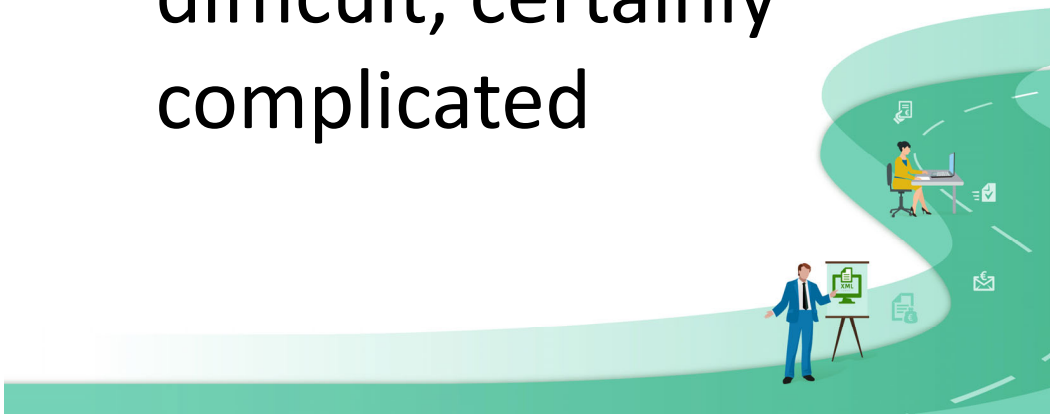
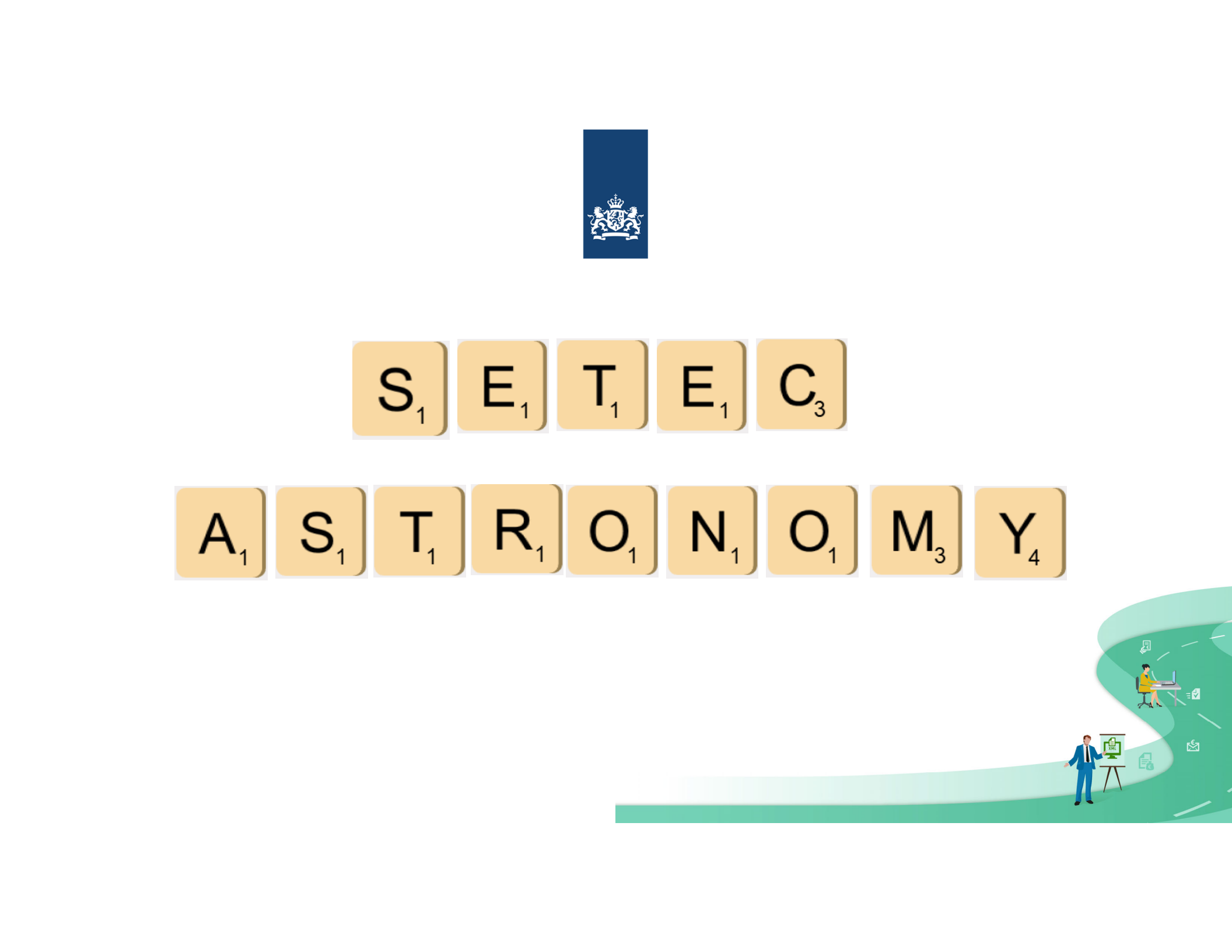
Robert Leyting

Logius PKIoverheid

PKI government and post-quantum cryptography

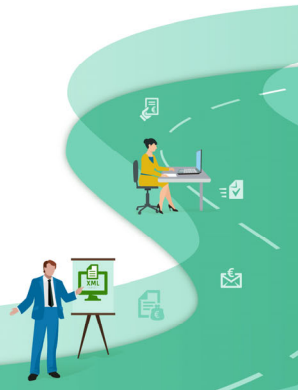
Not necessarily difficult, certainly complicated




S1 E1 T1 E1 C3
A1 S1 T1 R1 O1 N1 O1 M3 Y4

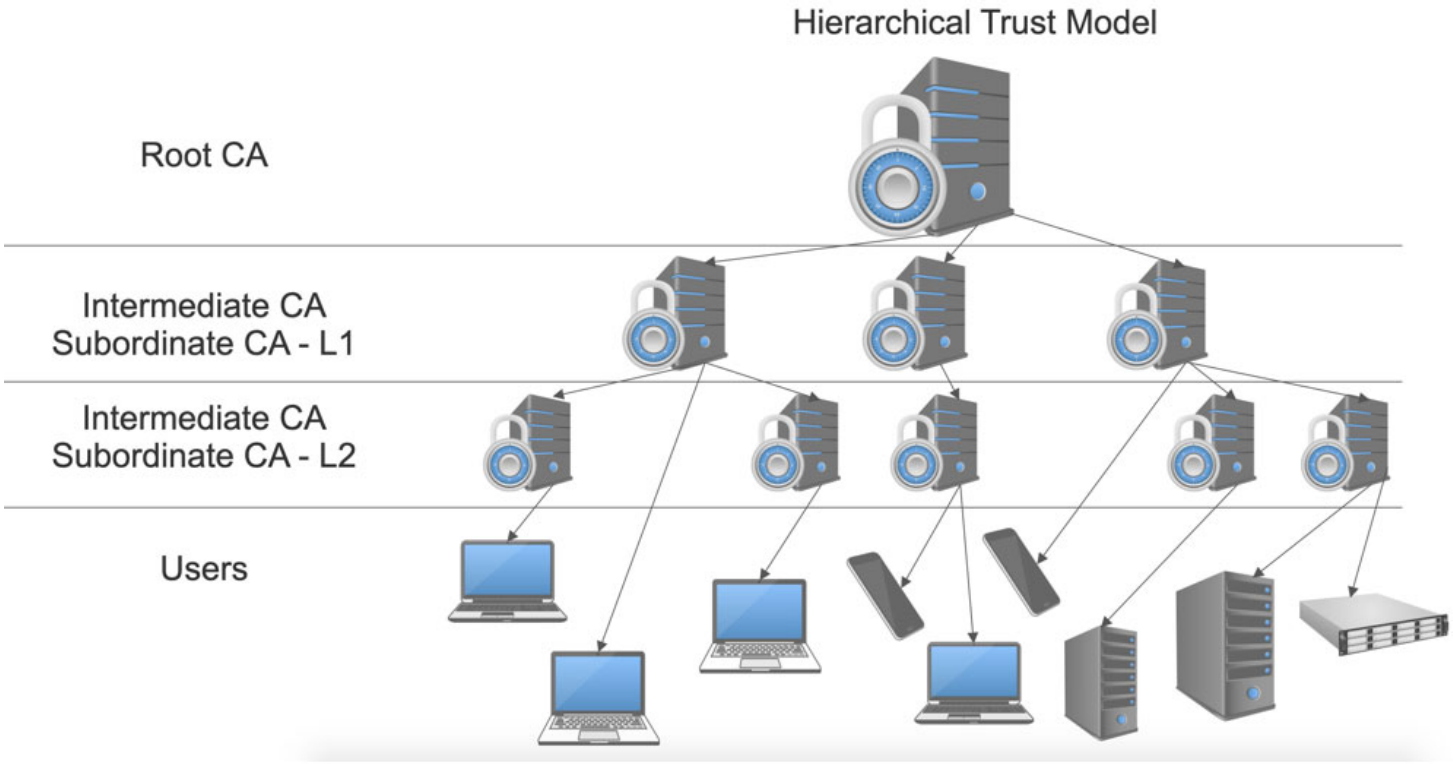
Intro

- Intended audience
- Quantum computing developments



What is a PKI

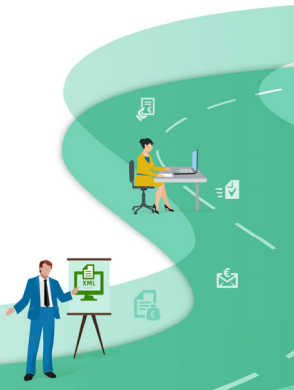
The impact Quantum Computing has on PKI and PKIoverheid



Bron afbeelding: https://medium.com/@meghdadshamsaei/trust-model-implementation-by-pki-7cddcdb72513

Broken

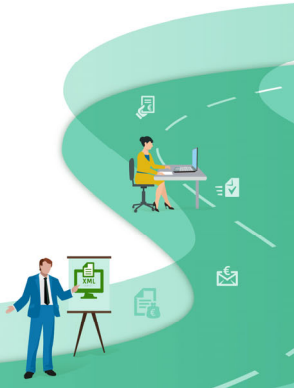
- Signatures (contracts!)
- Code signing (automatic software updates!)
- SSH Secure Shell protocol (remote management!)
- etc



How to mitigate

Replace broken crypto with quantum safe crypto

- Symmetric crypto
- Quantum safe asymmetric crypto
- Quantum crypto



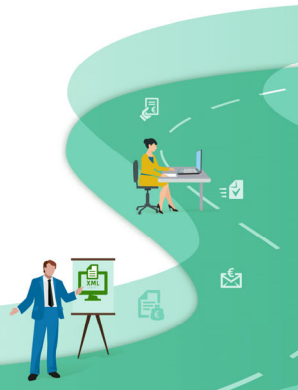
Timeline

- Finding right crypto
- Implementation

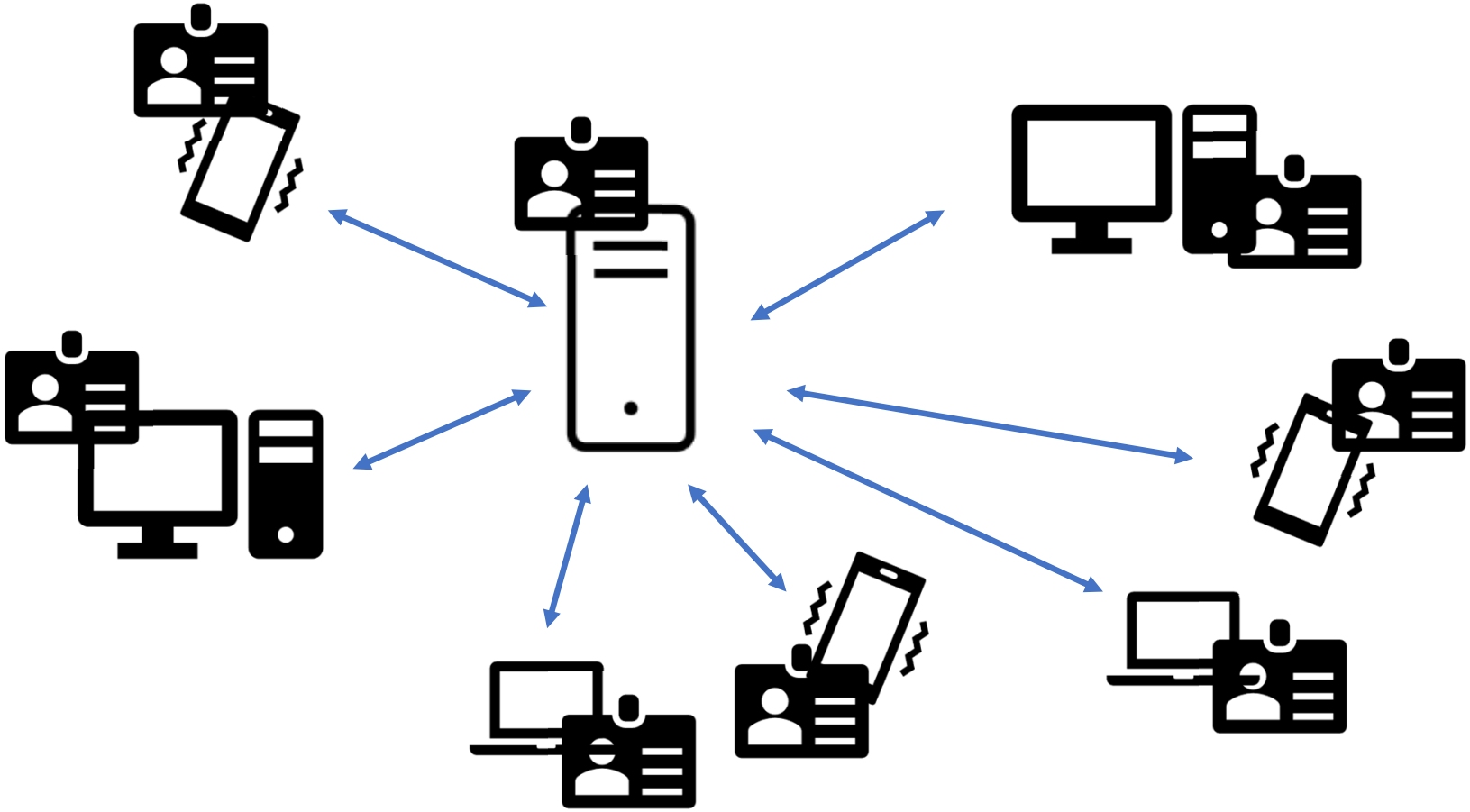
If above ready: DONE

But…..

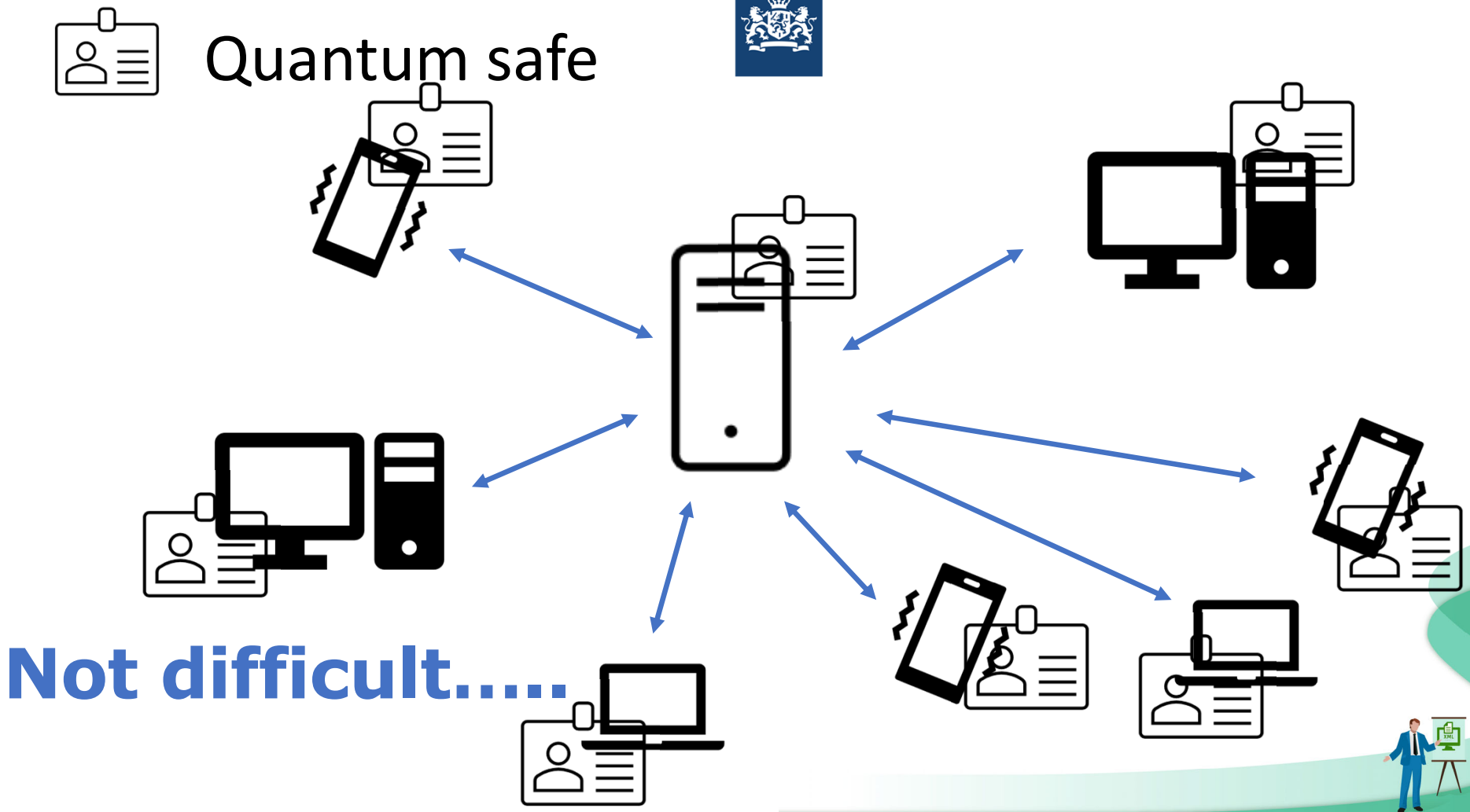
- +Security lifetime of data (store & decrypt)



Quantum broken



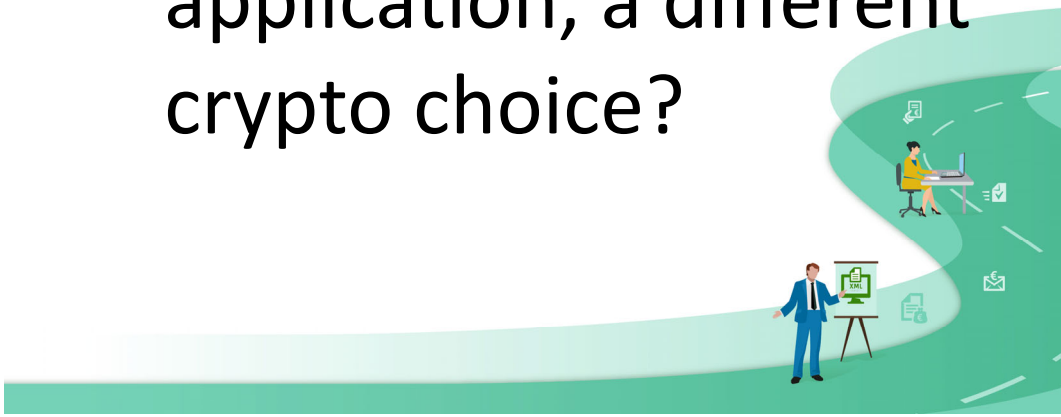
Quantum safe



Not difficult.....

Definitely complex

- Dual PKI infrastructure?
- Forced replacement or natural attrition (1/2/3 years)?
- Depending on the application, a different crypto choice?



PKI overheid infrastructure renewal

- Design specifications
- Tender (european procurement rules)
- Contracts, agreements
- Building infrastructure
- Auditing & certification

Hapkido

Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations

- Logius offers a PhD position
- Research will start in the coming months

We have left the station

Destination??

Wrap-up

- There is a lot at stake
- A lengthy process
- Lots of dependencies
- Many possibilities and variations