Federal Office
for Information Security

Post-quantum Cryptography: Standardisation & Migration

Antonia Weinhold, GI 2024, 25.11.2024

Agenda

- Motivation
- Post Quantum Cryptography Standardisation
- Hybrid Solutions
- Migration

Motivation

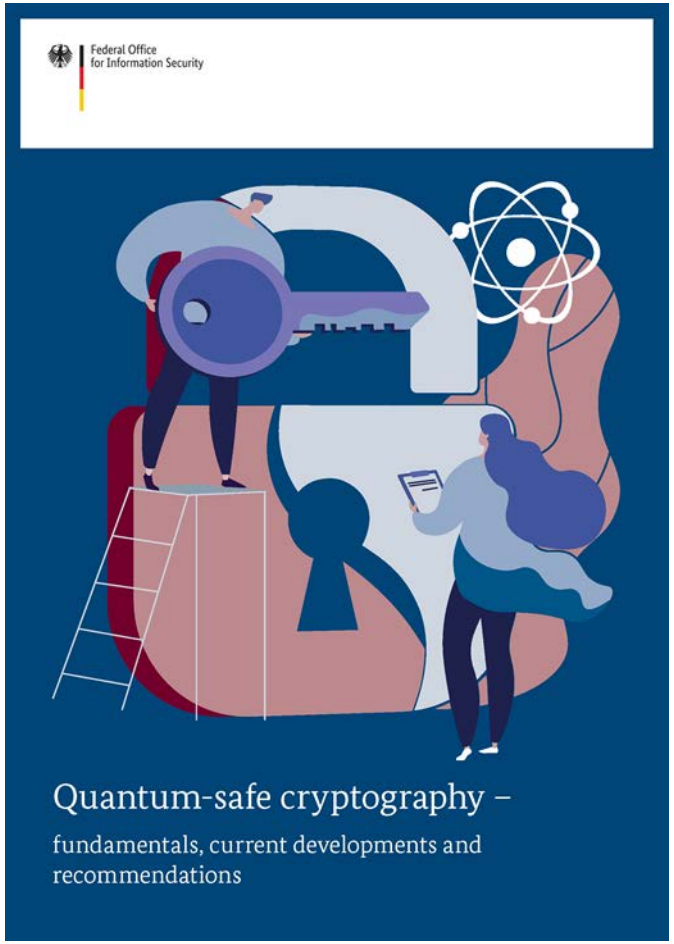
Working Hypothesis and Scenarios

„Cryptographically relevant quantum computers will be available early in the 2030s.“

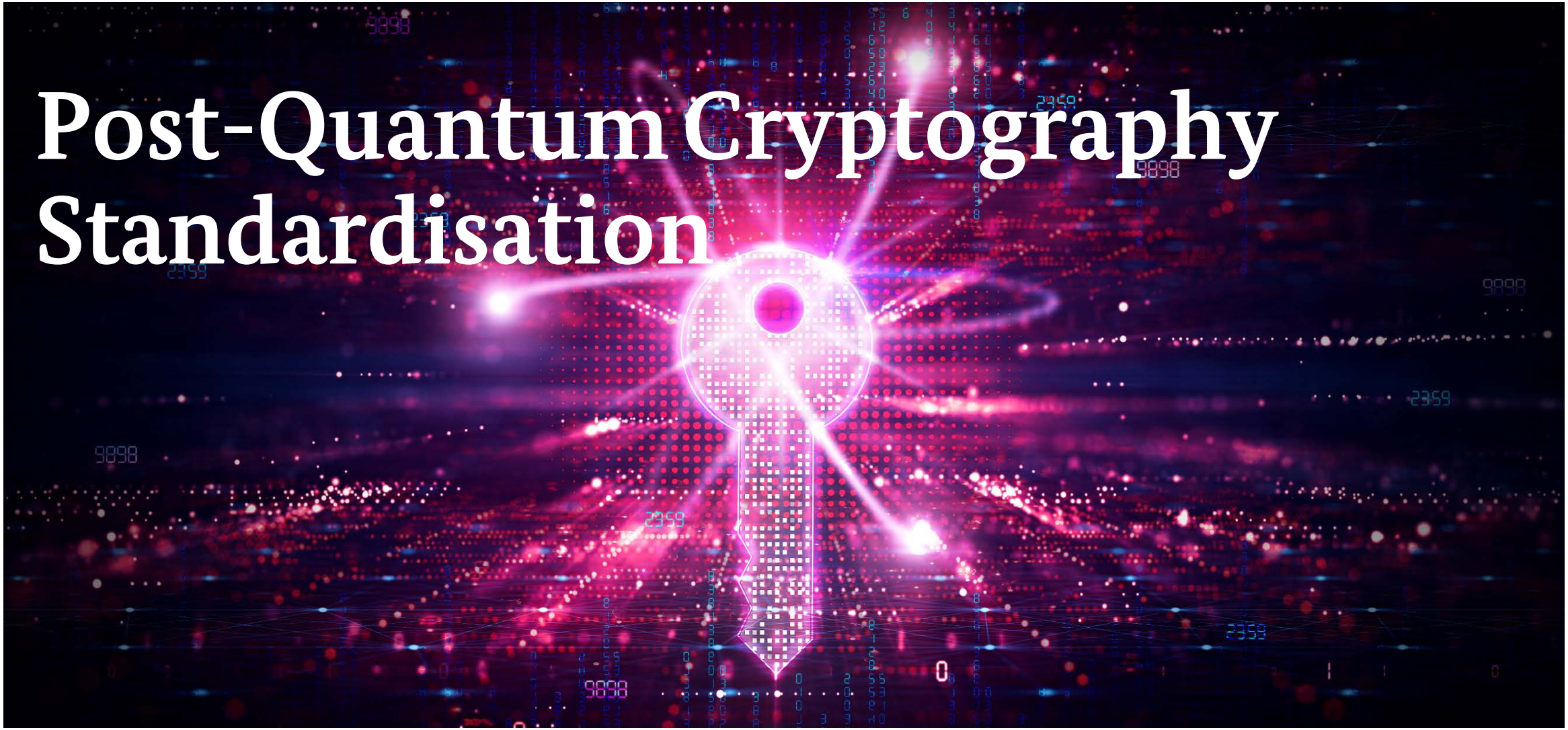
(This is **not** a prediction but rather a guideline for conservative risk assessment.)

Scenarios:

- *Store now, decrypt later* → quantum-safe encryption
- *Complex migration* (e.g. PKI) → quantum-safe authentication



Post-Quantum Cryptography Standardisation



Deutschland
Digital•Sicher•BSI•

NIST Standards

July 2022: First Selection

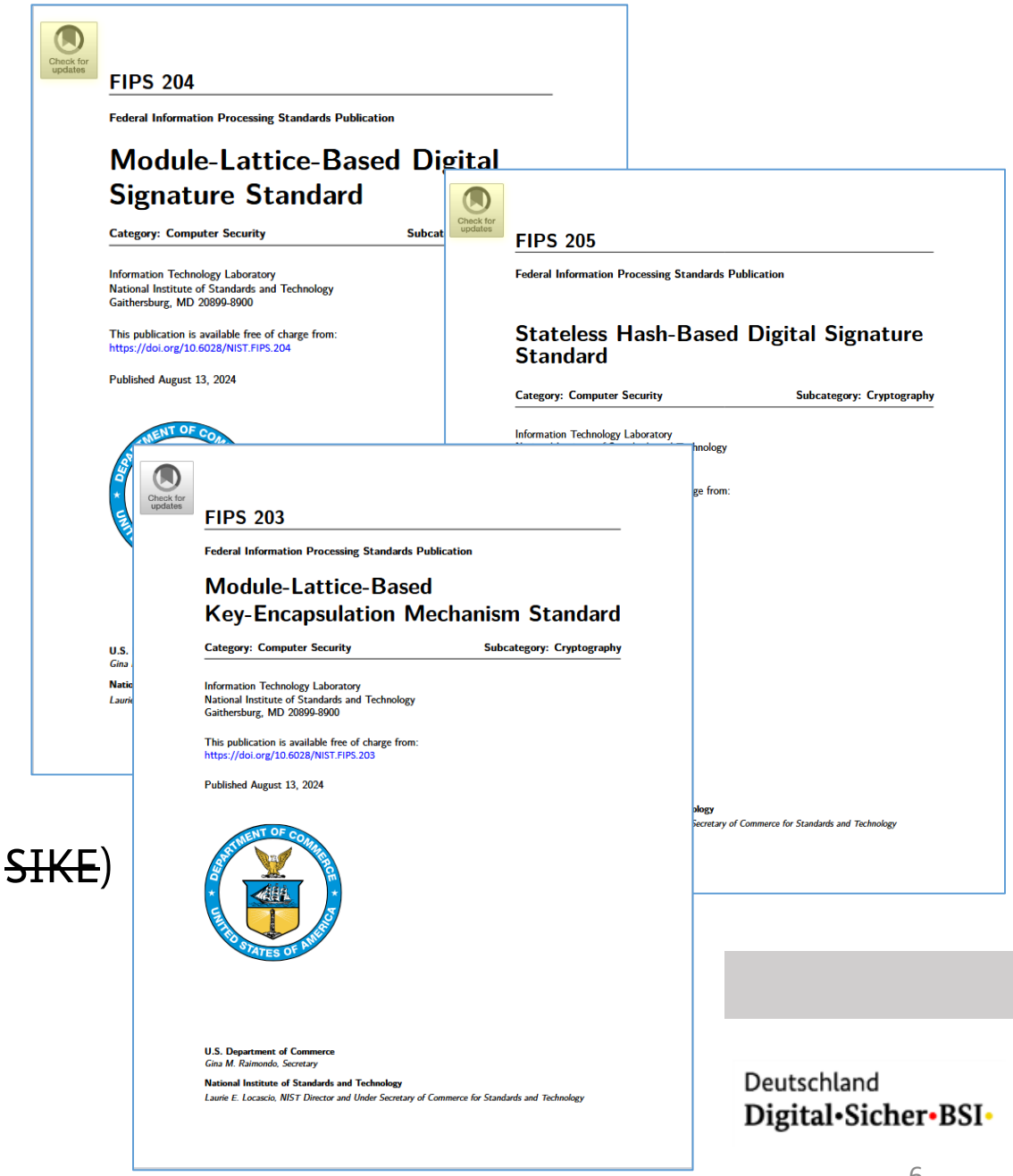
- 1 KEM: Kyber
- 3 DSA: Dilithium, Falcon, SPHINCS

August 2024: Final Standards

- FIPS 203: ML-KEM (Kyber)
- FIPS 204: ML-DSA (Dilithium)
- FIPS 205: SLH-DSA (SPHINCS+)

Current developments

- 4th round (BIKE, HQC, Classic McEliece, ~~SIKE~~)
- Selection of further signatures ongoing



Deutschland Digital•Sicher•BSI•

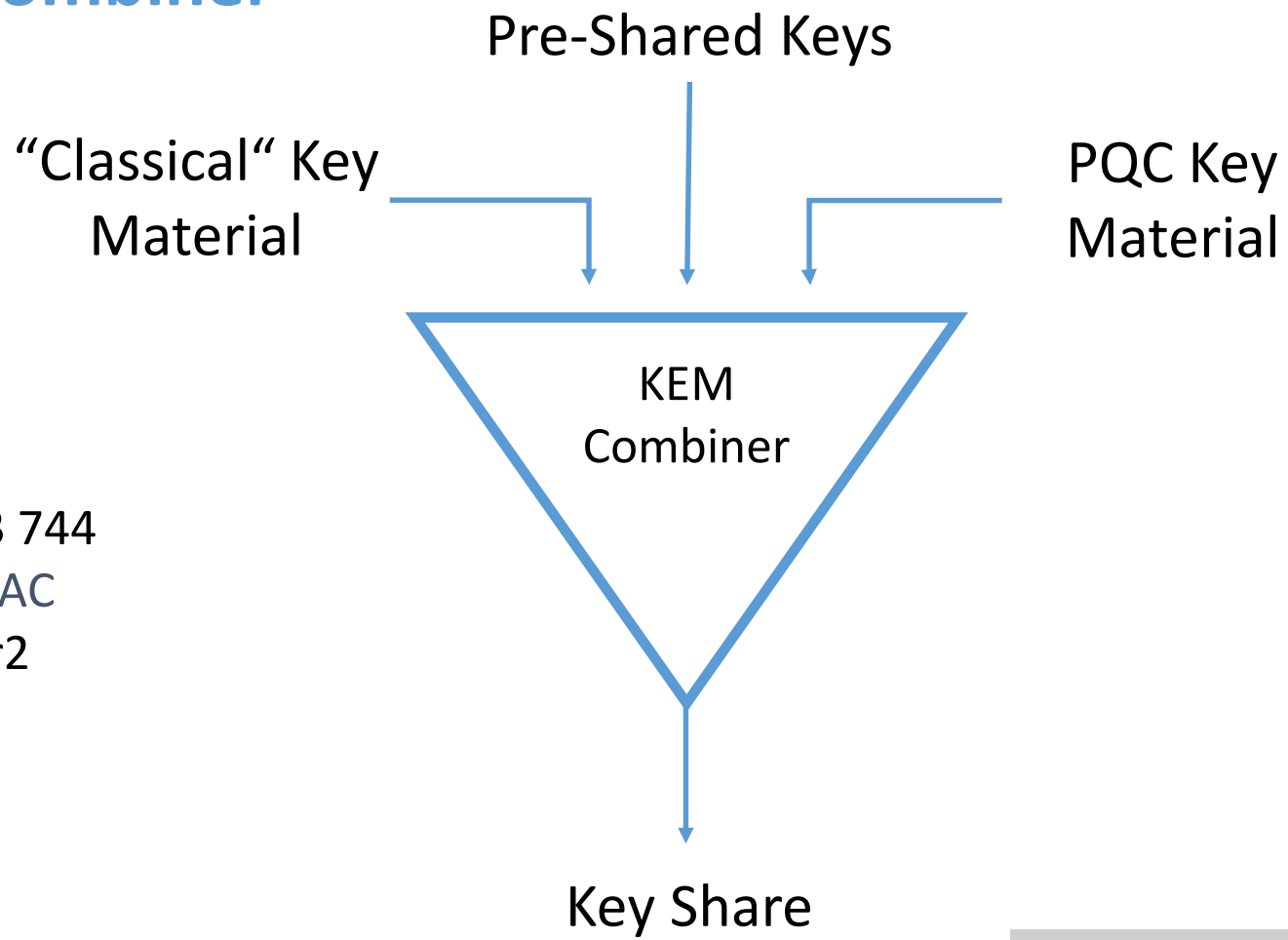
Hybrid Solutions

Hybrid Key Exchange: KEM Combiner

- Goal:
  Construction is secure as long as
  at least one of the inputs is secure.

- Currently Standardized :
  - CatKDF & CasKDF from ETSI TS 103 744
  - The Keccac (SHA3, KMAC) and HMAC based KDFs from NIST SP 800-56Cr2

- Alternatively: Double encryption



Deutschland Digital•Sicher•BSI•

Authentication: Multiple Digital Signatures

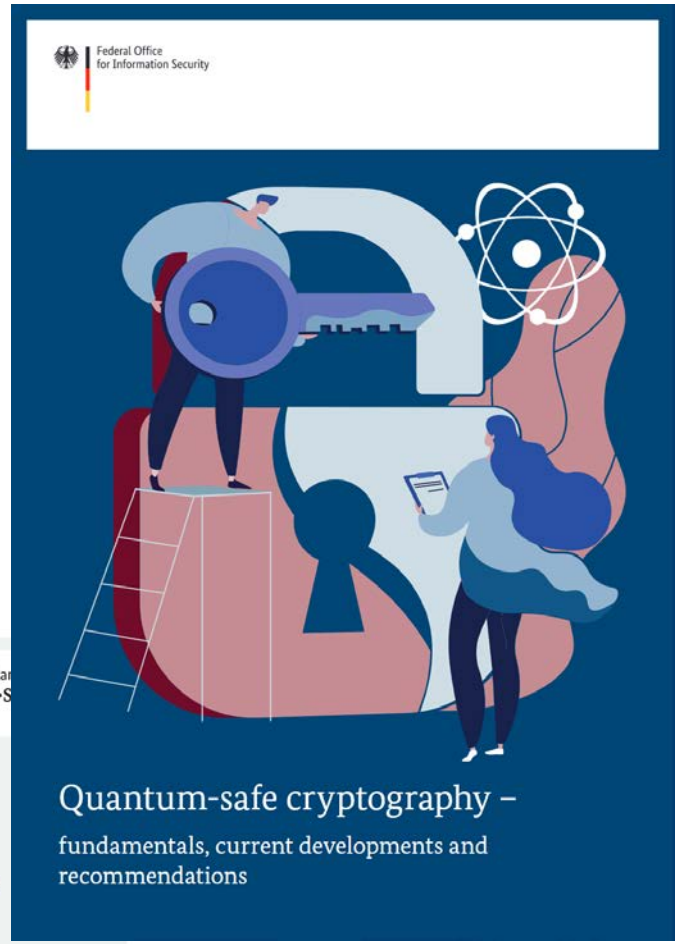
- Multiple independent signatures: “classical“ + PQC, excluding hash-based
- (Alternatively: Multiple enveloped signatures)
- Signature is valid if and only if all (independent) signatures verify
- Concrete proposals @IETF

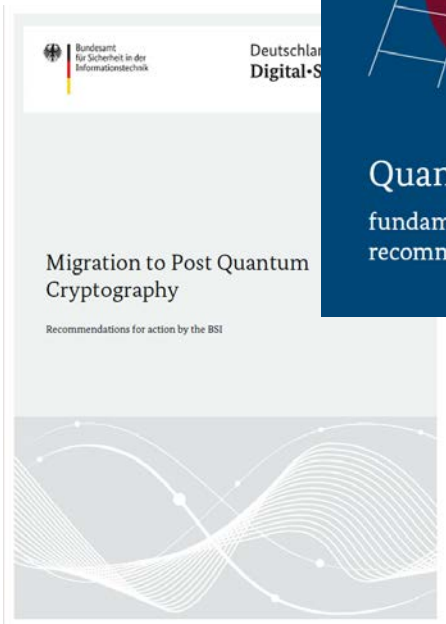
Migration

BSI Guide „Quantum-safe cryptography“

In 2021 BSI published the guideline
Quantum-safe cryptography – fundamentals, current developments and recommendations:

- Background on *quantum computers*, *PQC*, *protocols*, *QKD*
- Developments in politics, research and industry
- Recommendations for actions (excerpt):
  - Preparation: cryptographic inventory!
  - Hybrid solutions for KEMs and signature schemes
  - Cryptographic agility



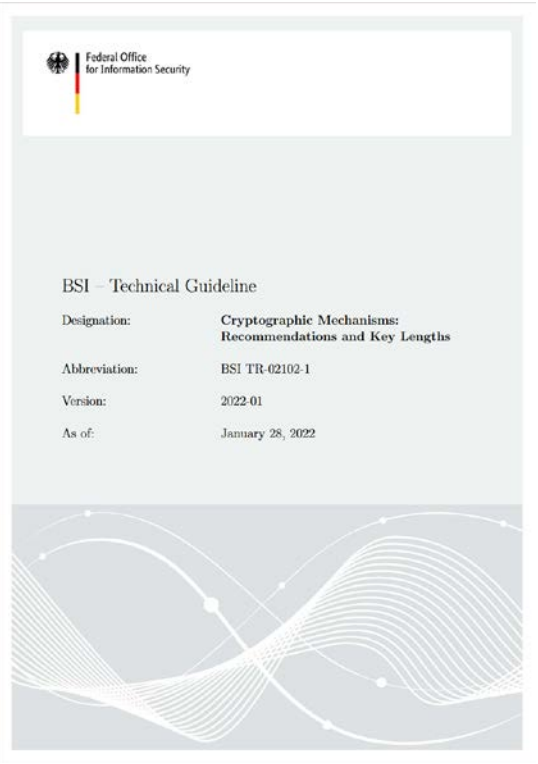


Reference: www.bsi.bund.de/dok/pqmigration-en

Deutschland
Digital•Sicher•BSI•

BSI Technical Guideline TR-02102-1

- Key Encapsulation Mechanisms:
  - *FrodoKEM* and *Classic McEliece*
  - *ML-KEM (intended now standard is available)*
- Digital Signature Schemes:
  - *ML-DSA (intended now standard is available)*
  - *SLH-DSA (intended now standard is available)*
  - *LMS/HSS* and *XMSS/XMSS^MT*
- *Parameters: NIST security categories 3 and 5*
- Only *hybrid solutions*, i.e. PQC + “Classical”, except for HBS

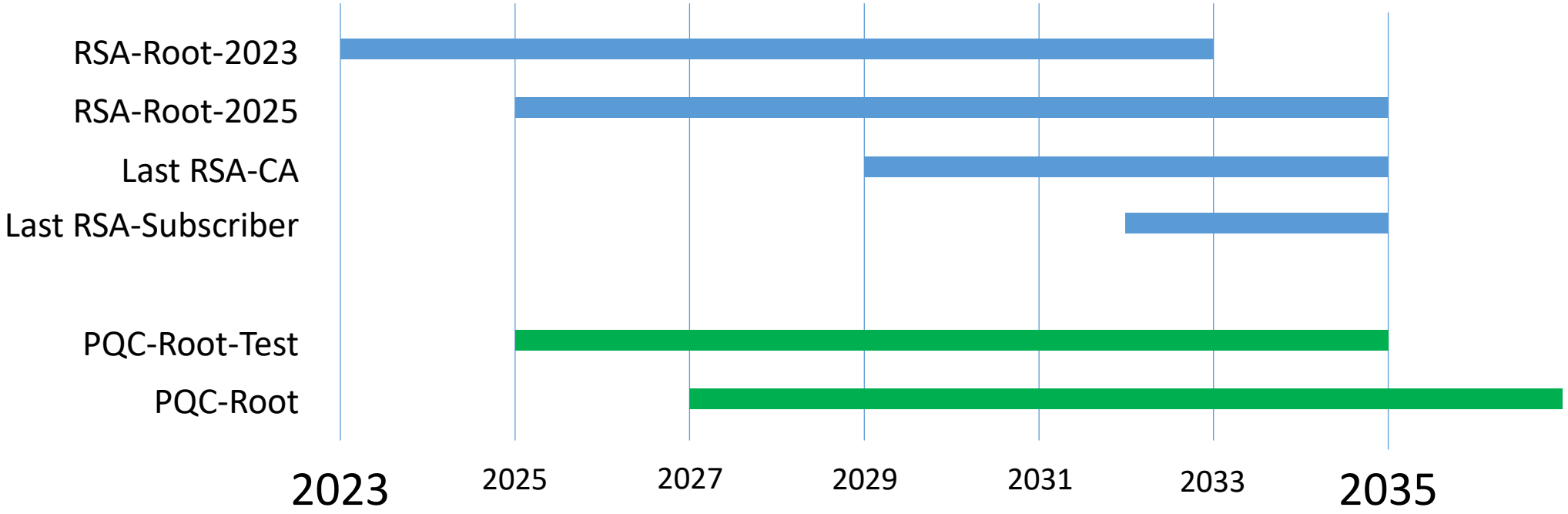


Deutschland
Digital•Sicher•BSI•

BSI‘s current PQC projects

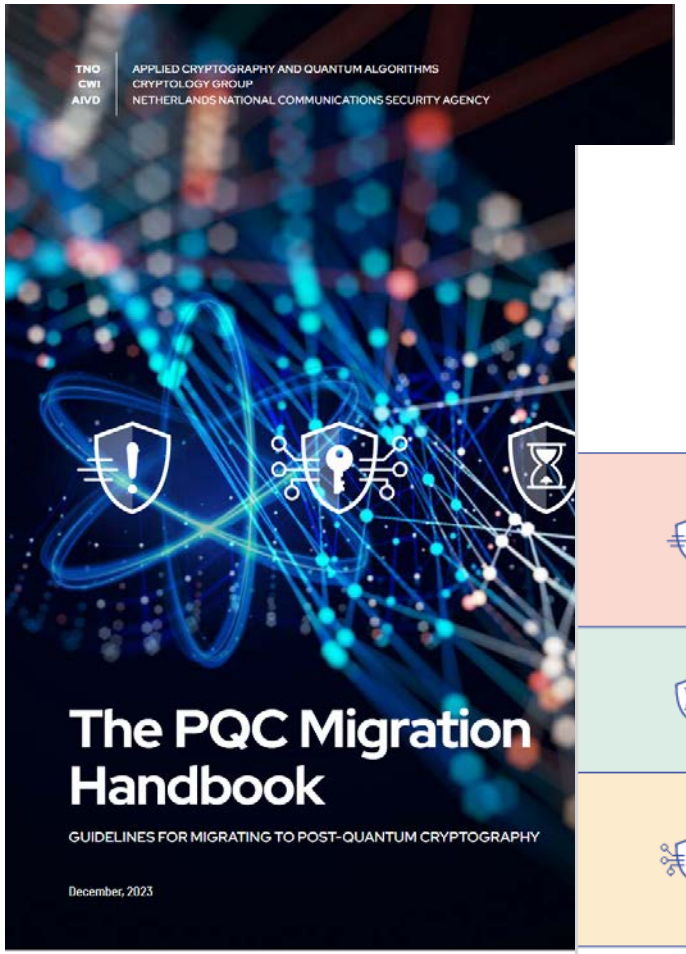
- PQC in the cryptographic library Botan:
  - FrodoKEM, Classic McEliece, Kyber
  - Dilithium, SPHINCS+, XMSS, LMS/HSS
  - TLS 1.3 hybrid key exchange
- PQC in OpenPGP and Thunderbird
  - IETF I-D “PQC for OpenPGP” (coming soon)
  - Implementation in Thunderbird and RNP/Botan
  - Implementation in GnuPG/libgcrypt

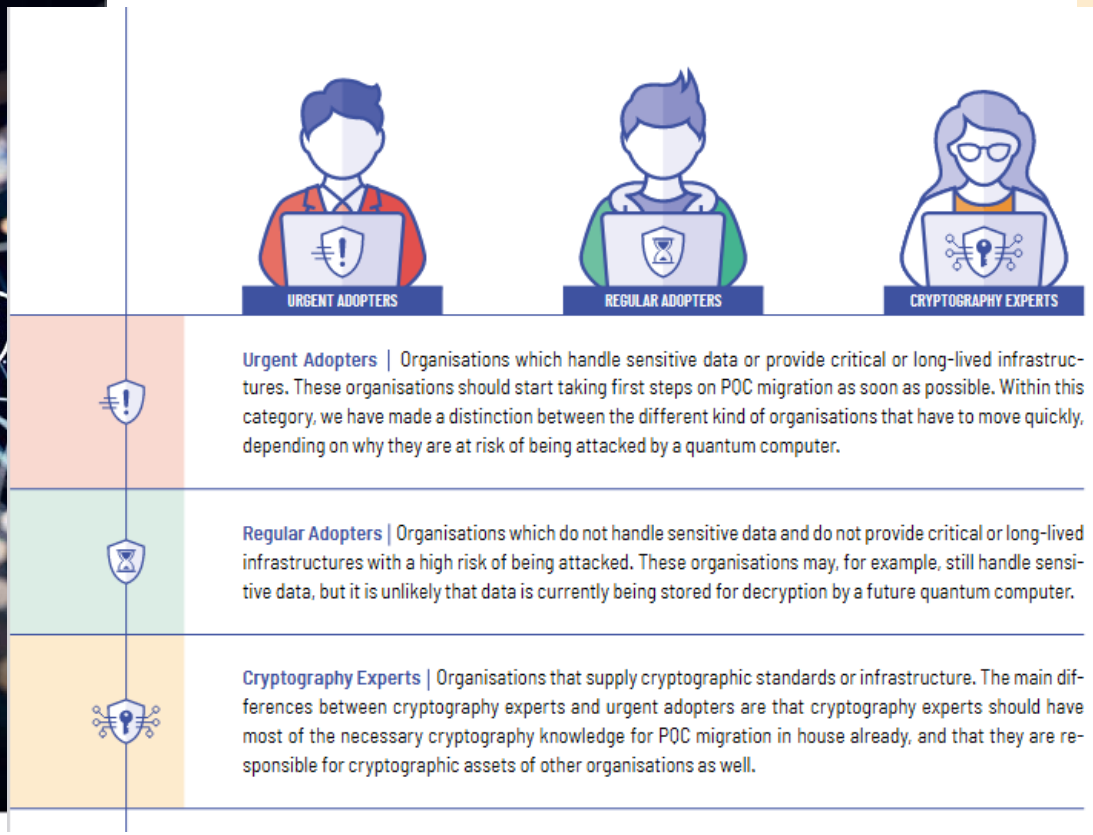
Optimistic Migration Plan V-PKI



Deutschland
Digital•Sicher•BSI•

Netherlands: PQC Migration Handbook





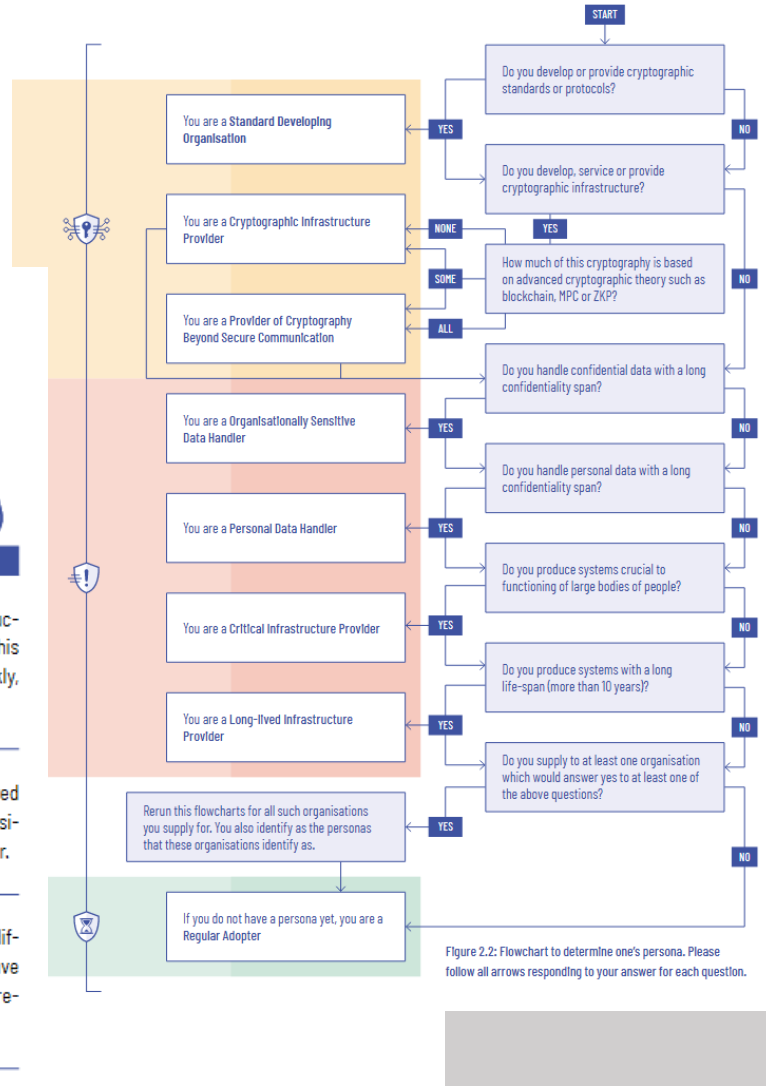


Figure 2.2: Flowchart to determine one's persona. Please follow all arrows responding to your answer for each question.

Deutschland Digital•Sicher•BSI•

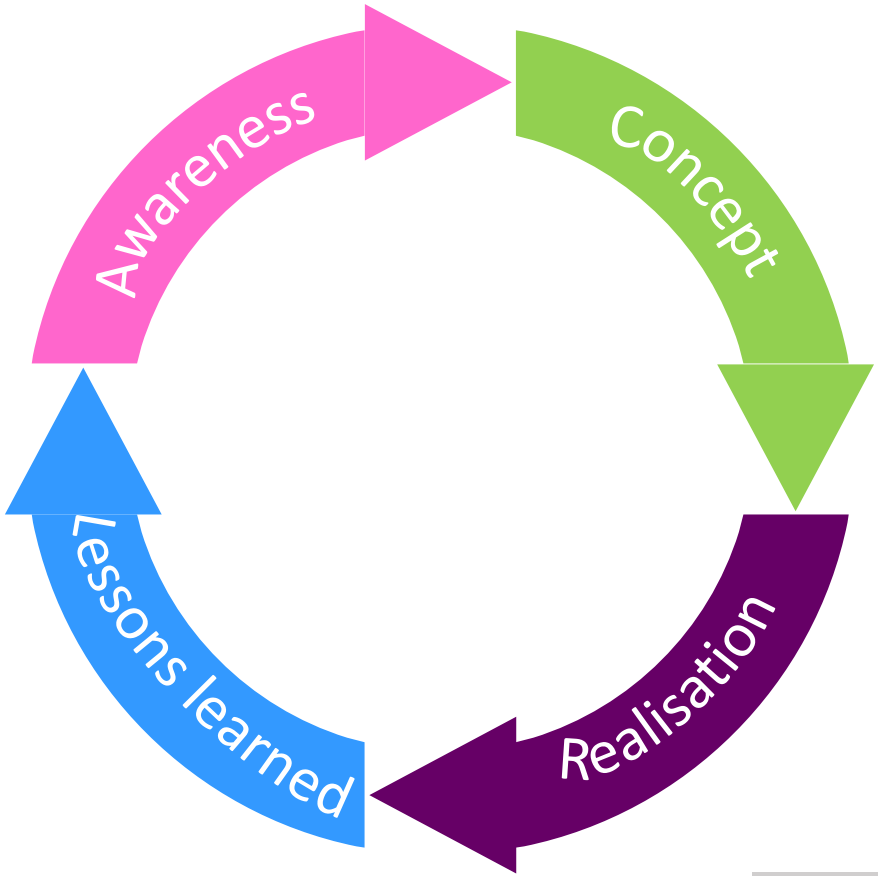
Migration to Quantum-safe Systems

- A circular and iterative process

- Building blocks of migration iterations
  - FW/SW Upgrade and updates
  - Multi-KEM and Multi-Signatures (hybrid)
  - Public-key infrastructures
  - Cryptographic protocols

Take home:

You can start today to build your cryptography inventory!



Thank you for your attention!

Deutschland
Digital•Sicher•BSI•

Antonia Weinhold

antonia.weinhold@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Federal Office for Information Security

Godesberger Allee 87
53175 Bonn
www.bsi.bund.de