Transport Layer Security
Internet-Draft
Intended status: Standards Track
Expires: 5 October 2025

R. Salz
Akamai Technologies
N. Aviram

3 April 2025

TLS 1.2 is in Feature Freeze
draft-ietf-tls-tls12-frozen-08

Abstract

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

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-tls-tls12-frozen/.

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/tlswg/tls12-frozen.

Status of This Memo

This Internet-Draft will expire on 5 October 2025.

Table of Contents

1. Introduction

Use of TLS 1.3 [TLS13] is growing, and it fixes most known deficiencies with TLS 1.2 [TLS12]. Examples of this include encrypting more of the traffic so that it is not readable by outsiders and removing most cryptographic primitives 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 outside of urgent security fixes (as determine by TLS WG consensus), and the exceptions listed in Section 4, no changes will be approved for TLS 1.2.

This prescription pertains to TLS only. As such, it does not pertain 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]. First 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 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 the focus of efforts within the TLS Working Group is exclusively TLS 1.3 or later. Put bluntly, PQC for TLS 1.2 will not be specified (see Section 4) at any time and anyone wishing to deploy PQC should expect to be using TLS 1.3.

3. Security Considerations

This entire document is about security, and provides post-quantum 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 Designed Experts to constrain what type of entries can be added to existing registries.

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

* TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs

* TLS Exporter Labels

> All other TLS registries should have this Note added to them: Any TLS entry added after the IESG approves publication of {THIS RFC} 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 list of other TLS registries is as follows:

* 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/rfc/rfc5246>.

[TLS13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-12, 17 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-12>.

[TLS13REG] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-11, 11 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-11>.

5.2. Informative References

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

[ETSI] "CYBER; Migration strategies and recommendations to Quantum Safe schemes", n.d., <https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf>.

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

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

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

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

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

[TLSWG] "Transport Layer Security", n.d., <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