TNO innovation for life

CWI

CWI & TNO COLLABORATIONS ON PQC

MARC STEVENS & GABRIELE SPINI

21 April 2022

TNO innovation for life

CWI

TU Delft

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

ZYNYO.

Microsoft

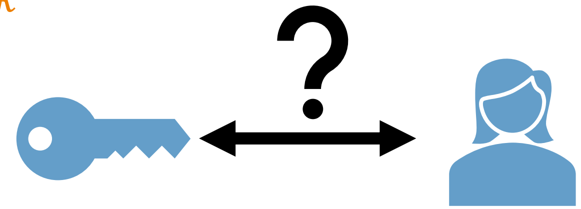
kpn

QUANTUM-SAFE PUBLIC-KEY INFRASTRUCTURES

THE HAPKIDO PROJECT | DR. GABRIELE SPINI

ASYMMETRIC CRYPTOGRAPHY

- Encryption:
  - If you have Alice's public key pk, can send encrypted messages to her
  - Only Alice can decrypt with sk
- Signatures:
  - If you have Alice' public key pk, can verify data signed by her
  - Only Alice can produce valid signature with sk



- **But:** how do you know pk is Alice's?
  - Substitute Alice with bank, website, …
  - Rather not meet at bench to exchange keys

ENTER PUBLIC-KEY INFRASTRUCTURES
PKIS FOR FRIENDS

- Solution: **Public-Key Infrastructures** or PKIs

- Ecosystems (entities, cryptographic functions, policies, software, hardware…) to
  - Link public keys to entities
  - Certify details of public-key usage (validity time, associated cryptographic scheme, etc.)
  - Manage revocation of compromised/expired keys
  - Certify identities
  - …

- Nowadays, PKIs are fundamental in enabling asymmetric cryptography
  And thus: internet, e-government, digital financial services, …

ENTERS QUANTUM
[OMINOUS MUSIC PLAYING]

- Large-scale quantum computer will break currently-used asymmetric cryptography

- This affects PKIs as well
  - Systems that rely on PKIs to manage their keys
  - PKI functionalities as well (sign certificates)

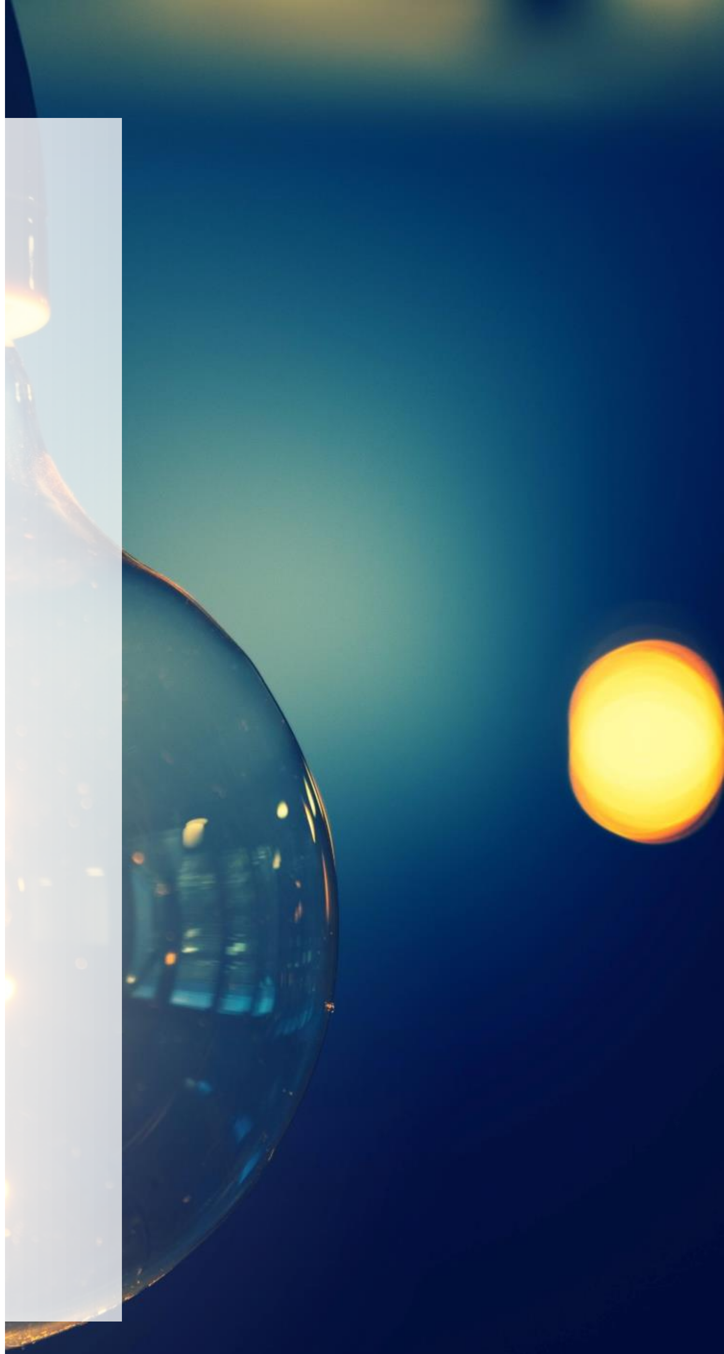
- PKIs are ecosystems; therefore, two consequences:
  - Lot of parties involved, on different levels (technical, legal, ...)
  - Interoperability is an issue: need for hybrid systems

HAPKIDO
A DUTCH INITIATIVE FOR QUANTUM-SAFE PKIS

- **H**ybrid **A**pproach for quantum-safe **P**ublic-**K**ey **I**nfrastructure **D**evelopment for **O**rganisations (HAPKIDO)

- Dutch initiative, funded by NWO (overarching Dutch Research Organisation)

- Five-year project, seven involved parties



THE CONSORTIUM
COMPLEX PROBLEMS DEMAND GREAT TEAM

- Cryptographic research
- Governance
- Moving to higher TRL
- PKI management, test lab
- Digital government
- Provider of digital identification & signing services
- Coordination, PoC development

HAPKIDO
WHERE ARE WE?

- Project started in October 2021
- Focus of first phase:
  - Establishing contacts
  - Gather requirements
  - Study of similar projects
  - Societal impact assessment
  - Study of challenges for specific sectors
- Stay tuned for more information!

PQC MIGRATION HANDBOOK – IN DEVELOPMENT

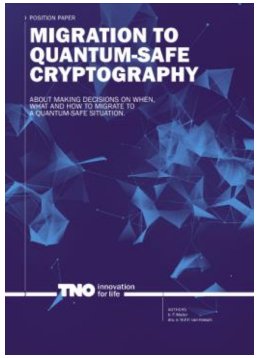
21 April 2022

HANDBOOK AIM

- Commissioned by NBV - Netherlands National Communications Security Agency

- Main goal: assist Dutch organizations in migration to PQC
  - Give concrete advice on migration
  - Tailored advice for different types of organizations
  - Inform on technological aspects
  - Specific advice for common cryptographic systems

- Starting points
  - TNO position paper
  - NBV Brochure



TYPES OF ORGANIZATIONS

- Categorization into similar types of organizations: “PQC Personas”

- Based on characteristics:
  - Attack surface
  - Type of systems
  - Type of data
  - Time pressure
  - Dependency on other organizations
  - Threat level

TAILORED MIGRATION ADVICE

- Three stages of migration
  1. Asset discovery
  2. Preparing the migration (per asset)
  3. Executing the migration (per asset)

Tailored advice for different PQC Personas

- **Urgent adopters**
  - Confidential and/or personal data
  - Critical and/or long-lived infrastructure
  - Suppliers to crucial organizations
- Late adopters
- (Cryptography Experts – e.g. NIST, NXP, Technolution, ...)


THANK YOU FOR
YOUR TIME
gabriele.spini@tno.nl
stevens@cwi.nl
innovation
for life