



The HAPKIDO Project

Dr. Gabriele Spini, TNO

Part 1: HAPKIDO, present and past

The Hapkido Project | Dr. Gabriele Spini



HAPKIDO

The project in a nutshell 1/2

- › 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

The project in a nutshell, 2/2

- › 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



CWI

- › Cryptographic research



TU Delft

- › Policy & Management



Microsoft

- › TSP, Moving to higher TRL



kpn

- › TSP, test lab



HAPKIDO



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

- › Digital government, policy authority “PKI govt”

ZYNYO.

- › Provider of digital identification & signing services

TNO

- › Coordination, PoC development

The focus so far: document electronic signatures

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

- › Often legally binding, regulated in e.g. eIDAS
- › Relevant standards: ETSI (e.g. PAdES)

- › Free and open source signing software provided by European Commission (not QS)

- › Motivation:
 - Less studied than e.g. PKI used for TLS (same certificate format, other challenges)
 - Relevant to consortium partners



The Progress so far

Management-and-policy track

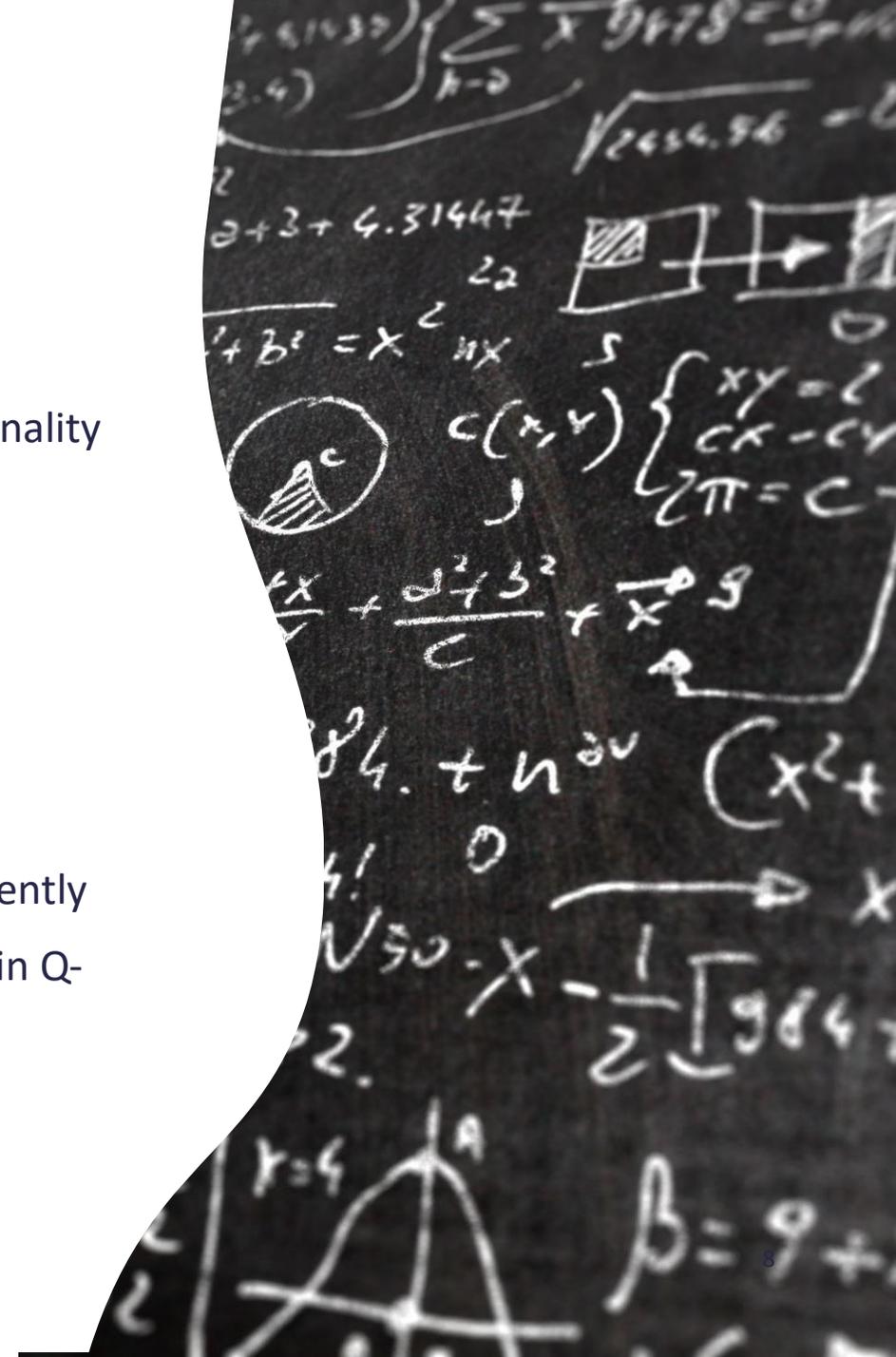
- › Three main lines of work:
 - › Societal impact assessment
 - Report soon to be finished
 - › Governance
 - Identified challenges in transition to QS PKI for public sector:
<https://dl.acm.org/doi/10.1145/3543434.3543644>
 - › Serious game to raise awareness
 - Requirements identified, moving to next 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

- › First PoC due end 2023
- › Some first observations:
 - Hybrid certificates standardized by ITU-T since 3 years, but not yet commonly implemented in free certificate-management tools:
need to pay or implement own tool
 - Little crypto agility for e.g. of document-signing software:
multiple schemes not taken into account
 - Need to collaborate to upgrade standards





Part 2: The Future of HAPKIDO



HAPKIDO

Looking forward: 2023

- › First PoC version
- › Societal impact assessment, including dissemination video
- › Requirement analysis
- › Report on quantum-safe cryptographic combiners



HAPKIDO

Looking forward: 2024 and beyond

- › More PoCs with different applications
- › Awareness-creation game
- › Massive Online Open Course
- › Self-assessment tool
- › Enrich website <https://tno.nl/hapkido>





HAPKIDO

Thank you for your attention!
Interested? gabriele.spini@tno.nl

Dr. Gabriele Spini