

Preparing for Q-Day

Migration timelines, policies & activities



Federal Office
for Information Security

Charlotte Weitkämper

July 10th, 2026

Secure Protocol Implementations in the Quantum Era – SPIQE 2026

Agenda

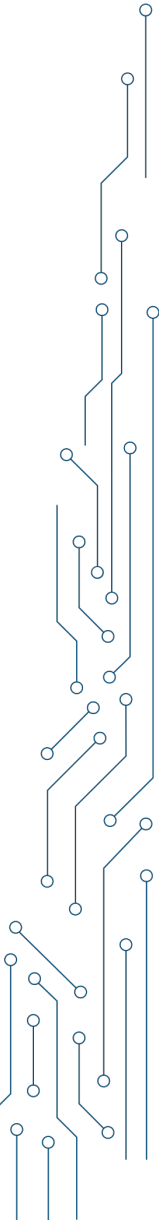
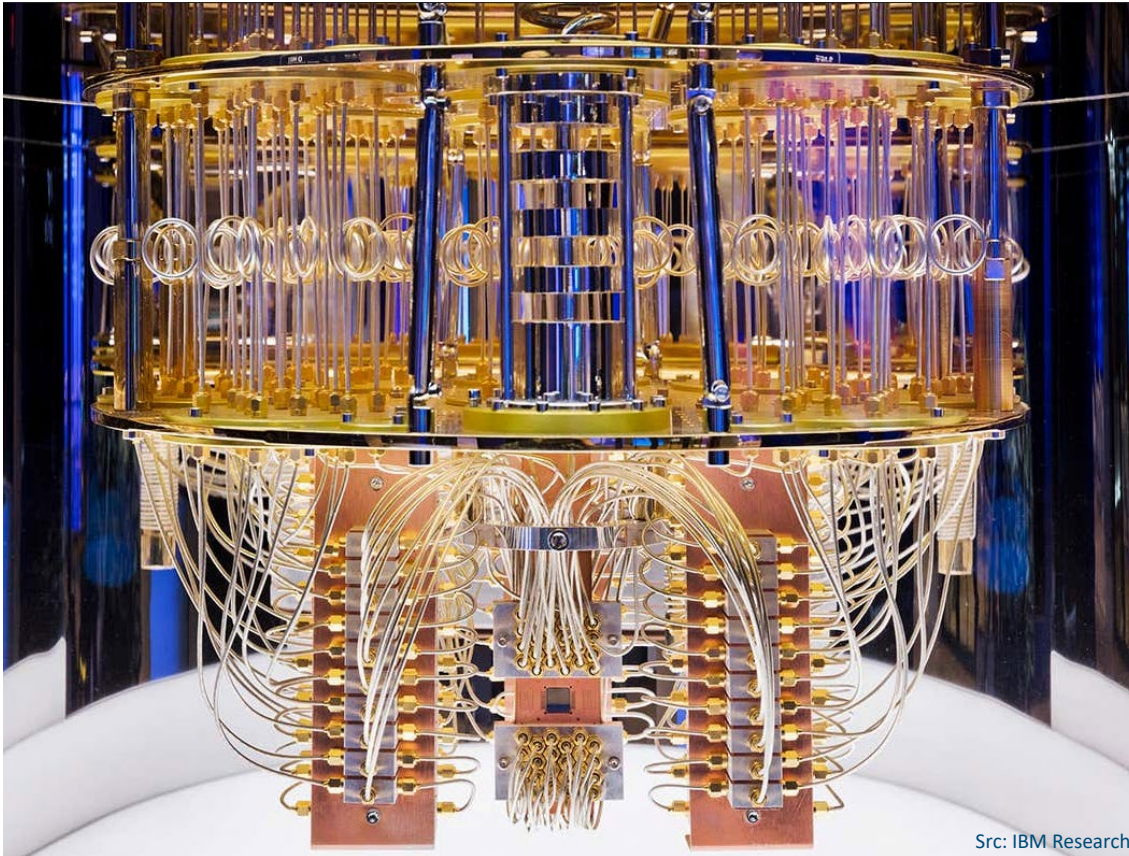
- Introduction: the Quantum Threat
- Migrating to PQC
 - Standardisation
 - Roadmaps
 - Best practices
- What's left to do?

The Quantum Threat

- How do QCs affect cryptography?
- When can we expect cryptographic relevance of QCs?

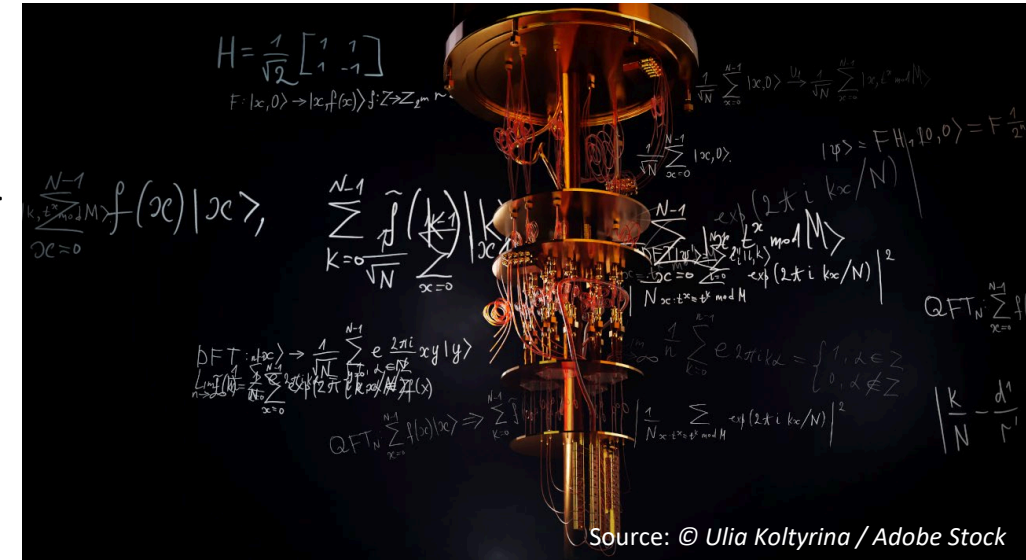
Quantum computers break asymmetric cryptography

Traditional algorithms are under threat when QCs become more powerful



Critical scenarios

- **Store now-decrypt later:** Adversaries may already store encrypted data today to decrypt it once large-scale quantum computers are available.
- **Complex systems:** Replacing or hardening cryptographic mechanisms in large and complex systems will require long periods of transition.



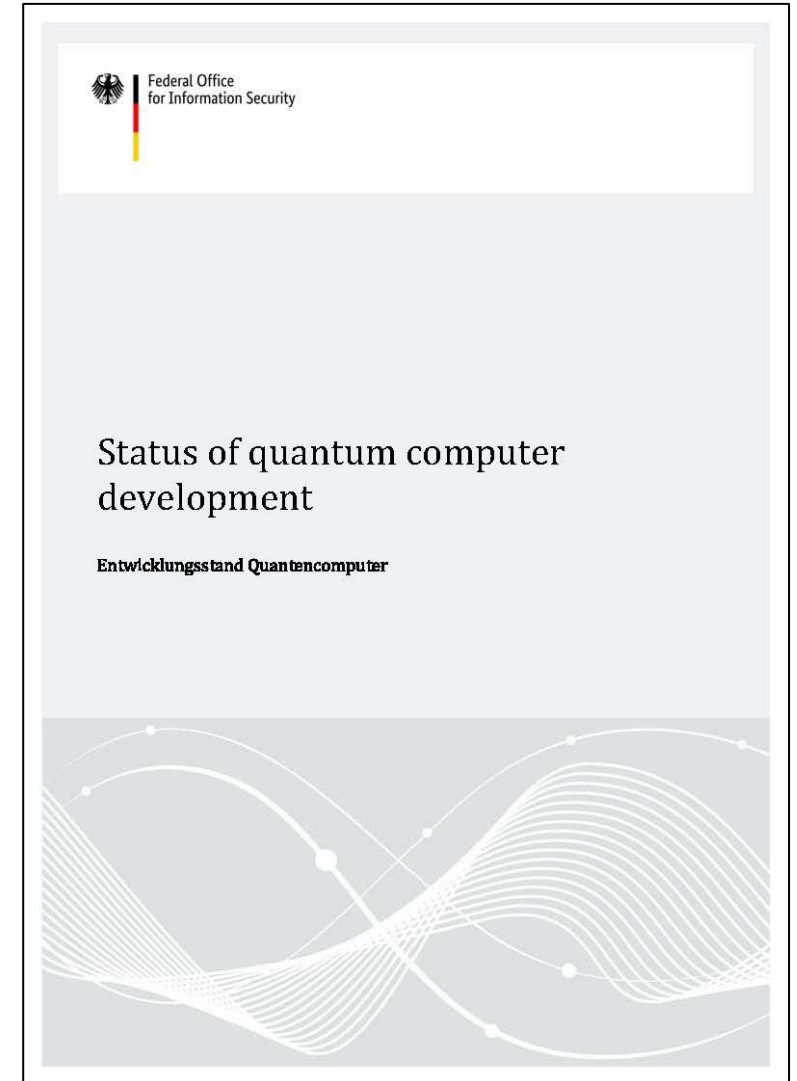
BSI Study “Status of quantum computer development”

Goals

- Overview of major quantum technologies,
- Relevant technological developments,
- Cryptographic impact.

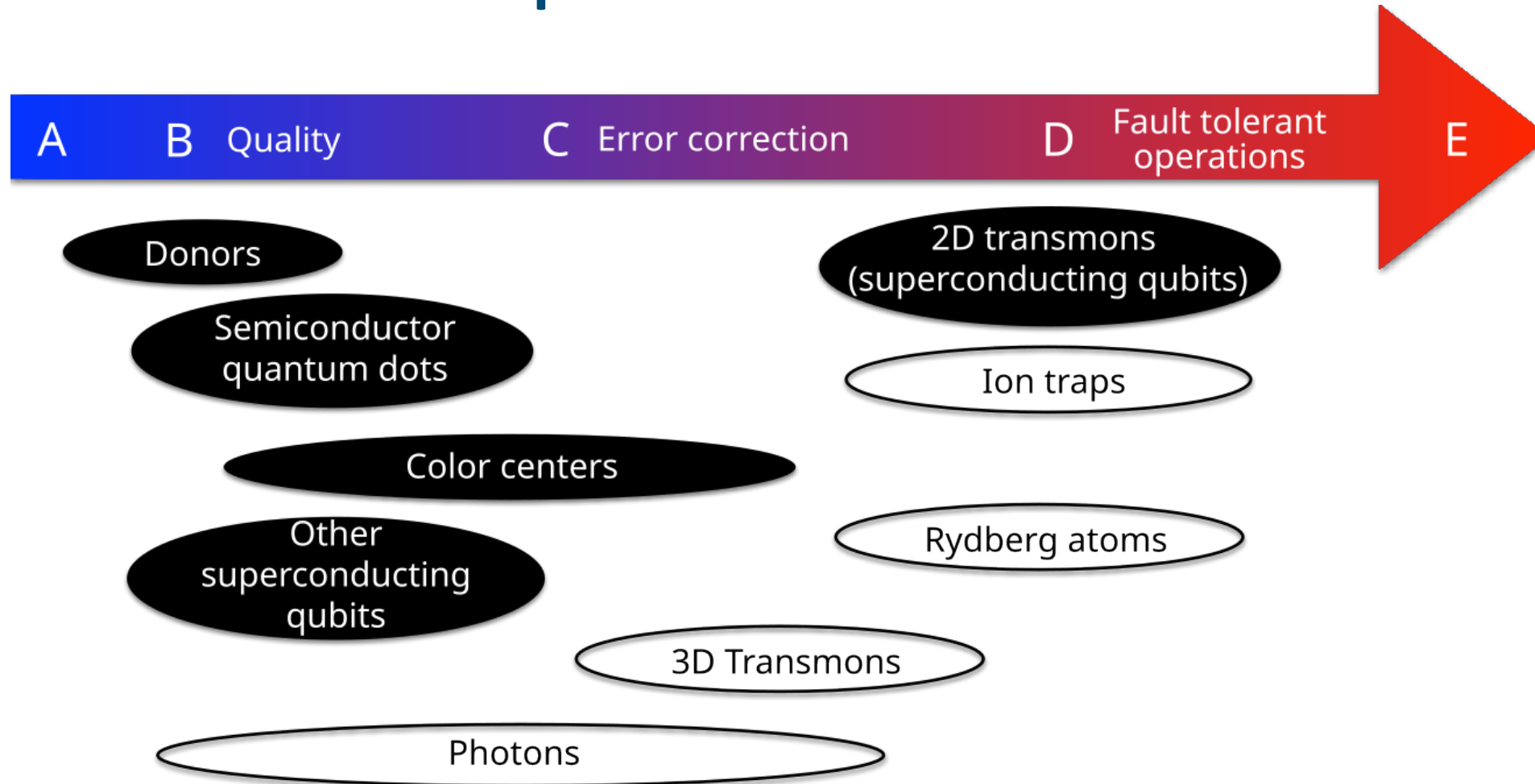
Versions

- Regular updates since 2018.
- Most recently in Dec. 2025 (Version 2.2).
- New BSI project: P1011 (currently in tender)



https://bsi.bund.de/dok/study_status_quantum_computer

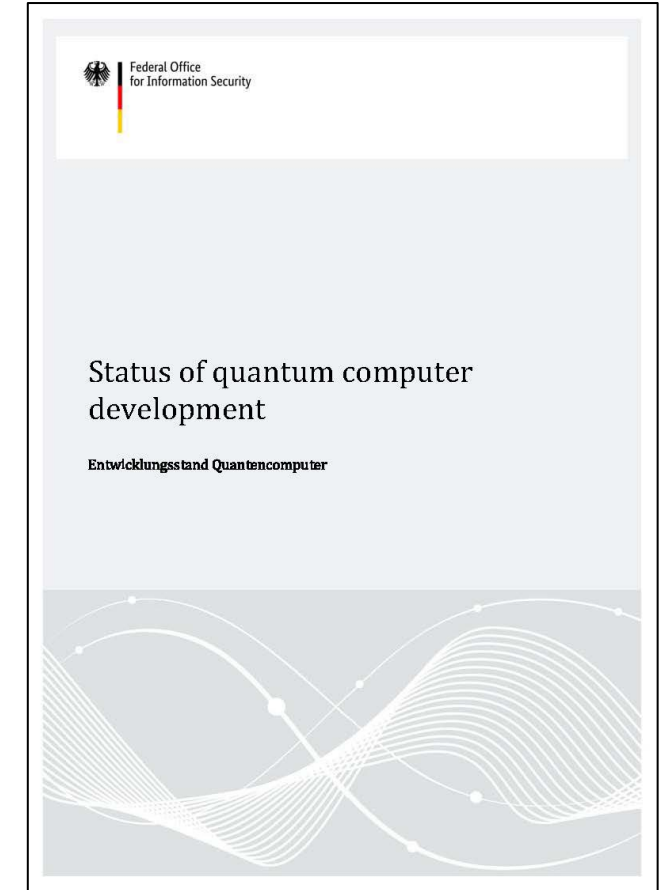
BSI Study “Status of quantum computer development”: Evaluation of the main platforms



BSI Study “Status of quantum computer development”

Key Observations (2025)

- Quantum computing is making steady progress towards cryptanalytic relevance.
- “[...] cryptographically relevant quantum computers are likely to be available within **15 years**.”
- In case of new developments in error correction and mitigation and relevant hardware, cryptographic relevance within **10 years** is possible.



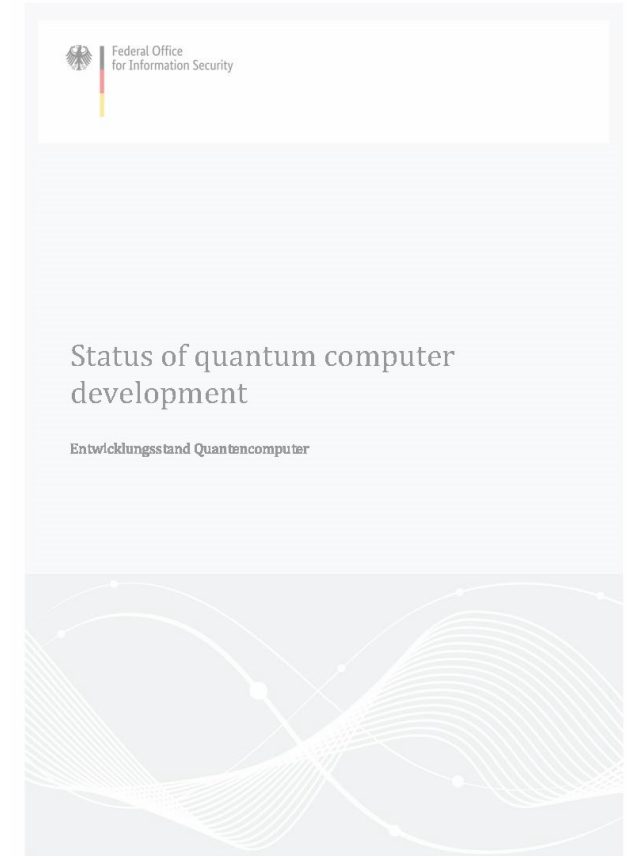
https://bsi.bund.de/dok/study_status_quantum_computer

BSI Study “Status of quantum computer development”

Key Observations (2025)

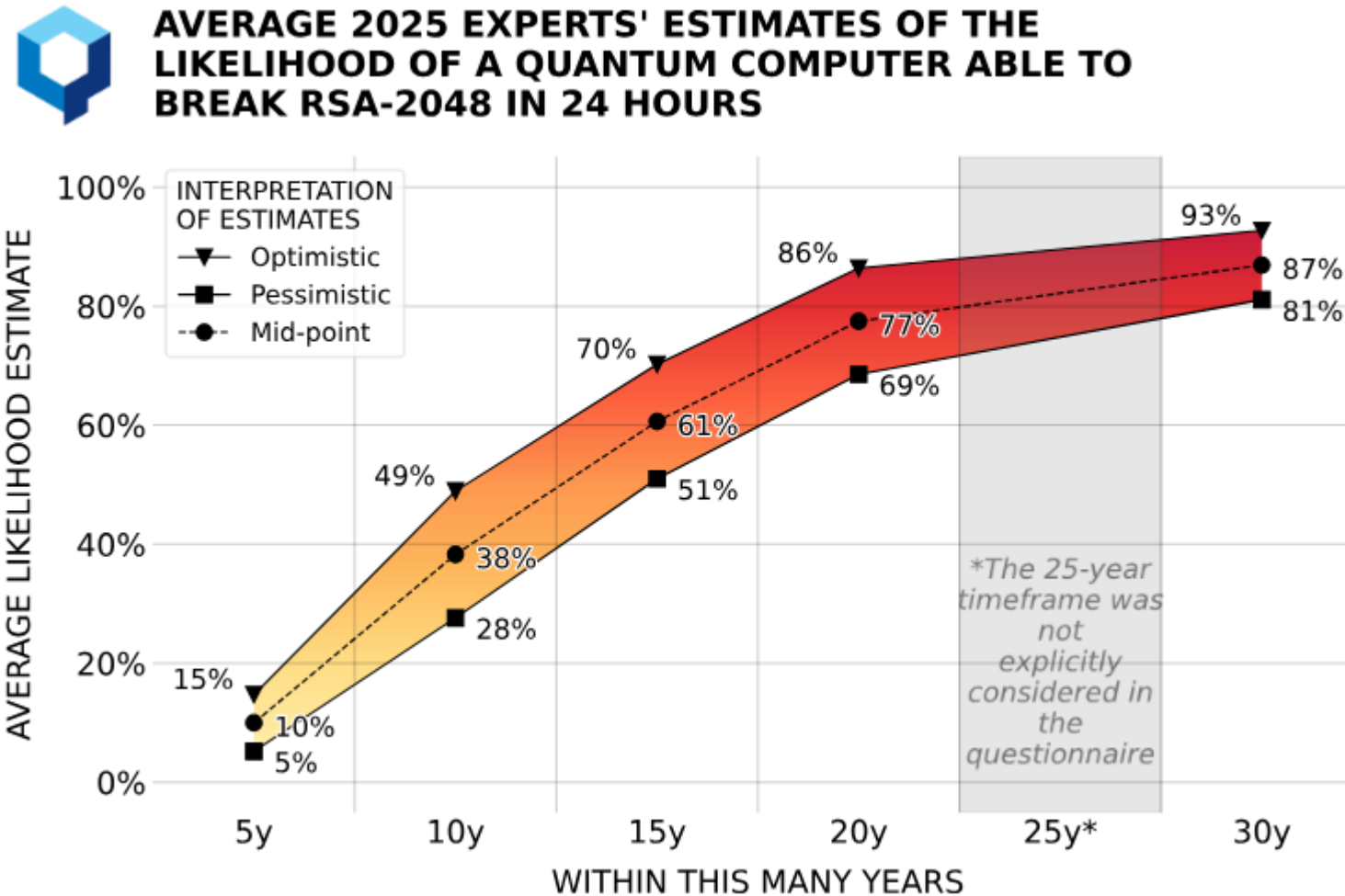
- Quantum computing is making steady progress towards cryptanalytic relevance.
- “[...] cryptographically relevant quantum computers are likely to be available within **15 years.**”
- In case of new developments in error correction and mitigation and relevant hardware, cryptanalytic relevance within 10 years is possible.

This means 2040!!!



https://bsi.bund.de/dok/study_status_quantum_computer

When can we expect “Q-Day” to happen?



The solution: Post-Quantum Cryptography (PQC)

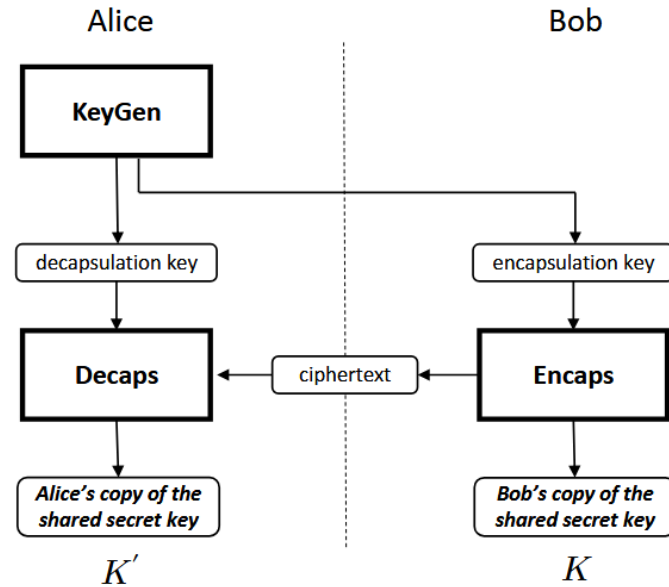
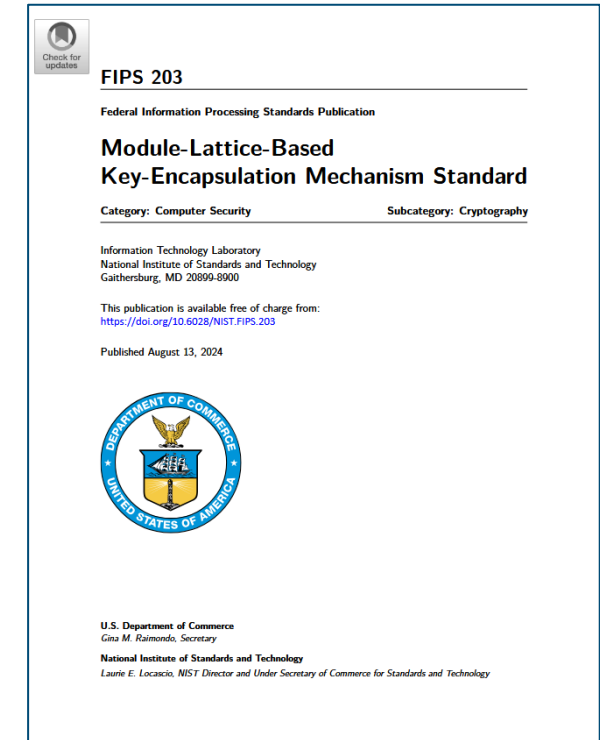


Figure 1. A simple view of key establishment using a KEM

Organisations standardising new PQC algorithms and protocols

- NIST
- ISO
- IETF
- ...



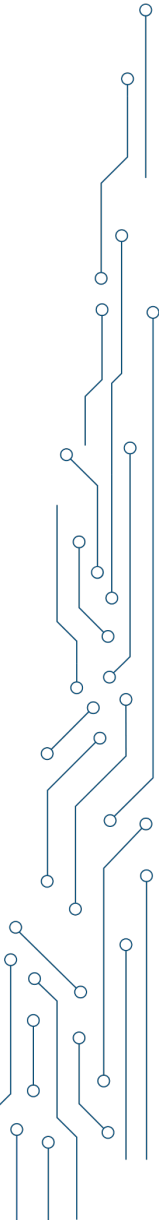
Migrating to PQC

- Why is migration necessary now?

PQC-Migration: Why now?

Cryptographic transitions take time

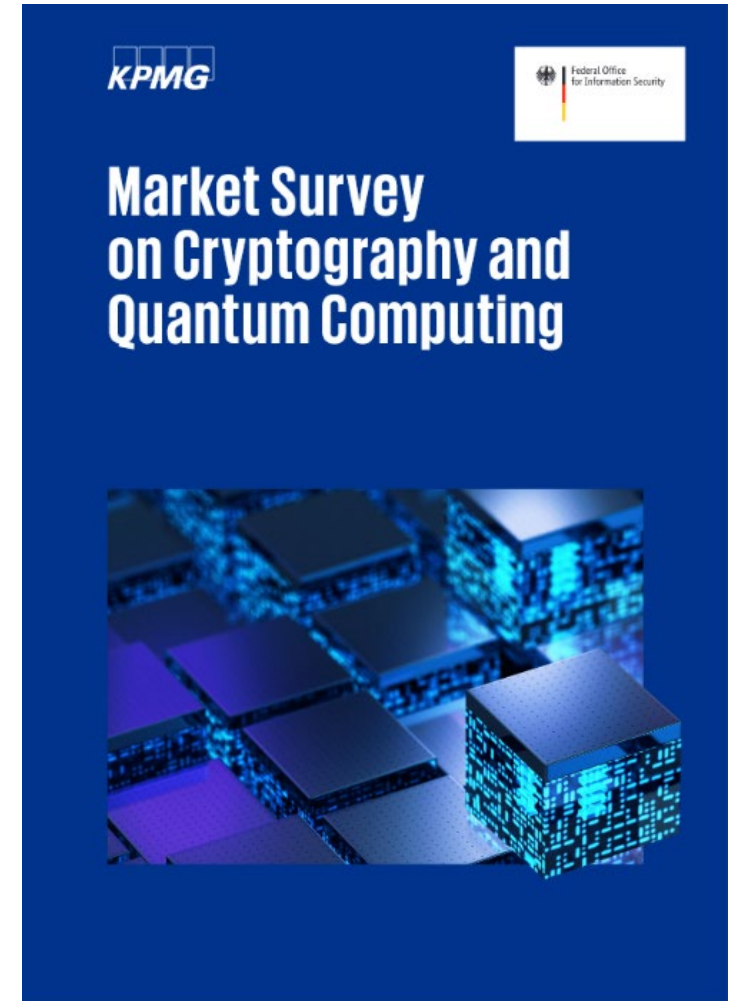
In 1977, the Data Encryption Standard (DES) became the first published encryption standard. The DES algorithm [2] had a 64-bit block size and a 56-bit key. Motivated by the threat of a practical brute-force attack against DES's 56-bit key, a variation of DES called Triple DES [3] (due to its capacity to perform DES operations with two or three 56-bit keys) was introduced in 1999 as a temporary solution before a stronger algorithm could be standardized and made available for use. This new and stronger algorithm, called the Advanced Encryption Standard (AES) [3] (with options for 128-, 192-, or 256-bit keys), was standardized in 2001. However, Triple DES continued to be used in many applications until it was finally disallowed in 2024. In all, the complete transition from Triple DES to AES took 23 years.



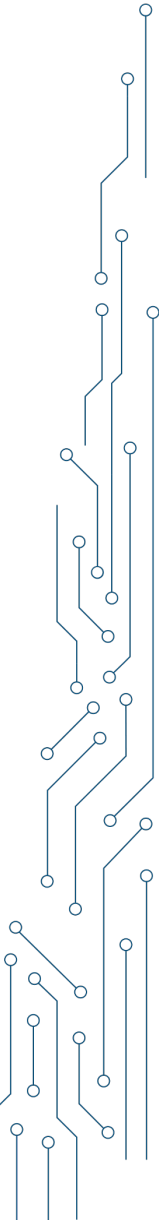
Are we prepared for CRQCs?

BSI & KPMG market survey from 2023:

- Main questions:
 - Are (German) businesses and public bodies aware of the quantum threat?
 - Have actions towards quantum-resilience been taken?
 - What is the level of preparedness?
- **Key finding:** Participants do not expect to migrate to quantum-safe cryptography in time
- Updated version? tbc



Market Survey
(only in German at the moment)



Standardisation, Roadmaps & Best Practices

BSI Guide “Quantum-safe cryptography”

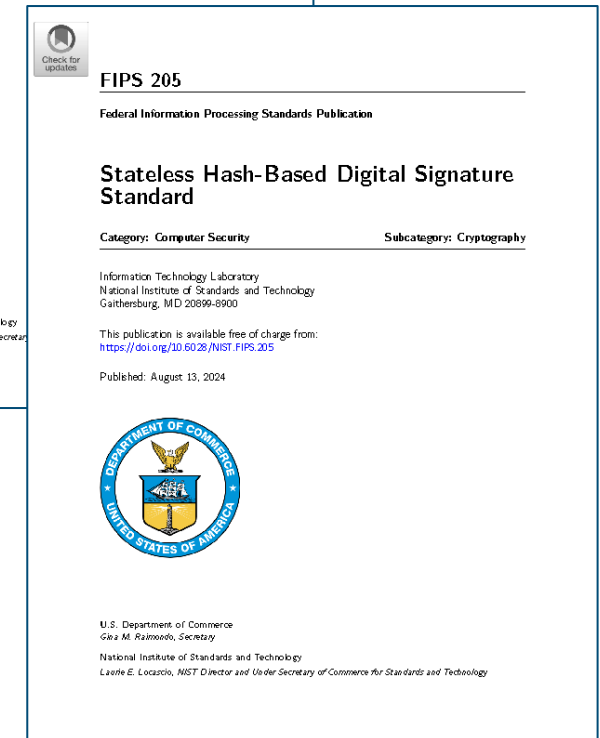
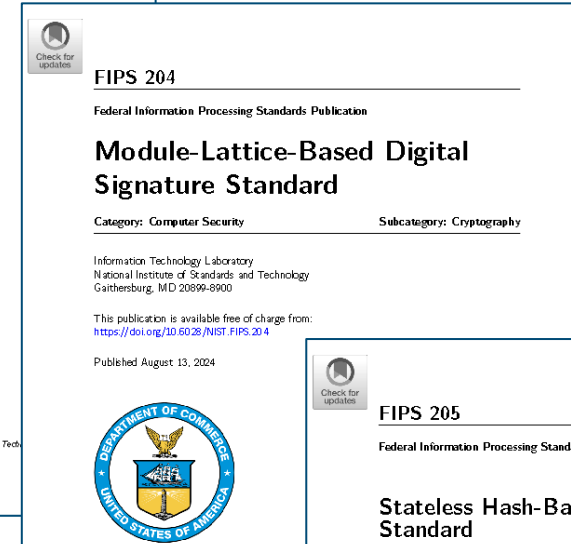
- BSI publication from 2021
- Background on quantum computers, PQC, protocols, QKD
- Developments in politics, research and industry
- Recommendations for actions (excerpt):
 - Preparation: cryptographic inventory
 - Cryptographic agility
- Hybrid solutions for KEMs and signature schemes



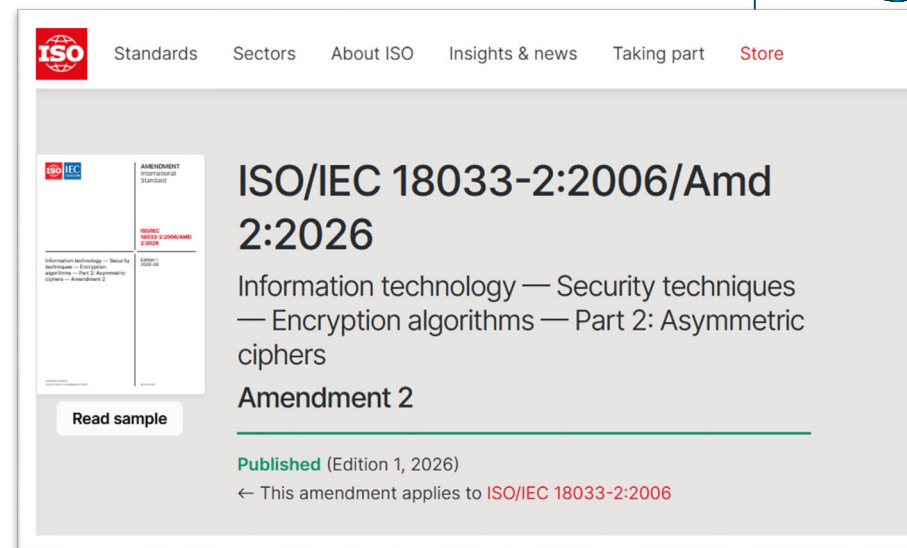
Global PQC Standardisation

- algorithmic level -

- NIST PQ-Standards
 - FIPS 203: ML-KEM
 - FIPS 204: ML-DSA
 - FIPS 205: SLH-DSA
 - (FN-DSA, HQC)
 - ...



- ISO Standardisation
 - FrodoKEM
 - Classic McEliece
 - ML-KEM
 - ...

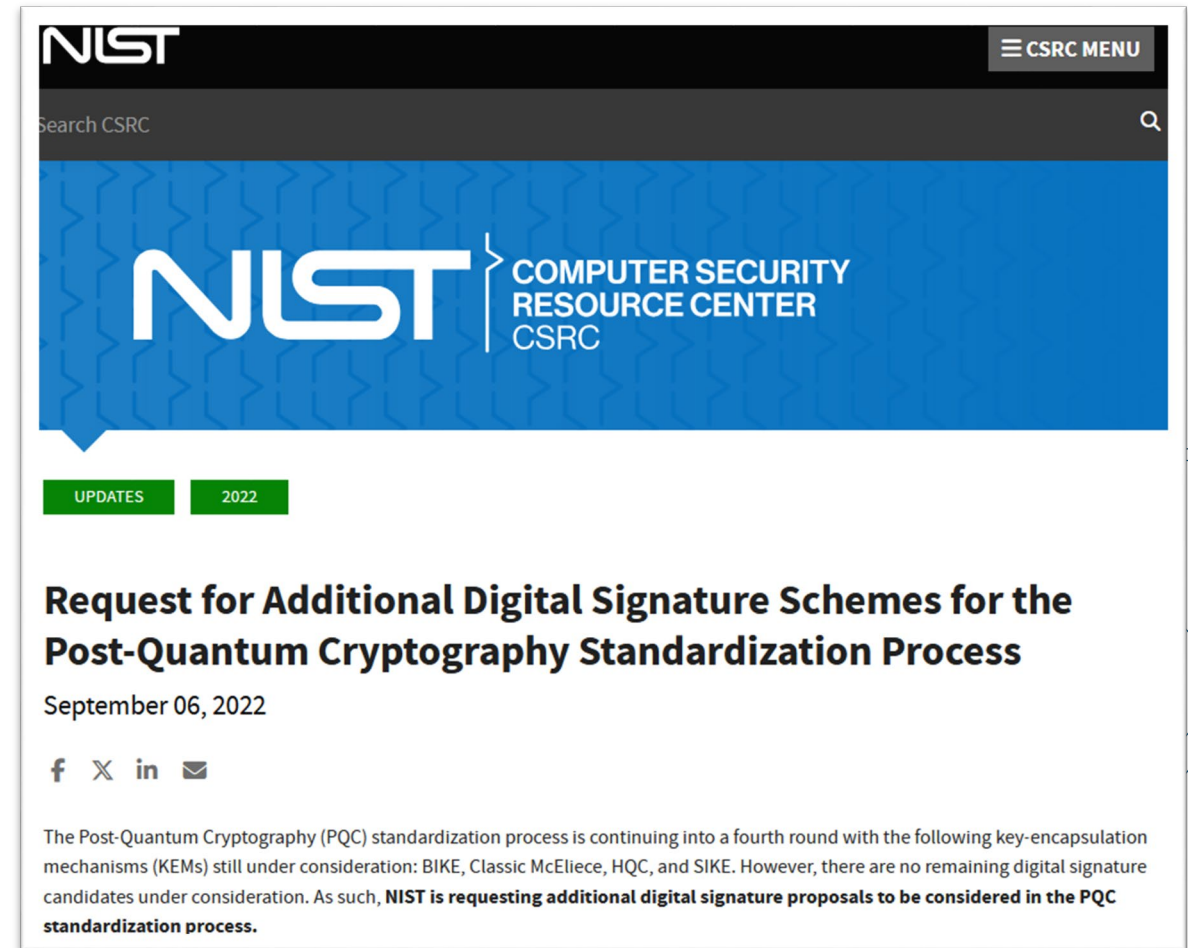


Global PQC Standardisation

- algorithmic level -

Requirements and considerations for standardisation

- General use vs specialised use cases
- Security proofs and sufficient cryptanalysis
- Diversity of underlying mathematical problems



Global PQC Standardisation

- protocol level -

IETF/IRTF activity

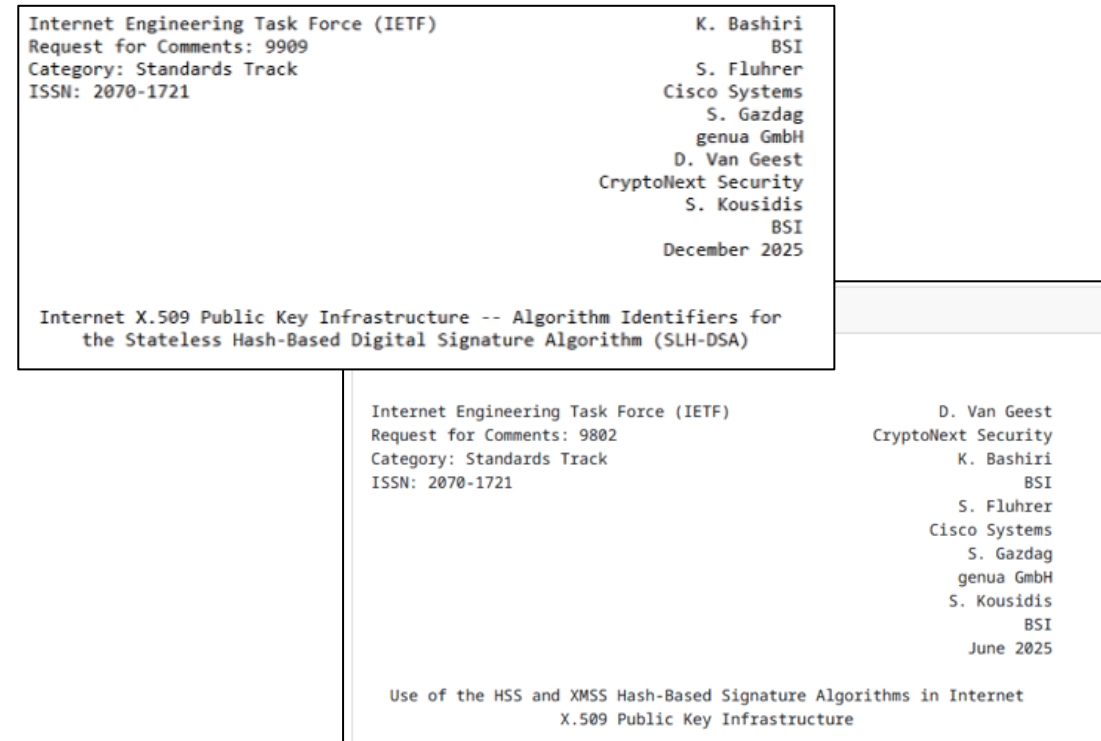
- Hash-based signatures in X.509 certificates
- PQC in OpenPGP -> RFC9980
- TLS 1.3
- IKEv2/IPsec
- ...

Example: PQ in TLS 1.3

- ML-KEM hybrid
- ML-KEM stand-alone
- ML-DSA stand-alone
- ML-DSA hybrid
- AuthKEM (hybrid KEM for authentication)

Publication pipeline

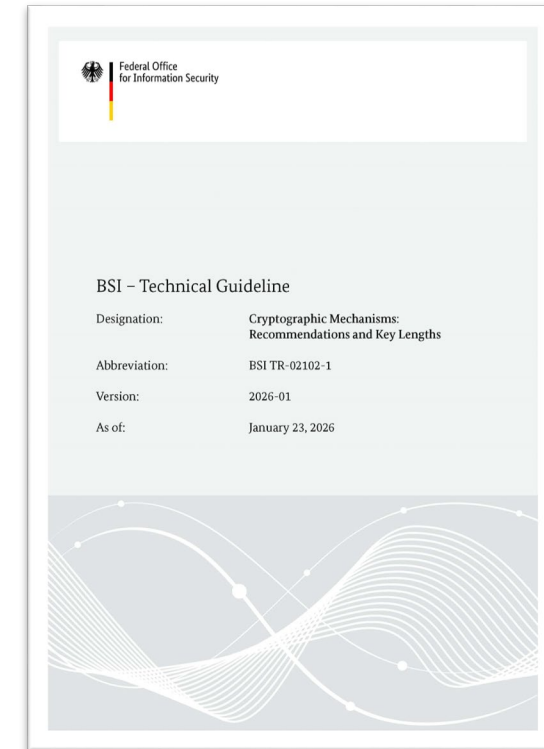
Not (yet) adopted



PQC recommendations by BSI

Technical Guideline TR-02102-1

- Key encapsulation mechanisms:
 - *FrodoKEM* and *Classic McEliece*
 - *ML-KEM*
 - ***(HQC-KEM when final standard is available)***
- Signature schemes:
 - *ML-DSA*
 - *SLH-DSA*
 - *LMS/HSS* und *XMSS/XMSS^{MT}*
- *Hybrid solutions* (PQC + classical) are recommended
- NIST Strength Categories III and V are recommended



PQC recommendations by BSI

Technical Guideline TR-02102-1

From 2032: classical asymmetric mechanisms **only in combination with PQC**

BSI empfiehlt Ende klassischer
asymmetrischer
Verschlüsselungsverfahren

Ort Bonn
Datum 11.02.2026



Quelle: © jjomathai / Adobe Stock

In its annual update of cryptographic recommendations (TR-02102), the German Federal Office for Information Security (BSI) advocates for the first time an **expiration date for classical asymmetric encryption methods**.

According to the BSI, these **methods should no longer be used alone by the end of 2031**, or as early as the end of 2030 for highly sensitive applications.

Instead, they should be combined in hybrid form with post-quantum cryptography. For classical signature methods, the **discontinuation of their sole use is planned for the end of 2035**.

European Roadmap for the Transition to PQC



EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

**on a Coordinated Implementation Roadmap for the transition to Post-Quantum
Cryptography**



Securing Tomorrow,
Today: Transitioning
to Post-Quantum
Cryptography

A joint statement from partners from 18 EU member states:

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish Transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxembourg, General Intelligence and Security Service BZK, Ministry of Interior and Kingdom Relations Netherlands and National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain



Bundesamt
für Sicherheit in der
Informationstechnik



Ministerie van Binnenlandse Zaken en
Koninkrijkrelaties

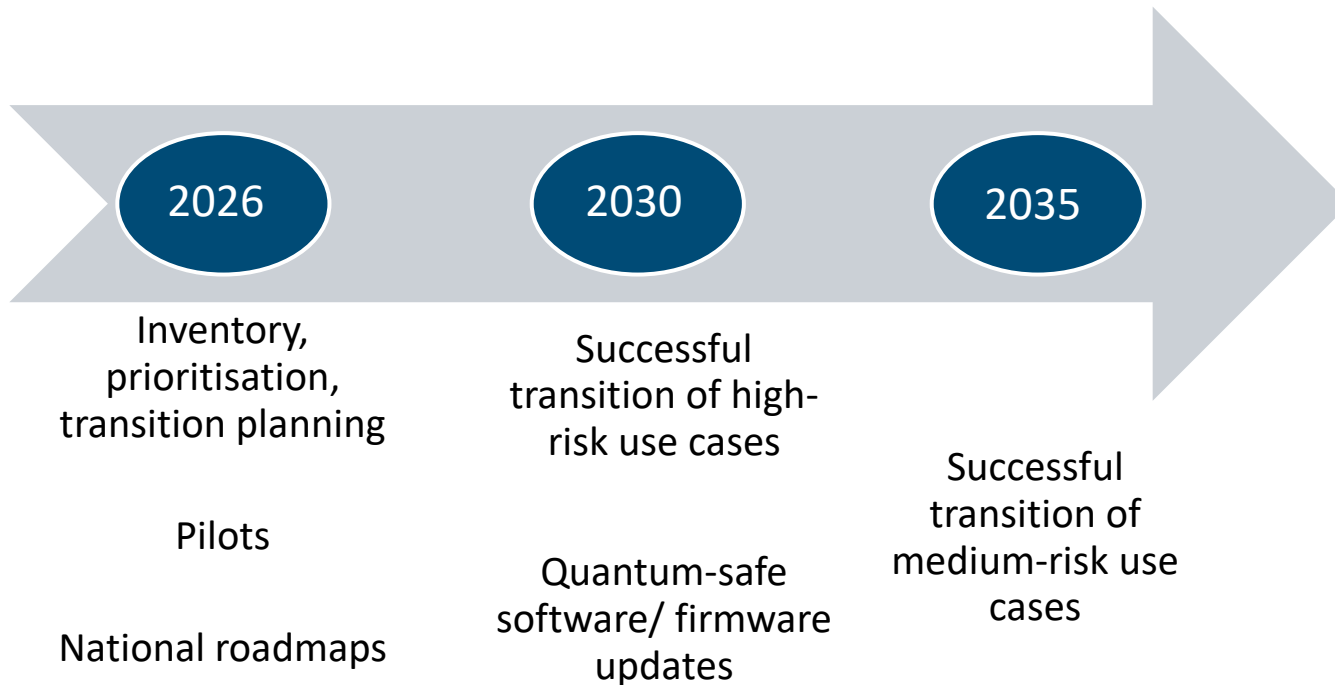


RÉPUBLIQUE
FRANÇAISE



European Implementation Roadmap for PQC

- Target audience: EU member states
- But recommendations are also applicable to different organisations

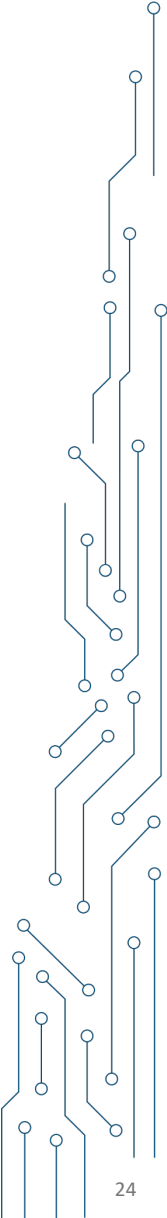


EU-Roadmap

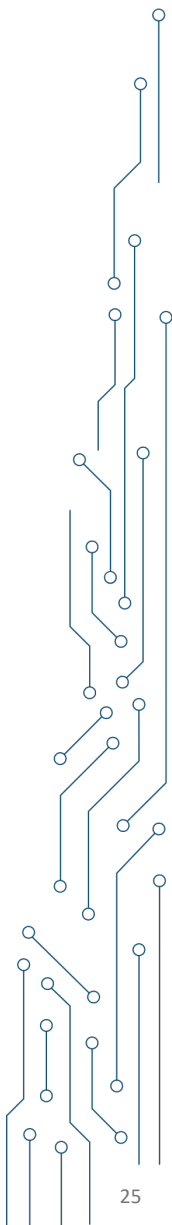
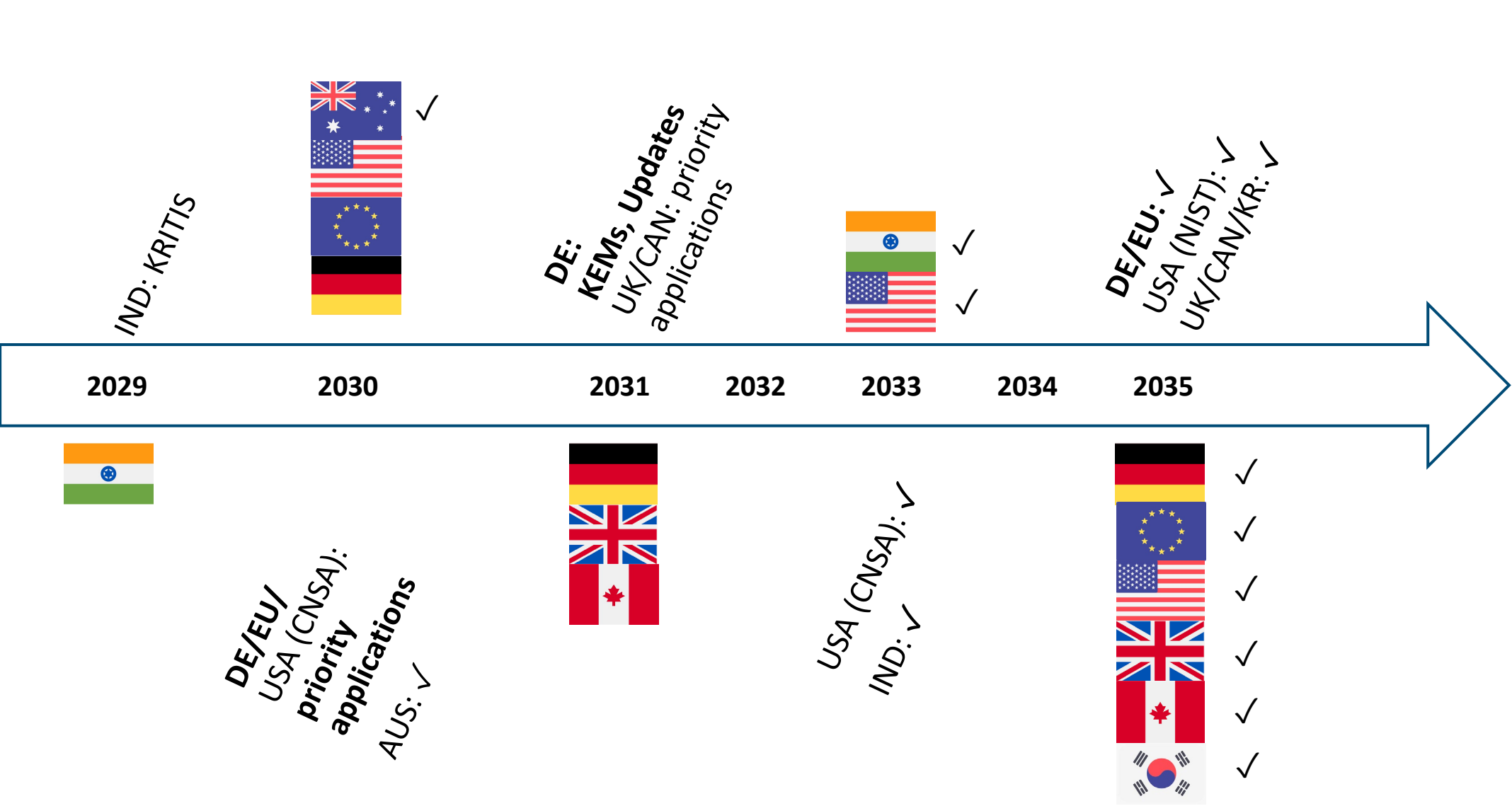
Timeline for the EU Transition to PQC

Milestones to reach

- By end of 2026
 1. PQC transition planning and pilots for high- and medium-risk use cases have been initiated
 2. Initial national PQC transition roadmaps have been established by all Member States.
- By end of 2030
 1. The PQC transition for high-risk use cases has been completed.
 2. PQC transition planning and pilots for medium-risk use cases has been completed.
 3. Quantum-safe software and firmware upgrades are enabled by default.
- By end of 2035
 1. The PQC transition for medium-risk use cases has been completed.
 2. The PQC transition for low-risk use cases has been completed as much as feasible.



International milestones



Certification: Cryptographic Guidelines for EUCC



European Cybersecurity Certification Group
Sub-group on Cryptography

Agreed Cryptographic Mechanisms

Version 2.0
April 2025

Primitive	Scheme	R/L	Notes
FF-DLOG	DH [SP800-56A, ISO11770-3]	R	57-KE-Auth, 58-DHSubgroupAttacks, 59-QuantumThreat
	DLIES-KEM [ISO18033-2]	R	
EC-DLOG	EC-DH [SP800-56A, ISO11770-3]	R	57-KE-Auth, 58-DHSubgroupAttacks, 59-QuantumThreat
	ECIES-KEM [ISO18033-2]	R	
LWE	ML-KEM [FIPS203]	R	57-KE-Auth, 60-Hybridization, 61-ML-KEM Parameters
	FrodoKEM [FRODO-KEM]	R	
LWE	ML-DSA [FIPS204]	R	51-Hybridization, 55-ML-DSA Parameters
HASH	XMSS [SP800-208]	R	53-OptionalHybridization, 54-StateManagement
	LMS [SP800-208]	R	
	SLH-DSA [FIPS205]	R	52-SLH-DSAParameters, 53-OptionalHybridization
RSA	PKCS#1v1.5 [RFC8017, PKCS1, ISO9796-2]	L	48-PKCSFormatCheck, 50-QuantumThreat

Immediate measures for PQC migration

Overall responsibility: Steering Committee

Inventory

- Where is cryptography used?
- Sensitivity of data
- Life-time of data
- Dependencies (e.g. supply chain)

Prioritisation

- Cost of migration vs. Losses in case of compromise
→ **Risk-based approach**
- Estimate transition duration

Planning/ Execution

- Create dedicated steering committee
- Consider cost in company finances
- Implement quick fixes /ad-hoc measures

- Consultation and coordination with (international) partners
- Think **crypto agility** and **interoperability**

PQC @ BSI

PQC migration @ BSI



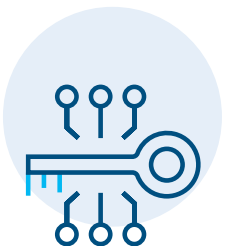
Steering group

- Coordinated PQ migration at BSI
- Blueprint for steering committee: “PQC migration of the federal government”



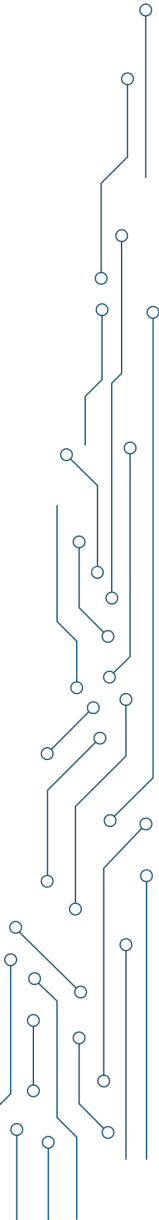
Administrative PKI (V-PKI)

- BSI maintains Root-CA
- Plan to migrate to PQC using a parallel approach



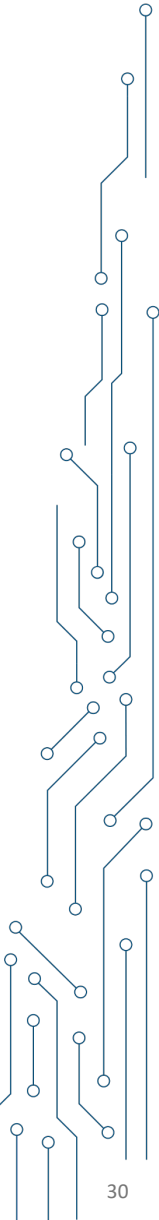
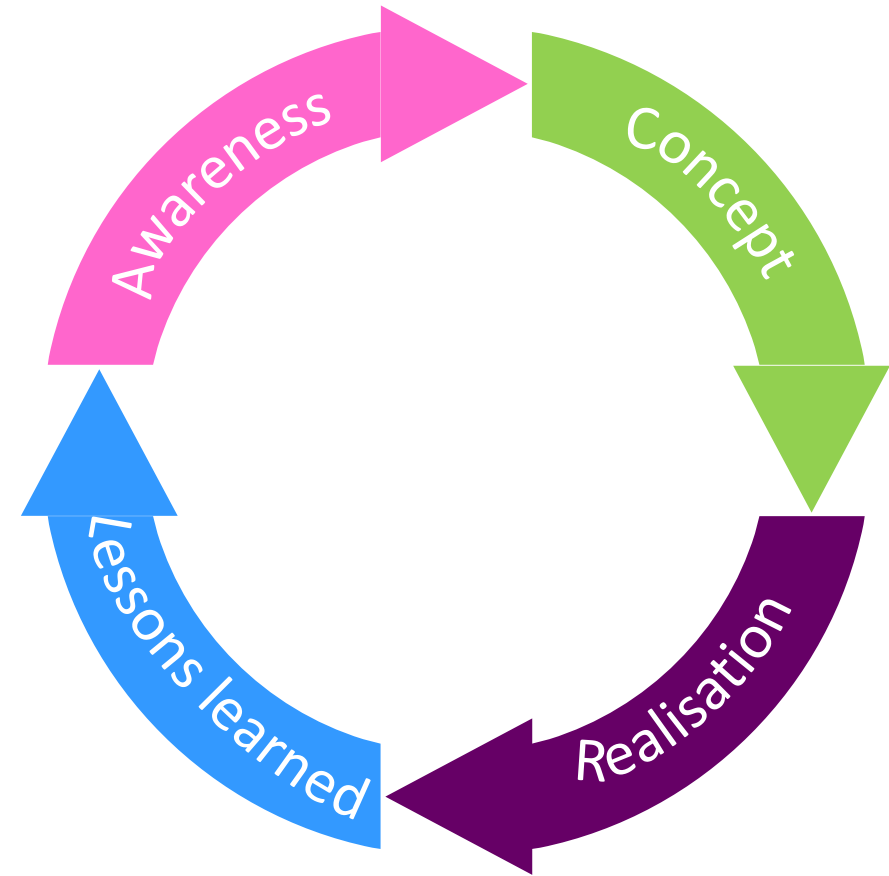
IT for Classified Information

- Evaluations at national and international level
- Migration roadmaps and action plans



Lessons learned from BSI steering committee

- Assigning responsibility is essential
- Involving divisions “far away from cryptography” helps obtain a more realistic approach
- Regular meetings keep members active and engaged
- Transition must be prioritised by executives



Example: Migration of Germany's Public Administration PKI ("V-PKI")

Goal: Trustworthy identity management for the public administration

Usage: S/MIME, TLS and other standard applications

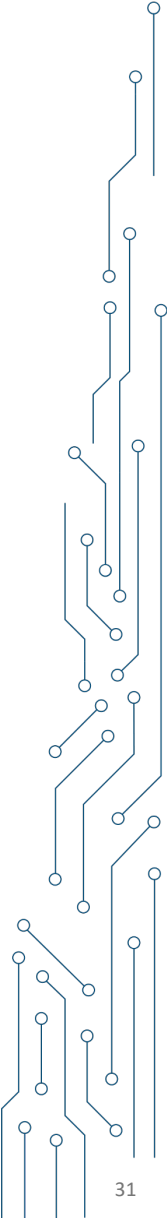
Scale: 6 Sub-CAs, approx. 500.000 subscribers

Algorithm: RSA4096



In order to migrate V-PKI to PQC...

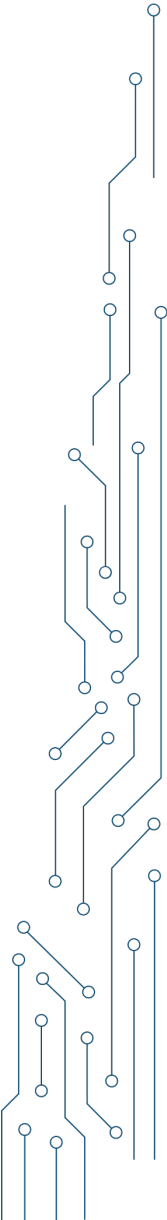
- ... new hardware security modules (HSMs) need to be developed.
- ... a quantum-safe PKI will be built in parallel to replace the existing PKI.
- ... different algorithms are currently being considered.



Quantum-safe V-PKI – Choice of signature schemes

Important criteria

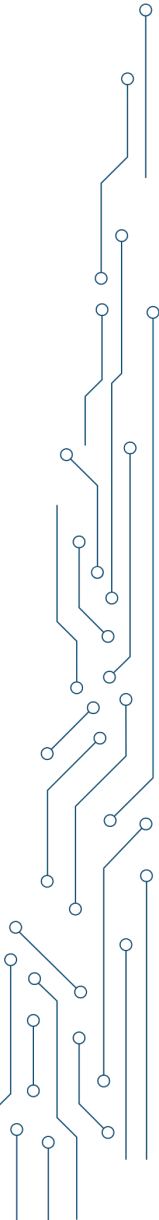
- Conservative security assumptions
 - with respect to a **classical** attacker
 - with respect to a **quantum** attacker
- Performance:
 - Small signature- and public key-size
 - Fast signature verification
- Compatibility with standard applications
- Easy handling on end user level



Quantum-safe V-PKI – Choice of signature schemes

Candidates

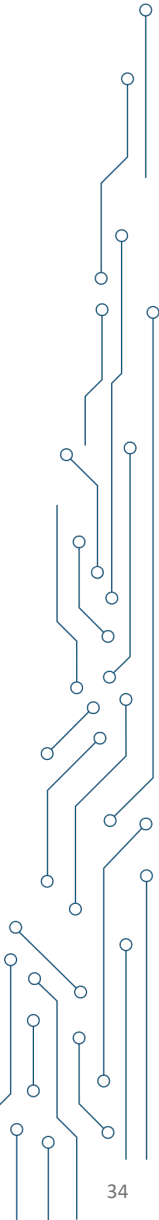
	Conservative security		Performance		
Algorithm	Classical Attacker	Quantum Attacker	SigSize+ PK-Size	SigVerTime	Handling on end user level
XMSS, LMS	✓	✓	✓✓	✓	X
SLH-DSA	✓	✓	X	✓	✓
SLH-DSA-Few	✓	✓	✓	✓	?
ML-DSA (pure)	X	X	✓	✓	✓
ML-DSA & ECDSA	✓	X	✓	✓	✓



Approval of Crypto-Products for Classified Information

Transition Roadmap for the Restricted Level (VS-NfD)

- Approved CI products must deploy **quantum-safe key exchange** and asymmetric cryptography from 1.1.2030.
- Approved CI products must provide **quantum-safe signatures** for software and firmware updates from 1.1.2030.
- CI PKIs must be able to offer **quantum-safe certificates** for root, sub-CAs and users after 31.12.2030.
- **Non-PKI authentication services** for CI must transition to quantum-safe algorithms until the end of 2030.

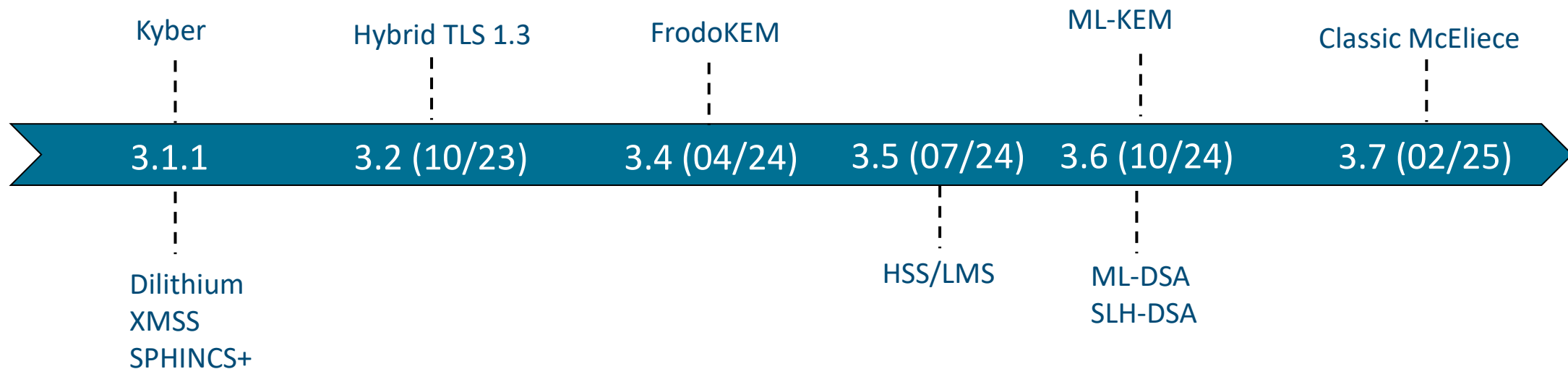


BSI project: Open-Source Crypto Library Botan

Github: [randombit/botan](https://github.com/randombit/botan)

- Latest Botan version: 3.12 (**BSI-approved: 3.7.1-RSCS1**) -> Audit of 3.12 coming soon
- Includes “BSI policy” which disables disallowed algorithms at runtime (if possible)
- This year: HQC-module (Rust), PQC integration into X.509 certificates

PQC integration timeline

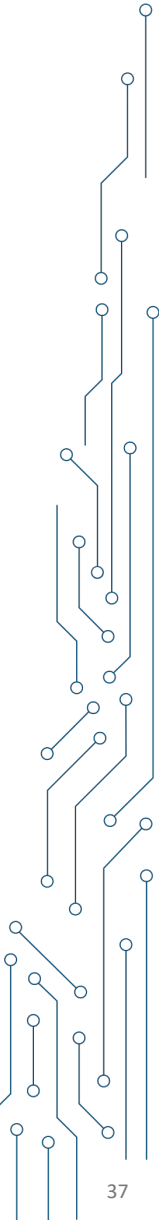


What's left to do?



Some challenges

- “New” algorithms:
 - Research and evaluation of side-channel attacks implementations of PQC e.g. on smartcards
 - Cryptanalysis and optimisation of Round 3-candidates in NIST “Additional Digital Signature Schemes” call
- Achieving cryptographic agility in different contexts
- Interoperability
- On the protocol level:
 - Hybridisation: standards for key derivation, implementation and deployment for key exchange and signatures/certificates
 - Formal verification of drafts and standards
- PQC solutions and/or analysis for specialised primitives or protocols, fancy crypto & upcoming topics, e.g.
 - PEC (ZKPs, FHE, MPC, ...)
 - DNS
 - PACE
 - ...
- CBOMs (tools, automatization, standard formats)
- ...



Thank you!

Dr. Charlotte Weitkämper
Division “Quantum-safe Cryptography and Cryptographic Applications”

charlotte.weitkaemper@bsi.bund.de
Federal Office for Information Security (BSI)
Godesberger Allee 87, 53175 Bonn

www.bsi.bund.de



Federal Office
for Information Security

Follow us:



Image : © AdobeStock/Nirut

Useful resources

- BSI Technical Guideline TR 02102-1: <https://www.bsi.bund.de/TR-02102>
- Quantum computer study: https://bsi.bund.de/dok/study_status_quantum_computer
- BSI “Quantum-Safe Cryptography”: <http://www.bsi.bund.de/dok/pqmigration-en>
- BSI: www.bsi.bund.de/Quanten
- EU Commission: Coordinated Implementation Roadmap: <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>
- AIVD, TNO, CWI: Handbook on PQC-migration: <https://publications.tno.nl/GGTSPU-5537757d40cc219a-46421-75772-e6CwRCyrOYzHLwr0-LOD/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf>
- Botan: <https://github.com/randombit/botan> and <https://github.com/sehlen-bsi/botan-docs>

Back up



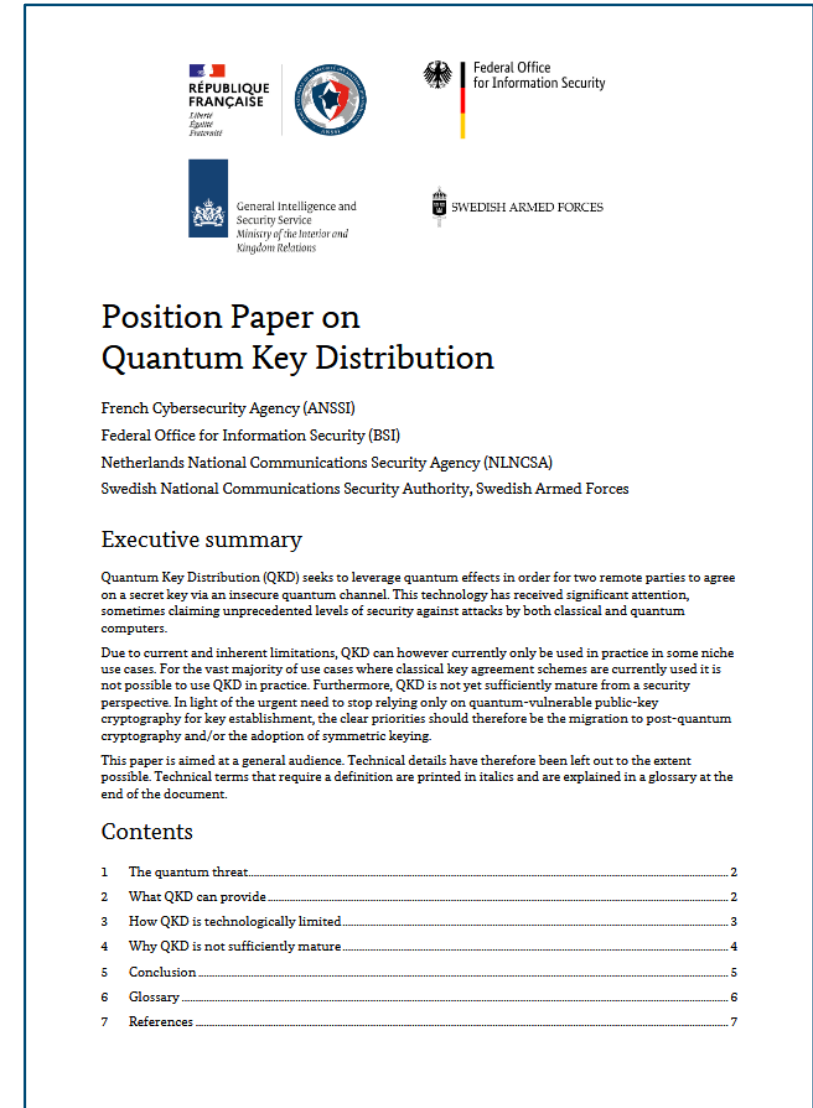
BSI position on QKD

Position Paper on Quantum Key Distribution

An alternative to PQC?

- **Theoretically**, QKD can provide information-theoretic security
- QKD is currently **unsuitable** for majority of use cases
- QKD is **not yet sufficiently mature** from a security perspective

→ The clear priorities should be the migration to PQC and/or the adoption of symmetric keying.



https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4