Post-Quantum

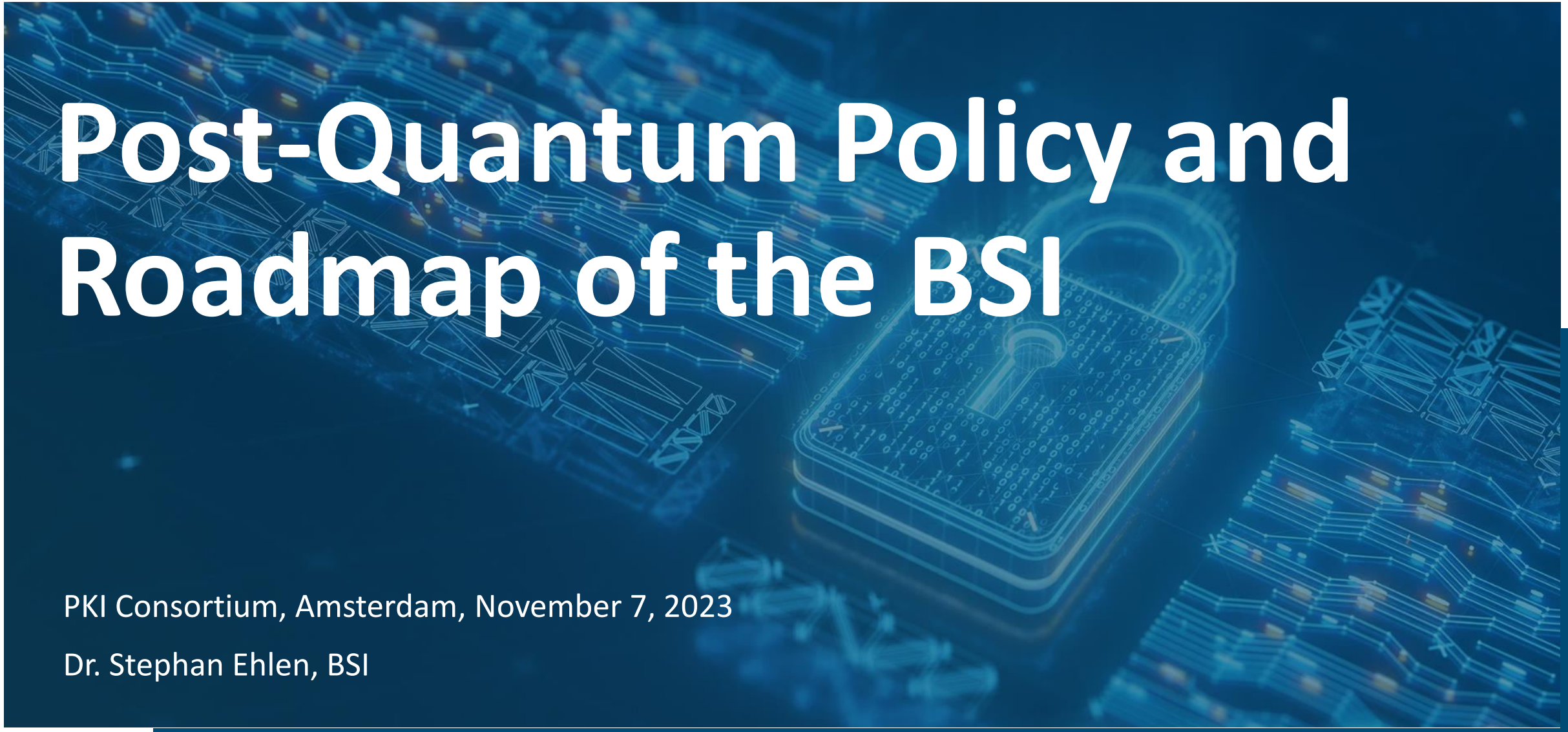
Cryptography Conference

Post-Quantum Policy & Roadmap of the BSI

Stephan Ehlen
The Federal Office for Information Security (BSI)

Federal Office
for Information Security

Post-Quantum Policy and Roadmap of the BSI



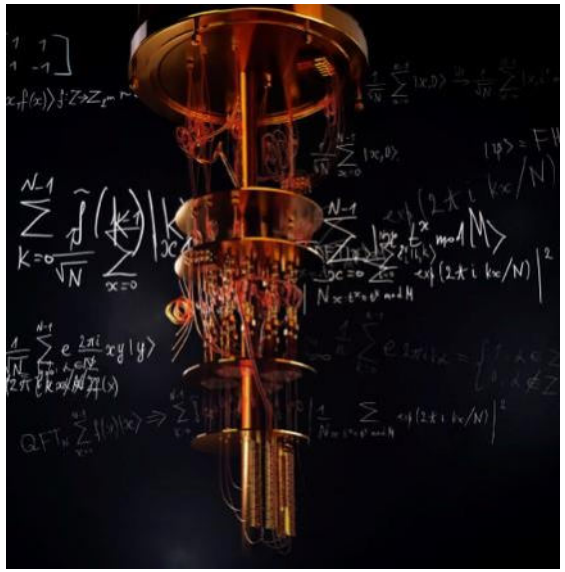
PKI Consortium, Amsterdam, November 7, 2023

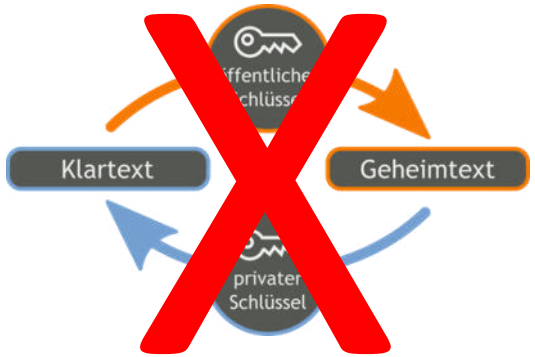
Dr. Stephan Ehlen, BSI

About me

- PhD in pure Mathematics (number theory)
  - Main interest: Modular forms and their arithmetic and geometric applications
- Since 2021 at the Federal Office for Information Security (BSI)
  - Main interest: Post-quantum cryptography, in particular lattice-based
- Associate professor (Privatdozent) in Mathematics at University of Cologne, Germany

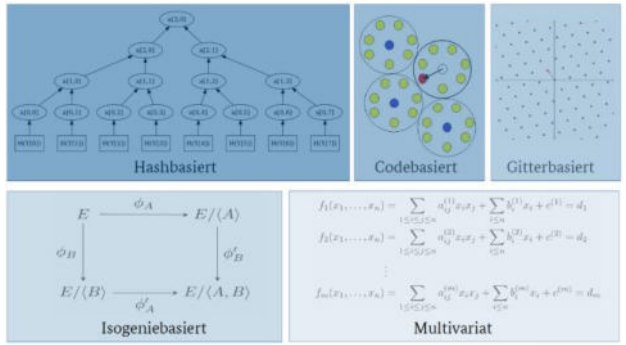
Why Quantum-safe Cryptography?



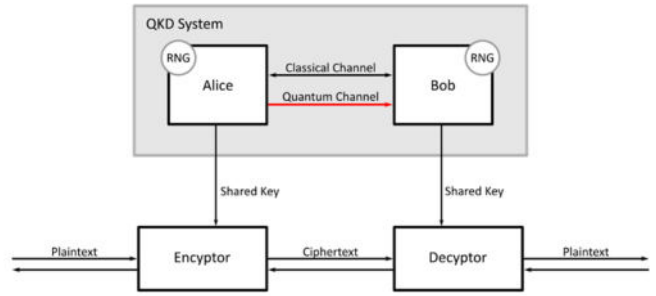


Current Public Key Cryptography
(RSA, (EC)DH, (EC)DSA)

Post Quantum Cryptography



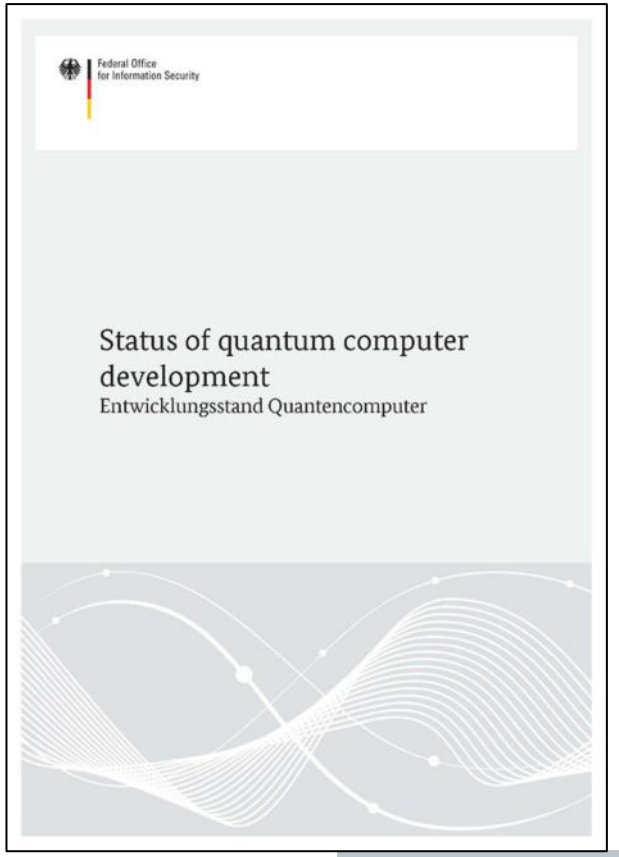
Quantum-safe Cryptography



Quantum Key Distribution

BSI Study „Status of quantum computer development“

- First published 2018, updated 2019 and 2020
- Available at www.bsi.bund.de/qcstudie
- Project lead: Prof. Frank Wilhelm-Mauch (FZ Jülich)
- 2023 update (available soon):
  - New developments in
    - Algorithms in the NISQ-era
    - Error correction and –mitigation
    - Hardware
  - No fundamental breakthrough
  - However, major leaps forward are possible if heuristic results are confirmed.



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.)

(BT-Drs. 19/26340)

Scenarios:

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

Political Guidelines

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

Deutscher Bundestag — Drucksache 20/6610

20. Wahlperiode — 28.04.2023

Unterrichtung

durch die Bundesregierung

Handlungskonzept Quantentechnologien der Bundes

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 26. April 2023.

Die Bundesregierung

Quantenkommunikation und Post-Quanten-Kryptografie

In der Quantenkommunikation und der Post-Quanten-Kryptografie will die Bundesregierung bis 2026 folgende Meilensteine erreichen:

- Etablierung von ersten abhörsicheren, d.h. quantenverschlüsselten, Kommunikationsteststrecken zwischen ausgewählten Behördenstandorten.
- Weitere Start-ups/Firmen sind im Bereich der Quantenkommunikation in Deutschland gegründet.
- Realisierung eines bundesweiten Glasfaser-Backbones für die Quantenkommunikation und die Zeit- und Frequenzverteilung.
- Demonstration erster Quantenrepeatertestrecken.
- Start erster Testsatelliten zur Quantenschlüsselverteilung.
- Erstellung einer Strategie der Bundesregierung für die Migration zu Post-Quanten-Kryptografie in Deutschland.
- Weiterführung der Migration zu Post-Quanten-Kryptografie für den Hochsicherheitsbereich.

- Einleiten der Migration zu Post-Quanten-Kryptografie in weiteren sicherheitskritischen Bereichen.
- Integration von Post-Quanten-Kryptografie-Verfahren in praxistaugliche IT-Sicherheitslösungen.

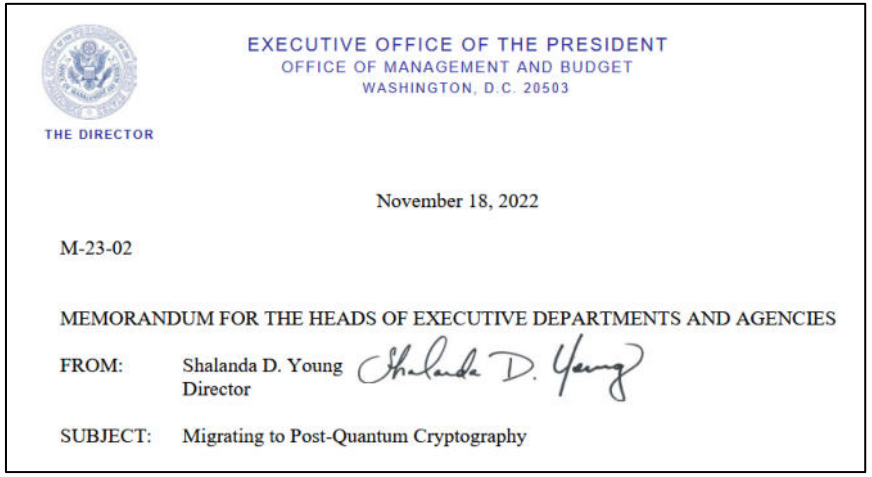
Für eine spätere Überführung in Produktivsysteme sind im Anschluss weitere Schritte im Bereich der Prüfung, Zulassung und technischen Ertüchtigung der beteiligten Komponenten und Infrastrukturen erforderlich.

Political Guidelines

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

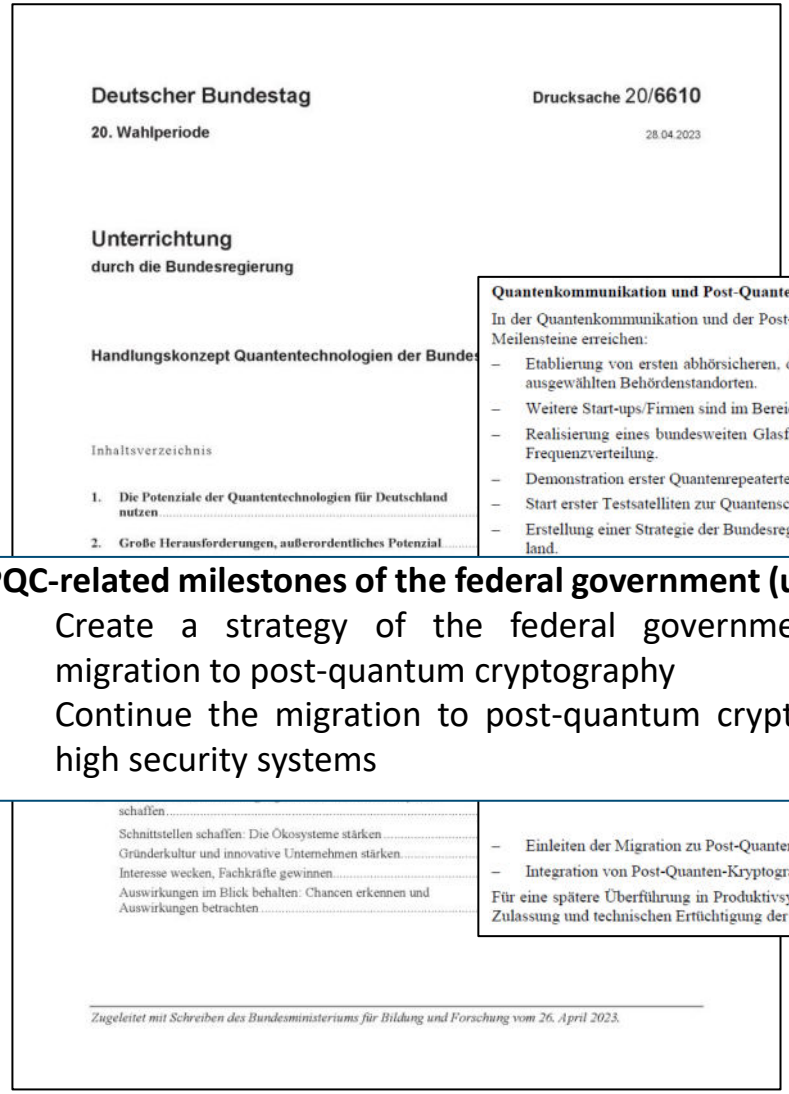
November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography



Deutscher Bundestag — Drucksache 20/6610

20. Wahlperiode — 28.04.2023

Unterrichtung
durch die Bundesregierung

Handlungskonzept Quantentechnologien der Bundes

Inhaltsverzeichnis

1. Die Potenziale der Quantentechnologien für Deutschland nutzen
2. Große Herausforderungen, außerordentliches Potenzial

schaffen
Schnittstellen schaffen: Die Ökosysteme stärken
Gründerkultur und innovative Unternehmen stärken
Interesse wecken, Fachkräfte gewinnen
Auswirkungen im Blick behalten: Chancen erkennen und Auswirkungen betrachten

Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 26. April 2023.

Die Bundesregierung

Quantenkommunikation und Post-Quanten-Kryptografie

In der Quantenkommunikation und der Post-Quanten-Kryptografie will die Bundesregierung bis 2026 folgende Meilensteine erreichen:

- Etablierung von ersten abhörsicheren, d.h. quantenverschlüsselten, Kommunikationsteststrecken zwischen ausgewählten Behördenstandorten.
- Weitere Start-ups/Firmen sind im Bereich der Quantenkommunikation in Deutschland gegründet.
- Realisierung eines bundesweiten Glasfaser-Backbones für die Quantenkommunikation und die Zeit- und Frequenzverteilung.
- Demonstration erster Quantenrepeaterteststrecken.
- Start erster Testsatelliten zur Quantenschlüsselverteilung.
- Erstellung einer Strategie der Bundesregierung für die Migration zu Post-Quanten-Kryptografie in Deutschland.

hsicherheitsbereich.

cher Bundestag – 20. Wahlperiode

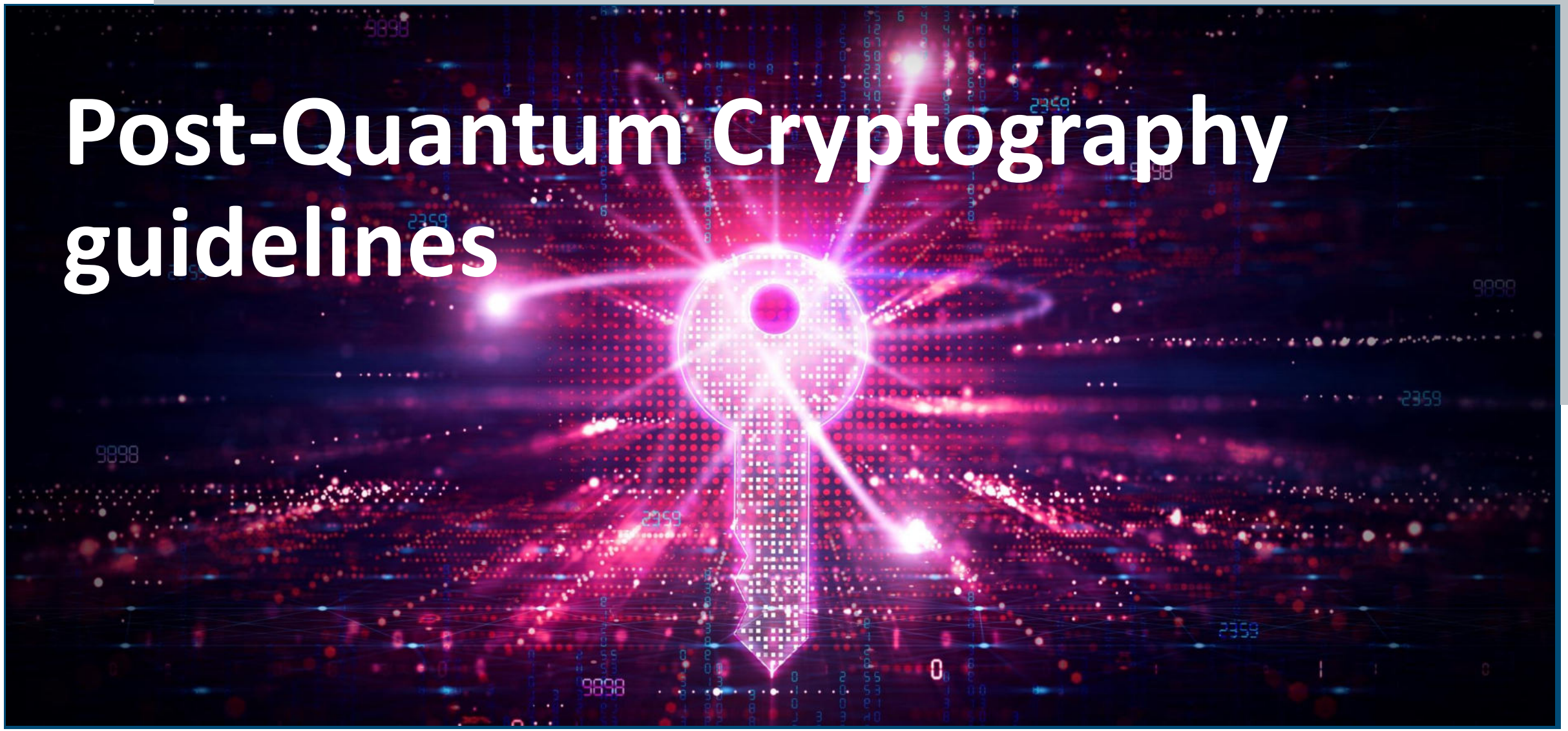
- Einleiten der Migration zu Post-Quanten-Kryptografie in weiteren sicherheitskritischen Bereichen.
- Integration von Post-Quanten-Kryptografie-Verfahren in praxistaugliche IT-Sicherheitslösungen.

Für eine spätere Überführung in Produktivsysteme sind im Anschluss weitere Schritte im Bereich der Prüfung, Zulassung und technischen Ertüchtigung der beteiligten Komponenten und Infrastrukturen erforderlich.

PQC-related milestones of the federal government (until 2026):

- Create a strategy of the federal government for the migration to post-quantum cryptography
- Continue the migration to post-quantum cryptography for high security systems

Post-Quantum Cryptography guidelines

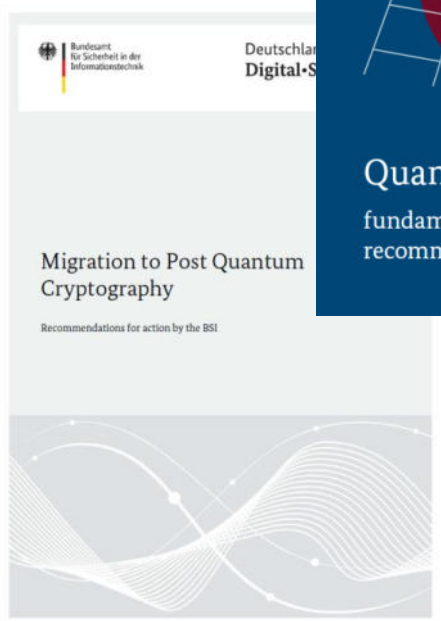


Federal Office
for Information Security

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

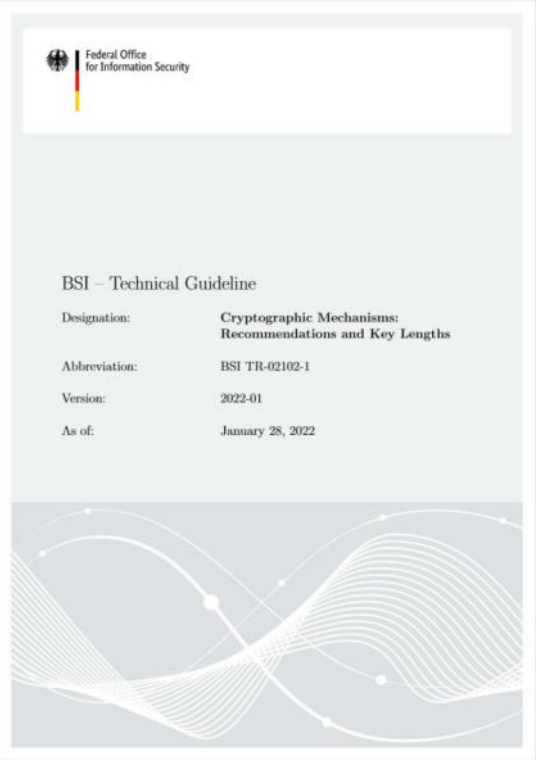


Reference: www.bsi.bund.de/dok/pqmigration-en

BSI Technical Guideline TR-02102-1

„Cryptographic Mechanisms: Recommendations and Key Lengths“

- Key Encapsulation Mechanisms:
  - *FrodoKEM* and *Classic McEliece*
- PQC only in *hybrid solutions*, i.e. PQC + “Classical”, except for HBS
- Stateful hash-based signatures
  - *LMS/HSS*
  - *XMSS/XMSS^MT*

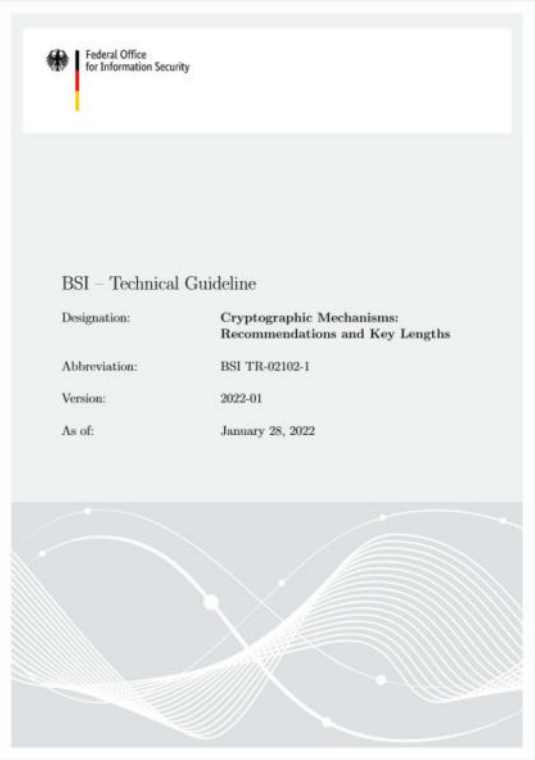


Reference: www.bsi.bund.de/TR-02102

BSI Technical Guideline TR-02102-1

Outlook (2024/2025):

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

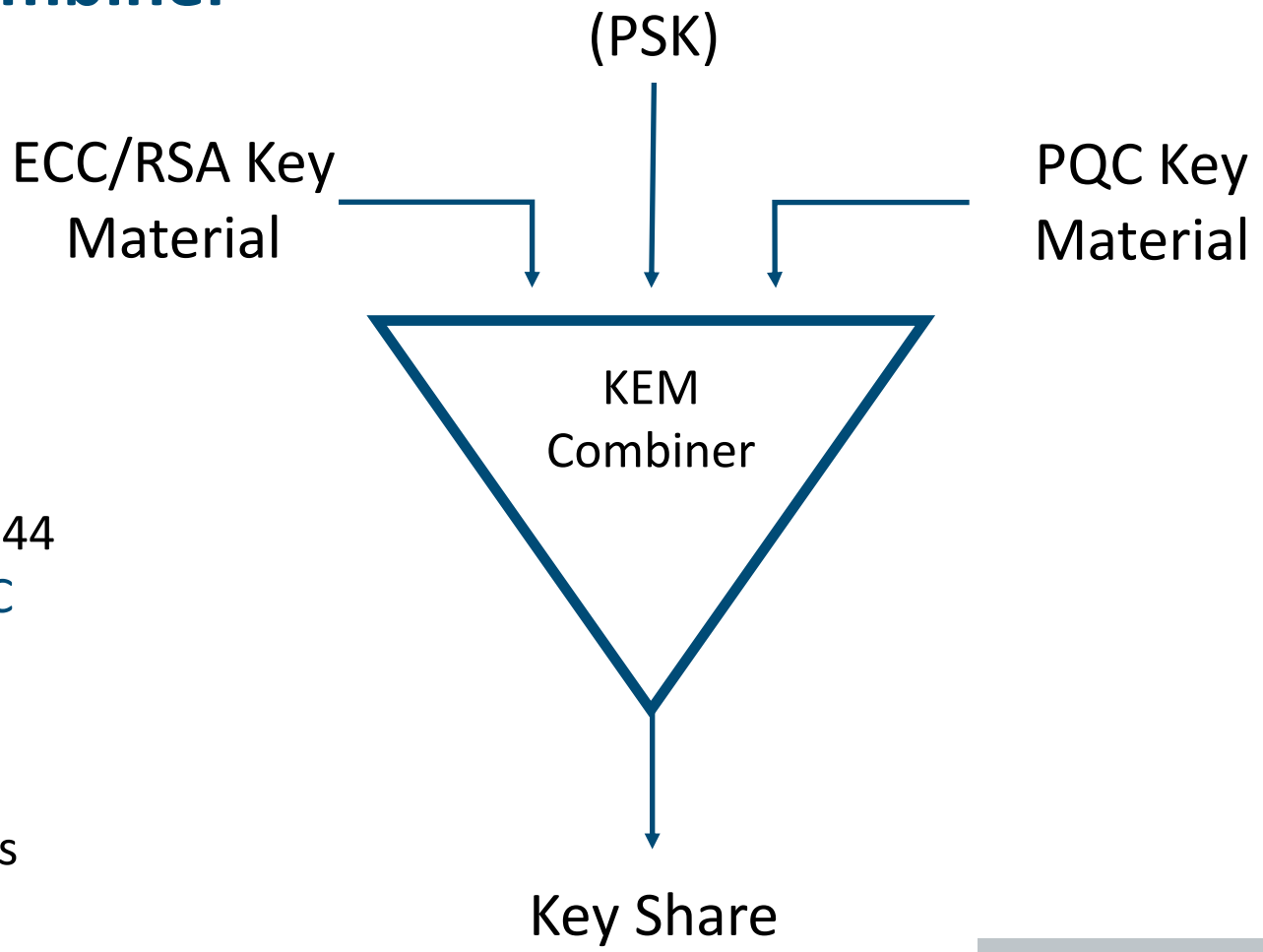


Hybrid Key Exchange: KEM Combiner

- Goal:
  Construction is secure as long as
  at least one component KEM is secure.

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

- Some relevant IETF drafts/RFCs:
  - draft-ounsworth-cfrg-kem-combiners
  - draft-ietf-tls-hybrid-design
  - RFC9370: Multiple Key Exchanges IKEv2



BSI‘s current PQC projects

- PQC in the cryptographic library Botan:
  - FrodoKEM*, Classic McEliece*, Kyber (* coming soon)
  - 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
- Quantum-safe PKI for Germany’s federal administration (“Verwaltungs-PKI”)
  → Tomorrow!

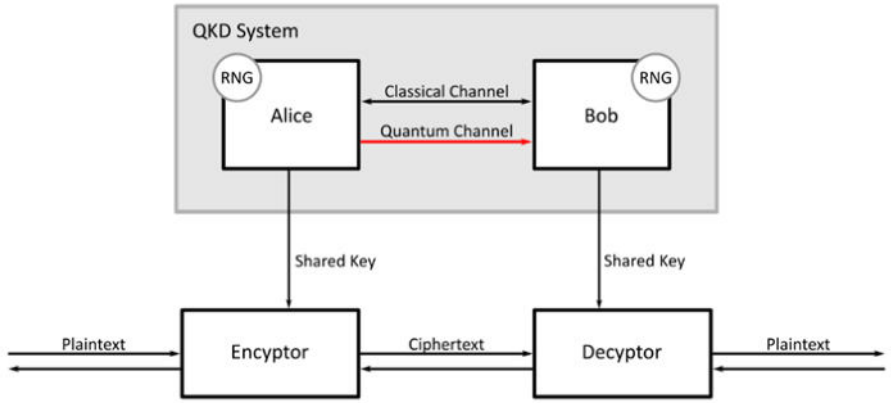
What about Quantum Key Distribution?

Quantum Key Distribution (QKD)

Some facts:

- Theoretical security is based on quantum-physical principles
- Only works for key agreement
- Requires specialized (and expensive) hardware
- Implementation security also has to be considered

  (in addition to theoretical security)
- Limitations of QKD make it only applicable for specific use cases



BSI‘s policy:

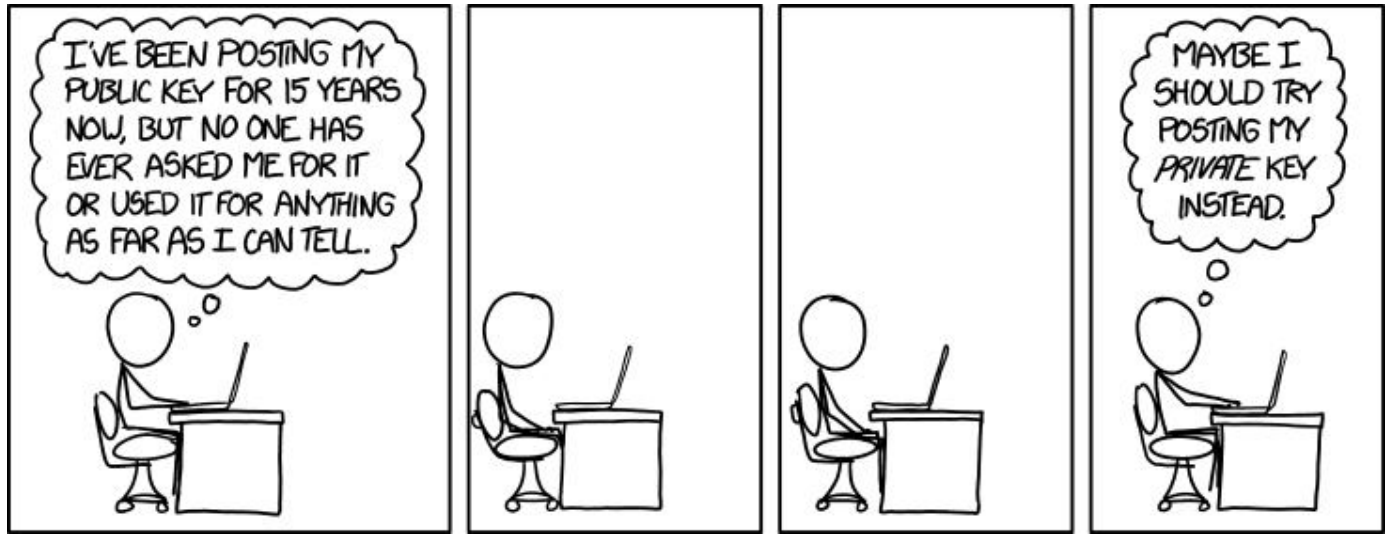
- **Migration to PQC has highest priority**
- QKD could potentially complement or backup PQC in the future

Wrap-up

- The public-key cryptography deployed today will be broken when large-scale quantum computers become available.
- *„Store now, decrypt later“* is a real threat & considerable migration times are to be expected.

  ⟶ PQC-migration has to be initiated **now**!

- In general, PQC should be used in hybrid mode together with RSA or ECC.
- QKD is not sufficiently mature from a security perspective.



Source: https://xkcd.com/1553/

Contact

Dr. Stephan Ehlen

Federal Office for Information Security
Godesberger Allee 185-189
53175 Bonn

stephan.ehlen@bsi.bund.de

quantum@bsi.bund.de

Deutschland
Digital•Sicher•BSI•

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

Federal Office
for Information Security

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia