Fraunhofer
AISEC

TRANSFER for Our FUTURE

Post-Quantum Cryptography

Migration Tradeoffs and Migration Modelling

Prof. Dr. Daniel Loebenberger, OMNISECURE 2026
Berlin, January 19, 2026

Guidelines on the State of Quantum-safe Cryptography

BSI (December 2021)

- Flexible software designs for new and further developments
- Use of symmetric keys with at least 192 bits
- Use of hybrid cryptographic methods
- Use of hash-based signature methods for software updates
- Migration to quantum-safe PKIs
- Adaptation of cryptographic protocols
- Pre-distribution of symmetric keys or use of QKD
- Conducting applied research projects

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Kryptografie
quantensicher gestalten

Grundlagen, Entwicklungen, Empfehlungen

Guidelines on the State of Quantum-safe Cryptography

BSI (December 2021)

- Flexible software designs for new and further developments
- Use of symmetric keys with at least 192 bits
- Use of hybrid cryptographic methods
- Use of hash-based signature methods for software updates
- Migration to quantum-safe PKIs
- Adaptation of cryptographic protocols
- Pre-distribution of symmetric keys or use of QKD
- Conducting applied research projects

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Kryptografie
quantensicher gestalten

Grundlagen, Entwicklungen, Empfehlungen

cf. Gazdag, S.-L., & Loebenberger, D. (2019). Post-Quantum Software Updates

Guidelines on the State of Quantum-safe Cryptography

BSI (December 2021)

- Flexible software designs for new and further developments
- Use of symmetric keys with at least 192 bits
- Use of hybrid cryptographic methods
- Use of hash-based signature methods for software updates
- Migration to quantum-safe PKIs
- Adaptation of cryptographic protocols
- Pre-distribution of symmetric keys or use of QKD
- Conducting applied research projects

cf. Herzinger, D., Gazdag, S.-L., & Loebenberger, D. (2021). Real-World Quantum-Resistant IPsec
Gazdag, S.-L., Grundner-Culemann, S., Guggemos, T., Heider, T., & Loebenberger, D. (2021). A Formal Analysis of IKEv2s Post-Quantum Extension
Gazdag, S.-L., et al. & Loebenberger, D. (2023). Quantum-resistant MACsec and IPsec for Virtual Private Networks.

Guidelines on the State of Quantum-safe Cryptography

BSI (December 2021)

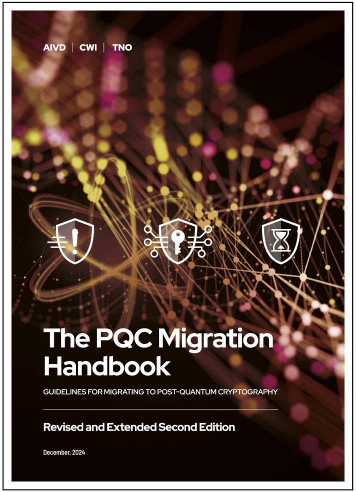
- Flexible software designs for new and further developments
- Use of symmetric keys with at least 192 bits
- Use of hybrid cryptographic methods
- Use of hash-based signature methods for software updates
- Migration to quantum-safe PKIs
- Adaptation of cryptographic protocols
- Pre-distribution of symmetric keys or use of QKD
- Conducting applied research projects

Bundesamt für Sicherheit in der Informationstechnik
Deutschland Digital•Sicher•BSI•
Kryptografie quantensicher gestalten
Grundlagen, Entwicklungen, Empfehlungen

cf. Hemmert, T., Lochter, M., Loebenberger, D. et al. (2021). Quantencomputerresistente Kryptografie: Aktuelle Aktivitäten und Fragestellungen

European Guidelines for Cryptographic Transition

December 2024 / June 2025



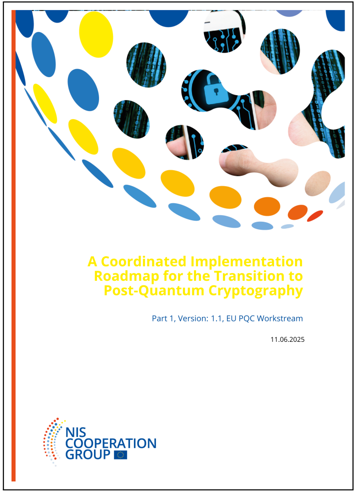
AIVD | CWI | TNO

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

Revised and Extended Second Edition

December, 2024



A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

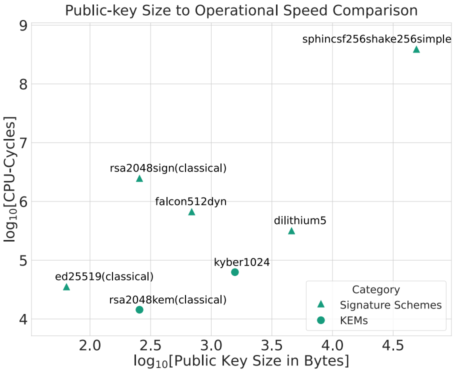
Part 1, Version: 1.1, EU PQC Workstream

11.06.2025

NIS COOPERATION GROUP

Replacement of Cryptographic Algorithms

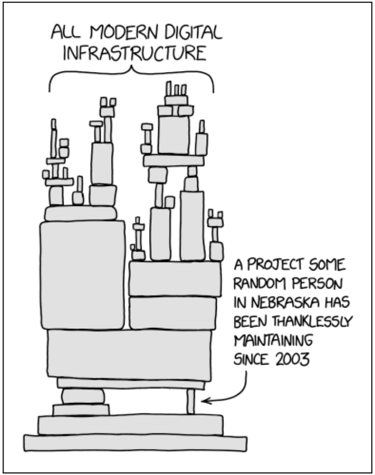
- Identification of affected algorithms
- Examination of the APIs of the crypto libraries
- Analysis of the data formats used
- Determining the calling OS and application code
- Determining the called OS and application code
- Quantitative description of algorithm features
- Identification of algorithmic dependencies
- Assessment of new trade-offs
- Possible impact of hybrid mechanisms



Data: `supercop`

Replacement of the Protocols Themselves

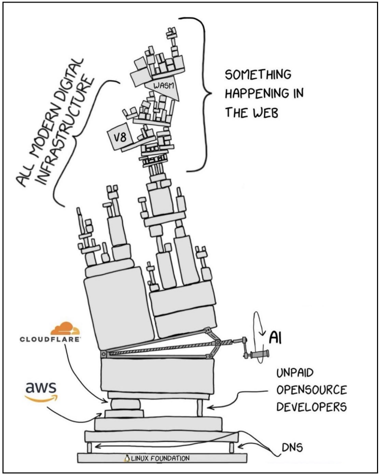
- Negotiation of cryptographic procedures
- Handshake protocols for key exchange
- Invocation of cryptographic procedures
- Current key sizes and hardware/software limits
- Thresholds for latency and throughput
- Sources of keys and certificates
- Possible use of cryptographic hardware
- . . .


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Source: https://xkcd.com/2347/

Replacement of the Protocols Themselves

- Negotiation of cryptographic procedures
- Handshake protocols for key exchange
- Invocation of cryptographic procedures
- Current key sizes and hardware/software limits
- Thresholds for latency and throughput
- Sources of keys and certificates
- Possible use of cryptographic hardware
- . . .


ALL MODERN DIGITAL INFRASTRUCTURE
SOMETHING HAPPENING IN THE WEB
WASM
V8
CLOUDFLARE
AI
aws
UNPAID OPENSOURCE DEVELOPERS
DNS
LINUX FOUNDATION

Source: Modern interpretation by `Equivalent_Site6616`

Remaining Operational Problems

since Ott et al. (2019)

There is no structured approach to cryptographic migration: the approaches for migration are always some kind of (guided) best-practice tasks

cf. Näther, C., Herzinger, D., Gazdag, S.-L., Steghöfer, J.-P., Daum, S., & Loebenberger, D. (2024). Migrating Software Systems Toward Post-Quantum Cryptography
Näther, C., Herzinger, D., Steghöfer, J.-P., Gazdag, S.-L., Hirsch, E., & Loebenberger, D. (2024). SoK: Towards a Common Understanding of Cryptographic Agility

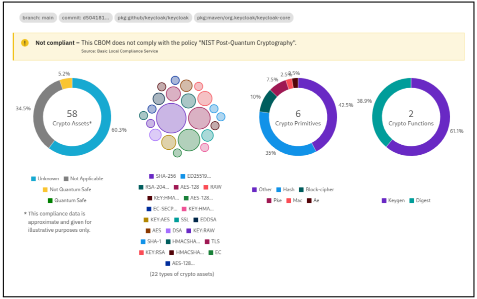
»We build our computers the way we build our cities – over time, without a plan, on top of ruins.«

(Ellen Ullman)

CBOMs to the Rescue

Semi-automated Generation of a Cryptographic Bill of Material

- CBOMs as special cases of SBOMs
- Tooling available, e.g. CycloneDX
- Suitable standardized data-formats (`json`)
- Collection of crypto on systems
- Proper visualization
- Manual assessment still often necessary
- LLMs facilitate analysis of human-readable descriptions of package managers
- However, asset collection in large infrastructures is an unsolved problem!



branch: main | commit: d504181... | pkg:github/keycloak/keycloak | pkg:maven/org.keycloak/keycloak-core

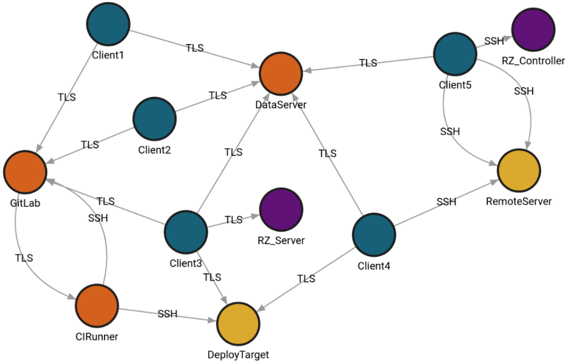
Not compliant – This CBOM does not comply with the policy "NIST Post-Quantum Cryptography".
Source: Basic Local Compliance Service

* This compliance data is approximate and given for illustrative purposes only.

cf. Hirsch, E., Raab, K., Bauer, T. J., & Loebenberger, D. (2025). Detecting Cryptographically Relevant Software Packages with Collaborative LLMs

CBOMs to the Rescue

Semi-automated Generation of a Cryptographic Bill of Material

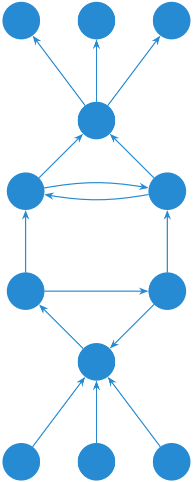


Store topological information from Wireshark / `pcap` in a graph database such as `memgraph`

Formalization of the Migration Problem

Migration Graphs

- Collect all dependencies in a graph
- The graph induces a topological order on the nodes
- Thus it models all possible migration strategies
- Opens the whole toolbox of graph algorithms for cryptographic migration!
    - Structural analyses of dependencies
    - Quantitative measures of migration characteristics
    - Minimization of cost
    - Analysis over time
    - ...
- Work in progress.

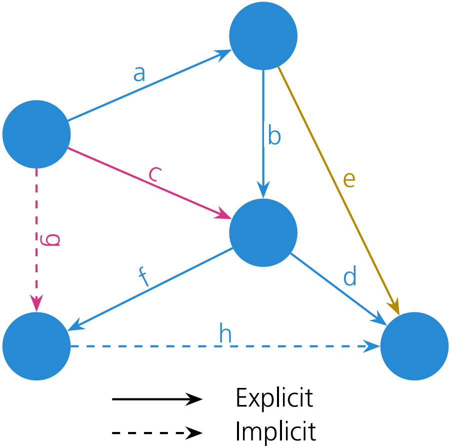


cf. Loebenberger, D., Gazdag, S.-L., Herzinger, D., Hirsch, E., Näther, C., & Steghöfer, J.-P. (2026). On the Formalization of Cryptographic Migration

Formalization of the Migration Problem

Extension: Dependency Graphs with Implicit Dependencies

- How to get the graph from real-world infrastructures?
- Start with explicit dependencies (*a*, *b*, *d*, *f*)
- Successively get rid of irrelevant or redundant dependencies (*c*, *e*, *g*)
- Iteratively add implicit dependencies (*h*)
- Employ a functional predicate to refine the model
- Repeat until model seems complete



cf. Nzetchuen, E., Igler, B., Loebenberger, D., & Stöttinger, M. (2026). Cryptographic Migration with Implicit Dependencies. Work in progress.

Post-Quantum Cryptography Competence Centre

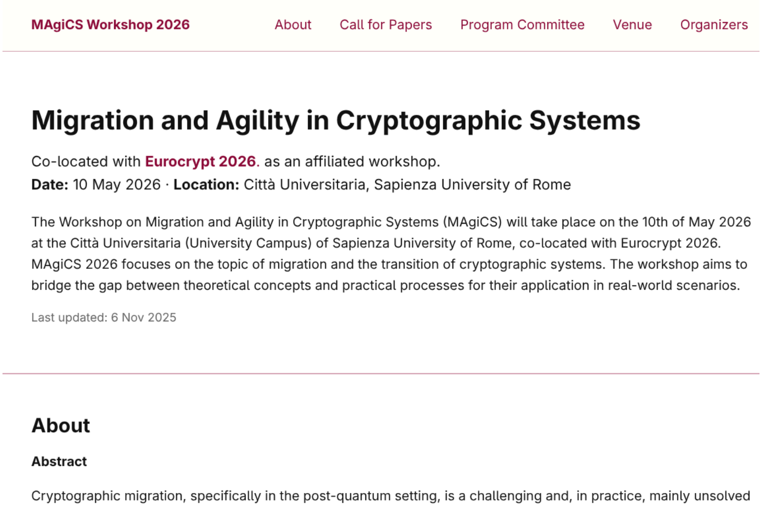
at Fraunhofer AISEC

- Preparation of security analyses
- Vendor-neutral evaluations
- Support for your post-quantum migration
- Initiation and execution of research projects
- PQC event Mai 04/05, 2026: PQC-Update at Fraunhofer AISEC in Garching

Registration via QR code or at `https://s.fhg.de/PQCKompetenz`

PQC Migration Workshop at Eurocrypt 2026 in Rome

Submission: February 01, 2026



Migration and Agility in Cryptographic Systems

Co-located with **Eurocrypt 2026**. as an affiliated workshop.

Date: 10 May 2026 · **Location:** Città Universitaria, Sapienza University of Rome

The Workshop on Migration and Agility in Cryptographic Systems (MAgiCS) will take place on the 10th of May 2026 at the Città Universitaria (University Campus) of Sapienza University of Rome, co-located with Eurocrypt 2026. MAgiCS 2026 focuses on the topic of migration and the transition of cryptographic systems. The workshop aims to bridge the gap between theoretical concepts and practical processes for their application in real-world scenarios.

Last updated: 6 Nov 2025

About

Abstract

Cryptographic migration, specifically in the post-quantum setting, is a challenging and, in practice, mainly unsolved

Contact

Prof. Dr. Daniel Loebenberger
daniel.loebenberger@aisec.fraunhofer.de

Fraunhofer Institute for
Applied and Integrated Security AISEC
Hermann-Brenner-Platz 1
92637 Weiden i.d.Opf.