Transport Layer Security
Internet-Draft
Intended status: Standards Track
Expires: 27 August 2026

B. E. Westerbaan
Cloudflare

23 February 2026

Updated recommendations for TLS keyshares
draft-westerbaan-tls-keyshare-recommendations-00

Abstract

This document updates the recommendations for key shares algorithms (TLS supported groups; previously EC Named Curve Registry) 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 27 August 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Conventions and Definitions 3
3. Security Considerations 4
4. IANA Considerations 4
4.1. Recommend 4
4.2. Discourage 4
5. References 8
5.1. Normative References 8
5.2. Informative References 8
Author's Address 9

1. Introduction

A future cryptographically relevant quantum computer can decrypt TLS handshakes recorded today that do not post-quantum algorithms for their key shares: algorithms designed to be resistant against quantum attack. This threat is known as store-now/decrypt-later (SNDL).

RFC9847 defines the permitted value of the "Recommended" column of the TLS Supported Groups registry (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8) as:

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.

N: Indicates that the item has not been evaluated by the IETF and that the IETF has made no statement about the suitability of the associated mechanism. This does not necessarily mean that the mechanism is flawed, only that no consensus exists. The IETF might have consensus to leave an items marked as "N" on the basis of its having limited applicability or usage constraints.

D: Indicates that the item is discouraged. This marking could be used to identify mechanisms that might result in problems if they are used, such as a weak cryptographic algorithm or a mechanism that might cause interoperability problems in deployment. When marking a registry entry as “D”, either the References or the Comments Column MUST include sufficient information to determine why the marking has been applied. Implementers and users SHOULD consult the linked references associated with the item to determine the conditions under which the item SHOULD NOT or MUST NOT be used.

Given the SNDL threat, the IETF cannot recommend key shares for general use that do not offer post-quantum resistance, and this document updates the TLS Supported Groups registry (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8) accordingly.

Among the currently registered post-quantum key share algorithms, IETF recommends X25519MLKEM768 for its 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.

4.1. Recommend

Value	Description	Recommended
4588	X25519MLKEM768	Y

Table 1

4.2. Discourage

Value	Description	Recommended	Comment
9	sect283k1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
10	sect283r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
11	sect409k1	D	Vulnerable to store-now/decrypt-later quantum attack, see

			TBA:this-document
12	sect409r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
13	sect571k1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
14	sect571r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
22	secp256k1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
23	secp256r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
24	secp384r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
25	secp521r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
26	brainpoolP256r1	D	Vulnerable to store-now/decrypt-later quantum attack, see

			TBA:this-document
27	brainpoolP384r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
28	brainpoolP512r1	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
29	x25519	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
30	x448	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
31	brainpoolP256r1tls13	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
32	brainpoolP384r1tls13	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
33	brainpoolP512r1tls13	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
34	GC256A	D	Vulnerable to store-now/decrypt-later quantum attack, see

			TBA:this-document
35	GC256B	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
36	GC256C	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
37	GC256D	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
38	GC512A	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
39	GC512B	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
40	GC512C	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
41	curveSM2	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
256	ffdhe2048	D	Vulnerable to store-now/decrypt-later quantum attack, see

			TBA:this-document
257	ffdhe3072	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
258	ffdhe4096	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
259	ffdhe6144	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document
260	ffdhe8192	D	Vulnerable to store-now/decrypt-later quantum attack, see TBA:this-document

Table 2

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>.

5.2. Informative References

[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>.

Author’s Address

Bas Westerbaan
Cloudflare
Email: bas@cloudflare.com