Transport Layer Security
Internet-Draft
Intended status: Standards Track
Expires: 29 August 2026

M. Usama Sardar
TU Dresden

25 February 2026

Update to Post-quantum Hybrid ECDHE-MLKEM Key Agreement for TLSv1.3 draft-usama-tls-ecdhe-mlkem-update-00

Abstract

This is a quick update of to-be RFC [I-D.ietf-tls-ecdhe-mlkem] for recommending the three hybrid key agreement mechanisms in TLS 1.3.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://muhammad-usama-sardar.github.io/tls-ecdhe-mlkem-update/draft-usama-tls-ecdhe-mlkem-update.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-usama-tls-ecdhe-mlkem-update/.

Discussion of this document takes place on the Transport Layer Security Working Group mailing list (mailto:tls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tls/. Subscribe at https://www.ietf.org/mailman/listinfo/tls/.

Source for this draft and an issue tracker can be found at https://github.com/muhammad-usama-sardar/tls-ecdhe-mlkem-update.

Status of This Memo

Table of Contents

1. Introduction

The readers are assumed to be familiar with [I-D.ietf-tls-ecdhe-mlkem] and [RFC9847].

1.1. Motivation

Given the risk of "hardvest-now, decrypt-later" attacks [I-D.ietf-pquip-pqc-engineers], we believe that the hybrid key agreement mechanisms need to be recommended.

Section 3 of [RFC9847] defines the meaning of "Y" in "Recommended" column as follows:

> Y: Indicates that the IETF has consensus that the item is RECOMMENDED. This only means that the associated mechanism is fit for the purpose for which it was defined. Careful reading of the documentation for the mechanism is necessary to understand the

> | applicability of that mechanism. The IETF could recommend
> | mechanisms that have limited applicability but will provide
> | applicability statements that describe any limitations of the
> | mechanism or necessary constraints on its use.

This draft aims to build the mentioned consensus.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Security Considerations

The security considerations of [I-D.ietf-tls-ecdhe-mlkem] apply.

4. IANA Considerations

This document requests the following updates to three entries in the TLS Supported Groups registry (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8), according to the procedures in Section 6 of [RFC9847].

4.1. SecP256r1MLKEM768

Recommended: Y

4.2. X25519MLKEM768

Recommended: Y

4.3. SecP384r1MLKEM1024

Recommended: Y

Value	Description	Recommended
4587	SecP256r1MLKEM768	Y
4588	X25519MLKEM768	Y
4589	SecP384r1MLKEM1024	Y

Table 1

5. References

5.1. Normative References

[I-D.ietf-tls-ecdhe-mlkem]
Kwiatkowski, K., Kampanakis, P., Westerbaan, B., and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3", Work in Progress, Internet-Draft, draft-ietf-tls-ecdhe-mlkem-04, 8 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-ecdhe-mlkem-04>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

5.2. Informative References

[I-D.ietf-pquip-pqc-engineers]
Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[RFC9847] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 9847, DOI 10.17487/RFC9847, December 2025, <https://www.rfc-editor.org/rfc/rfc9847>.

Acknowledgments

We thank the authors and contributors of [I-D.ietf-tls-ecdhe-mlkem] for their work. We thank Eric Rescorla for this proposal. We also thank Bas Westerbaan for the initial idea.

Author’s Address

Muhammad Usama Sardar
TU Dresden
Dresden
Germany
Email: muhammad_usama.sardar@tu-dresden.de