# Protecting electronic identity documents in the age of quantum computing

Robert Bach

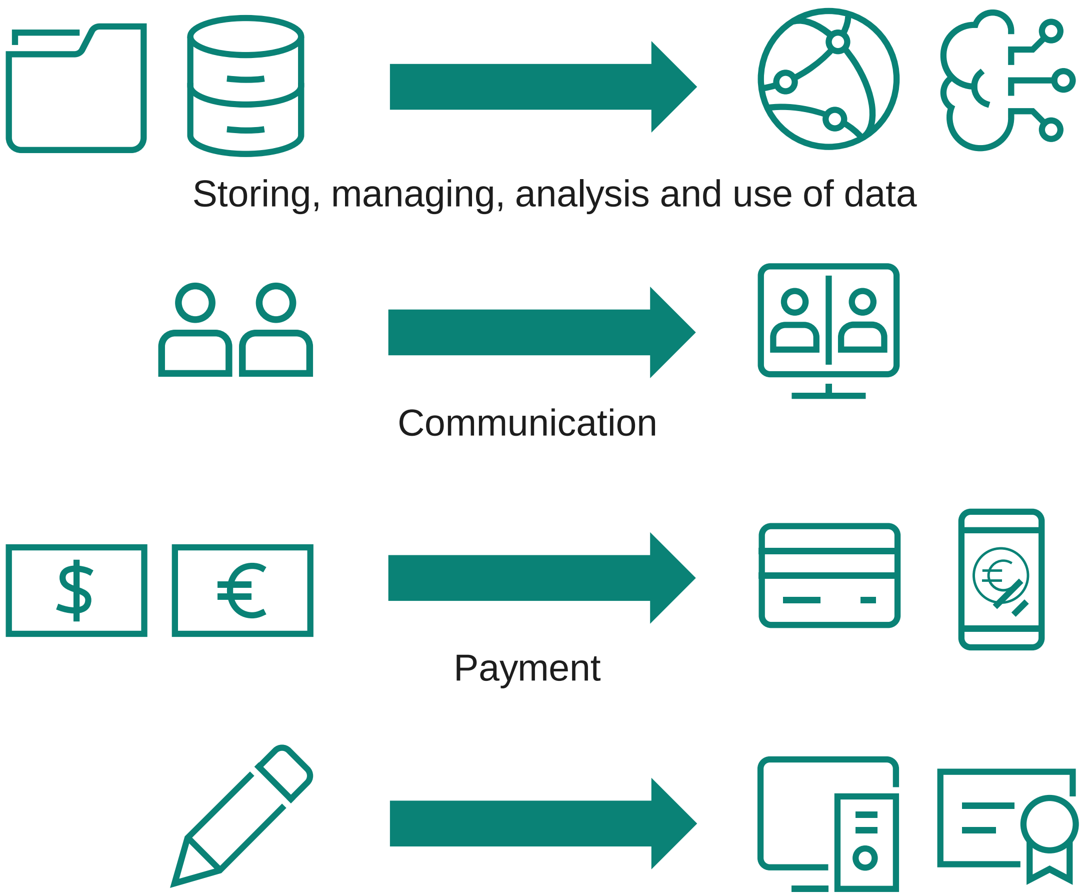
10-04-2024

# Table of contents

# Table of contents

# Fundamental shift in less than one century... and still accelerating

## Our lives have changed...



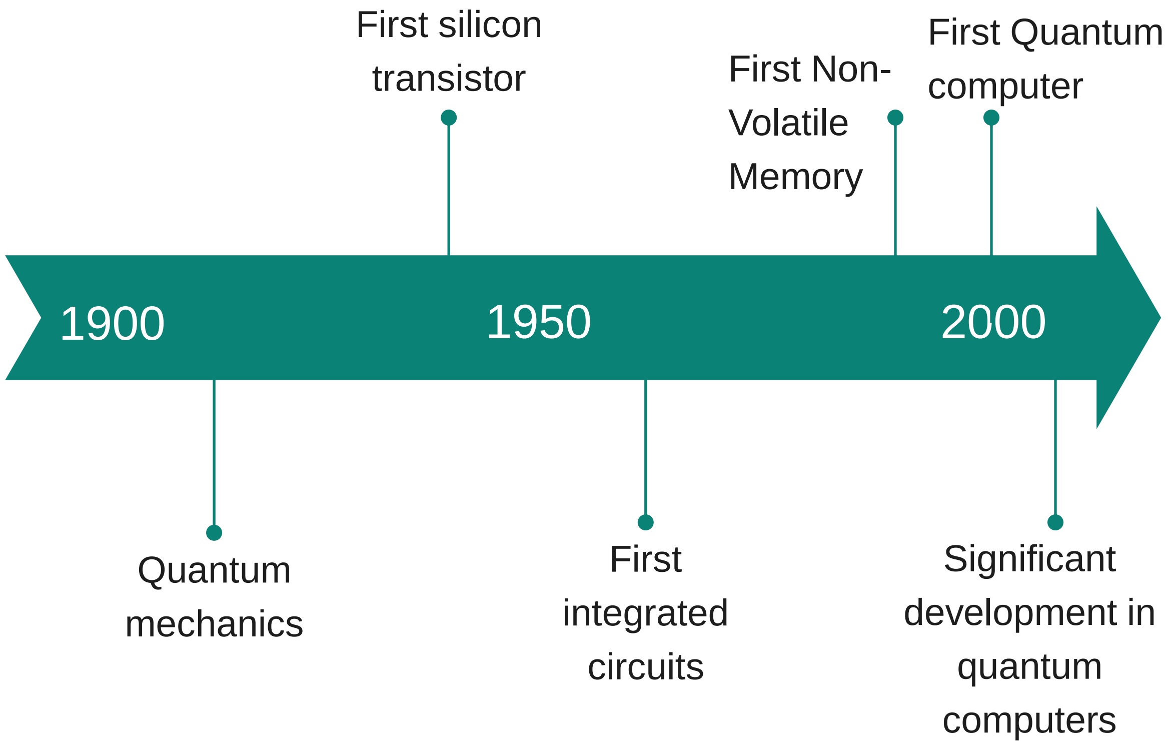
Storing, managing, analysis and use of data

Communication

Payment

Signing contracts

## ...with the invention of semiconductors



Quantum mechanics

First silicon transistor

First integrated circuits

First Non-Volatile Memory

First Quantum computer

Significant development in quantum computers

# Table of contents

# Conventional vs quantum computer

## Conventional computer

- Relies on binary bits
- Only represent 1 or 0 of binary information
- Performs computational steps sequentially

## Quantum computer

- Relies on quantum bits (qubits)
- Represents 0, 1 and any value in between simultaneously
- Computes in parallel (entanglement) on qubits

# Quantum computer at a glance

### Underlying principles

- Superposition
- Entanglement

### Good at

- Much faster problem solving such as
  - Finding an element in a large set
  - Finding an optimal solution

### Particularly good at

- Prime factorization

851 = a x b
a = ? b = ?

851 = 23 x 37

# Quantum computers – a threat to currently known security algorithms

**Asymmetric cryptography**

Public key – encryption; private key - decryption

Today

**RSA**

- **Security foundation:** Difficulty of factorization with sufficiently large numbers
- With today’s computers, factorization of sufficiently large numbers is practically not possible to break

Tomorrow

**Shor’s algorithm**

- Solves discrete logarithm problems such as factorization
- Exploits a property of the algorithm

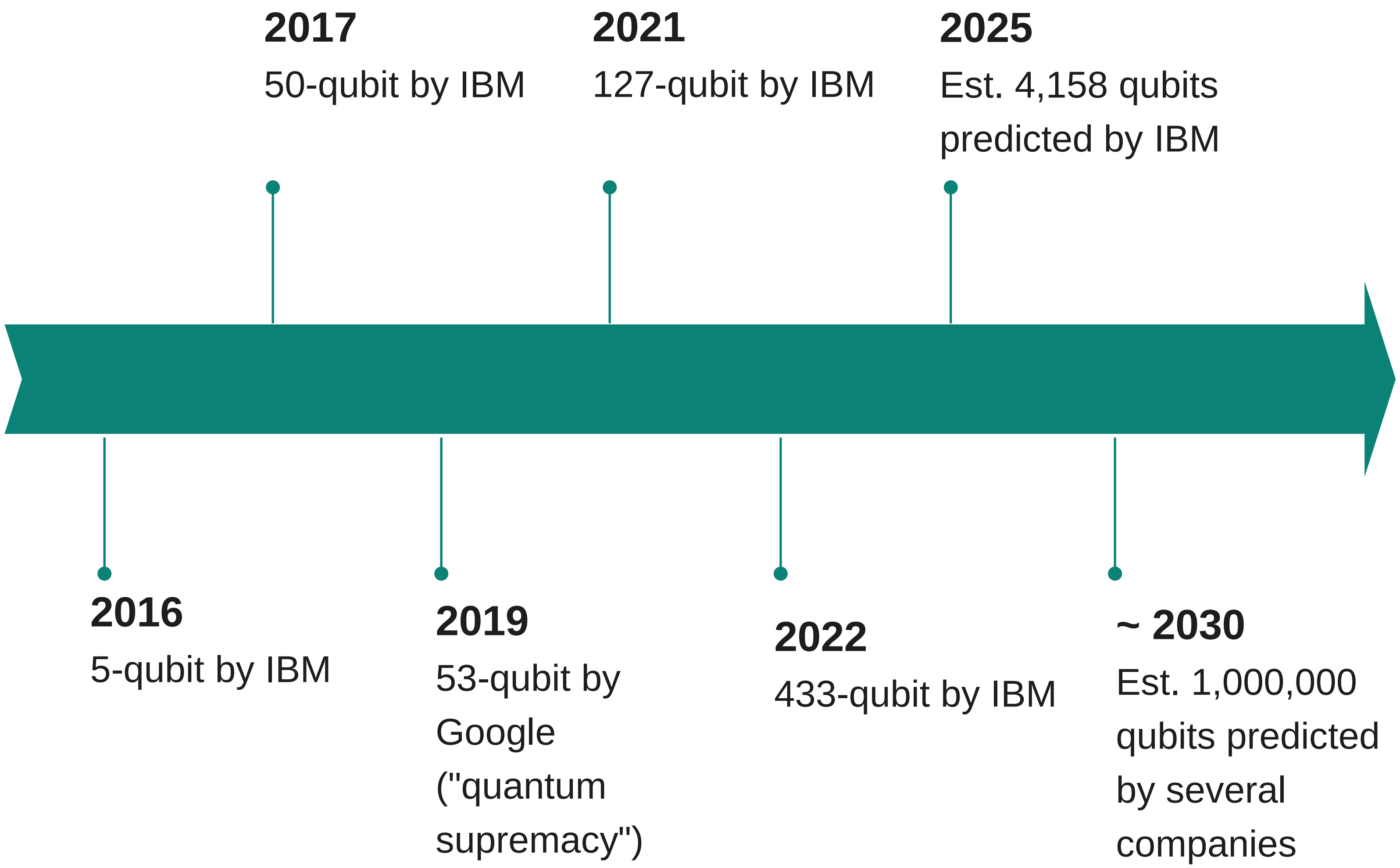
**Heavily affected – almost no security**
**RSA, ECDSA, ECDH**

**In a “quantum world”**

# Challenges, achievements, and the road ahead

## Challenges

- To have a **high number of stable** qubits (topic to be resolved: qubit decoherence)
- Scalability



**2016**
5-qubit by IBM

**2017**
50-qubit by IBM

**2019**
53-qubit by Google ("quantum supremacy")

**2021**
127-qubit by IBM

**2022**
433-qubit by IBM

**2025**
Est. 4,158 qubits predicted by IBM

**~ 2030**
Est. 1,000,000 qubits predicted by several companies

# Potential threats and implications on governmental identification and digital services

## Harvest now – decrypt later

- Access data with long shelf life & validity
  - Critical infrastructure
  - Defense and military communication systems
  - Biometric data such as fingerprints & IRIS

## Vulnerability of asymmetric cryptography

- Communication protocols
- Digital signatures

## Weakened security of gov applications

- Identity theft
- Misuse of identity
- Digital signature functionality of ID applications
- Lost credibility of the ID & gov digital services

**›› Post-Quantum Cryptography is the answer to secure our data and identity**

# Table of contents

# Post-Quantum Cryptography at a glance

## Post-Quantum Cryptography (PQC)

- “Refers to cryptographic methods that are assumed to be unbreakable even with the aid of a quantum computer”*

**Source: Federal Office for Information Security (BSI)*

- Aims to repel cryptanalysis performed by both quantum computer and conventional computer

## Quantum-secured crypto algorithms

- 6 families of PQC algorithms are known
- None of them is widely used today
- Best suited for smart cards:
  - Lattice-based
  - Hash-based

# Standardization effort of National Institute of Standards and Technology (NIST)

### Goal

- Develop cryptographic systems secured against quantum and conventional computer attacks
- Interoperate with existing communications protocols and networks

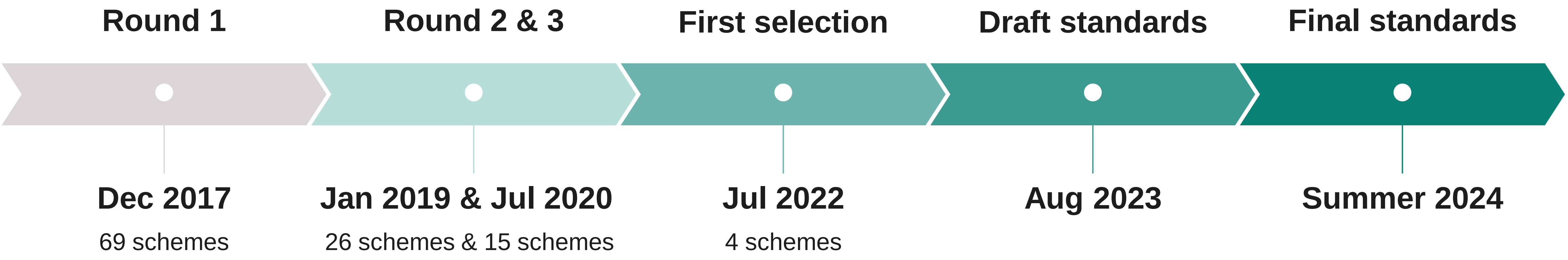
### Evaluation criteria

- Security
- Cost
- Algorithm and implementation characteristics

### Competition-like process

Submissions of key exchange, public-key encryption, signature schemes

- **From Infineon:** key exchange mechanism **NewHope** and digital signature scheme **SPHINCS+**



**Round 1**

**Dec 2017**

69 schemes

**Round 2 & 3**

**Jan 2019 & Jul 2020**

26 schemes & 15 schemes

**First selection**

**Jul 2022**

4 schemes

**Draft standards**

**Aug 2023**

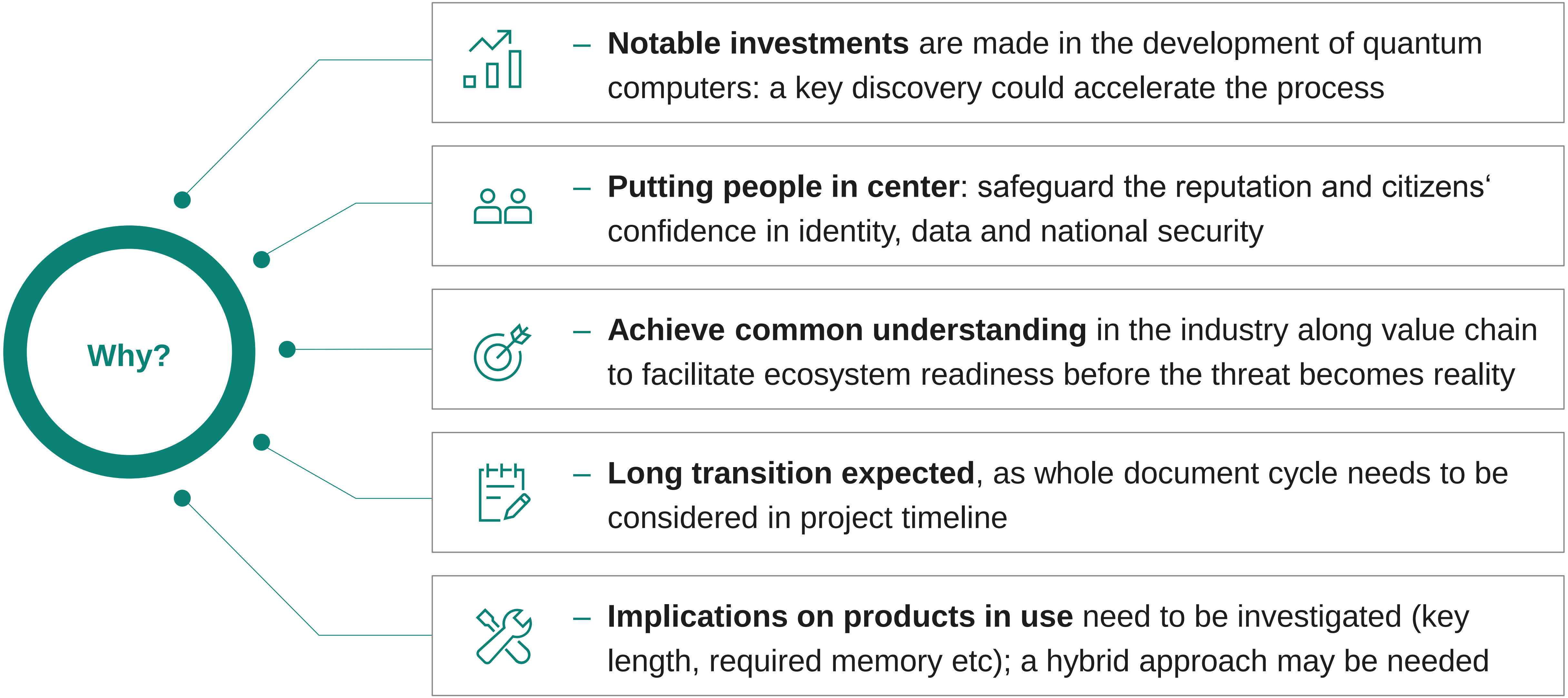
**Final standards**

**Summer 2024**

**CRYSTALS-Kyber (= „ML-KEM“) & CRYSTALS-Dilithium (=„ML-DSA“) are deemed best suited for smart cards**

# Table of contents

# Even without imminent security threat from quantum computers, immediate actions for risk mitigation is highly recommended



- **Notable investments** are made in the development of quantum computers: a key discovery could accelerate the process
- **Putting people in center**: safeguard the reputation and citizens‘ confidence in identity, data and national security
- **Achieve common understanding** in the industry along value chain to facilitate ecosystem readiness before the threat becomes reality
- **Long transition expected**, as whole document cycle needs to be considered in project timeline
- **Implications on products in use** need to be investigated (key length, required memory etc); a hybrid approach may be needed

# Ecosystem readiness: the prerequisite for a successful field implementation of quantum-proof electronic Identity Documents

### NIST process finalization

- Draft standards for selected schemes available, final standards expected in summer 2024
- Foundation for application standards

### Interoperatability-Test conformity

- Pilot project
- Learning cycle

### Application standards will be updated

- International / national
- Document functionality and lifetime
- Technical specification revision

### Regulations & certifications

- Revise regulations
- Refine certification process

### Proof of concept

› Upgraded document

› Upgraded personalization

› Upgraded infrastructure

### Migration plans

- Document, infrastructure (on firmware, protocol) and background system update
- Migration plan (& Tender)

# Table of contents

# Key takeaways

- The field of quantum computers is advancing and typical cryptography currently used in eID documents will be vulnerable

- Post-Quantum Cryptography is intended to be future-proof but standardization and market introduction will take many years

- Documents and infrastructure need to be upgraded
- Long transition periods with steep learning curve expected

**It is highly recommended to start the risk mitigation right now**

# Infineon contributes actively to a smooth transition to future-proof security solutions

## Research & Development

- Research on attacks and countermeasures to protect implementations of PQC against physical attacks
- Efficient implementation of PQC algorithms in ID-related protocols

## Trial Implementation

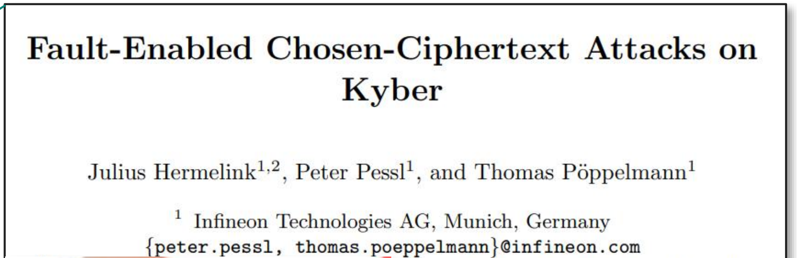
- Based on New Hope, an awarded post-quantum key-exchange algorithm
- 1st PQC on commercially available contactless security chip
- Facebook Internet Defence Prize 2016 & two Sesames Awards in 2017

## Standardization

- Submission of 2 proposals to NIST process
- Active participation in standardization activities
- Collaboration with academic community, customers and partners

## Public Funding Projects

- 6 running / finalized projects
- World’s 1st demonstrator for an electronic passport, based on a quantum computer-resistant Extended Access Control (EAC) protocol



Fault-Enabled Chosen-Ciphertext Attacks on Kyber

Julius Hermelink[1,2], Peter Pessl[1], and Thomas Pöppelmann[1]

[1] Infineon Technologies AG, Munich, Germany
{peter.pessl, thomas.poeppelmann}@infineon.com
ät der Bundeswehr München, Munich,
ermelink@unibw.de

ation process is in the third round,

Infineon