Transport Layer Security
Internet-Draft
Intended status: Standards Track
Expires: 2 August 2025

R. Salz
Akamai Technologies
N. Aviram

29 January 2025

TLS 1.2 is in Feature Freeze
draft-ietf-tls-tls12-frozen-06

Abstract

Use of TLS 1.3, ~~is growing~~ which~~and~~ fixes some known deficiencies in TLS 1.2, is growing. This document specifies that ~~outside~~ except~~of~~ urgent security fixes, 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.

Commenté [MB1]: «For TLS 1.2-only» would be more accurate as some of these are applicable to TLS1.3 as well. No?

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 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 2 August 2025.

Copyright Notice

Table of Contents

1. Introduction

~~Use of~~ TLS 1.3 [TLS13] ~~is growing, and it~~ fixes most known deficiencies with TLS 1.2 [TLS12], such as 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. Also, use of TLS 1.3 is growing.

Both TLS versions have several extension points~~,~~. ~~so i~~Items ~~like~~ such as 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, 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 Datagram Transport Layer Security (DTLS), ~~(~~in any DTLS version~~); it pertains to TLS only~~..

2. Implications for P~~p~~ost-~~quantum~~ Quantum ~~cryptography~~Cryptography

Cryptographically relevant quantum computers, once available, will have a huge impact on RSA, FFDH, and 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].

Commenté [MB2]: Not sure what is meant here. Do we mean new TLS version? Please reword. Thanks.

Commenté [MB3]: I'd like to check if this is consistent with this note in the registry: «Although TLS 1.3 uses the same cipher suite space as previous versions of TLS, TLS 1.3 cipher suites are defined differently, only specifying the symmetric ciphers and hash function, and cannot be used for TLS 1.2. Similarly, TLS 1.2 and lower cipher suite values cannot be used with TLS 1.3. »

Commenté [MB4]: Who will make the call about what is «urgent»? Is it the TLS WG? The IESG?

Commenté [MB5]: Provide examples

Commenté [MB6]: Please expand.

Commenté [MB7]: Any other similar pointer to share for other regions (non-US)?

In 2024, NIST released standards for [ML-KEM], [ML-DSA], and [SLH-DSA]. 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 WG [TLSWG], are working on ~~drafts~~ specifications to support hybrid algorithms and identifiers, for use during a transition from classic to a post-quantum world.

For TLS, it is important to note that the focus of these efforts is exclusively TLS 1.3 or later. Put bluntly, post-quantum cryptography for TLS 1.2 ~~WILL NOT~~won't be supported (see Section 4) at any time and anyone wishing to deploy post-quantum cryptography 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 registries [TLS13REG] in TLS registry groups 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.

Commenté [MB8]: I think the registry is authoritative here. I suggest to replace with Transport Layer Security (TLS) Parameters and Transport Layer Security (TLS) Extensions

This document does not introduce ~~There are no~~any new limits on the registrations for either of the following two registries:

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

- TLS Exporter Labels

This document request IANA to add this note to ~~All~~ all other TLS registries ~~should have this Note added to them~~: Any 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 ~~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 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 ~~registries~~ 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-11, 14 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-11>.

[TLS13REG] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-10, 3 November 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-10>.

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>.

[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