

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 August 2026.

## Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
1.1. Motivation . . . . .	2
2. Conventions and Definitions . . . . .	3
3. Security Considerations . . . . .	3
4. IANA Considerations . . . . .	3
4.1. SecP256r1MLKEM768 . . . . .	3
4.2. X25519MLKEM768 . . . . .	3
4.3. SecP384r1MLKEM1024 . . . . .	3
5. References . . . . .	4
5.1. Normative References . . . . .	4
5.2. Informative References . . . . .	4
Acknowledgments . . . . .	5
Author's Address . . . . .	5

## 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](mailto:muhammad_usama.sardar@tu-dresden.de)