

Position Paper - Accelerating the Deployment of Post-Quantum Authentication

Author: Jan Klaußner, D-Trust (Bundesdruckerei Group)

Submission Date: 4th September 2026

IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication (pqws)

Hybrid PQ/T Authentication

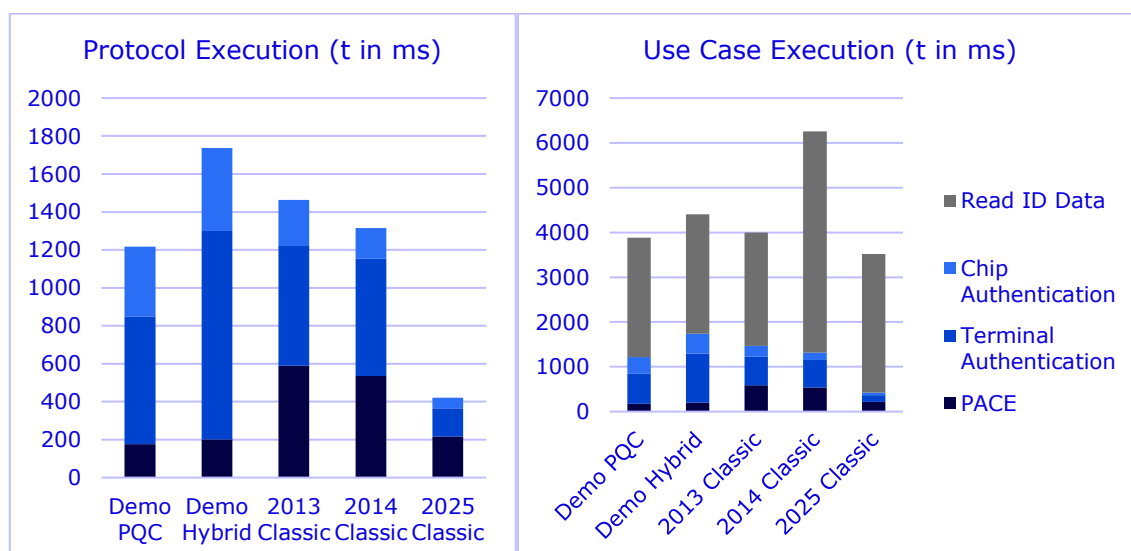
Hybrid authentication lets regulated infrastructures keep certified classical mechanisms while adding quantum-resistant protection for long-lived data and credentials.

European authorities recommend or expect hybrid mechanisms for key establishment and signatures in high-trust environments, including eID and trust services. For German TSPs and ID card providers under eIDAS, hybrid PQ/T authentication is therefore the practical way to meet current quantum-security expectations.

Bundesdruckerei and D-Trust participate in national and European projects on hybrid-capable PKIs and protocols, including PoQuID (quantum-secure passports and IDs), FLOQI (Post-Quantum PKI) and QSPECTRE (Quantum Safe PQC Signatures and PKIs for TSPs). PoQuID results included research to application-level key combiner published as PQ-EAC paper (<https://eprint.iacr.org/2023/352>).

Deployment evidence: German ID card and PoC CA

In joint application-level+Devrient, BSI, Infineon and Fraunhofer AISEC, Bundesdruckerei has demonstrated ID card and passport prototypes that employ Composite KEM and Composite Signatures in a complete end-to-end authentication within typical online-ID timing requirements.



As can be seen in the figures from our tests, while the Hybrid prototype (Demo Hybrid) is much slower than a current ID card (2025 Classic), the difference to a 2014 ID card is much smaller. When ID Data Transfer is considered, the performance overhead is negligible.

The prototypes run on existing certified hardware with accelerators for classical cryptography – for implementing PQ/T only a simple combiner needs to be added in terms of complexity compared

with pure PQC usage on that hardware. Compared with the original design from 2023, we have now switched to support Composite KEMs and Composite Signatures rather than a hybrid approach on the application level, to allow better modularization and reusability of the protocol's building blocks and harmonized certification processes across different use cases.

Why hybrids are our immediate and long-term choice

Hybrids provide quantum-secure authentication in critical infrastructures while reusing PKI structures and operational processes. They can be integrated as profile and implementation updates rather than full protocol replacements, accelerating deployment.

We consider hybrids a lasting concept, not only a temporary bridge. Algorithm implementation complexity is growing as well as the importance of its use. Having two independent cryptographic components in the authentication path increases resilience against such failures providing an effective way for implementing security in depth.

We see a need for more flexible hybrids like Intelligently Composed Algorithms (<https://eprint.iacr.org/2021/813.pdf>) to support gradual migration where different components can move to another algorithm at different speeds while staying interoperable.

Authenticated KEMs

Authenticated KEMs are already used as PQ/T hybrid in the German ID Card PQC, providing hybrid authenticated key establishment on constrained chips. We observed that KEM-based authentication is significantly faster than authentication with a signed nonce. Additionally, the KEM-based authentication provides repudiability, which is a desired feature in some use cases of eID.

We support further work on AuthKEMs in IETF and related forums, especially when available as generic protocol that can be aligned with other protocols such as EAC and eIDAS trust-service profiles. AuthKEMs, however, require protocol changes in deployed systems and must therefore be designed with migration and hybrid coexistence as explicit goals.

Merkle Tree Certificates

MTCs are an attractive approach for WebPKI and, with adaptations, for private PKIs and ID ecosystems, because they tightly couple issuance with transparency and scale post-quantum authentication efficiently. At the same time, the cosigner role introduces a new trust relationship — for example between CAs and external cosigners — that must be established and governed, including liability and audit aspects.

A rapid WebPKI shift to MTCs could also reduce investment and expertise around classical X.509 PKIs, risking ossification of the components still needed for hybrids and mixed chains in regulated infrastructures. MTC deployment should therefore be planned so that classical PKI capabilities remain robust during the transition.

Summary

Hybrids, AuthKEMs and MTCs are all valid paths. Hybrids are ready first as near drop-in enhancements for many existing authentication paths. Authenticated KEMs need protocol changes, and MTCs need both new protocols and new log and cosigner infrastructures.

Work on AuthKEMs and MTCs should proceed in lockstep with hybrid deployment and with coordinated migration plans. Otherwise, parallel ecosystems will compete for the same engineering and operational resources, and overall post-quantum authentication deployment will slow down instead of accelerating.