

Lessons from a Decade of Post-Quantum Authentication

Masoud Asadi, Ehsan Ghasemi, Mohsin Kahn, Ferhat Karakoç,
Anna Kåhre, Andreas Ljunggren, Santeri Paavolainen, John Preuß Mattsson,
Göran Selander, Sini Ruohomaa, Erik Thormarker, Juha Sääskilahti

Ericsson

October 12, 2026

Ericsson's PQC Migration Journey



- Ericsson started its post-quantum cryptography (PQC) migration project in 2015, shortly after the US government announced plans to transition to quantum-resistant algorithms.
- From the outset, authentication has been a major focus, with the goal of protecting Ericsson's products across hardware, software, and PKI.
- Achieving this requires standardized, trusted solutions that can be deployed globally and meet regulatory and compliance requirements.
- This position paper shares lessons learned over the past decade, outlines Ericsson's current migration plans.
- Full position paper: <https://www.ietf.org/slides/slides-pqws-s45-00.pdf>

Lessons Learned from PQC Authentication



- **Avoid stateful signatures.** XMSS and LMS require secure state management for every signature. NIST SP 800-208 prohibits private-key backups due to the risks they pose to state management. Given the resulting security and business continuity risks of state mismanagement and key loss, Ericsson product roadmaps forbid XMSS and LMS. Focus on FIPS 204, FIPS 205 and SP 800-230.
- **Private-key formats and seed-only representations.** Already in 2016, we concluded that seeds should be the canonical private-key format. Unfortunately, ML-DSA libraries support different formats, causing unnecessary complexity and interoperability problems. We encourage SDOs to mandate a single, seed-only private-key format in future standards.
- **Prefer SHA-3 over SHA-2.** SHA-2 is significantly more complex to use securely and have contributed to practical vulnerabilities, including side-channel vulnerabilities. Recent SPHINCS+ vulnerabilities demonstrate that even cryptography experts can make security-critical theoretical mistakes when using SHA-2. Section 11 of FIPS 205 illustrates this complexity. Use SHA-3 and (Turbo)SHAKE in all future systems following ML-DSA, ML-KEM, FN-DSA, HQC-KEM, etc.

Lessons Learned from PQC Authentication



- **Avoid floating-point.** Floating-point arithmetic is poorly suited to constrained environments and complicates cross-platform implementations. Recent work on Falcon's sensitivity to floating-point errors and high-performance fixed-point implementations reinforce our view that FN-DSA should eliminate floating-point arithmetic, as NIST now plans.
- **Prefer hedged signatures.** Following Ericsson's suggestions, NIST made hedged signing the ML-DSA default and plans to do the same for FN-DSA. Hedged signing combines fresh randomness to mitigate side-channel and fault-injection attacks with a deterministic component that protects against weak or compromised random-number generators.
- **Security Levels 1 and 2 are secure.** The idea that symmetric cryptography will be practically affected by CRQCs is a misconception. Quantum algorithms do not provide a practical quantum advantage against modern symmetric cryptography. The focus on upgrading symmetric cryptography is distracting from the urgent PQC migration. SLH-DSA level 1 is a good choice for constrained IoT.

Lessons Learned from PQC Authentication



- **NSA was right about the implementation risks of hybrid signatures.** Despite their simplicity, Ericsson has encountered two supplier implementations of non-composite hybrid signatures that fail to require both component signatures to be valid, confirming NSA warnings. Ericsson's own implementation behaves correctly.
- **SLH-DSA (and ML-DSA) performance is adequate.** SLH-DSA meets our telecom authentication needs across TLS, DTLS, QUIC, IKEv2, and SSH. We strongly prefer modest performance costs over hybrid-signature complexity; ML-DSA clearly meets our requirements. MTCs introduce substantial complexity to PKI and should be considered only if conventional ML-DSA certificates prove too slow.
- **Long transition periods demand early action.** PKIs and long-lived devices require lengthy transition periods, as recognized by the EU roadmap and CNSA. Deployed roots of trust are difficult to replace and often never updated. Long-term authentication keys and roots of trust are valuable targets and will likely be prioritized by attackers. Protecting systems over coming decades requires starting these transitions now.

Be careful with composite signatures



- **Shifts complexity to the PKI.** Composite signatures move complexity from protocols to the PKI, a poor trade-off that creates a combinatorial explosion.
- **Low maturity.** Standardization and implementation are years behind SLH-DSA and ML-DSA.
- **Reduced security.** Poorly designed composites introduce malleability vulnerabilities and destroy ML-DSA's beyond-unforgeability (BUFF) properties. Malleability and the lack of BUFF have caused many practical vulnerabilities.
- **Use-case restrictions are insufficient.** Public keys and certificates used in TLS and SSH have routinely been reused for other purposes. Developers cannot be expected to know when strong unforgeability (SUF-CMA) and BUFF are required.
- **Regulatory uncertainty.** Weak composites do not even qualify as hybrids under European definitions. Their global acceptance, and whether any composites will remain permitted after the traditional component is deprecated, remains unclear.
- **Prefer non-composite signatures.** They avoid creating new algorithms and allow the quantum-vulnerable component to be removed easily.
- **Ericsson guidelines prohibit composites that significantly weaken ML-DSA and all composites for long-term roots of trust.**

ML-DSA and SLH-DSA are the only mature options



- For systems subject to 2030 and 2031 migration deadlines, only ML-DSA and SLH-DSA are sufficiently mature for deployment, including non-composite hybrid authentication.
- FN-DSA and SQIsign should, for these use cases migrating around 2030, be regarded as potential future optimizations.
- At least nine interoperable TLS implementations support ML-DSA authentication, and at least four support SLH-DSA.

Table 1. *CipherSnake PQC capability test results as of 27 August 2026. CipherSnake is an internal Ericsson test suite for evaluating TLS 1.3 libraries, including interoperability and support for PQC key exchange, PKI, and authentication. Libraries are scored based on standard compliance and support for ML-DSA, SLH-DSA-SHAKE, X25519MLKEM768 (*), and MLKEM1024 (**). Some libraries were tested using pre-release versions (†).*

	Library	ML-DSA (PKI)	ML-DSA (auth)	SLH-DSA (PKI)	SLH-DSA (auth)	ML-KEM hybrid*	ML-KEM standalone**
★★★★	bouncycastle:1.85	✓	✓	✓	✓	✓	✓
★★★★	erlang-otp:29.0.4	✓	✓	✓	✓	✓	✓
★★★★	openssl:pre-4.1.0- fd2e286†	✓	✓	✓	✓	✓	✓
★★★★	wolfssl:pre-5.9.3-1e5216e†	✓	✓	✓	✓	✓	✓
★★★★	openssl:4.0.1	✓	✓	✓	✗	✓	✓
★★★★	wolfssl:5.9.2	✓	✓	✓	✗	✓	✓
★★	boringsl:0.20260803.0	✓	✓	✗	✗	✓	✓
★★	gnutls:3.8.13	✓	✓	✗	✗	✓	✗
★★	go-crypto:1.27	✓	✓	✗	✗	✓	✓
★★	nss:3.128	✓	✓	✗	✗	✓	✓
★★	rustls:0.23.43	✓	✓	✗	✗	✓	✓
★	openjdk:27-rc†	✗	✗	✗	✗	✓	✗
—	mbedtls:4.2.0	✗	✗	✗	✗	✗	✗
—	openjdk:26	✗	✗	✗	✗	✗	✗

Lightweight PQC is needed for IoT



- ML-KEM and ML-DSA are unsuitable for constrained IoT radio systems, particularly those with payloads of only a few tens of bytes, low transmission rates, and strict duty-cycle limits. This is especially evident for mutually authenticated key exchange.
- Constrained IoT radio needs SQIsign, MIKE, and NIKE-based authentication.

	Auth API	Mutual Authentication Algorithm	Ephemeral Key Exchange Algorithm	Total Message Size (bytes)	Authentication Key Size (bytes)
NIST PQC	Signature	ML-DSA-44	ML-KEM-512	6430	1312
	KEM	ML-KEM-512	ML-KEM-512	3160	800
	Signature	FN-DSA-512	ML-KEM-512	2930	897
	PSK	PSK	ML-KEM-512	1630	16
Other PQC / Research	Signature	FN-DSA-512	DAWN- β -512	2320	897
	KEM	DAWN- β -512	DAWN- β -512	1920	514
	Signature	Mayo 1	DAWN- β -512	1630	1168
	Signature	Mayo 2	DAWN- β -512	1350	5488
	Signature	SQISign-I	DAWN- β -512	1290	65
	Signature	UOV Is	DAWN- β -512	1180	66576
	PSK	PSK	DAWN- β -512	1020	16
	Signature	Mayo 2	MIKE	550	5488
	Signature	SQISign-I	MIKE	480	65
	Signature	UOV Is	MIKE	380	66576
	NIKE	MIKE	MIKE	220	80
	PSK	PSK	MIKE	220	16

