ETSI/IQC Quantum Safe Cryptography Event

Quantum-safe public key infrastructures: the HAPKIDO project

Dr. Gabriele Spini, TNO

14/02/2023

Part 1:
A (very) quick recap of public-key infrastructures

The Hapkido Project | Dr. Gabriele Spini

Public-Key Infrastructures

Recap 1/2

- PKIs: systems to distribute, manage and authenticate cryptographic public keys

- Consists of
  - Parties
  - Policies
  - Algorithms
  - Hardware

- Revolve around certificate:
  - Guarantee that public key belongs to certain party
  - Certify intended usage of the key
  - …

Public-Key Infrastructures
Recap 2/2

- Cryptographic core components of PKIs:
  - Digital signatures
  - Hash functions

- Applications of PKIs: many!
  - TLS (most visible: )
  - Authenticate users / servers / networks in WiFi, VPNs, SSH…
  - Certified signatures of documents
  - …

- Again, not only a technical/cryptographic concept

Part 2:
Quantum-safe public-key infrastructures

The Hapkido Project | Dr. Gabriele Spini

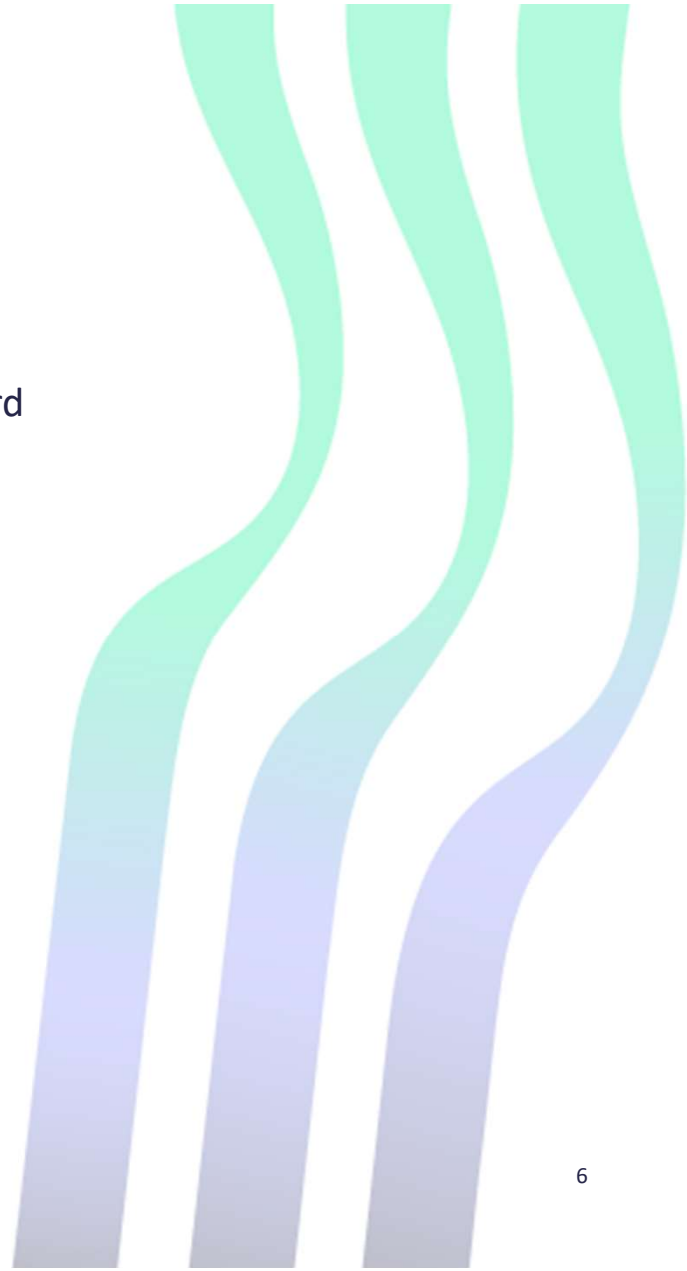
Quantum-safe Public-Key Infrastructures

Current state

- Two constructions for hybrid certificates in standardization:
  - ITU-T: Hybrid certificates with “alternative” key/scheme in latest X.509 standard
  - IETF: Hybrid certificates presented in draft

- Applications:
  - Huge focus on TLS
  - In general, focus on Internet protocols

- Mainly technical aspects investigated



Part 3:
HAPKIDO

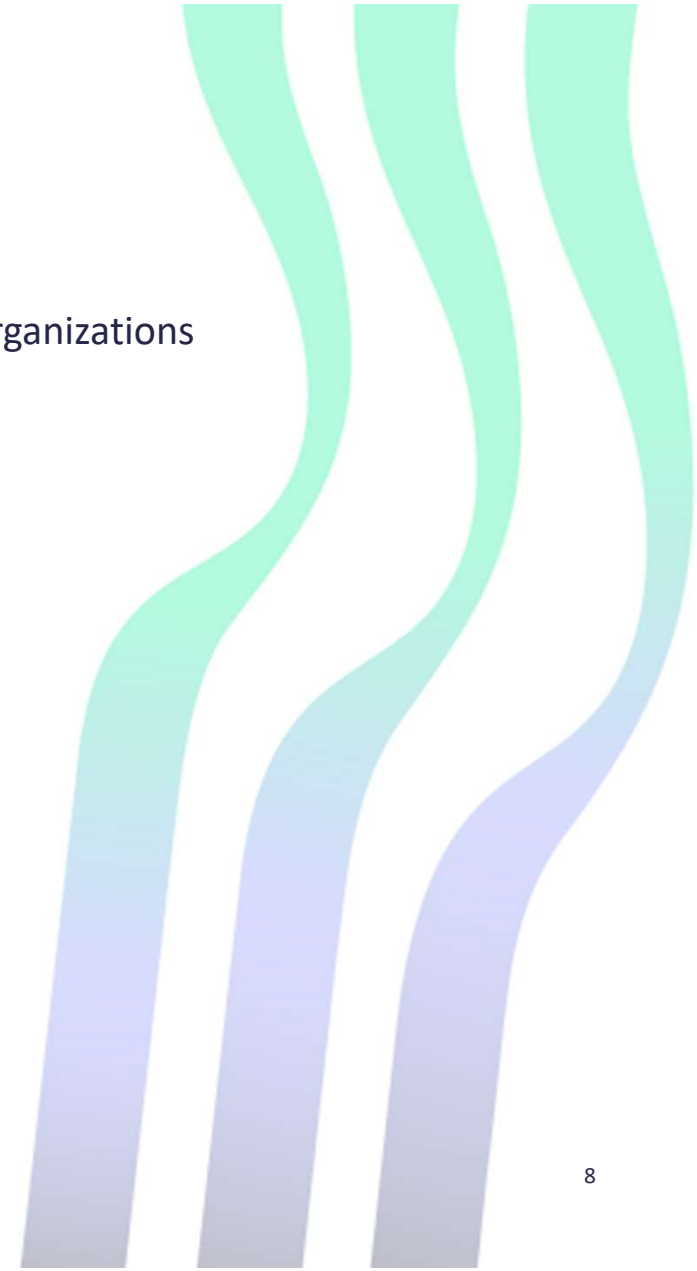
The Hapkido Project | Dr. Gabriele Spini

HAPKIDO

The project in a nutshell

- Hybrid Approach to quantum-safe Public-Key Infrastructure Development for Organizations
- Goal: study migration to hybrid quantum-safe PKIs in all aspects

- Technical
  - Provide proof-of-concept of PKI for different sectors/applications/use cases
  - Provide migration roadmap
- Fundamental
  - Study cryptographic security of combiners
- Policy and management
  - Governance study
  - Societal impact assessment
  - Raising awareness



HAPKIDO

Some more details about the plan

- 5-year project, started in fall 2021
- Financed by Dutch Research Council
- Involves Dutch organisations, international ambitions
- 4 sectors as per project proposal:
  1. Telecommunications
  2. Public sector
  3. Healthcare
  4. Financial

The Consortium

Great challenges demand great teams

- Cryptographic research
- Policy & Management
- TSP, Moving to higher TRL
- TSP, test lab
- Digital government, policy authority “PKI govt”
- Provider of digital identification & signing services
- Coordination, PoC development

The Progress so far
General remarks

- For this first phase of project:
  focus on PKIs for digital signing of (PDF) documents

- Often legally binding, regulated in e.g. eIDAS

- Motivation:
  - Less studied than e.g. PKI used for TLS (but same certificate format)
  - Relevant to all application domain of proposal
  - Relevant to consortium partners

The Progress so far

Management-and-policy track

- Three main lines of work:

- Societal impact assessment
  - Report soon to be finished

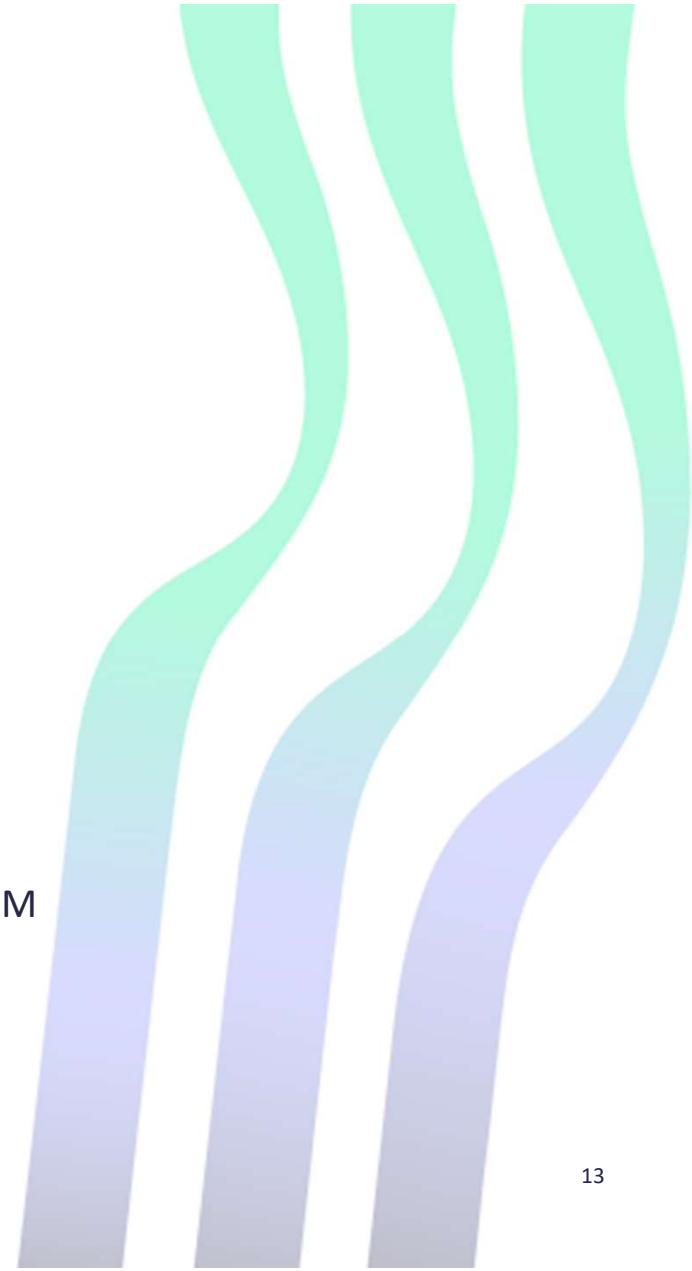
- Governance
  - Identified challenges in transition to QS PKI for public sector: https://dl.acm.org/doi/10.1145/3543434.3543644

- Serious game to raise awareness
  - Requirements identified, moving to next phase

The Progress so far

Cryptographic track

- Focus on cryptographic combiners
  - Combine several cryptographic schemes into one, having same functionality
  - Secure if at least one component secure
- Especially for KEM combiners, often no security proof in Q-ROM
- A first result:
  - Compiler to turn adaptive oracle-based schemes into static ones, efficiently
  - Consequence: construction of KEM combiner from PRF proven secure in Q-ROM
  - https://eprint.iacr.org/2022/773



The Progress so far

Technical track

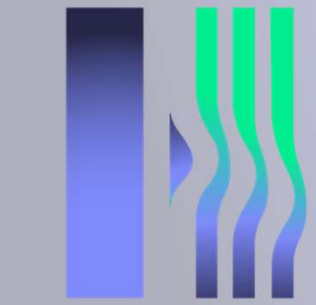
- Focus on hybrid PKI for document signing (eIDAS framework)
- First PoC due end 2023
- Some first observations:
  - Hybrid certificates standardized by ITU-T since 3 years, but not yet commonly implemented in certificate-management tools
  - Crypto agility (e.g. of signing software) often problematic: multiple schemes not taken into account

Part 4:
The future of HAPKIDO

The Hapkido Project | Dr. Gabriele Spini

HAPKIDO
Looking forward

- 2023:
  - First PoC version
  - Societal impact assessment
  - Requirement analysis
  - Report on quantum-safe cryptographic combiners
- 2024 and beyond:
  - More PoCs with different applications
  - Awareness-creation game
  - Massive Online Open Course
  - Self-assessment tool
  - Enrich website https://www.tno.nl/en/digital/digital-innovations/trusted-ict/hapkido/



Thank you for your attention!

Dr. Gabriele Spini