ETSI/IQC Quantum Safe Cryptography Conference 2026

PQC Ready German ID Card

Presented by:

17/06/2026

01

The Mission

„The sole use of **classic key agreement mechanisms** is only recommended until the **end of 2031** […]. For applications with **very high protection** requirements, the transition […] should already take place by the **end of 2030**. This is according to a joint recommendation by the BSI and European partner authorities […]. “

Federal Office for Information Security (BSI), TR-02102-1 “Cryptographic Mechanisms: Recommendations and Key Lengths”, Version: 2026-01

Challenges

Resource constrained Hardware

- ML-KEM & ML-DSA as only option

10 Year Validity Period

- Solution needed asap
- Immature implementation of new algorithms

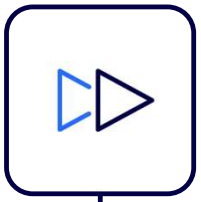
Complex Infrastructure

- Backwards compatible solution

Approach

Hybrid PQC

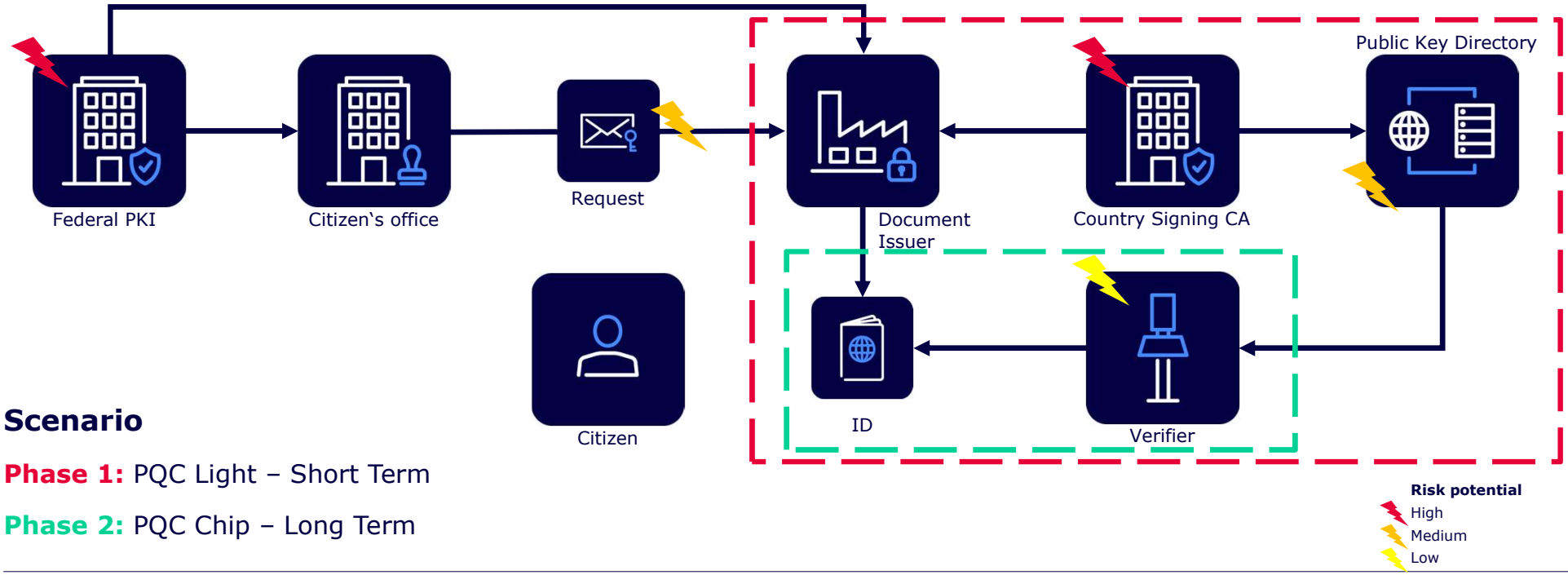
- Required by BSI
- Guardrail against immature algorithm and implementation



Two Step Migration

- PQC Light as quick win
- PQC Chip for complete migration

Possible Migration Scenario



Scenario

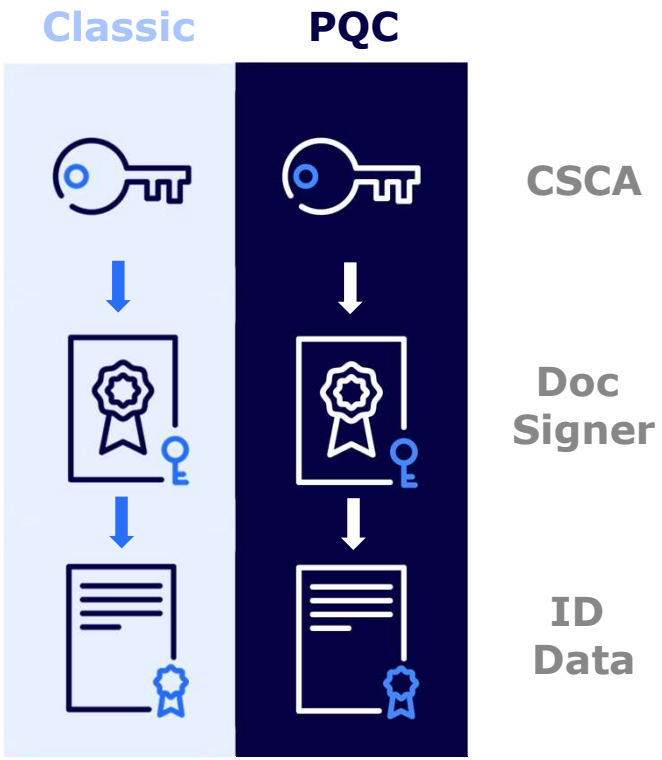
Phase 1: PQC Light – Short Term

Phase 2: PQC Chip – Long Term

PQC Light – Short Term
Prove of Authenticity

Quantum Safe Passive Authentication

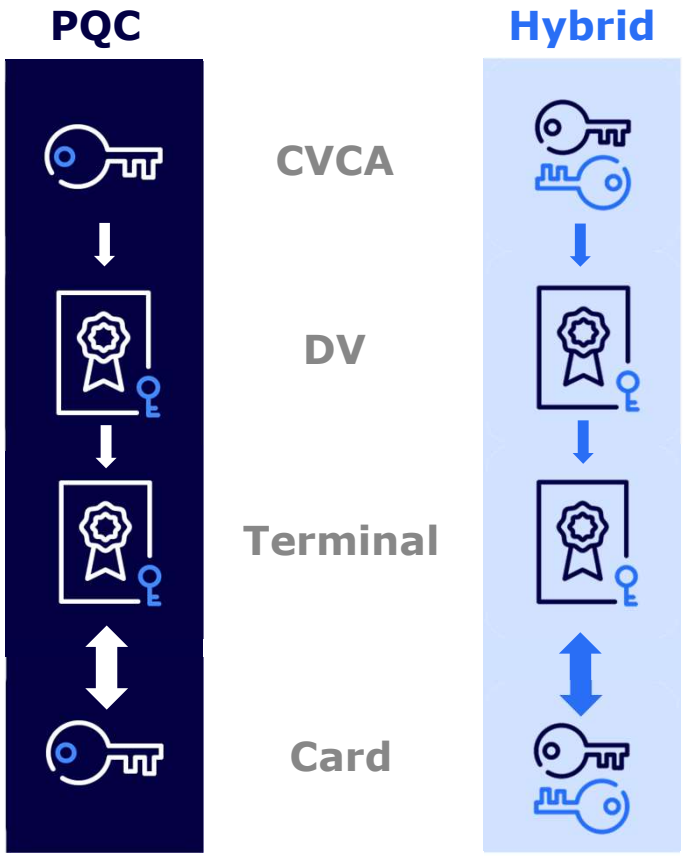
- Simplified: Digital seal over the identity data
- Add copy of identity data with a quantum safe signature
- Needs second PKI with Hybrid PQC
- **Off-Card** verification of the certificate chain and the signature of the CMS
- Ignored by legacy systems
- Algorithms:
  - Classic: ECDSA (Root), ECDSA
  - PQC: LMS (Root), Composite ML-DSA-65+ECDSA-bp256



PQC Chip – Long Term
Building Trust

PACE and Quantum Safe Extended Access Control (EACv1/v2)

- Terminal Authentication and Chip Authentication (EACv1/v2)
- **On-Card** signature verification and key agreement necessary
- **(Hybrid) ML-DSA as drop in** replacement,
  (Hybrid) ML-KEM requires **protocol changes**
- **First** Migration of Reader PKIs (TA) and Backends (CA), **then** ID Card
- Algorithms:
  - PQC: LMS (Root), ML-DSA-65, ML-KEM-768
  - Hybrid: LMS (Root),
    Composite ML-DSA-65+ECDSA-bp256,
    Composite ML-KEM-768+ECDH-bp256



02

The Card

Quantum-Secure Identity Card

Key Facts

- Proof-of-concept for ID card and reader (physical and App) based on production ready components
- Side Channel Resistant implementation of PQC on classic Hardware
- Classic, Hybrid and pure PQC protocols on the same card
- Algorithms: LMS, ML-DSA/ECDSA, ML-KEM/ECDH
- Conforming to ISO/IEC 7816 and IETF drafts
- Protocol performance comparable to classic protocols

Implementation Challenges

1

Missing Standards

- Standardization is currently ongoing or just has started
- Many contradicting drafts
- A lot of changes in the draft documents

2

Limited Resources

- Performance of the smartcard
- Memory availability
- No hardware acceleration for non-hash-based PQC algorithms

3

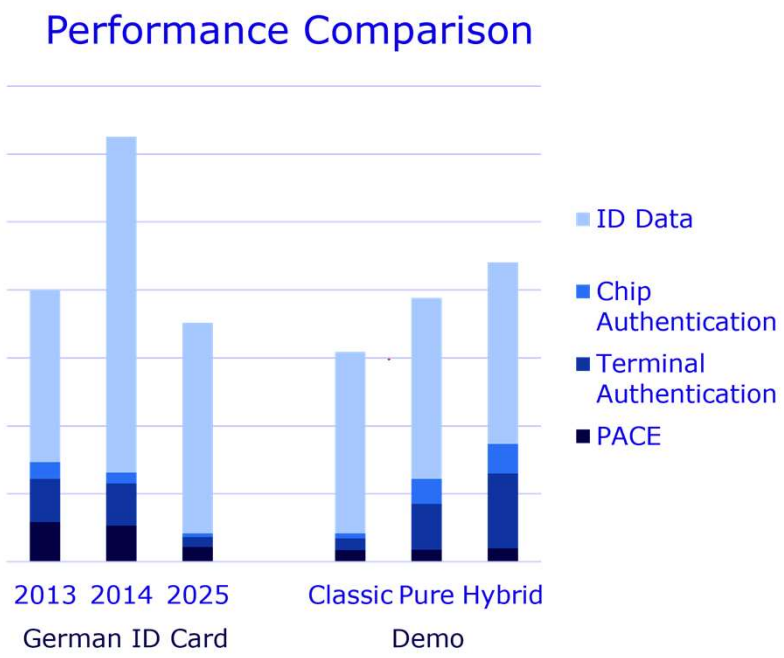
Missing Implementations

- PQC support in Crypto Libs just starting
- New algorithms not fully specified yet
- No support of PQC on current smartcards

Results
Use Case: Border Control

- **Overall performance has improved on classical chips** – new chip generations
- **Pure PQC and Hybrid Demos show similar use case performance** – comparable to older generations
- **Minimum performance requirements are well met** for PQC ID card
- **Reading the ID data heavily dominates** the use case

Pure PQC and Hybrid are well suited for real world ID use cases

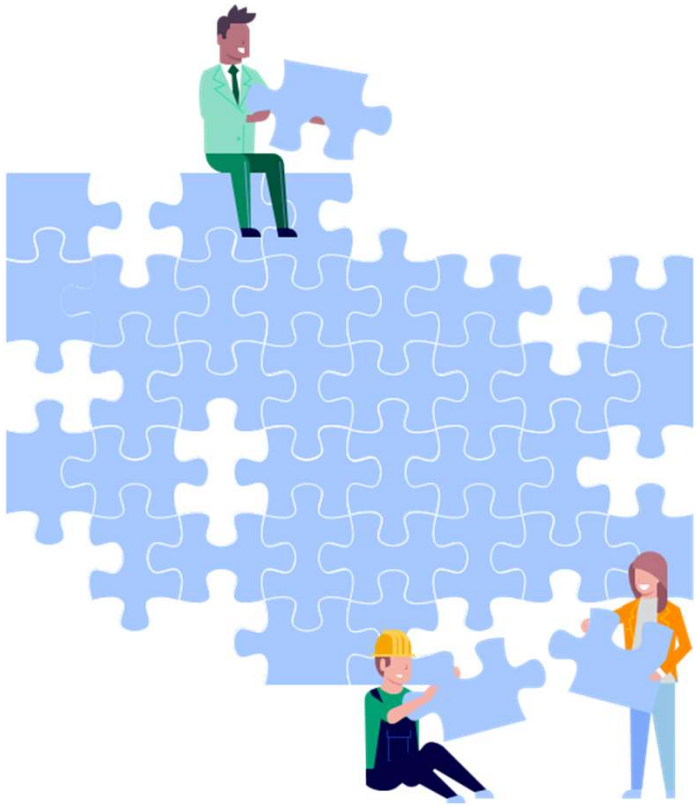



MARKETING
Mission accomplished!

Future Work

- Optimize performance and protocols
- Consider PQC alternatives for PACE
- Evaluate other algorithms and parameter sets for feasibility, e.g. SLH-DSA (reduced)
- Cryptoagility: Definition and handling
- Analyzing the whole eco system and find solutions for the missing parts, e.g. HSMs

Standardization is needed to create solutions



Key Takeaways

- **Hybrid PQC works**
- **Performance** on chip cards is acceptable, even on current state-of-the-art hardware
- **Sector specific** alignment required
- **Divide and migrate** – two-step approach allows early start with small effort

→ **Off to a strong start on the PQC journey**

Thank you.

Jan Klaußner

Bundesdruckerei GmbH
Innovations
email: jan.klaussner@bdr.de

Malte Kruse

Bundesdruckerei GmbH
Technology
email: malte.kruse@bdr.de