

Accelerating the Deployment of Post-Quantum Authentication

11.10.2026
IAB Workshop Prague 2026
Jan Klaußner

Hybrid is the practical deployment path

Preserve certified classical mechanisms and add **quantum-resistant protection** for long-lived data and credentials.



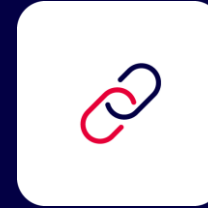
Regulated

Fits high-trust environments such as eID and trust services under European requirements



Reuse what works

Retains PKI structures and operational processes instead of replacing complete protocols.



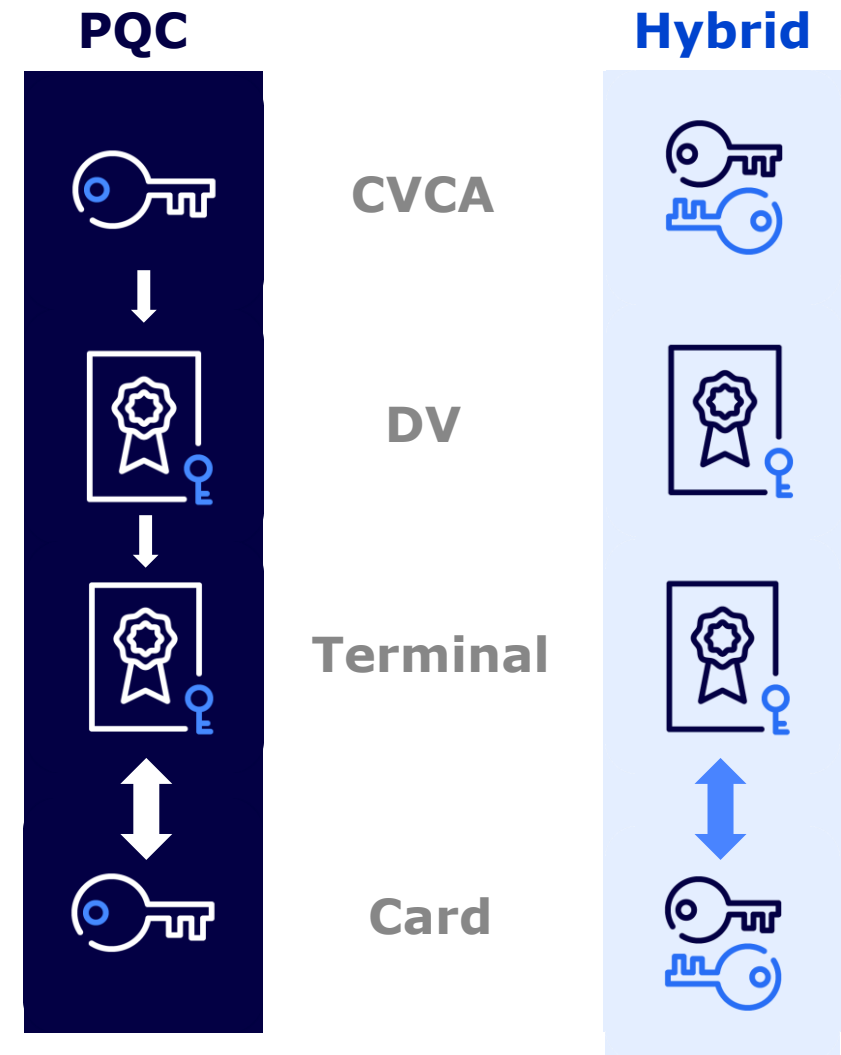
Defense in depth

Two independent cryptographic components improve resilience against implementation failures.

Deployment Evidence - German eID prototype

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



Demo Used with Classic, PQC and Hybrid

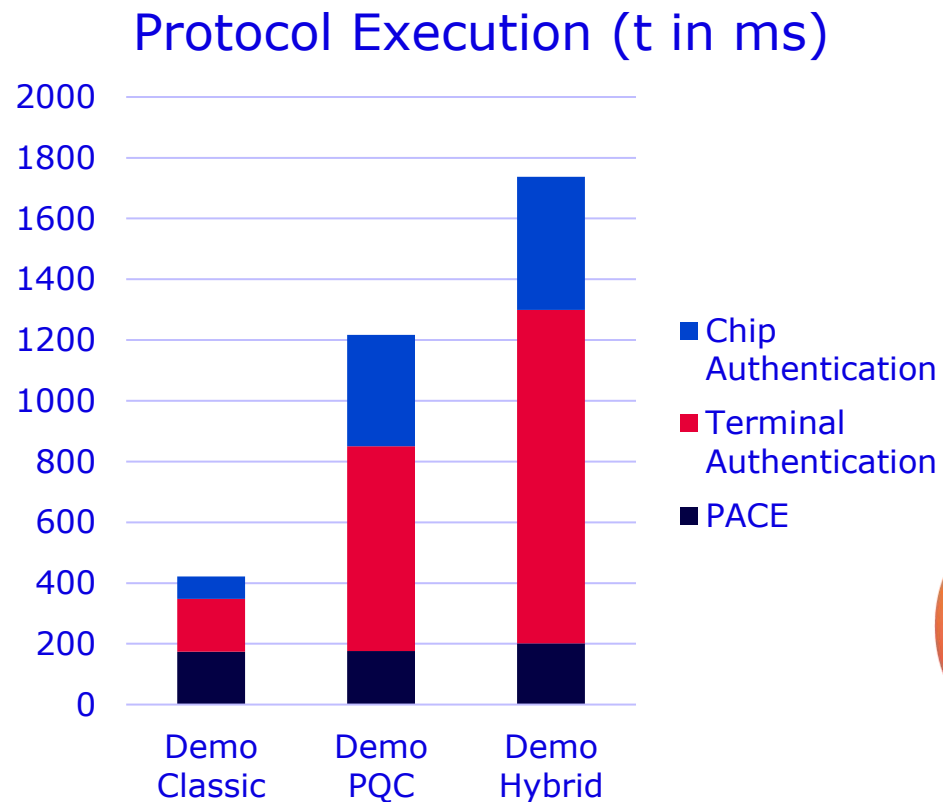
PACE PAKE protocol for verification of MRZ/CAN/PIN: Two executions of ECDH (unchanged)

Terminal Authentication Verification of access rights for accessing sensitive data: Two certificate and one signature verification

Chip Authentication Verification of chip's origin: One key agreement

Input/Output NFC communication included (848 kb/s), terminal overhead excluded

PQC and hybrid are similarly slow

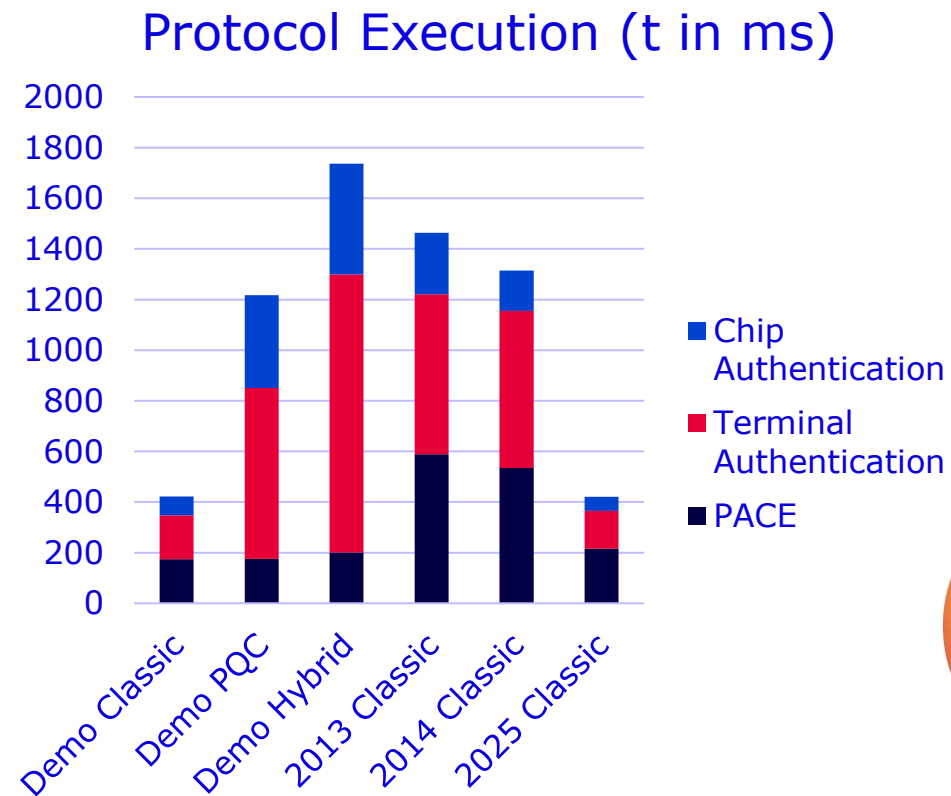


PQC Ready ID Compared with Older Chips

Overall performance has improved
significantly due to new chip generations

Minimum performance requirements are well met for the PQC ID card (and all the other cards tested)

**„PQC“ and „hybrid“ are
as fast as older classical chips**



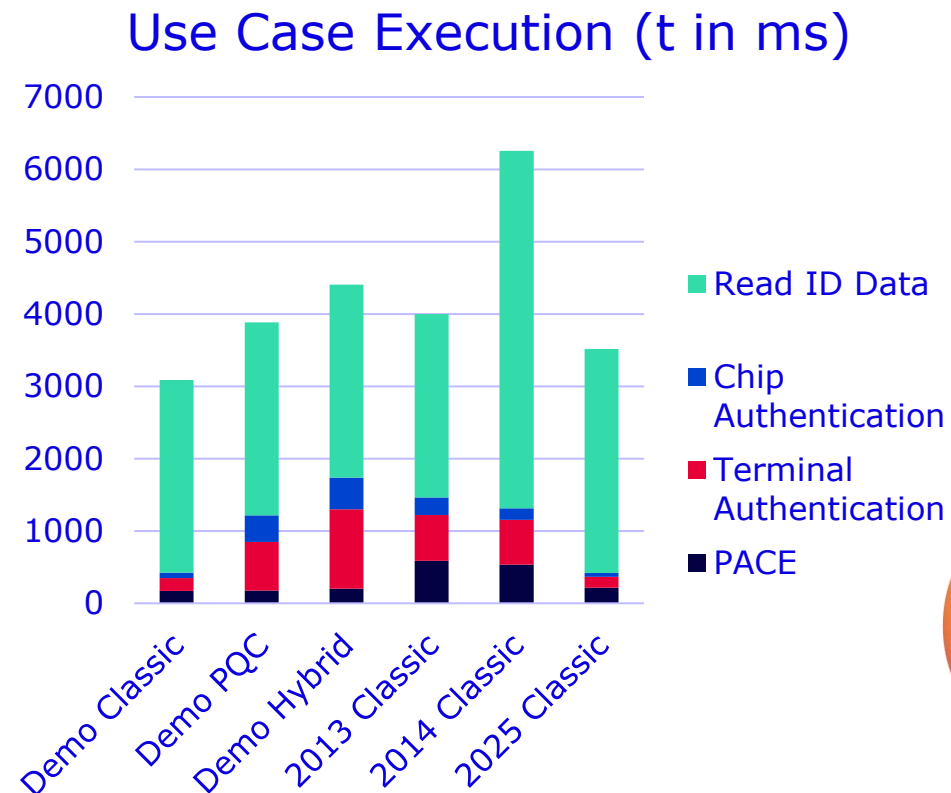
End-to-End Use Case: Border Control

PQC and Hybrid demos show similar use case performance compared to current classical chips and even better compared to some older generations.

Reading the ID data heavily dominates the the border control scenario.

Optimizing input/output operations may have more impact on overall performance than optimizing cryptographic operations.

„PQC“ and „hybrid“ are well suited for real world use



Different readiness, different dependencies

Hybrid authentication

- Near drop-in profile and implementation updates
- Reuses PKI and operations
- Ready first for broad deployment

Deploy

Authenticated KEMs

- Fast on constrained chips
- Can provide repudiation
- Requires protocol changes and hybrid design

Evolve

Merkle Tree Certificates

- Efficient PQ authentication with transparency
- Cosigner and monitor creates governance and liability questions
- diverts resources from PQC migration

Decide

Coordinate Migration - or slow it down

3 Tracks

1

Deploy hybrids first

Use near drop-in enhancements to secure existing authentication paths quickly.

2

Advance AuthKEMs and MTCs

Continue standards, protocol, governance, and infrastructure work in parallel.

3

Avoid competing authentication frameworks

Decide whether on MTCs or not for all WebPKI and others to avoid fragmenting scarce engineering and operational resources.

Thank you.

Jan Klaubner

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

Please note: This presentation is the property of D-Trust.
All of the information contained herein may not be copied, distributed or published,
as a whole or in part, without the approval of D-Trust.
© 2026 by D-Trust