Transport Layer Security
Internet-Draft
Updates: 8446, 9325 (if approved)
Intended status: Standards Track
Expires: 16 October 2026

B. E. Westerbaan
Cloudflare
M. Usama Sardar
TU Dresden

14 April 2026

Updated recommendations for TLS keyshares
draft-westerbaan-tls-keyshare-recommendations-02

Abstract

This document recommends X25519MLKEM768 for use in TLS by updating its entry in the TLS Supported Groups registry (previously EC Named Curve Registry) to Recommended in the light of the future arrival of cryptographically relevant quantum computers.

[[NOTE I use key share in the title and here as it’s more accurate than "group" and perhaps more well known in the context TLS than key agreement or key exchange.]]

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://bwesterb.github.io/draft-westerbaan-tls-keyshare-recommendations/draft-westerbaan-tls-keyshare-recommendations.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-westerbaan-tls-keyshare-recommendations/.

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/bwesterb/draft-westerbaan-tls-keyshare-recommendations.

Status of This Memo

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

This Internet-Draft will expire on 16 October 2026.

Copyright Notice

Table of Contents

1. Introduction

A future cryptographically relevant quantum computer (CRQC) [RFC9794] can decrypt TLS handshakes recorded today that do not use post-quantum algorithms for their key shares: algorithms designed to be resistant against quantum attack. This threat is known as "harvest now, decrypt later" (HNDL) [I-D.ietf-pquip-pqc-engineers].

To address this threat, this document updates the TLS Supported Groups registry (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8) to mark X25519MLKEM768 as Recommended (Y) as defined in Section 6 of [RFC9847], as it is a post-quantum key share with widespread support.

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

Before the arrival of a cryptographically relevant quantum computer (CRQC), a TLS connection that negotiated a non-post quantum key share can be recorded decrypted in the future.

After the arrival of a CRQC, allowing a non-post quantum key share to be negotiated allows for an active quantum attack that achieves MITM, even if the server certificate is post quantum.

4. IANA Considerations

This document updates 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] as follows.

Value	Description	Recommended
4588	X25519MLKEM768	Y

Table 1

5. References

5.1. Normative References

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/rfc/rfc9325>.

[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>.

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>.

[RFC9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/rfc/rfc9794>.

Authors' Addresses

Bas Westerbaan
Cloudflare
Email: bas@cloudflare.com

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