Quantum-safe Public-key Infrastructures

An overview of the HAPKIDO project

Dr. Gabriele Spini, TNO

HAPKIDO
101

- **H**ybrid **A**pproach for quantum-safe **P**ublic-**K**ey **I**nfrastructure **D**evelopment for **O**rganisations
- Dutch initiative, international scope/ambitions
- Project duration: 5 years (fall 2021 – fall 2026)
- Consortium: 7 parties (more on that later)

HAPKIDO

What’s special about it

- More specific than other migration projects, multidisciplinary approach

- 3 main levels:
  - Technical: develop actionable solutions
  - Fundamental: study security of hybrid systems
  - Human: describe governance, raise awareness

- Focus on replacement for current hardware (not QKD)

The Consortium

Great challenges demand great teams

CWI

- Cryptographic research

TU Delft

- Governance

Microsoft

- TSP, Moving to higher TRL

kpn

- TSP, test lab

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

- Digital government, policy authority “PKI govt”

ZYNYO.

- Provider of digital identification & signing services

TNO

- Coordination, PoC development

OK, that’s nice

Where are we?

- First year: focus on good start
  - Organising consortium work, establishing project structure
  - Reach out to stakeholders
  - Familiarising with topic, literature reviews, etc.

- Nevertheless, some nice results achieved already:
  - Publication on security proof of combiners
  - Publication on quantum-safe government

- Initial application area: certified documents (PAdES)
  - Less crowded area than e.g. SSL

What about the future?

Looking into 2023/2024

- Societal Impact Assessment, including video dissemination
- Report on governing QS PKIs
- Design of serious game
- First version PoC

HAPKIDO

Thank you for your time!

www.tno.nl/hapkido

Dr. Gabriele Spini, TNO