ERICSSON

Date: September 15, 2025

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

# Comments on NIST SP 800-56 Series Decision Proposal

Dear NIST,

Thanks for your continuous efforts to produce well-written, user-friendly, and open-access security documents. We support the proposed changes in the NIST SP 800-56 series decision proposal [1]. The excellent requirements in SP 800-56A remain highly relevant also in the post-quantum setting. For example, NSA's CNSA 2.0 profiles specifies that *"an ephemeral private key shall be used in exactly one key-establishment transaction"* for ML-KEM as well, which is a critical security practice [2–3].

Please find below some additional comments from Ericsson:

- We support the proposal to clarify that $x$-coordinate-only implementations of certain ECC key-agreement schemes are permitted. Given that NIST generally permits that *"a conforming implementation may replace the given set of steps with any mathematically equivalent set of steps"*, our understanding was that this is already allowed. We also recommend that NIST explicitly state that a protocol may transfer and store only the $x$-coordinate, provided that the corresponding $y$-coordinates are temporarily computed to perform the mandatory point validation. An example of a standardized protocol that mandates transmitting only the $x$-coordinate is EDHOC, specified in RFC 9528 [4].

- We agree that it makes sense not to add X25519 and X448 as approved key-exchange schemes, since standalone use of ECC will be disallowed after 2035. While we consider X25519 and X448 to be the only suitable elliptic-curve options for hybridizing ML-KEM and HQC-KEM, the key point is that SP 800-227, not SP 800-56, defines mechanisms for hybridizing PQC KEMs in a way that preserves IND-CCA2 security. If hybridization is employed, we recommend that NIST explicitly encourage the use of X25519 and X448. Notably, hybridization with X25519 is already the de facto standard in TLS 1.3, DTLS 1.3, QUIC, and SSH.

- We welcome allowing KMAC as an option for randomness extraction. In the future we think both industrial systems and national security systems should use SHAKE aligning with ML-KEM and ML-DSA. SHAKE offers superior theoretical and practical properties compared to SHA-2 and can often significantly reduce implementation complexity [5], as illustrated, for example, in Section 11 of FIPS 205 [6].

John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols
On behalf of the Ericsson Cryptography Team

# References

[1] NIST Proposes to Update SP 800-56A and Revise SP 800-56C
https://csrc.nist.gov/news/2025/proposal-for-sp-800-56-reports

[2] ML-KEM is Great! What's Missing? (Paper)
https://csrc.nist.gov/csrc/media/Events/2025/workshop-on-guidance-for-kems/documents/papers/ml-kem-is-great-paper.pdf

[3] ML-KEM is Great! What's Missing? (Slides)
https://csrc.nist.gov/csrc/media/Presentations/2025/ml-kem-is-great/images-media/ml-kem-is-great.pdf

[4] Ephemeral Diffie-Hellman Over COSE (EDHOC)
https://www.rfc-editor.org/rfc/rfc9528.html

[5] Ericsson comments on NIST SP 800-227 (Key-Encapsulation Mechanisms)
https://csrc.nist.gov/files/pubs/sp/800/227/ipd/docs/sp800-227-ipd-public-comments-received.pdf

[6] Stateless Hash-Based Digital Signature Standard
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf