Stream: Internet Engineering Task Force (IETF)
RFC: 9851
Category: Standards Track
Published: January 2026
ISSN: 2070-1721
Authors: R. Salz N. Aviram
Akamai Technologies

RFC 9851
TLS 1.2 is in Feature Freeze

Abstract

Use of TLS 1.3, which fixes some known deficiencies in TLS 1.2, is growing. This document specifies that no changes will be approved for TLS 1.2 outside of urgent security fixes (as determined by TLS Working Group consensus), new TLS Exporter Labels, and new Application-Layer Protocol Negotiation (ALPN) Protocol IDs. This applies to TLS only; it does not apply to DTLS (in any DTLS version).

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9851.

Copyright Notice

Table of Contents

1. Introduction 2
2. Implications for Post-Quantum Cryptography (PQC) 2
3. Security Considerations 3
4. IANA Considerations 3
5. References 4
5.1. Normative References 4
5.2. Informative References 4
Acknowledgments 5
Authors' Addresses 5

1. Introduction

TLS 1.3 [TLS13] fixes most known deficiencies with TLS 1.2 [TLS12] and its use is growing. Some examples of the fixes include encrypting more of the traffic so that it is not readable by outsiders and removing most cryptographic primitives that are now considered weak. Importantly, TLS 1.3 enjoys robust security proofs.

Both versions have several extension points. Items like new cryptographic algorithms, new supported groups (formerly "named curves"), etc., can be added without defining a new protocol. This document specifies that no changes will be approved for TLS 1.2 outside of urgent security fixes (as determined by TLS Working Group consensus) and the exceptions listed in Section 4.

This applies to TLS only. As such, it does not apply to DTLS, in any DTLS version.

2. Implications for Post-Quantum Cryptography (PQC)

Cryptographically relevant quantum computers, once available, are likely to greatly lessen the time and effort needed to break RSA, finite-field-based Diffie-Hellman (FFDH), or Elliptic Curve Cryptography (ECC) which are currently used in TLS. In 2016, the US National Institute of Standards and Technology (NIST) started a multi-year effort to standardize algorithms that will be "safe" once quantum computers are feasible [PQC]. Initial discussions in the IETF community happened around the same time [CFRGSLIDES].

In 2024, NIST released standards for [ML-KEM], [ML-DSA], and [SLH-DSA]. Many other countries and organizations are publishing their roadmaps, including the multi-national standards organization ETSI [ETSI].

While the industry was waiting for NIST to finish standardization, the IETF has had several efforts underway. A working group was formed in early 2023 to work on the use of Post-Quantum Cryptography (PQC) in IETF protocols [PQUIPWG]. Several other working groups, including TLS [TLSWG], are working on specifications to support hybrid algorithms and identifiers, for use during a transition from classic to a post-quantum world.

It is important to note that effort within the TLS Working Group is focused exclusively on TLS 1.3 or later. Put bluntly, PQC for TLS 1.2 will not be specified (see Section 4) at any time; anyone wishing to deploy PQC should expect to use TLS 1.3.

3. Security Considerations

This entire document is about security and provides post-quantum security concerns as an additional reason to upgrade to TLS 1.3.

4. IANA Considerations

No TLS registries [TLS13REG] are being closed by this document. Rather, this document modifies the instructions to IANA and the TLS Designated Experts to constrain the type of entries that can be added to existing registries.

This document does not introduce any new limitations on the registrations for either of the following two registries:

- TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs
- TLS Exporter Labels

The following note has been added to the other TLS registries:

> Any TLS entry added after the IESG approves publication of RFC 9851 is intended for TLS 1.3 or later, and makes no similar requirement on DTLS. Such entries should have an informal indication like "For TLS 1.3 or later" in that entry, such as the "Comment" column.

At the time of publication, the note has been added to the following TLS registries:

- TLS Alerts
- TLS Authorization Data Formats
- TLS CachedInformationType Values
- TLS Certificate Compression Algorithm IDs

- TLS Certificate Status Types
- TLS Certificate Types
- TLS Cipher Suites
- TLS ClientCertificateType Identifiers
- TLS ContentType
- TLS EC Curve Types
- TLS EC Point Formats
- TLS ExtensionType Values
- TLS HandshakeType
- TLS HashAlgorithm
- TLS Heartbeat Message Types
- TLS Heartbeat Modes
- TLS KDF Identifiers
- TLS PskKeyExchangeMode
- TLS SignatureAlgorithm
- TLS SignatureScheme
- TLS Supplemental Data Formats (SupplementalDataType)
- TLS Supported Groups
- TLS UserMappingType Values

Any TLS registry created after this document is approved for publication should indicate whether the actions defined here are applicable.

5. References

5.1. Normative References

[TLS12] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[TLS13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 9846, DOI 10.17487/RFC9846, January 2026, <https://www.rfc-editor.org/info/rfc9846>.

[TLS13REG] 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/info/rfc9847>.

5.2. Informative References

[CFRGSLIDES] McGrew, D., "Post Quantum Secure Cryptography Discussion", IETF 95 Proceedings, April 2016, <https://www.ietf.org/proceedings/95/slides/slides-95-cfrg-4.pdf>.

[ETSI] ETSI, "CYBER; Migration strategies and recommendations to Quantum Safe schemes", Version 1.1.1, ETSI TR 103 619, July 2020, <https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf>.

[ML-DSA] NIST, "Module-Lattice-Based Digital Signature Standard", NIST FIPS 204, DOI 10.6028/NIST.FIPS.204, August 2024, <https://csrc.nist.gov/pubs/fips/204/final>.

[ML-KEM] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard", NIST FIPS 203, DOI 10.6028/NIST.FIPS.203, August 2024, <https://csrc.nist.gov/pubs/fips/203/final>.

[PQC] NIST, "Post-Quantum Cryptography (PQC)", January 2017, <https://csrc.nist.gov/projects/post-quantum-cryptography>.

[PQUIPWG] IETF, "Post-Quantum Use in Protocols", <https://datatracker.ietf.org/wg/pquip/about/>.

[SLH-DSA] NIST, "Stateless Hash-Based Digital Signature Standard", NIST FIPS 205, DOI 10.6028/NIST.FIPS.205, August 2024, <https://csrc.nist.gov/pubs/fips/205/final>.

[TLSWG] IETF, "Transport Layer Security", <https://datatracker.ietf.org/wg/tls/about/>.

Acknowledgments

We gratefully acknowledge Amanda Baber, David Dong, and Sabrina Tanamal of IANA for their help in revising and clarifying Section 4.

Authors' Addresses

Rich Salz
Akamai Technologies
Email: rsalz@akamai.com

Nimrod Aviram
Email: nimrod.aviram@gmail.com