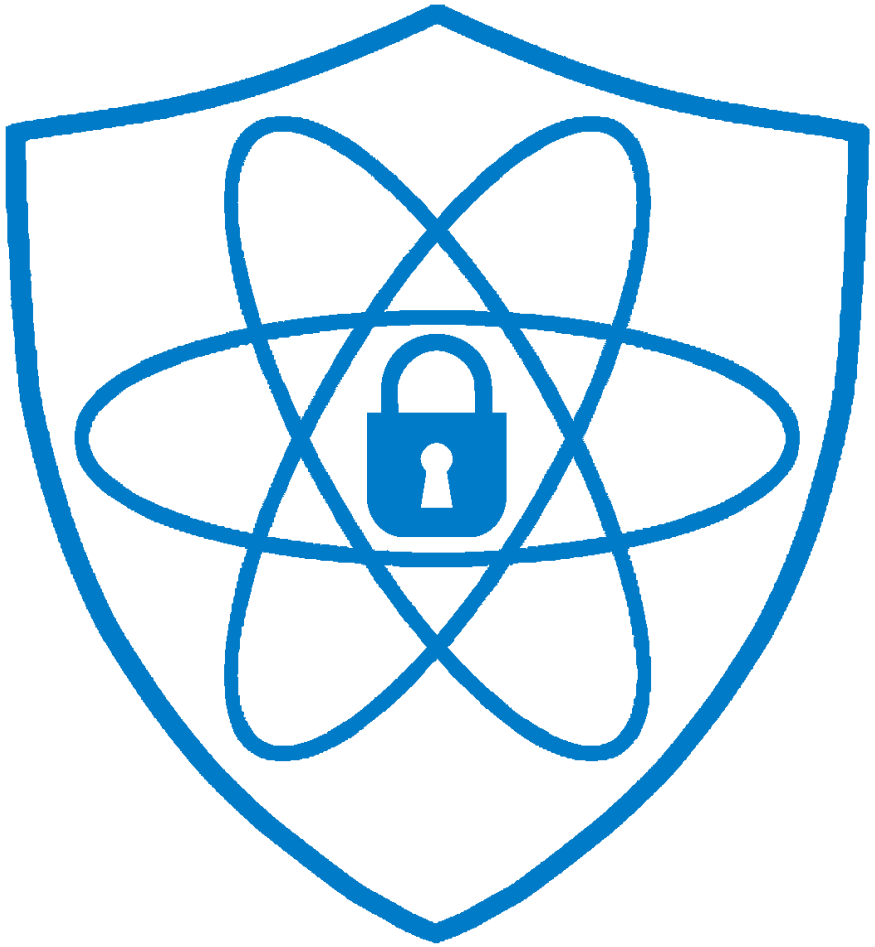
Post-Quantum

Cryptography Conference

Your cryptography will be broken, prepare yourself now!

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

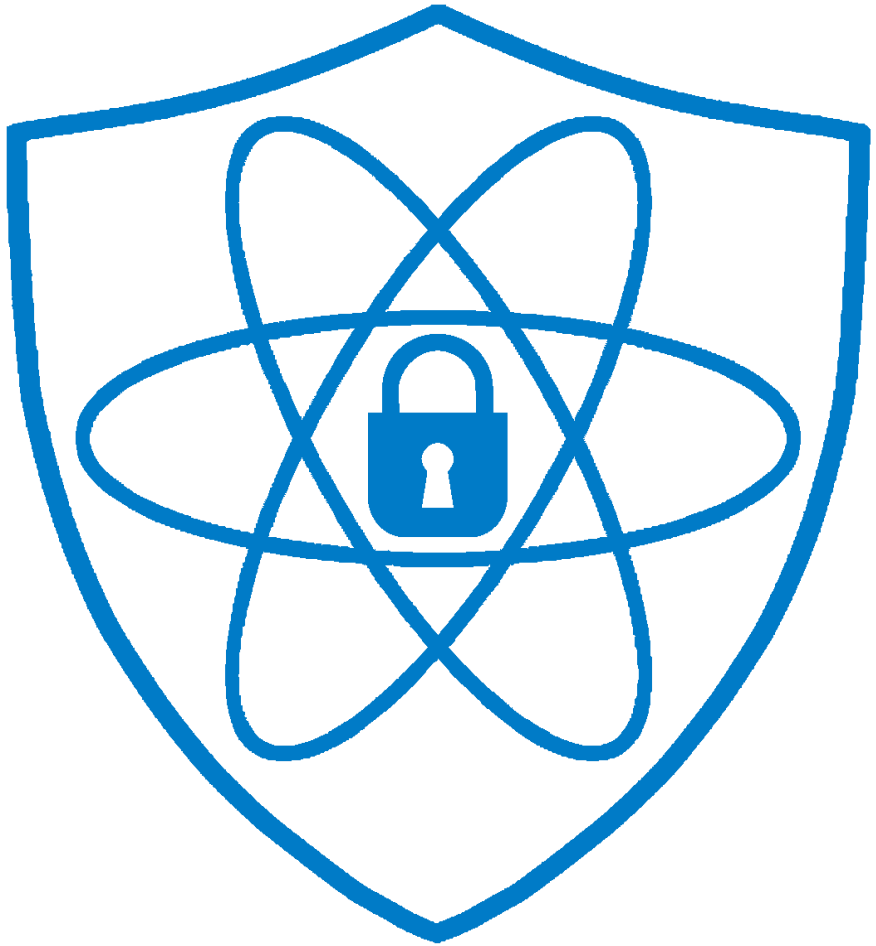
Anita Wehmann

Germain van der Velden

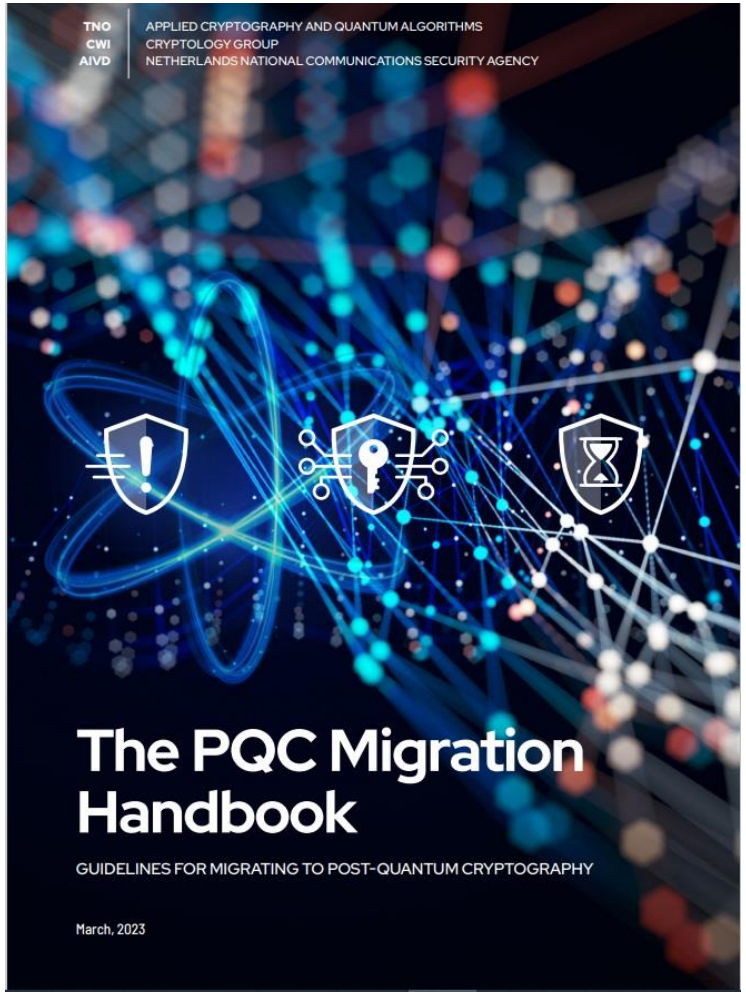
Agenda

Introduction

- Recap presentation nov 7th
- Interactive: discussion
- What you can and should do now



PQC Migration



[The PQC Migration Handbook | Publication | AIVD]

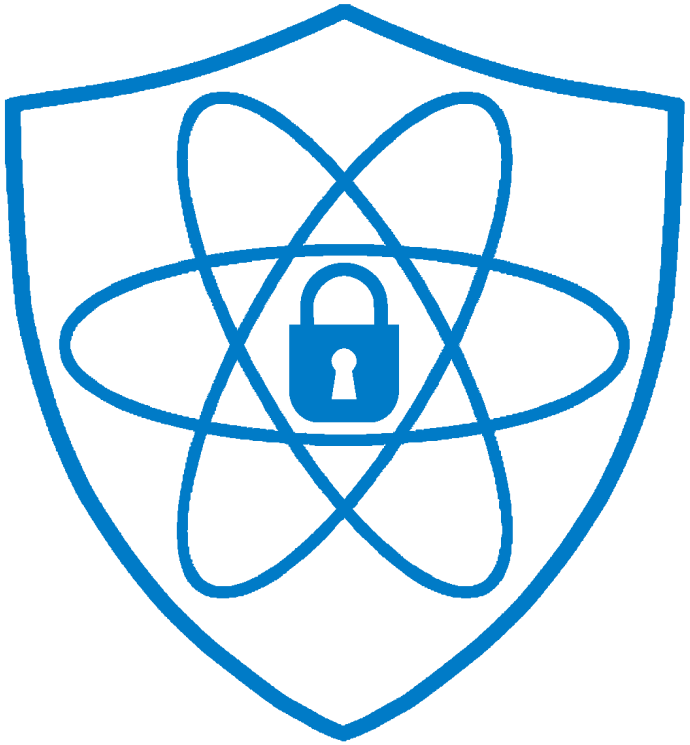
Handbook

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

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

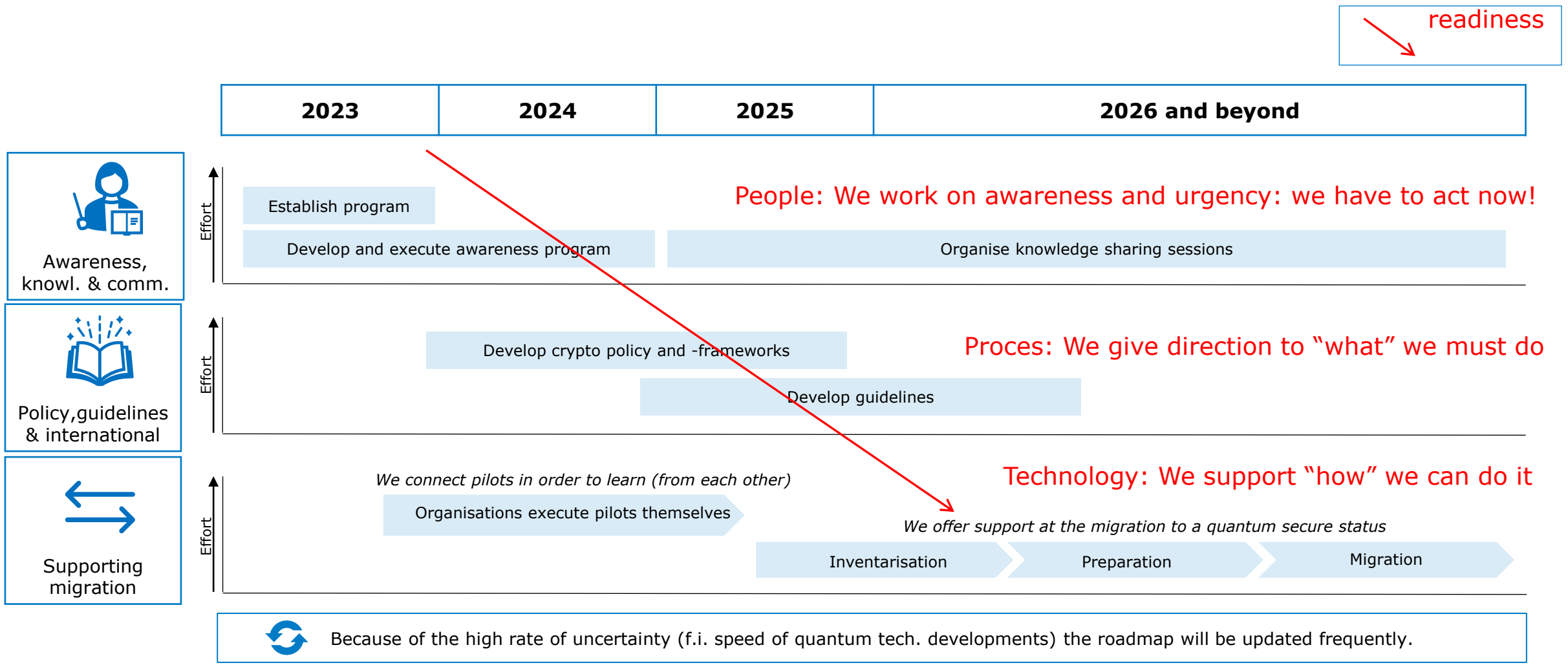
QsC Gov supports and stimulates through:

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

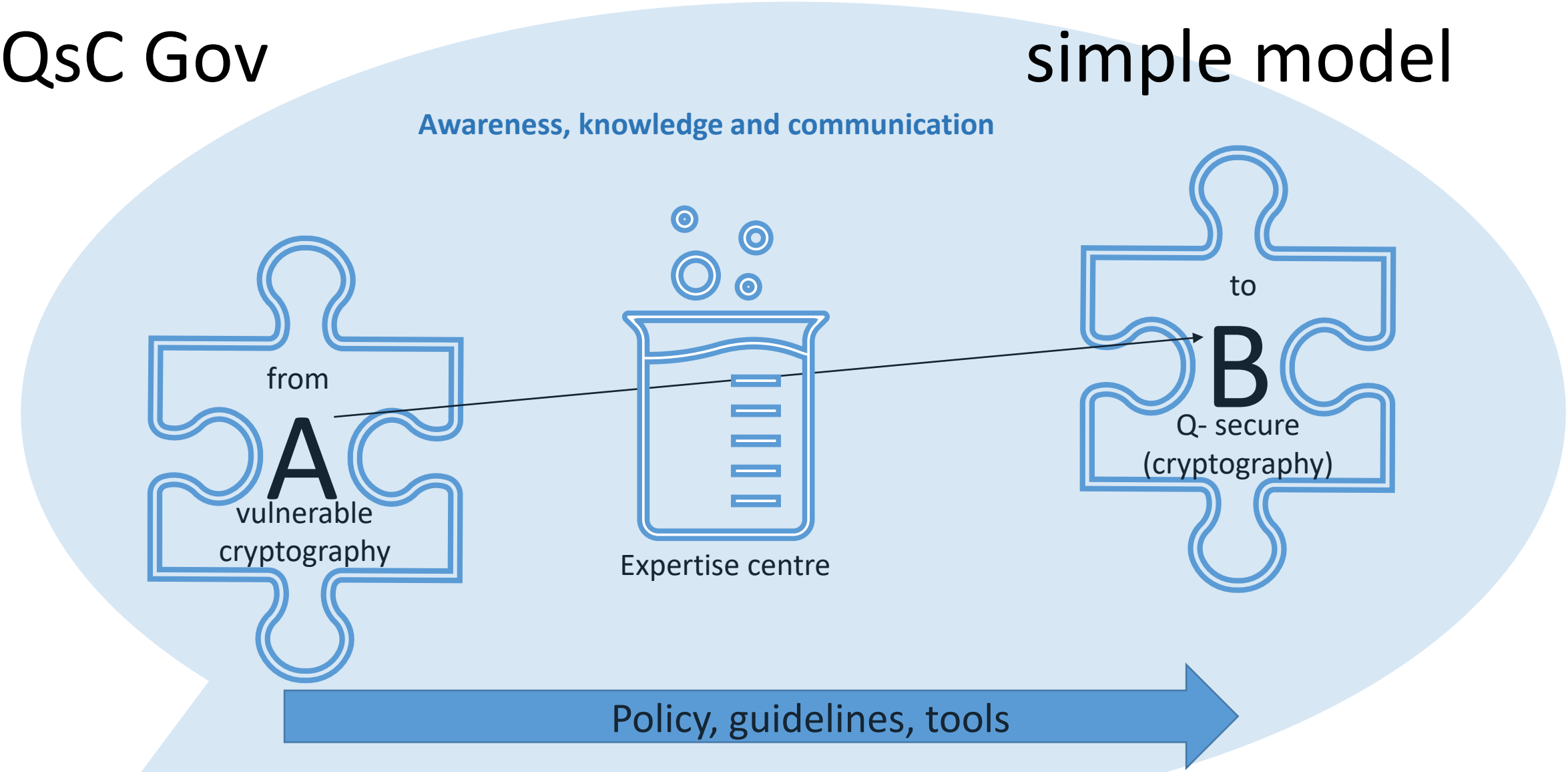
Creating adequate policy, frameworks and guidelines to support the Dutch ministries in their responsibility

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

Roadmap Quantum secure Cryptography Gov



QsC Gov simple model



Interactive:

- Do you know what cryptography you have in use?
- Can we still communicate? What about interoperability, standards?
- (How) can we work together in solving migration problems?

What you can and should do now

What you can do now:

- Know your "crown jewels"
- Protect information that must stay confidential for a long time (after 2030)
- Add the quantum threat to your *risk management process*
- Symmetric cryptography: use longer keys
- Add demands to (future) cryptography in tenders

Preparation for later changes:

- Know *which cryptography is in use where* (asset management)
- Perform preparation changes (TLS 1.3)
- *Talk with your suppliers* about cryptography used in their products and their preparation

TIP: Look at the (first) steps in the PQC-migration handbook, The PQC Migration Handbook | Publication | AIVD

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