Migrating Time- and Security-Critical PKIs to PQC: SWIM & C-ITS

Authors: Anni Karinsalo, Sara Nikula, Sami Lehtonen

Constraint-driven PQC feasibility

For critical PKIs, PQC feasibility is dominated less by isolated crypto-operation timings than by system effects: certificate size, chain depth, fragmentation, algorithm negotiation, and validation sequencing.

SWIM and C-ITS expose this differently. In SWIM, predictable session establishment and trust-path validation matter at least as much as raw primitive speed. In C-ITS, short communication windows mean extra authentication bytes directly consume channel budget that safety messages would otherwise use.

The practical question is therefore not “Which PQ signature is fastest?” but “Which certificate/profile/transport combination still fits inside the operational time budget?”

System constraints

SWIM

- Predictable sestablishment and trust-path validation are central.
- PQC stress first appears in certificate session /profile growth and transport overhead.

C-ITS

- Short radio windows make every extra authentication byte compete with useful safety payload.
- Pseudonym-certificate carriage and channel capacity dominate before verification latency does.

Algorithm benchmarks are necessary, but certificate handling, chain depth, and transition design decide feasibility.

Migration failure points differ by ecosystem, but certificate handling, transport overhead, and hybrid complexity dominate both.

Migration recommendations

Design for crypto-agility at certificate/profile level first; one-shot algorithm substitution is rarely realistic in safety-critical ecosystems.
Minimise chain depth and avoid protocol patterns that repeatedly resend bulky certificates or require ambiguous fallback behavior.
Treat hybrid as a temporary, tightly policy-constrained phase. If negotiation can silently degrade security under load, the migration design is not finished.

Case study: SWIM and C-ITS

SWIM: X.509-based trust with EACP-style certificate handling; chain validation and interoperability are central constraints.
C-ITS: ETSI/IEEE certificate formats and authenticated V2X messaging; certificate carriage and mobility compress the available validation window.
Shared migration issue: long system lifetimes make prolonged classical+PQC coexistence unavoidable even when standards prefer rapid replacement.

Size inflation spans orders of magnitude while verification remains comparatively manageable. For cert-heavy V2X, payload growth is the dominant bottleneck.

Indicative benchmark view

ECDSA	338 B | ~0.078 ms verification
HAWK	935 B | ~0.064 ms
Falcon	1.8 kB | ~0.036 ms
MAYO	2.1 kB | ~0.091 ms
SPHINCS+ (FIPS 205)	8.1 kB | ~1.5 ms
CROSS	13.2 kB | ~0.422 ms

DENM-style authenticated message sizes from the paper show why channel capacity, not primitive speed alone, drives PQC suitability in V2X.

Benchmark implications

Verification cost alone does not eliminate lattice signatures; message and certificate growth is usually the harder system-level limit.
In the paper’s DENM-style construction, authenticated message length moves from about 338 B with ECDSA to about 935 B (HAWK), 1.8 kB (Falcon), 8.1 kB (SPHINCS+), and more than 13 kB (CROSS). Those bytes matter more than microseconds when links are short-lived or heavily shared.
Hybrid deployments multiply state: dual trust hierarchies, algorithm negotiation, fallback logic, extra testing, and more complex failure handling.

Conclusion

- **Critical PKI migration is a protocol-and-operations problem, not only an algorithm-selection problem.**
- **Compact signatures and short chains are strategically preferable, but migration readiness is decided by certificate profiles, transport behavior, and downgrade-resistant hybrid policies.**
- **Near-term recommendation: benchmark end-to-end on target hardware and traffic models before committing to certificate formats or migration sequencing.**

www.vttresearch.com

Contact: Anni Karinsalo, Senior Scientist
Tel. +358 40 761 5082, anni.karinsalo@vtt.fi

www.pqc.fi

† Falcon: selected by NIST; FN-DSA standardization (FIPS 206) in progress. * HAWK, MAYO, CROSS: NIST “additional signature schemes” Round-2 candidates (not standardized yet).