HAPKIDO

# HAPKIDO

# And the migration to Quantum-safe Public-key Infrastructures

Gabriele Spini | TNO
Nitesh Bharosa | TU Delft

# Agenda

| | |
|---|---|
| 12:00-12:15 | Opening |
| 12:15-13:00 | Presentation by Gabriele Spini (TNO) and Nitesh Bharosa (TU Delft) |
| 13:00-13:15 | Lunchbreak |
| 13:15-14:00 | Break-out: In deelsessies aan de slag met vraagstukken en acties onder leiding van de TU Delft en TNO. |
| 14:00 | Afsluiting |

## Stelling

# Mijn organisatie is gereed om de migratie naar kwamtumveilige crypto aan te kunnen.

# HAPKIDO

1. Wat is HAPKIDO?
2. Wat zijn de resultaten tot nu toe?
3. Wat staat er op de roadmap?
4. Interactie: wat kun jij met HAPKIDO?

# HAPKIDO
## Towards Quantum-safe PKIs

# HAPKIDO
## Some general info

- 5-year project, started in fall 2021
- Financed by NWO

TNO

TU Delft

CWI

Logius
*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*

kpn

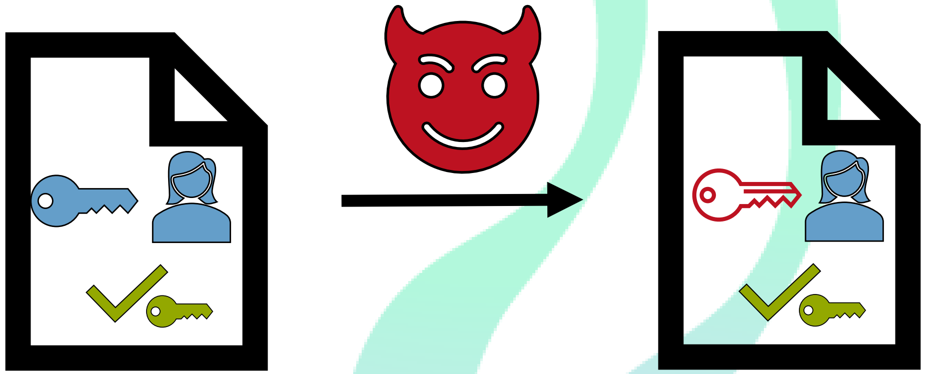
ZYNYO.

Microsoft

# Quantum computing and Cryptography

## Why HAPKIDO?

- Current asymmetric cryptography: broken by (large enough) quantum computer
  - PKIs no longer able to certify keys (can forge cryptographic digital signature)
  - Keys certified by PKIs no longer provide security guarantees (authenticity / confidentiality)



- When? Nobody knows but 10 years is considered realistic

- Why bother now?
  - Store-now-decrypt-later attacks
  - Migrating complex IT systems takes a lot of time (more relevant to PKIs)

# Enter HAPKIDO

## The project in a nutshell

- Hybrid Approach to quantum-safe Public-Key Infrastructure Development for Organizations
- Research project (no actual migration yet)
- Focus on hybrid PKIs
  No quantum technology
- Multi-disciplinary approach
  1. Technical
  2. Cryptographic fundamentals
  3. Governance aspects

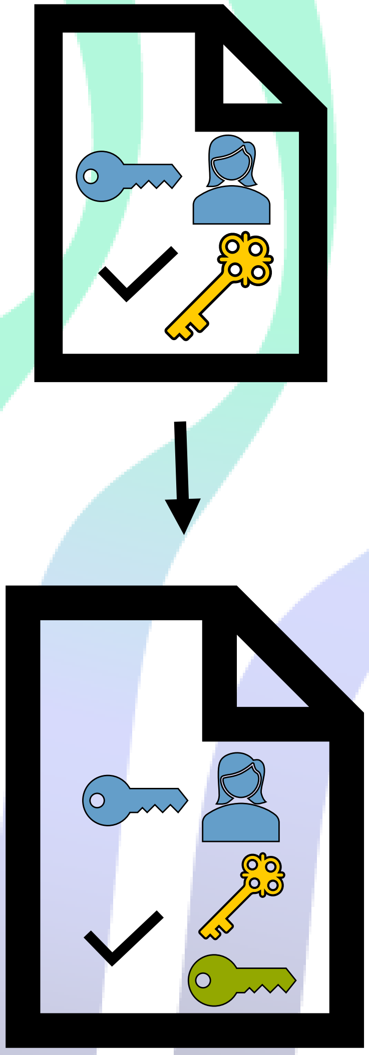
# Why hybrid?

## The H of HAPKIDO

- Hybrid: switching from classical to post-quantum in one go (“big-bang approach”) not feasible
  - Too many parties and systems involved: interoperability
  - Insufficient trust in post-quantum building blocks: can’t start too early

- Therefore: aim for systems that use both classical and post-quantum
  - When interfacing with “legacy” party/system: ignore post-quantum part
  - When possible, use both. System secure as long as one component secure

- However, this is not trivial:
  - Details are complex and security proofs are sometimes lacking
  - Attack surface increases
  - Need to “manage” both classical and post-quantum parties/systems



# HAPKIDO in the big picture

## What else is happening?

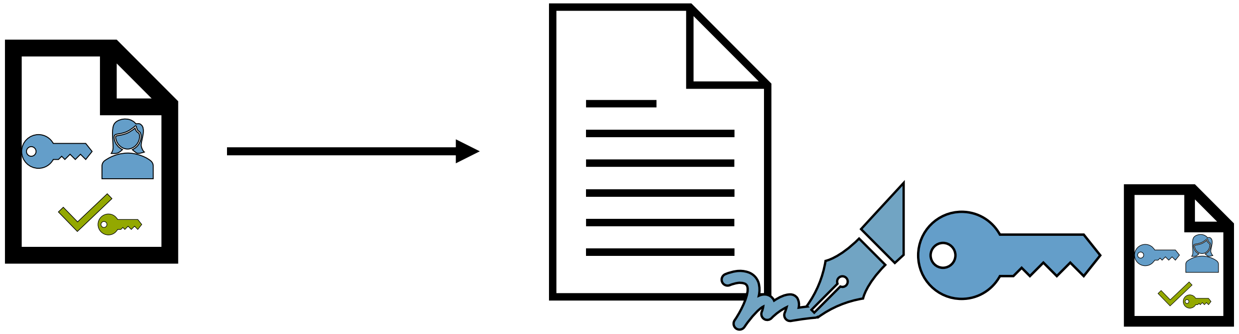
- Standardisation of Post-Quantum Crypto:
  - Building blocks: NIST, ISO
  - Protocols: IETF, GSMA, ETSI
  - Certificates (X509): ITU-T (“alternative” fields), IETF (“composite signature” drafts)

- Research initiatives:
  - BSI in Germany (focus on “German PKIOverheid”)
  - Research projects from number of TSP
  - NIST NCCOE

# Overview of Technical track

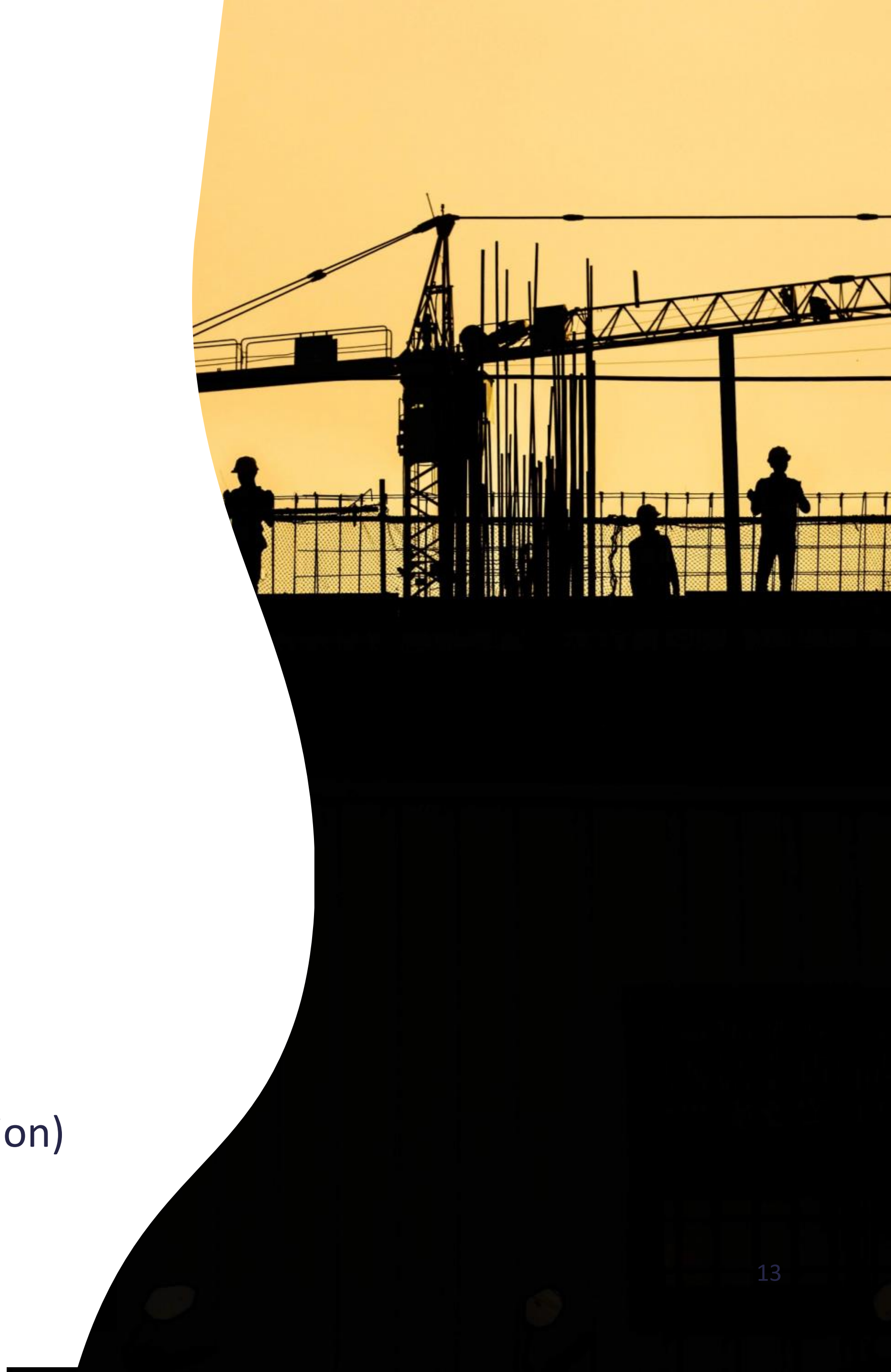
## Building Proofs of Concept

- Focus: PKIs for electronic signature of document



- (Much) less studied than e.g. TLS
- Legally binding
- Regulated in eIDAS

- Working hybrid version of DSS (official software from European Commission)
- Pending modification of PDF reader for testing & validation



# Overview of Cryptographic track

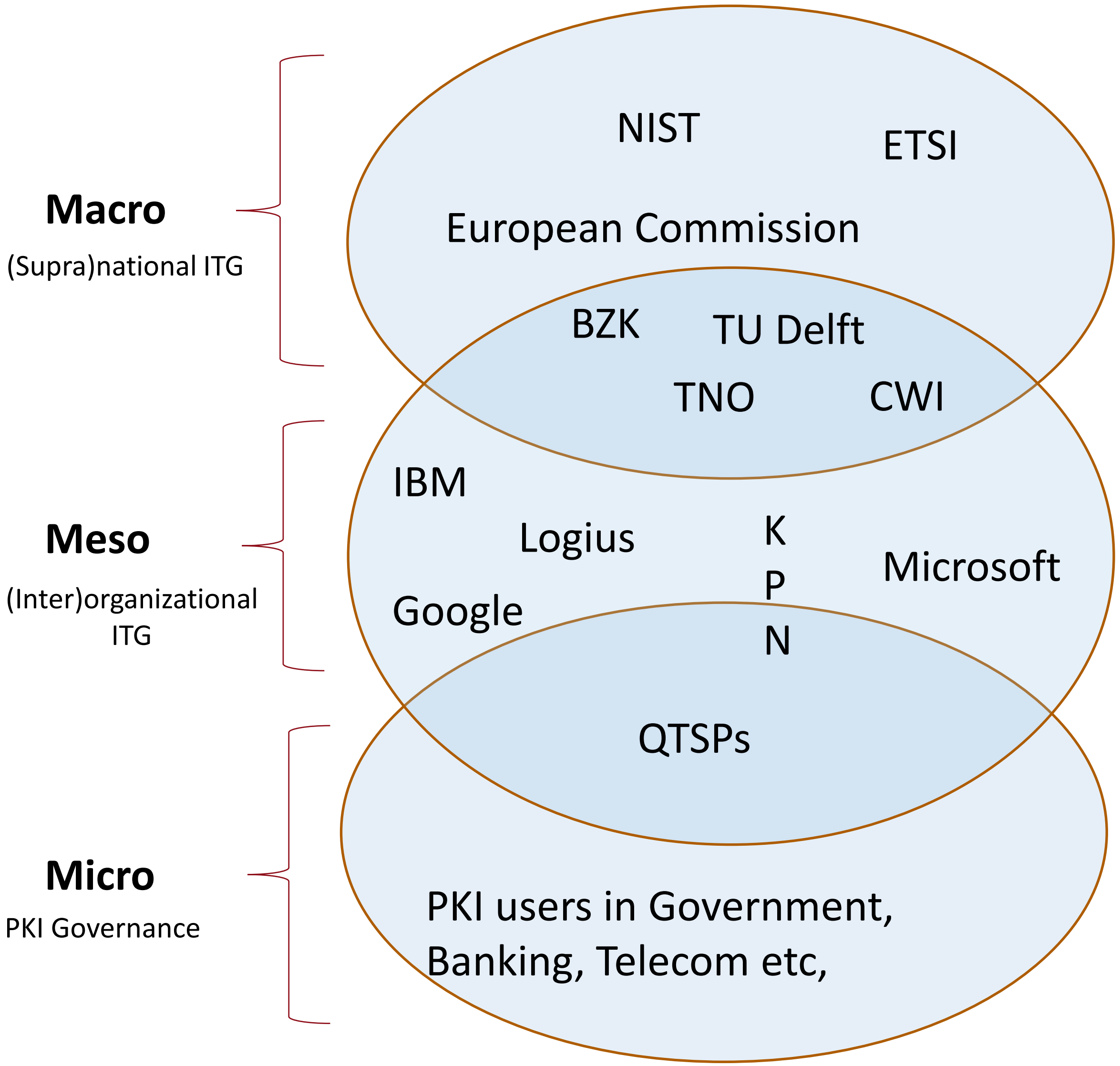
(Keeping it simple)

- Focus on mathematical security proofs
  - Well-established for classical cryptographic systems, much less for quantum-safe ones
  - Take quantum attackers into account

- Results so far:
  - Security of KEM combiners  
    (intuition: combining two encryption schemes into a single hybrid one)
  - Found mistake in security proof of Dilithium and fixed it

# Governance landscape

Spelers op PQC



**Macro**

(Supra)national ITG

**Meso**

(Inter)organizational ITG

**Micro**

PKI Governance

NIST

ETSI

European Commission

BZK

TU Delft

TNO

CWI

IBM

Logius

K
P
N

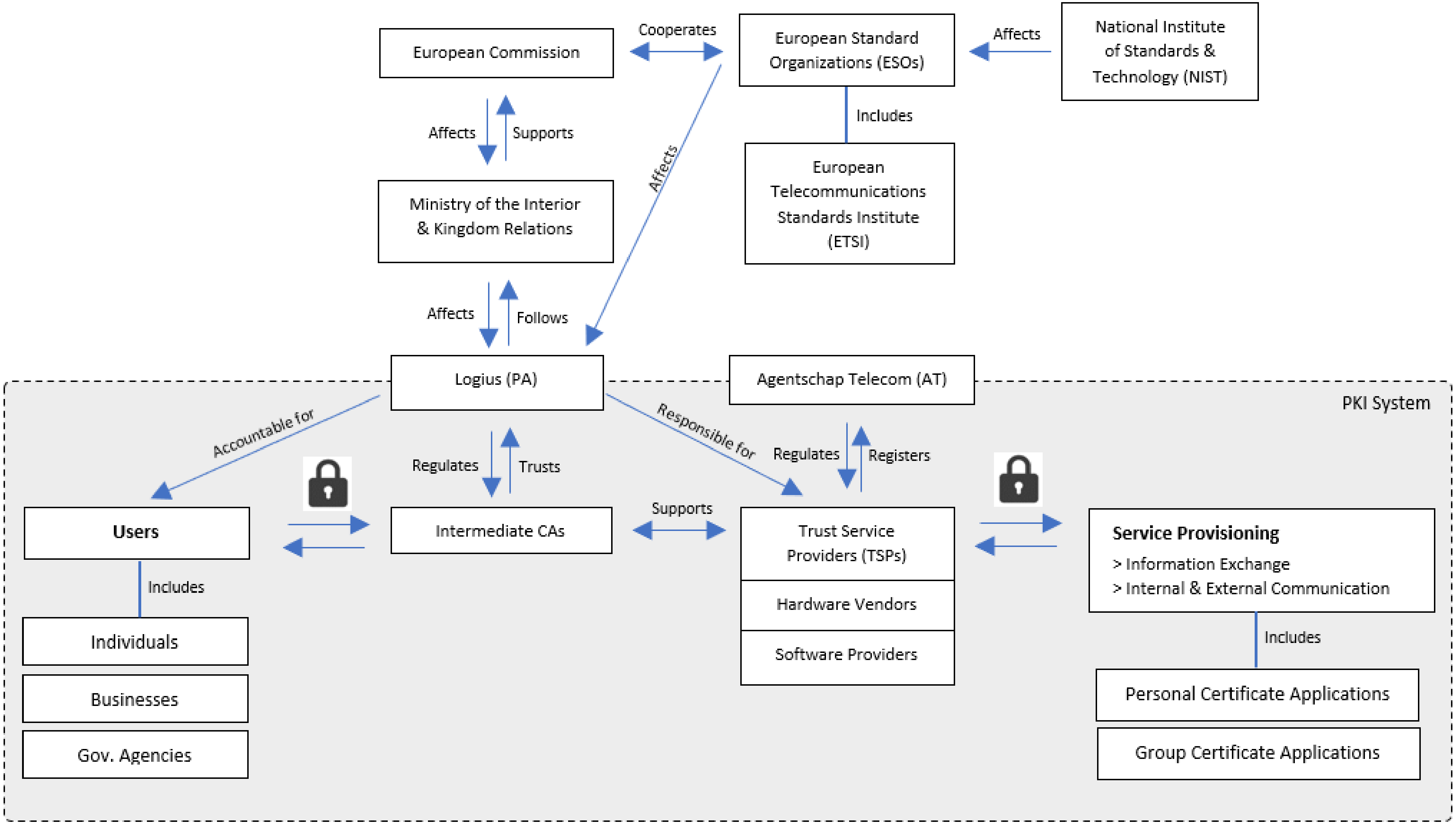
Microsoft

Google

QTSPs

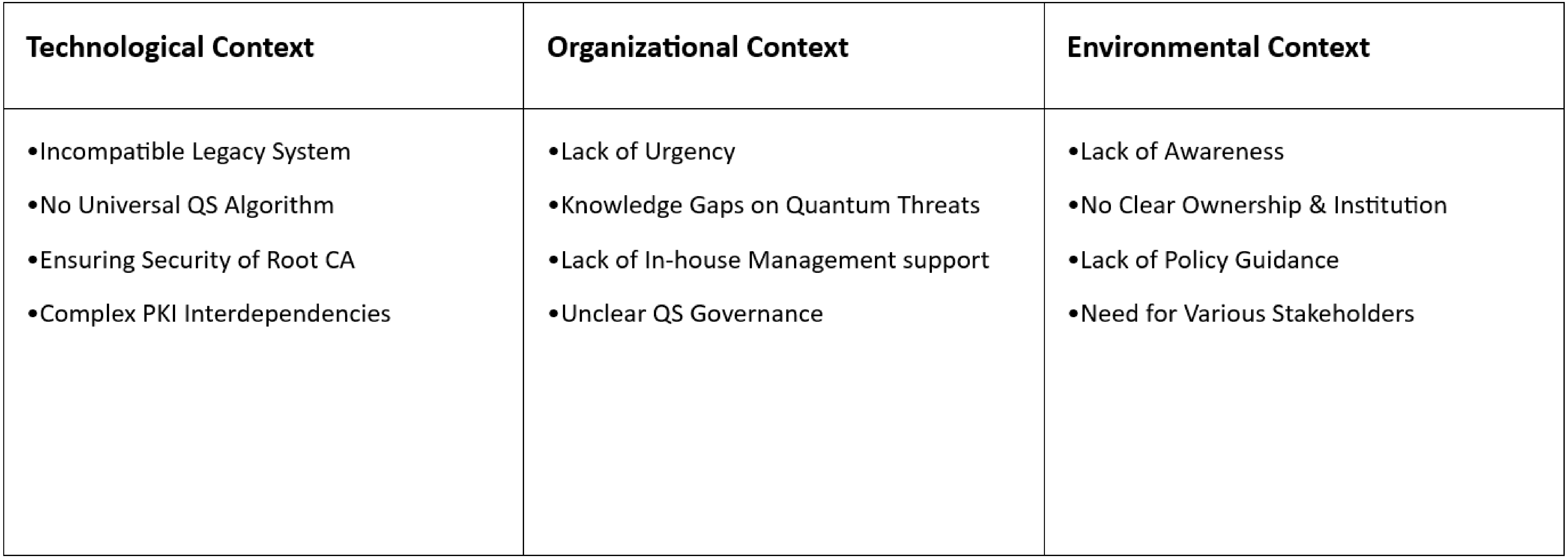
PKI users in Government, Banking, Telecom etc,

# Governance landscape



Source: Kong, I. 2022. PhD Proposal.

# Governance challenges



| Technological Context | Organizational Context | Environmental Context |
|---|---|---|
| •Incompatible Legacy System | •Lack of Urgency | •Lack of Awareness |
| •No Universal QS Algorithm | •Knowledge Gaps on Quantum Threats | •No Clear Ownership & Institution |
| •Ensuring Security of Root CA | •Lack of In-house Management support | •Lack of Policy Guidance |
| •Complex PKI Interdependencies | •Unclear QS Governance | •Need for Various Stakeholders |

Source: Kong, I., Janssen, M.& Bharosa, N. 2022. Challenges in the Transition towards a Quantum-safe Government.

# Whats on the roadmap (1/2)

## The way forward: 2023

- First full PoC
- Requirement analysis
- Report on governing quantum-safe PKIs
- Report on quantum-safe cryptographic combiners

# Whats on the roadmap (2/2)

Looking forward: 2024 and beyond

- More PoCs, likely with different applications
- Serious Game: collective action game
- Massive Online Open Course
- Self-assessment tool
- Enrich website https://tno.nl/hapkido

# HAPKIDO

A consortium of

TU Delft

TNO innovation for life

ZYNYO.

kpn

Microsoft

Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

CWI
Centrum Wiskunde & Informatica