Lessons from the “Post Quantum Support Action”

Building PQC Awareness and Supporting Migration in Practice

date 03.12.2025
place The Hague
author **Frank Morgner**, Jan Klaußner

Post Quantum Support Action

Supported by the European Union

DIGITAL- ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC call in project 101190512 PQCSA

Key data

TU Eindhoven (NL),
Bundesdruckerei (DE),
CryptoExperts (FR),
KU Leuven (BE),
Trinity College Dublin (IRL)

Project Duration 2025-2027

PQCSA

Project Goals

PQC Standardisation
PQC migration roadmaps
Raise PQC awarenes

How we work

SDOs: ISO/IEC, ICAO, IETF, GP, …
Events with Academia/Industry/…

This talk

Presentation of PQCSA activities.
Post EU Project on building awareness for post quantum cryptography and supporting standardization and adoption of quantum secure solutions.

Experience from PQC workshops.

- Insufficient standardisation
- Missing tools for migration
- Need to strengthen incentives

bundesdruckerei.

01

Our experiences

From Standardisation
and PQCSA events

PQCSA Activities

Standardisation (ongoing)

- ISO/IEC (cryptography, smart cards)
- ICAO (travel documents)
- IETF LAMPS (Hybrids)
- Globalplatform (secure elements)
- CAB Forum, PKI Consortium (PKI Migration)

Planned

- Co-located events with
  - OSS conference
  - SDO for cryptography experts
  - CA day for PKI migration
- **https://pqcsa.eu/events.html**

2025 | 2026 | 2027

Workshops and Events

- PQCSA summer school
- Workshop on migration
- PQC migration for automotive industry

Project Wrap Up

Finalized reports and recommendations

Who of YOU has actively used PQC today?

Everyone uses Post-Quantum-Crypto!

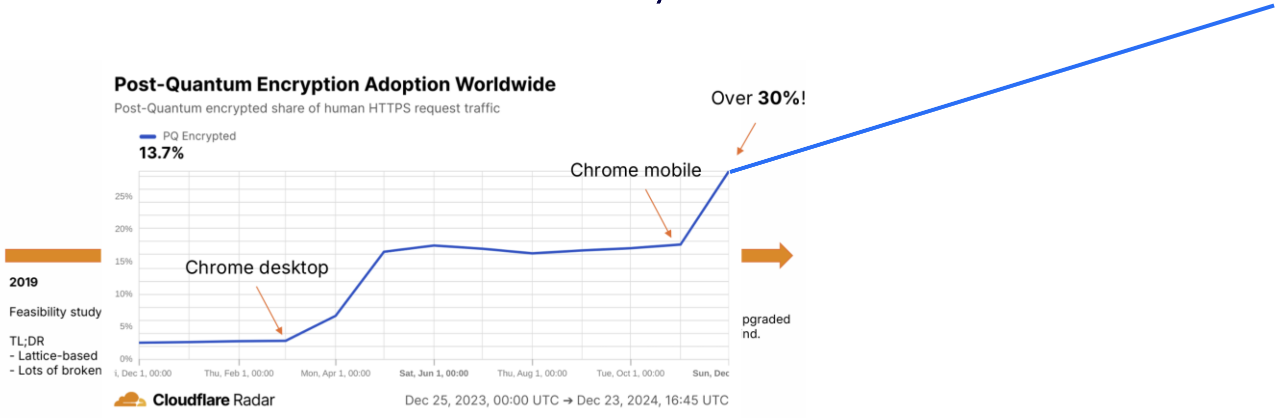
Messengers have adopted PQC

WhatsApp, Signal, iMessage adapted their protocols, apps and servers to use hybrid key exchange with ML-KEM

Big parts of the web adopted PQC

Chrome, Firefox, … use hybrid key exchange with ML-KEM by default. Content Delivery Network Cloudflare serves 20% of the web content and offers hybrid key exchange with ML-KEM

Hybrid PQ Encryption over **50%**
Today 4.12.2025



2025 Valenta: Why the Internet isn't ready for Post-Quantum Certificates

PQC Migration going well?
in most cases not so much…

Heterogeneous systems

Many different stakeholders with varying (performance) constraints and update cycles

Protocol ossification

Despite being designed to be upgradeable, any flexibility that isn't used in practice is probably broken, because of faulty implementations

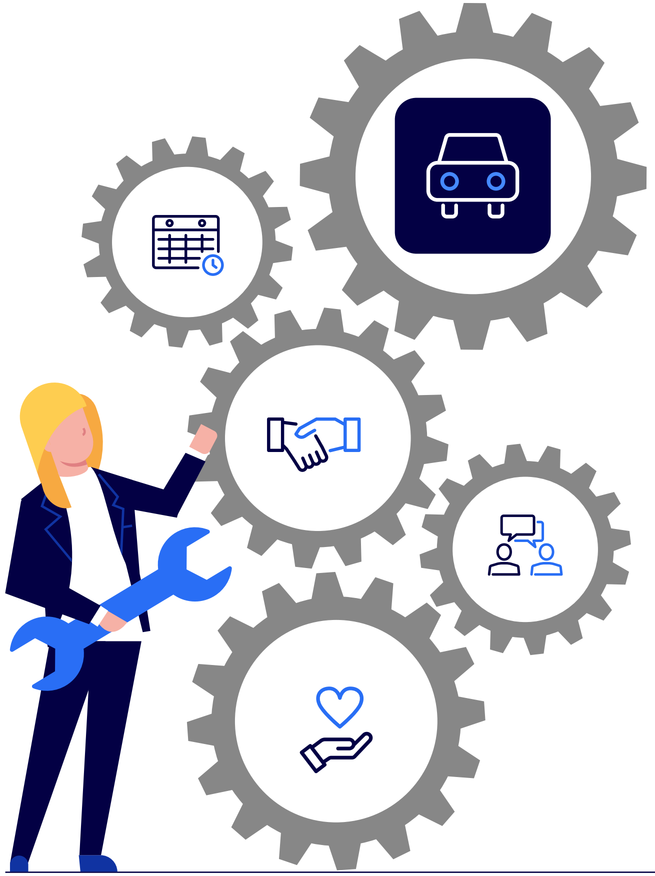
Mixed signals and missing incentives

Massive amount of new work on PQC appears like it is still not ready, even for experts

02

Experiences with Automotive Industry

Automotive and Cryptographic Agility?



Lifetime considerations

- Lifetime of a single car is around 30 years
- New production vehicles are planned around 8 years ahead
- Yet no focus on PQC, due to competing incentives

Heterogeneous systems

- Huge supply chain, well orchestrated, good infrastructure
- 100-300 Microcontroller eligible for software updates
- APIs and standards in Automotive industry lacking PQC capabilities

PQC roadmap relevant, but to what extent?

- CRA relevant for cars, NIS2 relevant for online services
- Unclear whether use cases are “high” or “medium risk”
- No real mandatory requirement for PQC

03

Experience with Identity Documents

PQC Ready ID Card

Press Release

Germany Sets Standards for Secure Identity Documents in the Age of Quantum Computers

- Post-quantum cryptography (PQC): preparatory work completed to make the next generation of the ID card the first in the world to be equipped with chips secured against attacks by quantum computers
- "A decisive step for the future security of digital identities"
- The technical foundation was developed by Bundesdruckerei, Giesecke+Devrient (G+D), the
  Security (BSI) and Infineon, and is currently one of its kind.
- Early implementation of hybrid PQC is crucial since ID cards are valid for ten years

Berlin/Munich, 10 November 2025 – Since its introduction in 2010, it has been regarded as one o
issued documents in the world: the German ID card with its integrated online ID function (eID). T
future, new ID cards must be protected against attacks by quantum computers – this applies to
cards issued in the coming years. These government-issued documents are valid for ten years. O
Bundesdruckerei GmbH and G+D have developed a technical foundation that is so far unique wor
technology company and the international security technology company jointly initiated develop
BSI and implemented it on specialised chips from the semiconductor manufacturer Infineon.

The migration of the German ID card will then take place in two phases: First, the ID data will be
quantum-resistant digital signature scheme. This will be followed by a full transition to quantum-

The feasibility study (proof of concept) is one of the world's first functional implementations of a
cryptography and post-quantum cryptography, in line with current recommendations for quantu
"Bundesdruckerei and G+D are the first in Germany to have demonstrated that highly secure, qu
as encryption and authentication, is possible on ID card chips. This is a decisive step for the futu
Dr Kim Nguyen, Senior Vice President Innovation at Bundesdruckerei.

"The question is no longer whether there will be a future with quantum computers that can break
but when this so-called Q-Day will come. Companies are already testing the use of quantum com
science and drug discovery", says Gabriel von Mitschke-Collande, Member of the Management B
have to act now to protect our digital infrastructure. The transition to quantum-resistant encrypt
necessity. That is why we are very pleased that, together with Bundesdruckerei, we have outlined
innovative potential of quantum computers with the appropriate security technology."

Quantum computing technology has made great progress in many respects in recent years, but
achieved and remains associated with major challenges. Powerful, error-correcting quantum com
mathematical problems, such as computing discrete logarithms or prime factorisations, significa
This capability also has a dark side: quantum computers have the potential to break established
precisely, certain key exchange and digital signature schemes. As a result, they pose an increasin
IT systems and data. In particular, the sensitive personal data in government-issued ID documen
against potential quantum attacks with post-quantum cryptography (PQC). An EU roadmap envis
high-risk use cases by 2030.

"Equipping the ID card chip with post-quantum cryptography is highly relevant, because from 20
quantum computers that can break current cryptographic schemes. By then at the latest, it mus
secure ID cards. We can be proud that Germany is taking a leading role in future-proof protection
emphasises BSI President Claudia Plattner. The BSI researches and documents the state of quan
regularly updated study.

G+D has many years of experience with PQC on hardware security elements through its participa
Research, Technology and Space's funding projects Aquorypt and Quoryptan. A key technological
the ID card chip was meeting the new security requirements while minimising the footprint of the resource-intensive PQC algorithms. With the proof of concept for the quantum-secure ID card, the companies have paved the way to securely integrating PQC schemes into the ID card. The Infineon chips used in the proof of concept offer a new chip design that facilitates fast and side-channel-resistant software implementation of PQC algorithms.

The Bundesdruckerei has also been working on post-quantum cryptography and quantum computing for many years. Together with Infineon and the Fraunhofer Institute for Applied and Integrated Security (AISEC), Bundesdruckerei developed the world's first demonstrator for an electronic passport in 2022 that also meets the high security requirements for the era of quantum computing. Information on Bundesdruckerei's quantum projects can be found here.

G+D has compiled further details on PQC and which cryptographic schemes could be broken by quantum computers here.
Information and recommendations from the BSI on PQC can be found here.

Highlights and Key Facts

- Proof-of-concept implementation targetting side channel resistance
- eID and eMRTD protocols
- Hybrid cryptography for documents and terminals
- Combination of LMS, ML-DSA/ECDSA, ML-KEM/ECDH
- PQC conforming to ISO/IEC 7816 and IETF drafts
- Hybrid performance near classical performance

Challenges

- International standardisation for travel documents (ICAO) is just starting
- Documents have long validity periods
- Heterogeneous infrastructure

https://www.bundesdruckerei.de/de/newsroom/pressemitteilungen/deutschland-setzt-massstaebe-fuer-sichere-ausweisdokumente-im-zeitalter-der-quantencomputer#

Migration in two steps

1. **PQC-Light** – Securing passive authentication
   - Create and verify PQC (hybrid) Signature on ID data
   - Changes to certification and interoperability testing relatively small
   - New document PKI and management systems necessary
   - Potentially huge impact on infrastructure
   - Short term realization possible

2. **PQC-Chip** – Active PQC protocol usage (CA, TA, PACE)
   - Usage of classical cryptography and PQC (also hybrid) for all parties
   - New chip architecture to support quantum secure cryptography
   - Realization can be planned long term

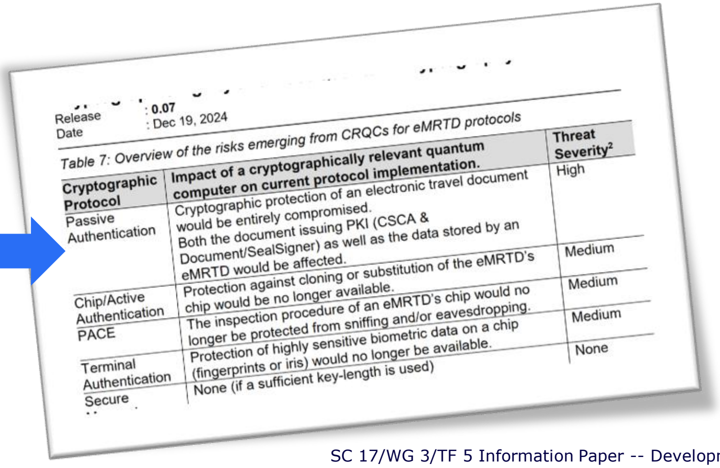

Release : 0.07
Date : Dec 19, 2024

Table 7: Overview of the risks emerging from CRQCs for eMRTD protocols

Cryptographic Protocol	Impact of a cryptographically relevant quantum computer on current protocol implementation.	Threat Severity[2]
Passive Authentication	Cryptographic protection of an electronic travel document would be entirely compromised. Both the document issuing PKI (CSCA & Document/SealSigner) as well as the data stored by an eMRTD would be affected.	High
Chip/Active Authentication	Protection against cloning or substitution of the eMRTD's chip would be no longer available.	Medium
PACE	The inspection procedure of an eMRTD's chip would no longer be protected from sniffing and/or eavesdropping.	Medium
Terminal Authentication	Protection of highly sensitive biometric data on a chip (fingerprints or iris) would no longer be available.	Medium
Secure	None (if a sufficient key-length is used)	None

SC 17/WG 3/TF 5 Information Paper -- Developments regarding Cryptographic Agility and Post Quantum Cryptography for eMRTDs

Conclusion

- PQC awareness is present in many communities
- Intrinsic incentives often too weak for PQC adoption
- Standards and tools applying the new cryptographic building blocks need to be developed

→ **Strengthen incentives to migrate to PQC, e.g. via existing regulation frameworks**
Push standardisation, and tools for interoperability and migration

Contacts

Frank Morgner

Bundesdruckerei GmbH
Innovation
E-Mail: frank.morgner@bdr.de

Jan Klaußner

Bundesdruckerei GmbH
Innovation
E-Mail: jan.klaussner@bdr.de