MONET +

Post-Quantum Cryptography

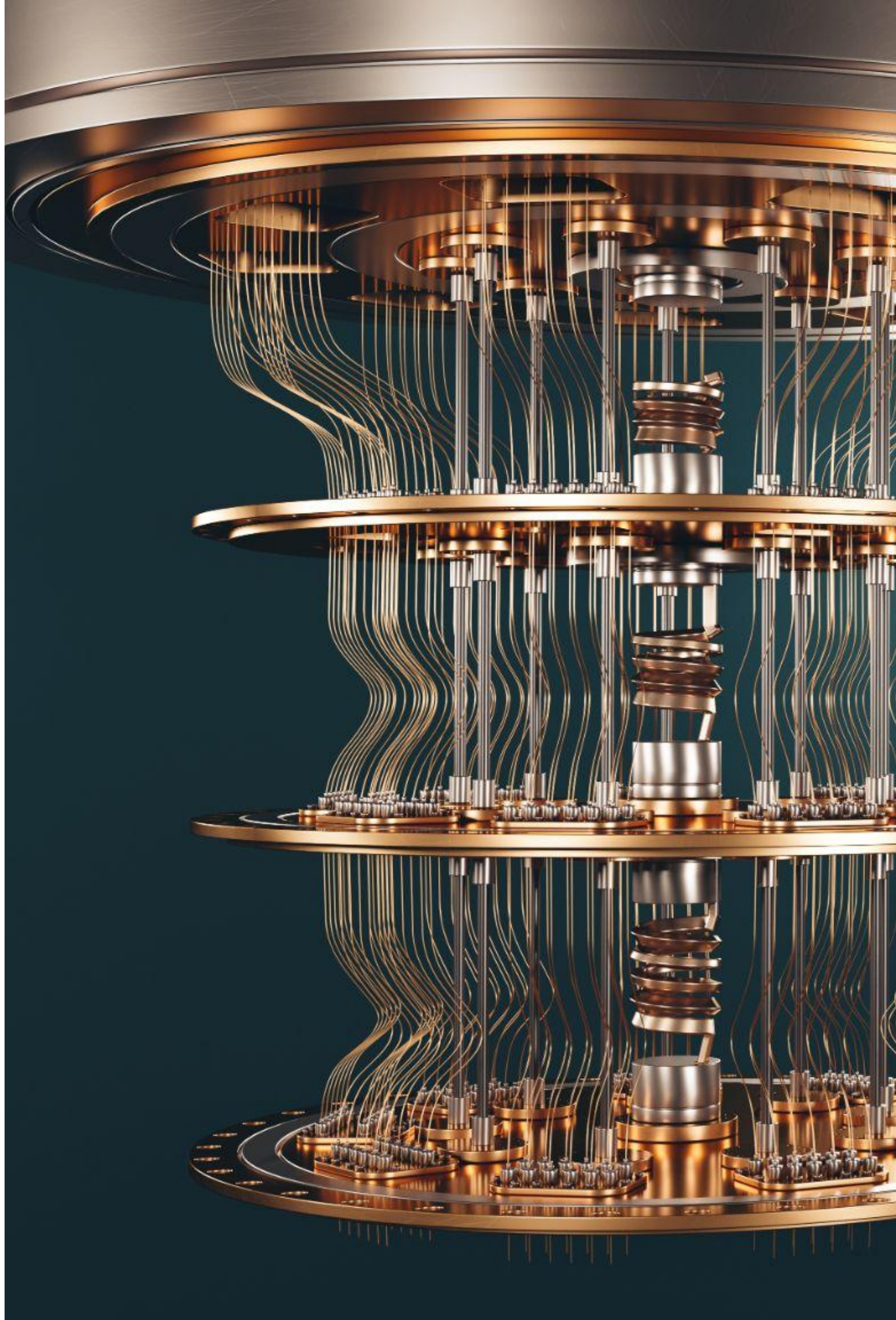
Security Talk Praha

Mgr. Anežka Pejlová
Security Architect

What is PQC?

Quantum computers

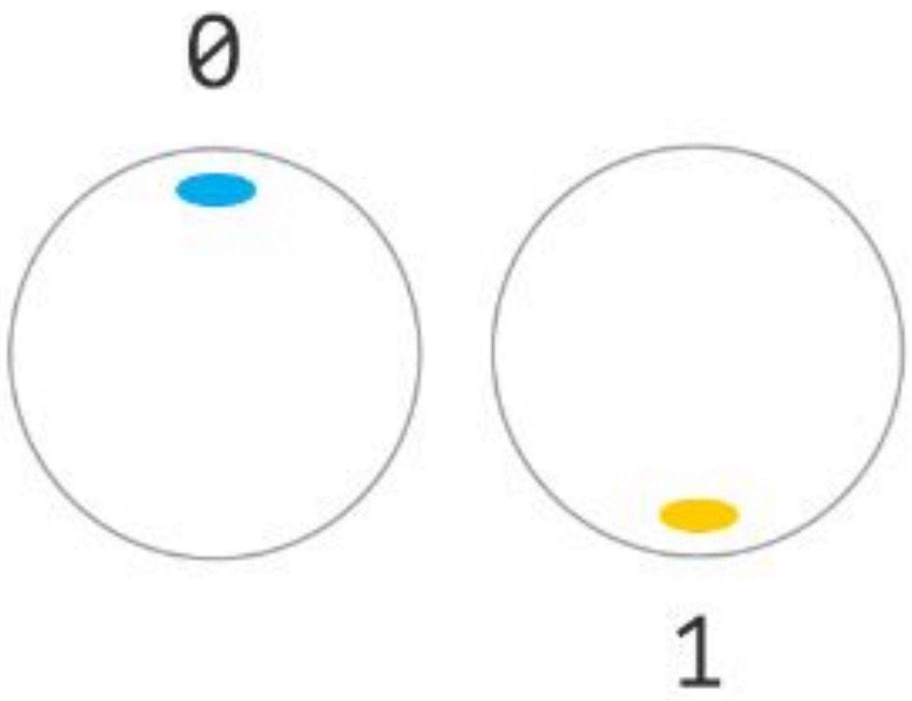
- change of paradigm in computer world
- more effective solution to some hard problems
- significant progress/breakthrough in
  - AI
  - optimization problems
  - discovery/development process
  - financial modeling
  - weather forecasting
  - cybersecurity
  - …



Classical vs. Quantum computer

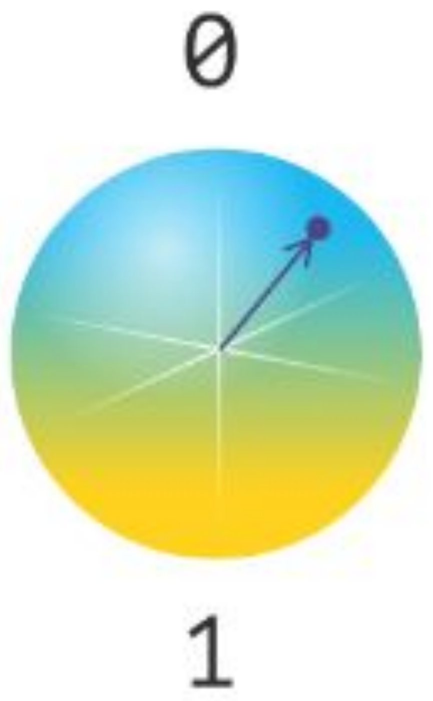
bits

- 0 or 1
- nothing in between
- classical



qubits

- any superposition between 0 and 1
- measurement = final state
- dependent on the probability of superposition
- quantum



What is cryptographically relevant quantum computer (CRQC)?

- classical cryptography is based on “hard” mathematical problems
  - factorization
  - discrete logarithm
- “hard” = **classical** computer **cannot** solve it **efficiently**
- **CRQC** is capable of **efficiently** solving these “hard” problems

Post-quantum cryptography (PQC)

- cryptography secure against attacks by quantum computers (CRQC)
- based on different mathematical concepts
- PQ algorithms are feasible on classical computers
  - vs. quantum cryptography

Why to bother with PQC?

MONET +

Quantum impact on classical cryptography

Which systems are **NOT affected** by CRQC?

Quantum impact on classical cryptography

Shor's algorithm (1994)

- factorization (RSA)
- discrete logarithm (DH, ECC)

Asymmetric cryptography

Grover's algorithm (1996)

- state space search (keys, collisions)

Symmetric cryptography

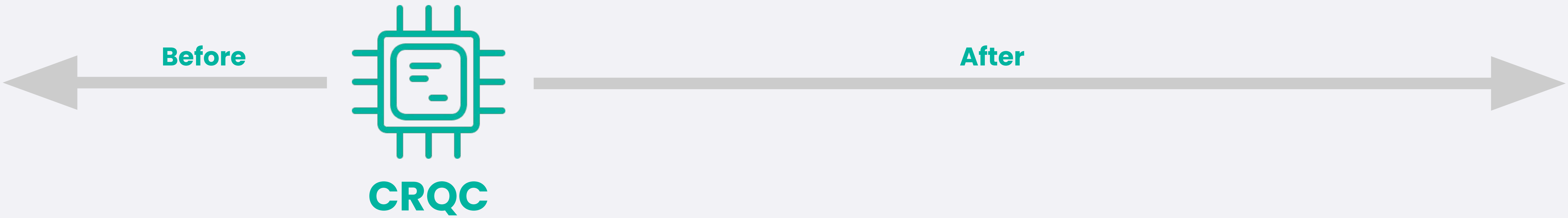
What does it mean “affected”?

Encryption

- confidentiality
- privacy

Signature

- integrity
- non-repudiation
- authentication



Store now…

…Decrypt later

Impersonate users by fraudulent authentication

Manipulate digitally signed documents

Are we ready?

Standards

Algorithms

- NIST standards (08/2024)
  - ML-KEM
  - ML-DSA
  - SLH-DSA
  - FN-DSA (draft)
- IETF RFCs (2018/2019)
  - XMSS signatures
  - LM signatures

Usage

- ITU-T / ISO-IEC / RFC (X.509)
- OID / NIST CSOR (alg IDs)

Coming standards

NIST

- additional KEMs
- on-ramp signatures

China/Korea

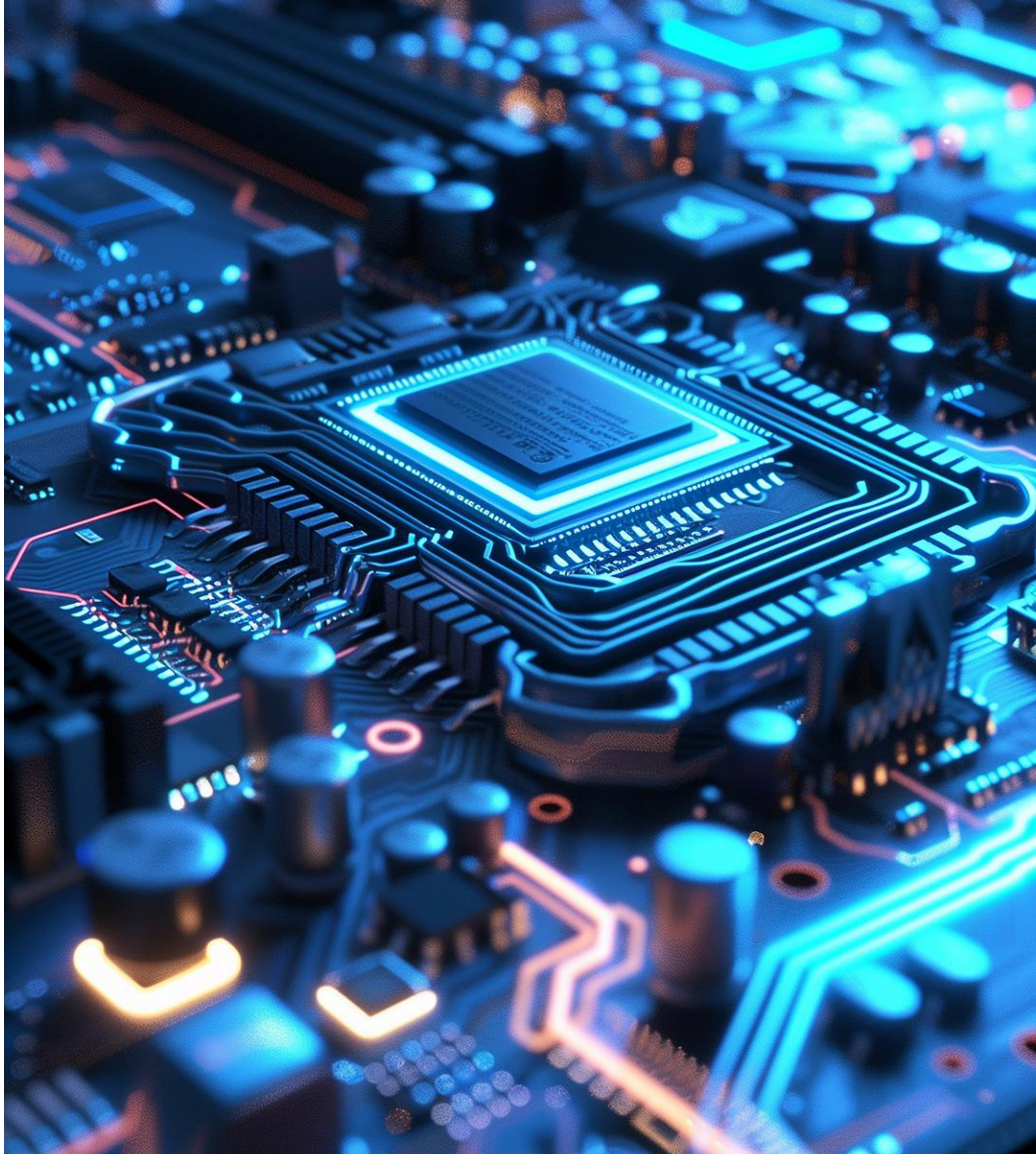
- own standards
- expected 2024-28

EU

- ISO/IEC 18033-2:2006/CD Amd 2 - under development
- incl. of NIST standards expected

Support in HW/SW

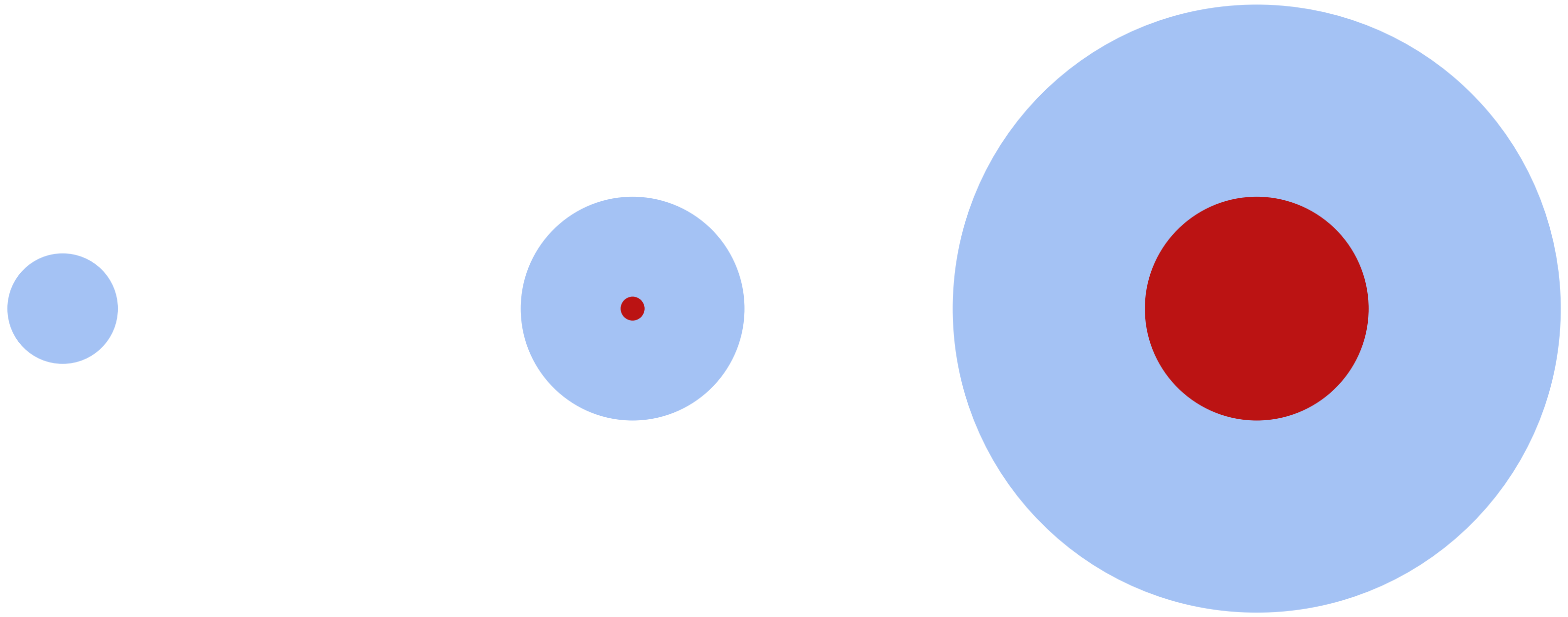
- OQS project
  - TLS, SSH, X.509, CMS, S/MIME
  - Utimaco, Thales, Entrust, IBM, Cisco, Debian, SandboxAQ, …
- proprietary implementations
  - Microsoft (SymCrypt)
  - Google (Tink)
  - …
- HSMs and SCs
  - Thales
  - IBM, Entrust



When?

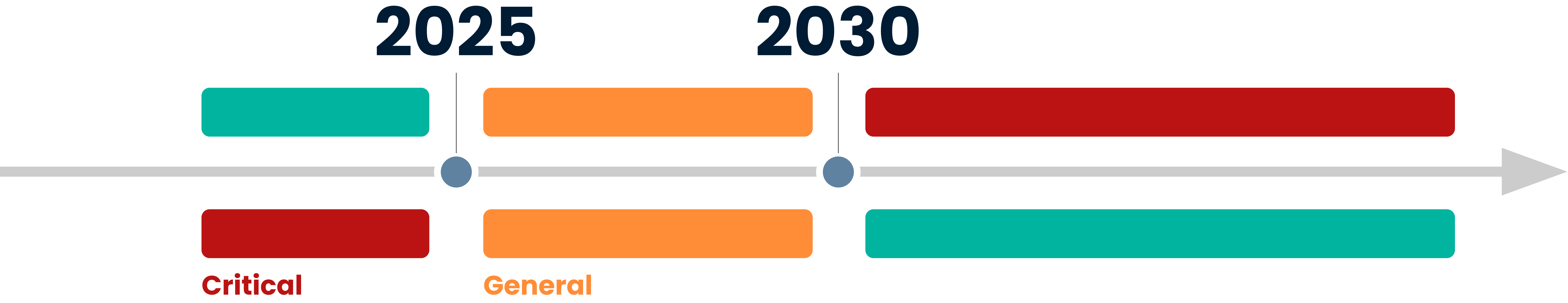
Evolution of quantum computers

→ 2018 → 2021 → 2024 → 2026 / 2031 / Later?



CRQC maturity

Harvest now… …decrypt later



2025

2030

Critical

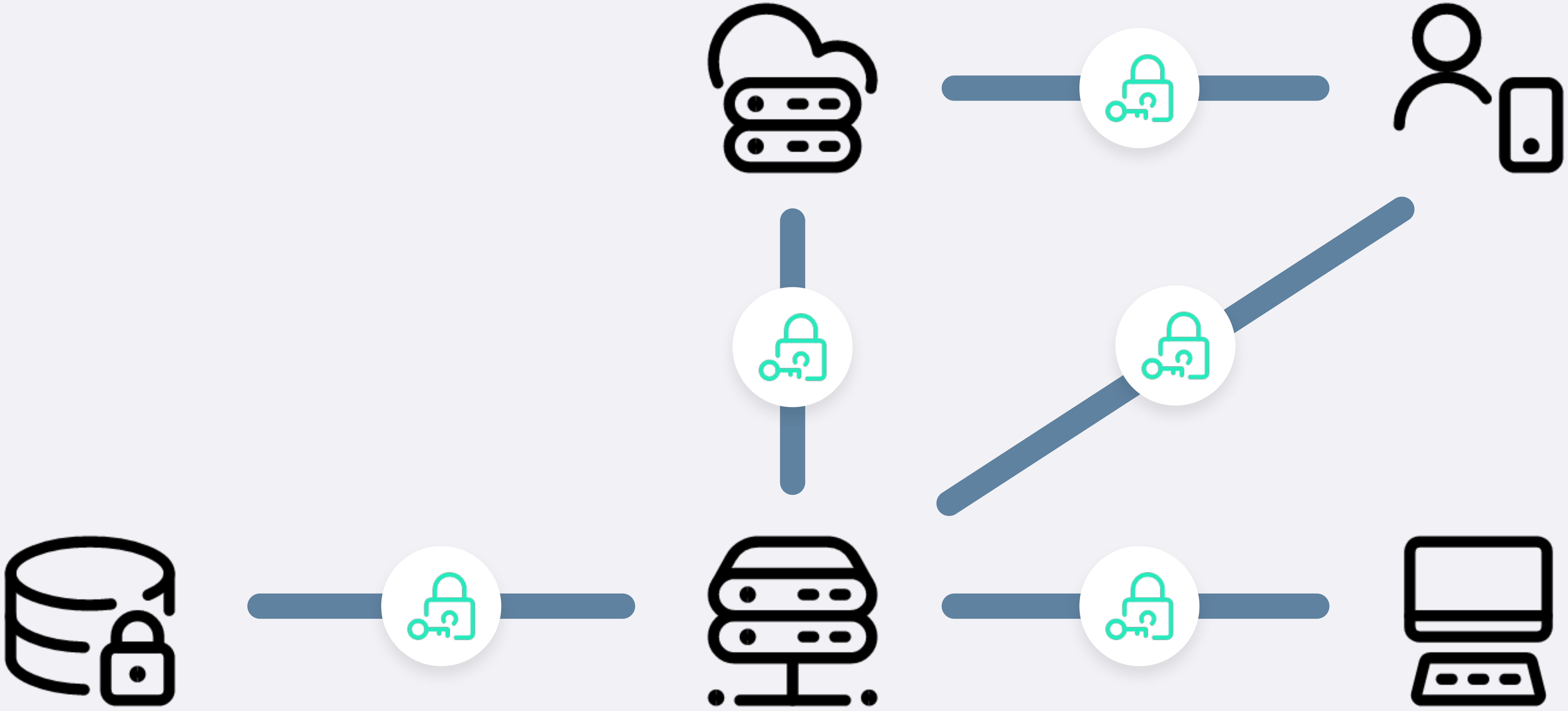
General

Start now… …relax later

PQC readiness

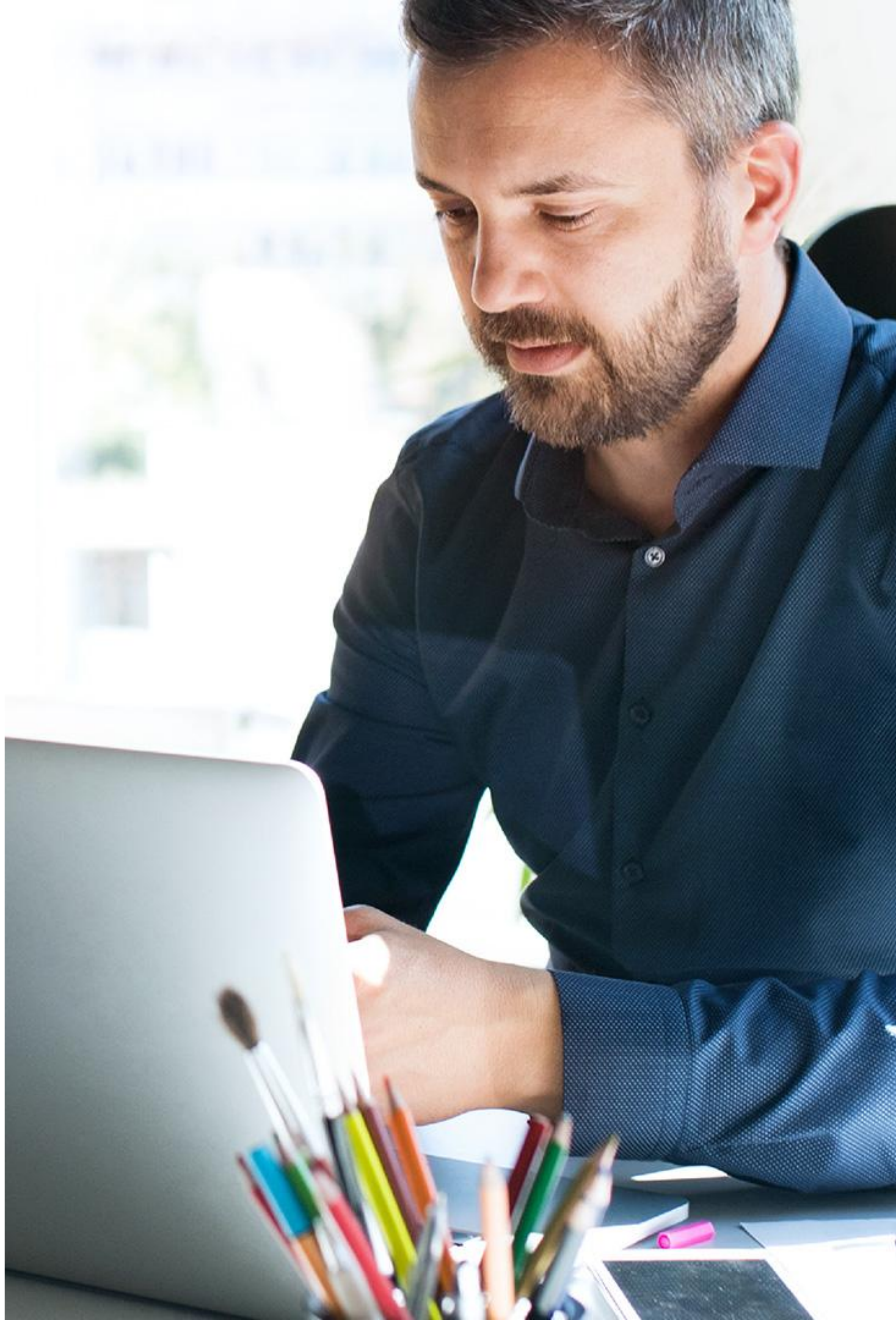
What and where needs to be changed?

MONET +



Cryptographic inventory

- activity identifying all places and purposes, where and why is which crypto used in the system
- prerequisite for planning and prioritization of migration
- not just code but documentation as well



Crypto-agility

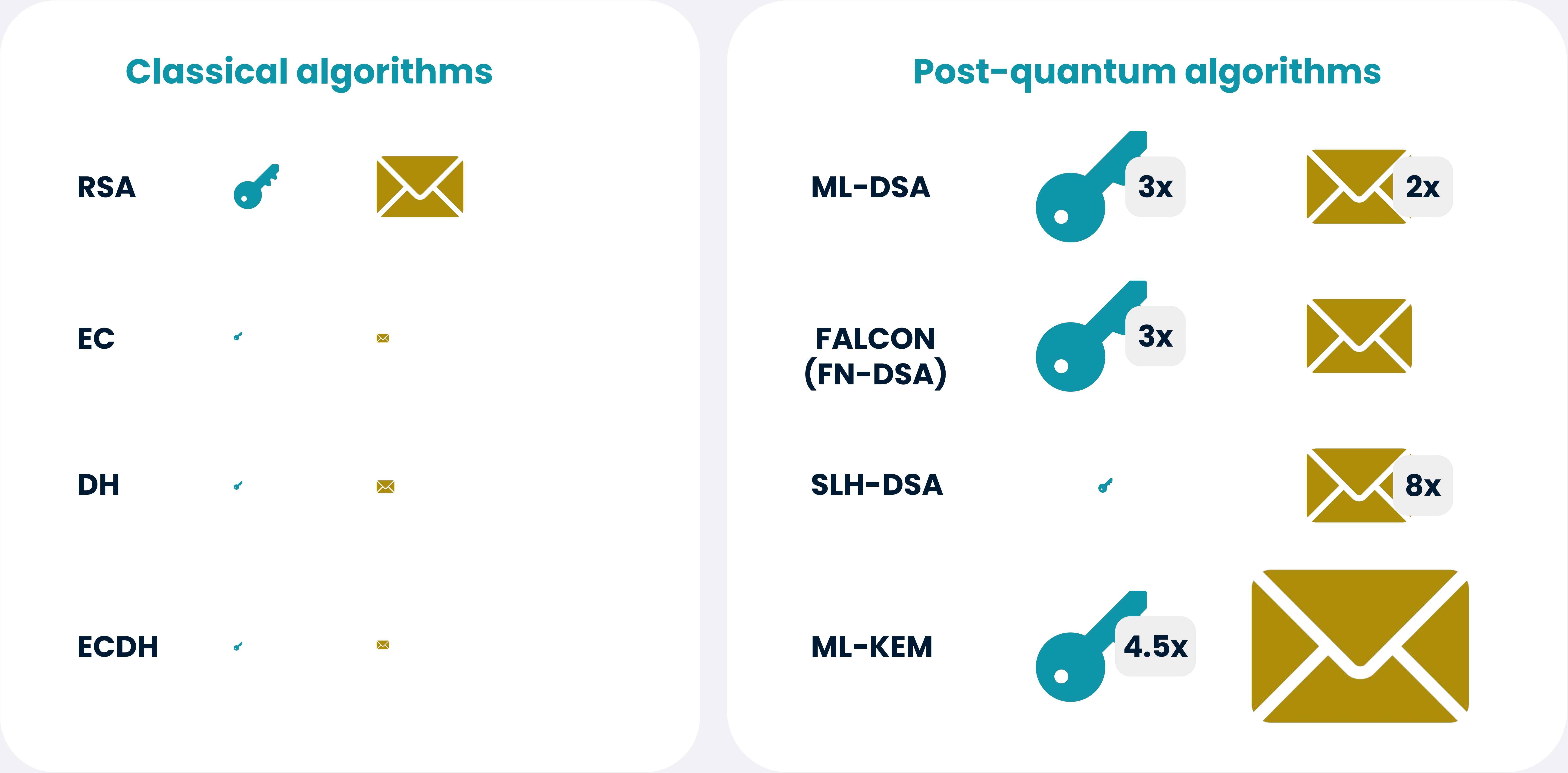
- design supporting smooth change of crypto primitives without extensive system changes
- ideal - drop-in replacement
- for the shift classical -> post-quantum practically infeasible

Migration playbook

- cryptographic inventory
- identification of assets and its dependencies
- criticality and lifespan of asset security
- migration priorities and staging
- migration strategies
- desired changes and impacts
- proposed tools/libs/solutions
- expected costs
- testing and validation strategies

Can we make a simple switch?

Key and signature/message size



Classical algorithms

RSA

EC

DH

ECDH

Post-quantum algorithms

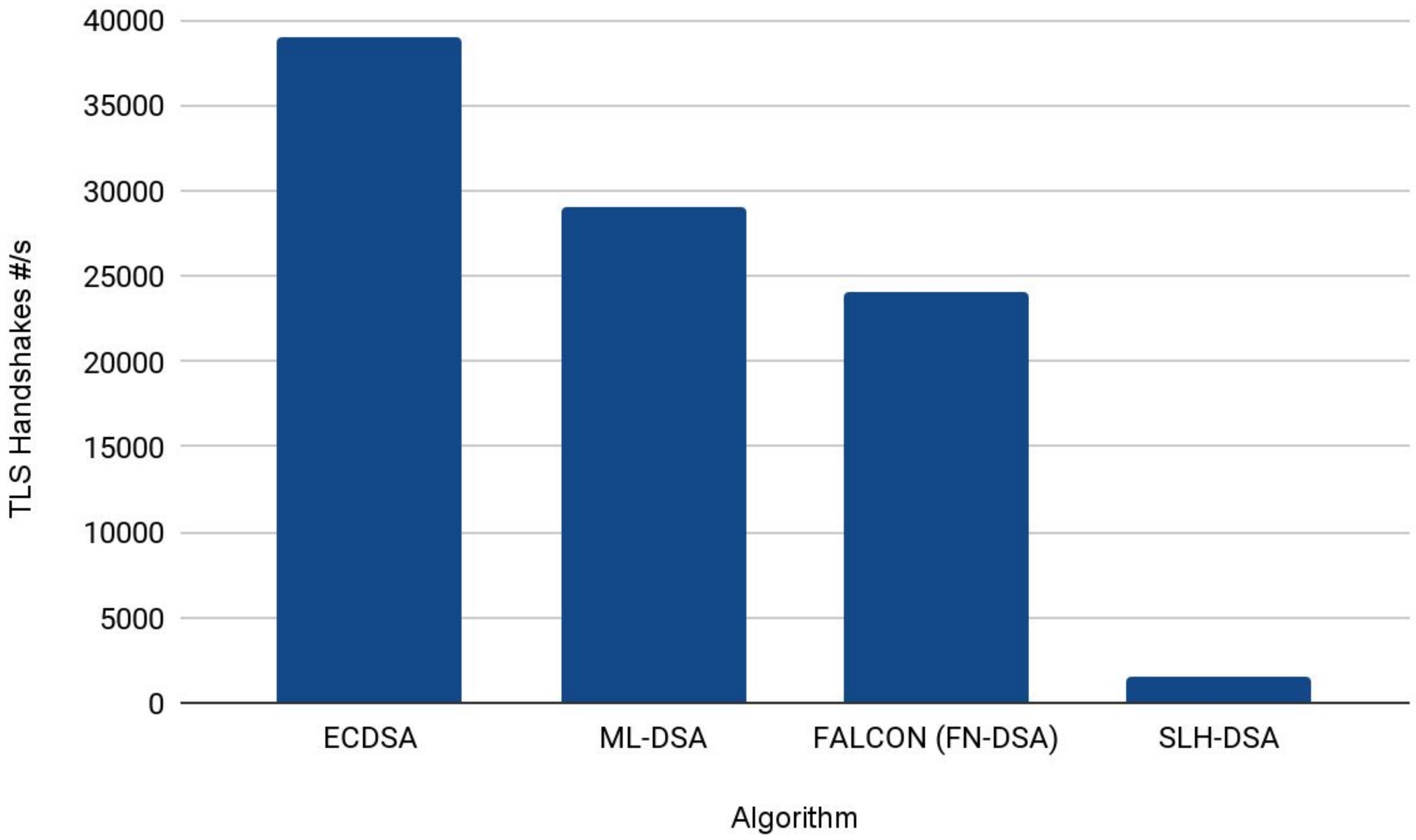
ML-DSA 3x 2x

FALCON
(FN-DSA) 3x

SLH-DSA 8x

ML-KEM 4.5x

Signature generation speed



Classical vs. Post-quantum

- significant differences in parameters
  - key and signature/message sizes
  - operation speed
  - implementation performance and scaling
- different PQ algorithms of the same type

  => different applications
- complicated update in HW components

How to migrate?

Migration approaches

Direct

- replacement of classical algorithm with PQC
- easier, better integration, more efficient
- only if we rely on PQC

Hybrid

- replacement for composed variant classical+PQC
- Concatenated vs. Composite vs. Nested
- resistant against cracking of one of the elements
- complicated interoperability

Migration strategy

Crypto-inventory

know your cryptographic assets

Crypto-agility

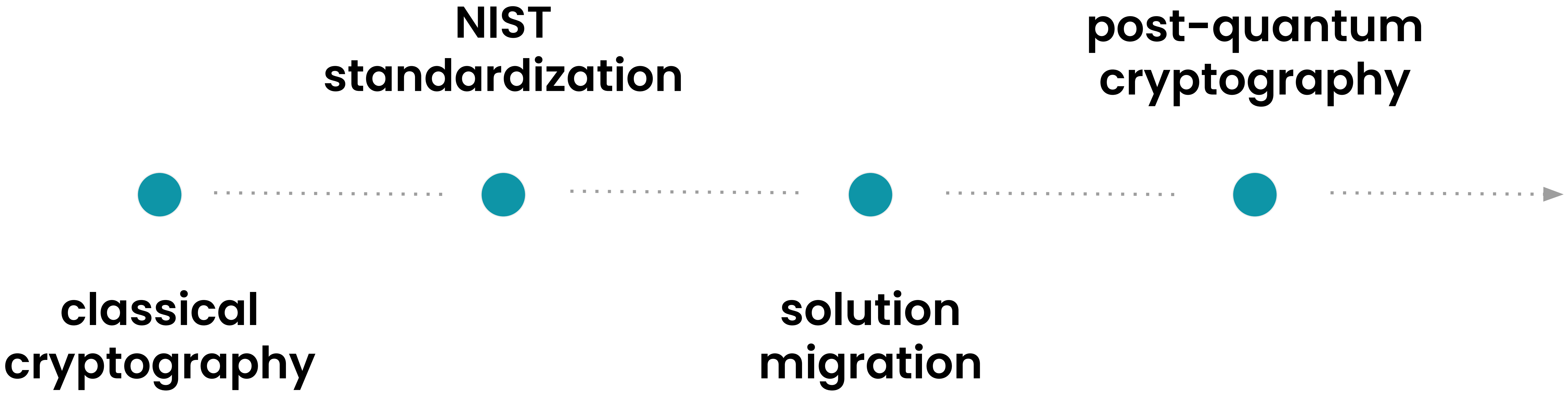
automated and flexible processes for key/alg switching

Hybrid approach

choosing the right hybridisation strategy

Key takeaways

Timeline



classical cryptography

NIST standardization

solution migration

post-quantum cryptography

Mosca’s Theorem

X = Security Shelf life

Y = Migration Time

Z = Time to compromise

⚠

If $X + Y > Z$ then system can be compromised!

NOW!

Is the best time to start
with PQ migration preparation

PQC in Monet+

Postquantum Audit Framework (PAF)

First touch with PQC, SW-based audit marking signatures

MONET+

PoC with smart card

Prepare solution for robust PQ-ready signature UCs

THALES

PoC with HSM

Build PQ-ready CA as a keystone for PQ-ready PKI

IBM

How can we help you?

- ✓ map the environment
  - technical view
  - recommendation of (security) authorities
- ✓ create crypto-inventory
- ✓ build crypto-agile solutions
- ✓ define migration strategy for each case
- ✓ decide priorities
- ✓ prepare robust migration playbook
- ✓ migrate to PQ-ready solution case by case

MONET+

monetplus.com