

IAB PQWS · PRAGUE · 11-12 OCTOBER 2026

Post-Quantum Authentication in Enterprise and Mobile Networks

Tirumaleswar Reddy.K

Nokia

Hannes Tschofenig

University of the Bundeswehr Munich

THE CORE CLAIM

Migration follows a long, sequential critical path



Step 5 must match step 1: operator CAs must support the PQ algorithm the device module supports

Migration cannot complete faster than the slowest step.

The dominant barriers sit outside the authentication protocols: hardware, product cycles, certification, PKI dependencies, cross-organisation coordination.

CONTEXT

These networks are not the Web

	Web PKI	Enterprise and mobile
Relying parties	Updated in days or weeks	Deployed for 5 to 15 years
Trust anchors	Managed and updated by the browser	Installed at manufacture
Issuance	ACME, short lifetimes	CMP, EST; long lifetimes
Transport	TCP or QUIC recovers loss	IKEv2, EAP: loss restarts the exchange
Key storage	Server keys only, in secure elements such as HSMs	Device keys in secure elements sized for RSA and ECC
Disabling old algorithms	Central, by browser vendors	Every dependent device upgraded or retired

OBSERVATION 1

Two gates no protocol change can remove

Manufacturing gate

- Algorithm fixed on the production line
- IDevID (802.1AR) or 3GPP vendor certificate bootstraps the operator identity
- Upgrading the operator PKI does not change it
- Service life of 10 to 15 years

Trust-anchor gate

- To authenticate the device, the operator enrolment server needs the PQ manufacturer CA as a trust anchor
- The device learns the operator CA from a manufacturer-signed message, for example a BRSKI voucher; the device must be able to verify a PQ manufacturer signature
- If either side switches to PQ before the other trusts it, enrolment fails
- Some IoT devices cannot update anchors at all

OBSERVATION 2

Some limits are firmware, some silicon

FIXABLE OVER TIME

Algorithm support

- TPM 2.0 v1.85 adds ML-KEM and ML-DSA, not SLH-DSA
- Some TPMs ship with PQ; others can add it by firmware update
- Each new PQ algorithm needs a TPM spec revision, firmware release and recertification

FIXED AT DESIGN

Hardware resources

- ML-DSA signing needs far more memory than verification
- Secure elements and light HSMs sized for RSA and ECC
- Firmware cannot add memory or compute

Mobile Networks. SIM-based devices authenticate with symmetric keys: they need PQ verification for firmware and PQ key exchange for forward secrecy, not PQ signing.

OBSERVATION 3, CONTINUED

Firmware signing

Why it differs

- Composite ML-DSA is not SUF-CMA against quantum adversaries; the specification advises against it where that is required
- Firmware signatures must stay valid for the device lifetime

Hash-based options

- HSS/LMS, XMSS: fast verification, moderate size, state management required
- SLH-DSA: stateless, larger and slower
- SP 800-230 draft: further SLH-DSA parameter sets

Composite for authentication does not remove the need for a separate PQ signing hierarchy and trust anchor.

OBSERVATION 4

Large credentials cause failures, not just latency

IKEv2 message with a PQ certificate chain, fragmented per RFC 7383



No selective retransmission. The whole message is resent after the timer expires. More fragments, more chance the exchange stalls or fails.

Web

TCP or QUIC recovers a single lost packet.
Size costs latency.

EAP

RFC 9191: practical limits on certificate
data EAP can carry.

Ongoing work

IPSECME reliable transport; EMU PQ
enhancements to EAP-TLS.

OBSERVATION 4, CONTINUED

Merkle Tree Certificates merit evaluation here

landmark-relative MTC replaces the CA signature in the end-entity certificate. Standardised in PLANTS; private PKI use cases are being explored.

Helps most

TLS, IKEv2, EAP: credentials sent during authentication.

Example: Merkle Tree Certificates in IKEv2

Helps little

Firmware signing: kilobytes beside a multi-megabyte artefact.

OBSERVATION 5

The security benefit arrives only when the traditional path is retired

While it is accepted, an attacker can downgrade to it.

Web PKI

Browsers can disable it centrally, but only after the long tail of servers deploys PQ credentials.

Meanwhile, HSTS-like pinning blocks downgrade per server. Example: PQC Continuity (TLS)

Enterprise and mobile

The operator sets policy, but its long tail is devices that may need replacing, not just updating.

Migration guidance should cover

- 1 Hardware, PKI and certification, not just protocols
- 2 Manufacturer credentials and trust anchors
- 3 Signing and verification capability, per module
- 4 Smaller PQ credentials
- 5 Completion means the traditional path is retired