MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

# MINDSHARE AGENDA

**GET APP**

# Status and Struggles of Migration towards Post-Quantum Cryptography

Lea Nagler

Referat V32: Quantum-safe Cryptography and Cryptographic Applications

Bundesamt
für Sicherheit in der
Informationstechnik

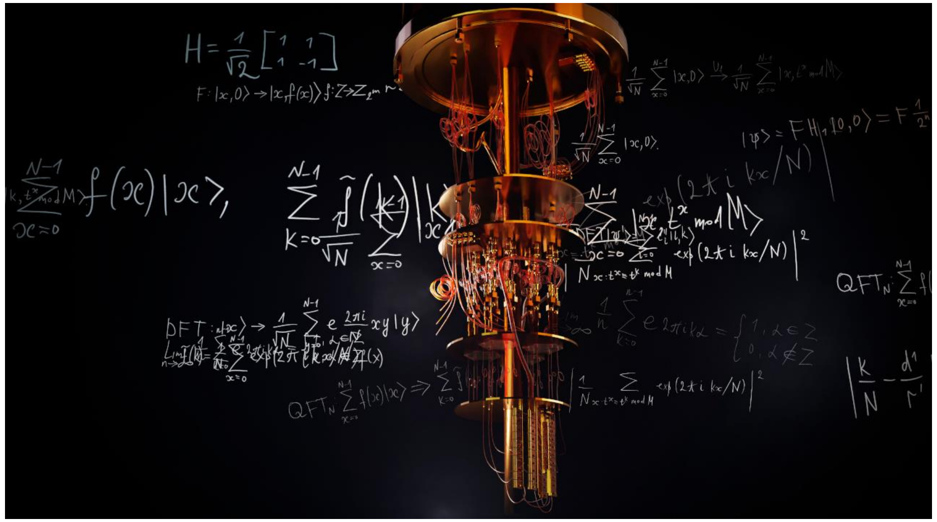
# The Quantum Threat

Bild: © AdobeStock/Azazul

# The Quantum Threat

Sufficiently large fault-tolerant quantum computers would be able to break most of the public-key cryptosystems in use today (in particular RSA and ECC).

Adversaries may already store encrypted data today to decrypt it once large-scale quantum computers are available.

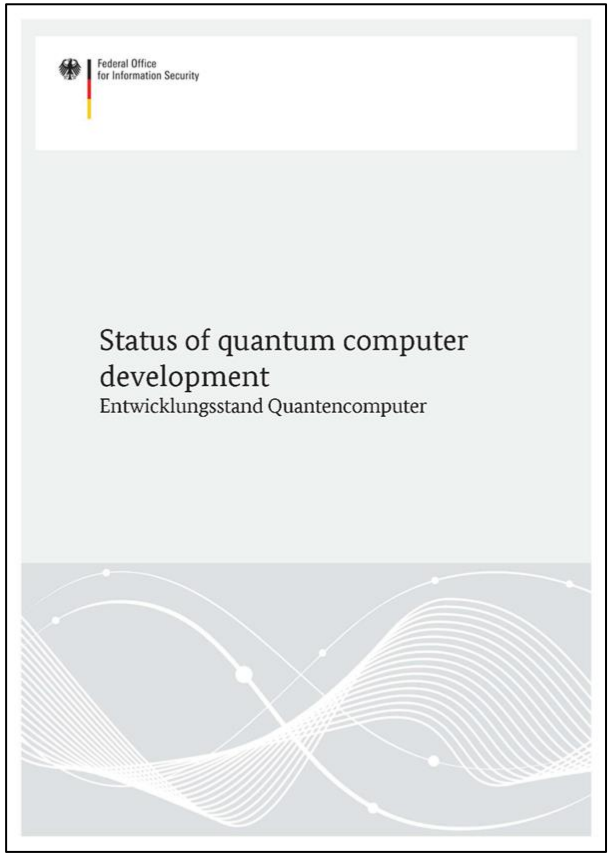


Source: *© Ulia Koltyrina / Adobe Stock*

Bundesamt
für Sicherheit in der
Informationstechnik

# BSI Report "Status of quantum computer development"

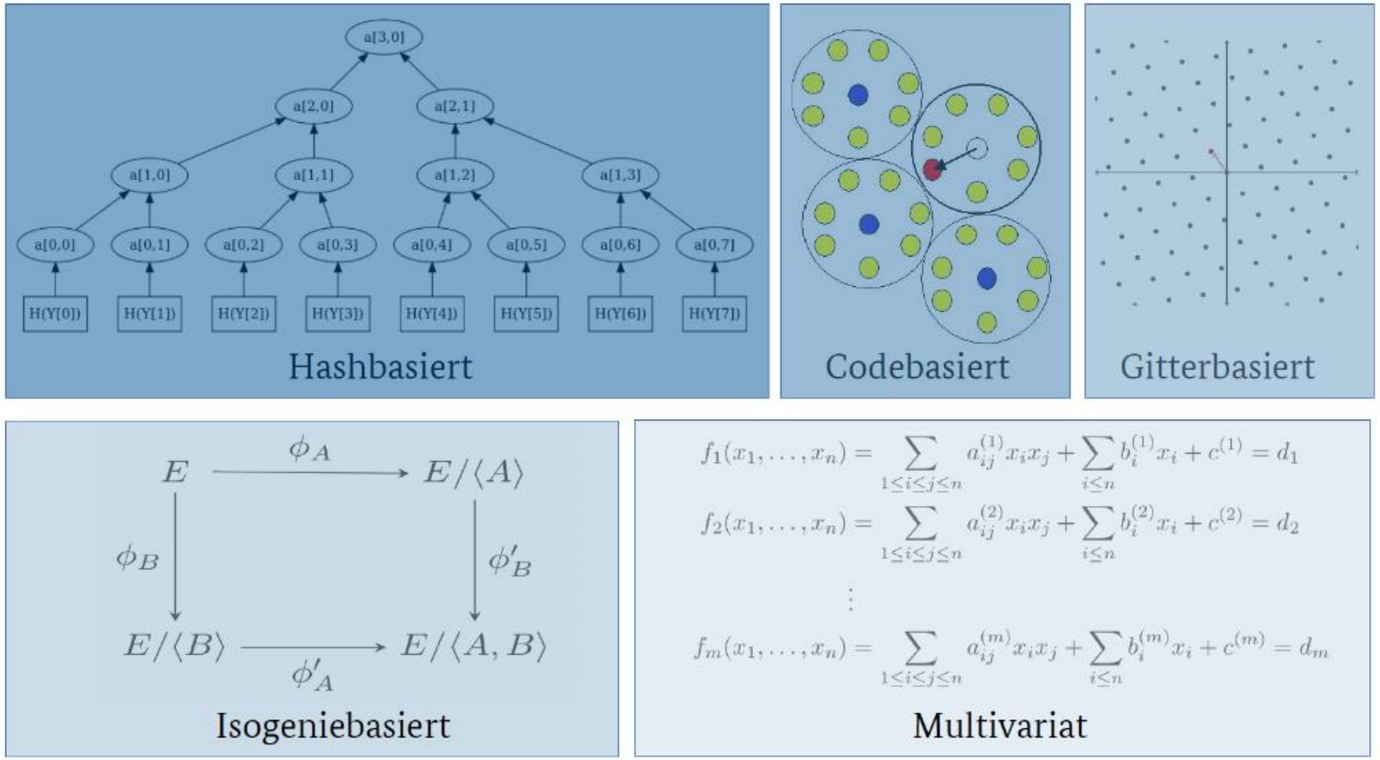
- First published in 2018, latest update January 2025
- Project lead: Prof. Frank Wilhelm-Mauch (FZ Jülich)
- Subcontractor: Prof. Rainer Steinwandt (University of Alabama in Huntsville)
- Quantum computing is making steady progress towards cryptanalytic relevance.
- **It is likely that a cryptographically relevant quantum computer will be realised within the next 16 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

# Mitigation: Post-Quantum Cryptography

# What is Post-Quantum Cryptography (PQC)?




PQC = Cryptographic algorithms that can be run on classical hardware and are deemed secure against attacks by both classical and quantum computers.

It comprises both **signature schemes** and **key agreement mechanisms**.

# Timeline of PQC standardization

- August 2015: NSA announces it will migrate national security systems to post-quantum cryptography.
- December 2016: NIST publishes call for proposals for the standardization of post-quantum algorithms
- November 2017: Submission deadline for first-round candidates
- January 2022: Publication of White House Memorandum, ordering federal agencies to migrate to PQC by 2035
- August 2024: Three NIST PQC standards published after evaluation of algorithms over three rounds
  - ML-KEM: lattice-based key encapsulation mechanism
  - ML-DSA: lattice-based signature algorithm
  - SLH-DSA: hash-based signature algorithm
- March 2024: NIST announces it will standardize HQC (a code-based KEM) as a result of fourth round

# PQC Recommendations in BSI Technical Guideline TR-02102-1

- Key encapsulation mechanisms:
    - *FrodoKEM* and *Classic McEliece*
    - *ML-KEM*
- Signature schemes:
    - *ML-DSA*
    - *SLH-DSA*
    - *LMS/HSS* und *XMSS/XMSS^MT*
- Parameters*:* NIST Security Strength *Categories 3 and 5*
- *Hybrid solutions (*PQC + classical) are recommended
- Exception: Hash-based signatures can be used without hybridization

# Certification: Cryptographic Guidelines for EUCC

enisa

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 | 57-KE-Auth, 60-Hybridization, 62-FrodoKEM Parameters |

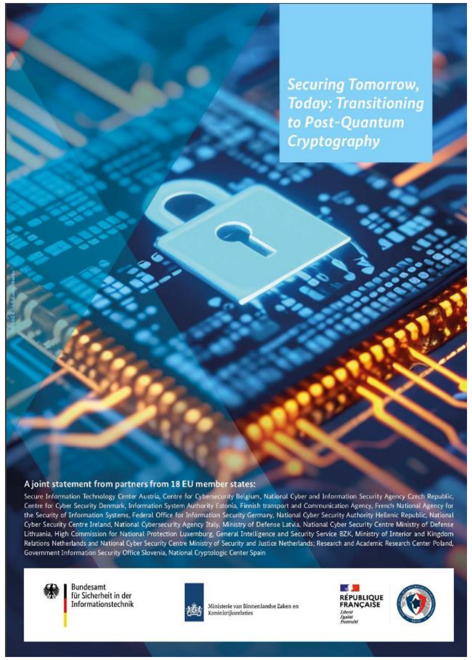
| | | | |
|---|---|---|---|
| LWE | ML-DSA [FIPS204] | R | 51-Hybridization, 55-ML-DSA Parameters |
| HASH | XMSS [SP800-208] | R | 53-OptionalHybridization, 54-StateManagement |
| | LMS [SP800-208] | R | |
| | SLH-DSA [FIPS205] | R | 52-SLH-DSAParameters, 53-OptionalHybridization |
| RSA | PKCS#1v1.5 [RFC8017, PKCS1, ISO9796-2] | L | 48-PKCSFormatCheck, 50-QuantumThreat |

# Recommendations for Transitioning

# Joint Statement: Securing Tomorrow, Today

Inventory ✚ Prioritisation ✚ Planning and execution

- So far signed by agencies from 20 EU member states
- Make the transition to post-quantum cryptography a top priority.
- Start the transition now.
- Deploy PQC in hybrid solutions.
- Most sensitive use cases should be protected against the quantum threat by the end of **2030.**




https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html

# Commission Recommendation

EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

**COMMISSION RECOMMENDATION**

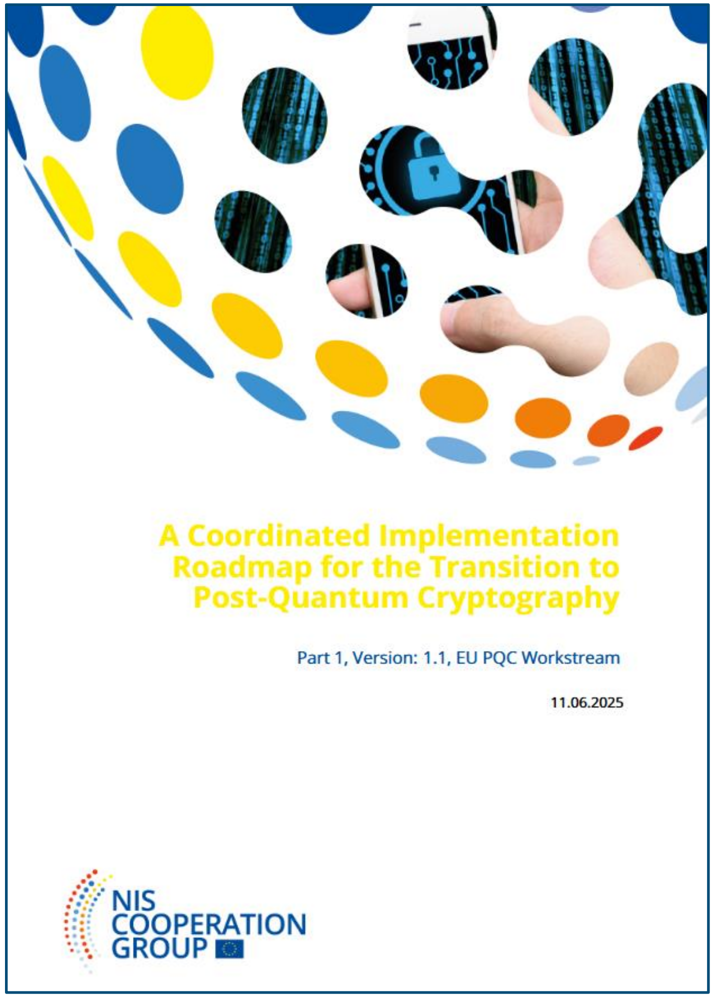
**of 11.4.2024**

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

“The Post-Quantum Cryptography Coordinated Implementation **Roadmap** should be available **after a period of two years** following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap.”

# European Implementation Roadmap for PQC

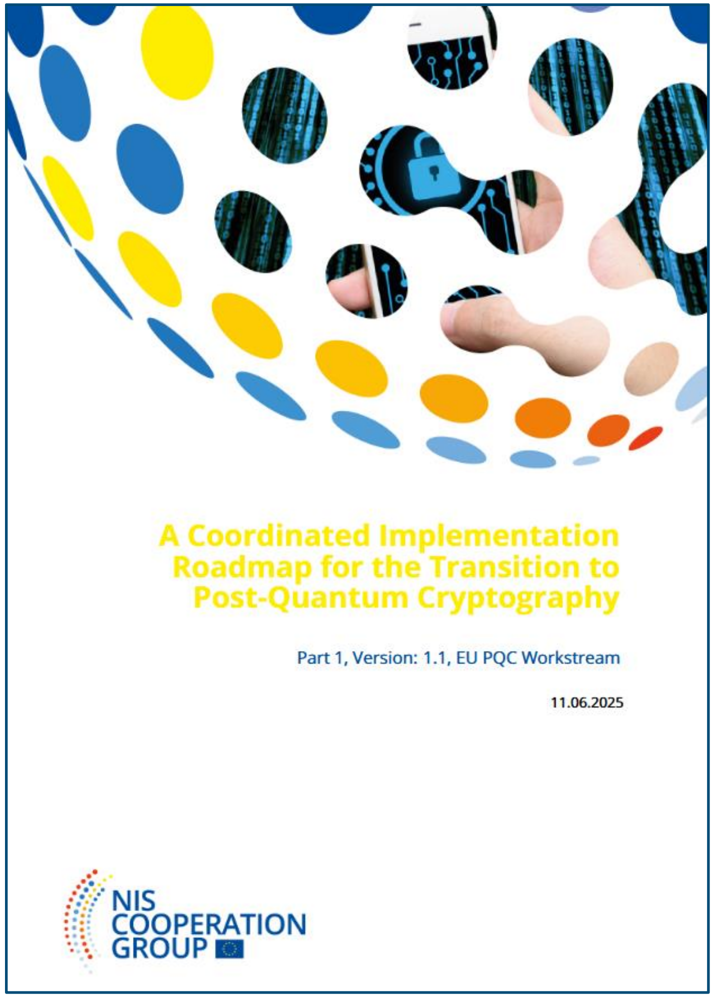
- Target audience: EU member states
- But recommendations are also applicable to different organisations
- Comprehensive proposal to member states to coordinate individual PQC transition strategies
- Contains a rough timeline for the transition



# Timeline

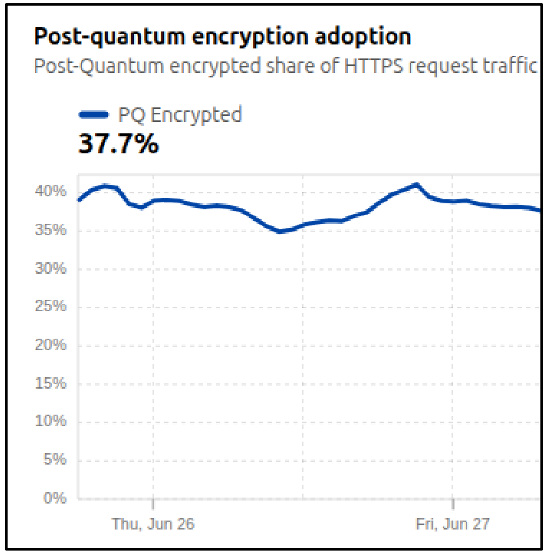
**Timeline for the transition to PQC**

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

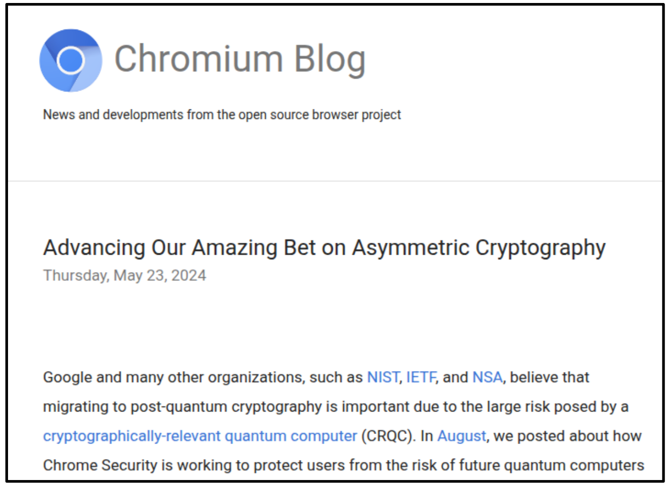


# What do we have and what do we still need?

# You are probably using PQC already




Cloudflare: 37.7% of HTTPS requests are PQC-encrypted



Chromium Blog

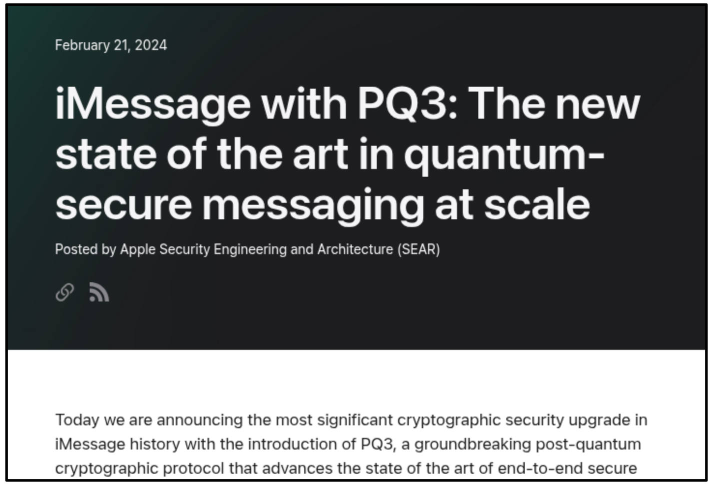
News and developments from the open source browser project

Advancing Our Amazing Bet on Asymmetric Cryptography

Thursday, May 23, 2024

Google and many other organizations, such as NIST, IETF, and NSA, believe that migrating to post-quantum cryptography is important due to the large risk posed by a cryptographically-relevant quantum computer (CRQC). In August, we posted about how Chrome Security is working to protect users from the risk of future quantum computers

Chrome uses TLS 1.3 with ML-KEM768+X25519 for key agreement by default

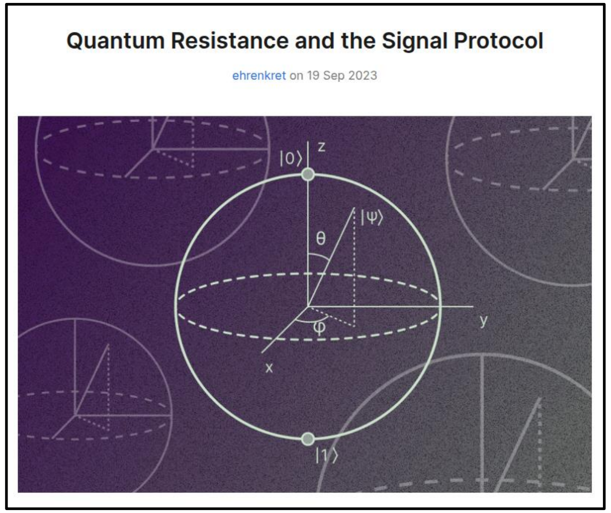


February 21, 2024

iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

Posted by Apple Security Engineering and Architecture (SEAR)

Today we are announcing the most significant cryptographic security upgrade in iMessage history with the introduction of PQ3, a groundbreaking post-quantum cryptographic protocol that advances the state of the art of end-to-end secure



Quantum Resistance and the Signal Protocol

ehrenkret on 19 Sep 2023

# Cryptographic Protocols

- IKEv2: RFC9370 “multiple Key exchanges“ in combination with RFC9242 “Intermediate Exchange“, RFC7383 “Message Fragmentation“ with some  drafts for use of ML-KEM, FrodoKEM, SLH-DSA and ML-DSA
- TLS: Draft “Hybrid key exchange in TLS 1.3“
- TLS Alternative: Draft “KEMTLS/AuthKEM“
- SSH: “PQ/T Hybrid Key Exchange in SSH“, Draft “Module-Lattice Key Exchange in SSH“
- X.509: Drafts at “last call“ for ML-DSA, ML-KEM, SLH-DSA; LMS/XMSS waiting for publication

```
Initiator                                   Responder
------------------------------------------------------------
<-- IKE_SA_INIT (additional key exchanges negotiation) -->

<-- {IKE_INTERMEDIATE (additional key exchange)} -->

                         ...

<-- {IKE_INTERMEDIATE (additional key exchange)} -->

<-- {IKE_AUTH} -->
```

# Cryptographic Libraries

- Botan 3.6.1: further development via BSI-Project supporting ML-KEM, FrodoKEM, Classic McEliece, ML-DSA, XMSS, SPHINCS+
- Liboqs by Open Quantum Safe supporting ML-KEM, FrodoKEM, ML-DAS, HQC, BIKE, SPINCS+, XMSS, LMS, …
- SymCrypt (OpenSource library of Microsoft) supporting ML-KEM, ML-DSA, XMSS, LMS
- AWS LibCrypto (OpenSource library of Amazon) supporting ML-KEM and ML-KEM with ECDHE for TLS 1.3
- OpenSSL 3.5.0 supporting ML-KEM, ML-DSA, SLH-DSA since April 2025

# Devices for classified information in Germany

- SINA L3 Box H
- SINA L3 Workstation H
- SINA Communicator
- ADVA L1 Encryptor
- All the other devices like L3 Gateways for lower classification levels, mobile solutions … Some already in developement, some waiting for: …

Bundesamt für Sicherheit in der Informationstechnik

# Certified Smartcards

- Infineon Smartcard with ML-KEM, ML-DSA to come.
- Chip and hardware vendors are in the developement phase, there are not many Chips supporting post-quantum available yet.
- Implementing an algorithm in a side-channel-resistant manner takes a lot of time and expertise!

# Post-Quantum Cryptography for digital Identities

- Certificate formats to be defined.
- Protocols to be defined, e.g. PQ-PACE
- Digital identities in passports are based on chips!
- The lifetime of a digital identity in this context is long, e.g. 10 years.
- What about EUDI-Wallet?

# Post-Quantum Cryptography for EUDI-Wallet

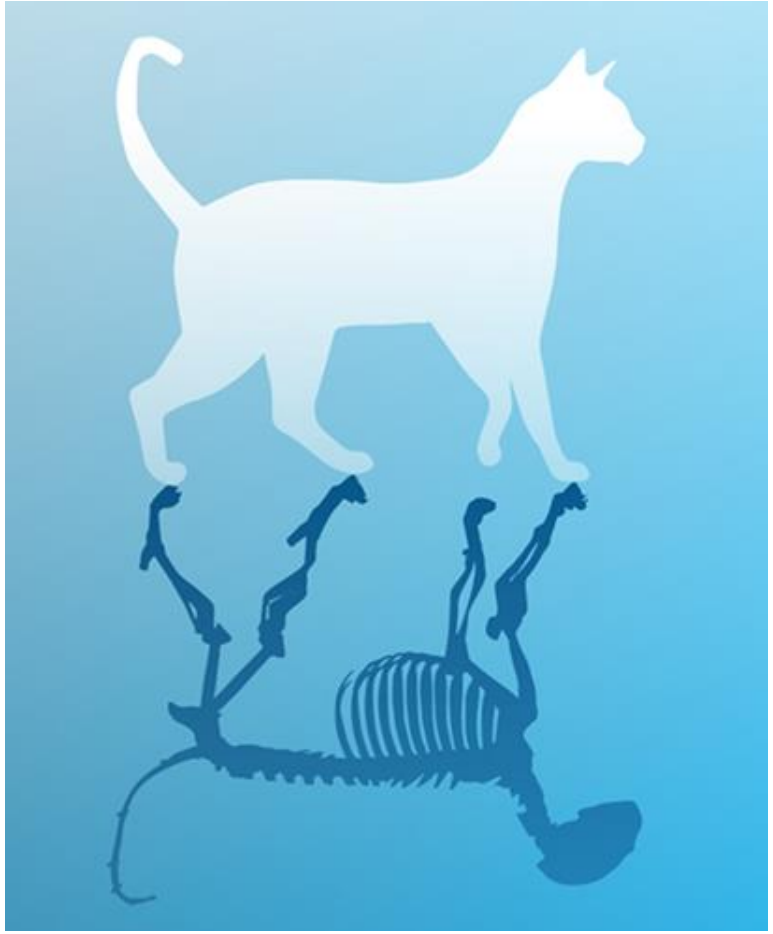
- EUDI-Wallet also should be built upon cryptography implemented in hardware – identities musn‘t be copied!
- Getting access to secure elements in phones is hard, getting them to support new algorithms is even harder.
- The first iteration of the Wallet won‘t have Post-Quantum algorithms implemented and shall be built upon a remote HSM.
- It will be hard to achieve improvements (Anonymous Credentials) considering anonymity and post-quantum at the same time!

EU Digital Identity
Wallet

# Conclusion

- Due to store-now-decrypt-later, the quantum threat is already relevant today.
- The first standards and implementations for post-quantum cryptography are now available.
- PQC should be deployed in hybrid mode.
- Migrating encryption to PQC is more urgent, but migrating signatures may take a long time.
- More specialized applications like anonymous credentials are not ready yet for migration.

Further information: www.bsi.bund.de/Quanten



Bundesamt
für Sicherheit in der
Informationstechnik

Lea Nagler
Referat V 32: Quantum-safe Cryptography and Cryptographic Applications

**Lea.nagler@bsi.bund.de**

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

**www.bsi.bund.de**

Follow us:

# Approaches for Anonymous Credentials

- Approach with classical cryptography: one-time certificates with salted-hashes used as commitments for selective disclosure.

  Issuer unlinkability not possible!

  A lot of keys to be saved and certificates to be signed

- Signatures with efficient protocols: Design the signature in a way that proving possession of a signature to a committed value is “easy“ for issuer unlinkability

  example: BBS(+) (pairing/dlog-based), CL signatures (RSA-based)

  practical approaches not post-quantum yet!

- Classical signatures with general purpose proofs: Use general purpose proof systems to prove possession of a signature to a committed value for issuer unlinkability

  example: ECDSA with Ligero-proof-system

# Example: Migration of the Public Administration PKI (Verwaltungs-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: RSA

Root 10y — Sub-CA 6y — Subscriber 3y

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 eventually replace the existing PKI.
- … different algorithms are currently being considered.

# Position Paper on Quantum Key Distribution

## ANSSI, BSI, NLNCSA, Swedish NCSA

- On a theoretical level, QKD can provide information-theoretic security.
- For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice.
- 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.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office
for Information Security

General Intelligence and
Security Service
Ministry of the Interior and
Kingdom Relations

SWEDISH ARMED FORCES

Position Paper on
Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

This paper is aimed at a general audience. Technical details have therefore been left out to the extent possible. Technical terms that require a definition are printed in italics and are explained in a glossary at the end of the document.

MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

# TAKE A MINUTE AND GIVE US FEEDBACK