Stream:	Internet Engineering Task Force (IETF)
RFC:	9847
Updates:	8447
Category:	Standards Track
Published:	October 2025
ISSN:	2070-1721
Authors:	J. Salowey	S. Turner
---	---	---
	Venafi	*sn3rd*

RFC 9847
IANA Registry Updates for TLS and DTLS

Abstract

This document updates the changes to the TLS and DTLS IANA registries made in RFC 8447. It adds a new value, "D" for discouraged, to the "Recommended" column of the selected TLS registries and adds a "Comment" column to all active registries that do not already have a "Comment" column. Finally, it updates the registration request instructions.

This document updates RFC 8447.

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/rfc9847.

Copyright Notice

Table of Contents

1. Introduction

This document instructs IANA to make changes to a number of the IANA registries related to Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). These changes update the changes made in [RFC8447].

This specification adds a new value, "D" for discouraged, to the "Recommended" column of the selected TLS registries and adds a "Comment" column to all active registries that do not already have a "Comment" column.

This specification also updates the registration request instructions.

2. Terminology

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. Updating "Recommended" Column's Values

The instructions in this document update the "Recommended" column, originally added in [RFC8447] to add a third value, "D", indicating that a value is discouraged. The permitted values of the "Recommended" column are:

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 "Reference" or the "Comment" 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.

Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126]. Not all items defined in Standards Track RFCs need to be set to "Y" or "D". Any item not otherwise specified is set to "N". The column is blank for values that are unassigned or reserved unless specifically set.

3.1. Recommended Note

Existing registries have a note on the meaning of the "Recommended" column. For the registries discussed in the subsequent sections, this note is updated with a sentence describing the "D" value as follows:

> Note: If the "Recommended" column is set to "N", it does not necessarily mean that it is flawed; rather, it indicates that the item has not been through the IETF consensus process, has limited applicability, or is intended only for specific use cases. If the "Recommended" column is set to "D", the item is discouraged and **SHOULD NOT** or **MUST NOT** be used, depending upon the situation; consult the item's references for clarity.

4. TLS ExtensionType Values Registry

In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS ExtensionType Values" registry as follows:

- Adjusted the registration procedure related to setting the "Recommended" column as follows:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].

- Added a reference to this document under the reference heading.
- Updated the "Recommended" column with the changes listed below. Entries keep their existing "Y" and "N" entries except for the entries in the following table. IANA has added a reference to this document for these entries.

Value	Extension Name	Recommended
4	truncated_hmac	D
40	Reserved	D
46	Reserved	D
53	connection_id (deprecated)	D

Table 1

- Updated the note on the "Recommended" column with text in Section 3.1.
- For the truncated_hmac, added the following link to the "Reference" column: https://www.iacr.org/archive/asiacrypt2011/70730368/70730368.pdf
- For the two Reserved values above, added the following link in the "Reference" column: https://mailarchive.ietf.org/arch/msg/tls-reg-review/5BD62HBFjo_AsW-Y8ohVuWEe1gI/

5. TLS Cipher Suites Registry

Several categories of cipher suites are discouraged for general use and are marked as "D".

Cipher suites that use NULL encryption do not provide the confidentiality normally expected of TLS. Protocols and applications are often designed to require confidentiality as a security property. These cipher suites **MUST NOT** be used in those cases.

Cipher suites marked as EXPORT use weak ciphers and were deprecated in TLS 1.1 [RFC4346].

Cipher suites marked as anon do not provide any authentication, are vulnerable to on-path attacks, and were deprecated in TLS 1.1 [RFC4346].

RC4 is a weak cipher and is deprecated in [RFC7465].

DES and the International Data Encryption Algorithm (IDEA) are not considered secure for general use and were deprecated in [RFC5469]. MD5 and SHA-1 are also not secure for general use and were deprecated in [RFC9155].

In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS Cipher Suites" registry as follows:

- Adjusted the registration procedure related to setting the "Recommended" column as follows:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].
- Added a reference to this document under the reference heading.
- Updated the "Recommended" column with the changes listed below. Entries keep their existing "Y" and "N" entries except for the entries in following table. IANA has added a reference to this document for these entries. This document does not make any changes to the "DTLS-OK" column.

Value	Description	Recommended
0x00,0x1E	TLS_KRB5_WITH_DES_CBC_SHA	D
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA	D
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA	D
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5	D
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5	D
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5	D

Value	Description	Recommended
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	D
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA	D
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA	D
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	D
0x00,0x2A	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	D
0x00,0x2B	TLS_KRB5_EXPORT_WITH_RC4_40_MD5	D
0x00,0x2C	TLS_PSK_WITH_NULL_SHA	D
0x00,0x8A	TLS_PSK_WITH_RC4_128_SHA	D
0x00,0xB0	TLS_PSK_WITH_NULL_SHA256	D
0x00,0xB1	TLS_PSK_WITH_NULL_SHA384	D
0xC0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA	D
0xC0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	D
0xC0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA	D
0xC0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA	D
0xC0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA	D
0xC0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA	D
0xC0,0x3A	TLS_ECDHE_PSK_WITH_NULL_SHA256	D
0xC0,0x3B	TLS_ECDHE_PSK_WITH_NULL_SHA384	D
0xC0,0xB4	TLS_SHA256_SHA256	D
0xC0,0xB5	TLS_SHA384_SHA384	D

Table 2

- Updated the note on the "Recommended" column with text in Section 3.1.

6. TLS Supported Groups Registry

In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS Supported Groups" registry as follows:

- Updated the registration policy to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].

- Added a reference to this document under the reference heading.
- Updated the "Recommended" column with the changes listed below. Entries keep their existing "Y" and "N" entries except for the entries in following table. IANA has added a reference to this document for these entries.

Value	Description	Recommended
1	sect163k1	D
2	sect163r1	D
3	sect163r2	D
4	sect193r1	D
5	sect193r2	D
6	sect233k1	D
7	sect233r1	D
8	sect239k1	D
15	secp160k1	D
16	secp160r1	D
17	secp160r2	D
18	secp192k1	D
19	secp192r1	D
20	secp224k1	D

Value	Description	Recommended
21	secp224r1	D

Table 3

- Updated the note on the "Recommended" column with text in Section 3.1.
- Removed the "Elliptic curve groups" note from the registration procedures table.
- For each of the entries above, added the following link to the "Comment" column: https://datatracker.ietf.org/meeting/118/materials/slides-118-tls-rfc8447bis-00

7. TLS Exporter Labels Registry

This document updates the registration procedure for the "TLS Exporter Labels" registry and updates the "Recommended" column allocation. IANA has updated the "TLS Exporter Labels" registry as follows:

- Changed the registration procedure from Specification Required to Expert Review and updated it to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].

- Added a reference to this document under the reference heading.
- Entries kept their existing "Recommended" column "Y" and "N" entries.
- Updated the note on the "Recommended" column with text in Section 3.1.
- Updated the note on the role of the expert reviewer as follows.

> Note: The role of the designated expert is described in [RFC8447], Section 17. Even though this registry does not require a specification, the designated expert [RFC8126] will strongly encourage registrants to provide a link to a publicly available specification. An Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. is suitable for these purposes. The expert may provide more in-depth reviews, but their approval should not be taken as an endorsement of the exporter label. The expert also verifies that the label is a string consisting of printable ASCII characters beginning with "EXPORTER". IANA **MUST** also verify that one label is not a prefix of any other label. For example, labels "key" or "master secretary" are forbidden.

- Renamed the "Note" column to "Comment".

8. TLS Certificate Types Registry

In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS Certificate Types" registry as follows:

- Adjusted the registration procedure related to setting the "Recommended" column as follows:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].
- Added a reference to this document under the reference heading.
- Entries kept their existing "Recommended" column "Y" and "N" entries.
- Updated the note on the "Recommended" column with text in Section 3.1.

9. TLS HashAlgorithm Registry

TLS 1.0 and TLS 1.1 were deprecated [RFC8996], TLS 1.2 will be in use for some time. In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS HashAlgorithm" registry as follows:

- Updated the registration procedure to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].
- Added a reference to this document under the reference heading.
- Updated the "TLS HashAlgorithm" registry to add a "Recommended" column as follows:

Value	Description	Recommended
0	none	Y
1	md5	D
2	sha1	D
3	sha224	D
4	sha256	Y
5	sha384	Y
6	sha512	Y

Value	Description	Recommended
8	Intrinsic	Y

Table 4

- Added a note on the "Recommended" column with text in Section 3.1.

10. TLS SignatureAlgorithm Registry

TLS 1.0 and TLS 1.1 were deprecated [RFC8996], TLS 1.2 will be in use for some time. In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS SignatureAlgorithm" registry as follows:

- Updated the registration procedure to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].

- Added a reference to this document under the reference heading.
- Updated the "TLS SignatureAlgorithm" registry to add a "Recommended" column as follows:

Value	Description	Recommended
0	anonymous	N
1	rsa	Y
2	dsa	N
3	ecdsa	Y
7	ed25519	Y
8	ed448	Y
64	gostr34102012_256	N
65	gostr34102012_512	N

Table 5

- Added a note on the "Recommended" column with text in Section 3.1.

11. TLS ClientCertificateType Identifiers Registry

TLS 1.0 and TLS 1.1 were deprecated [RFC8996], TLS 1.2 will be in use for some time. In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS ClientCertificateType Identifiers" registry as follows:

- Updated the registration procedure to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].
- Added a reference to this document under the reference heading.
- Updated the "TLS ClientCertificateType Identifiers" registry to add a "Recommended" column as follows:

Value	Description	Recommended
1	rsa_sign	Y
2	dss_sign	N
3	rsa_fixed_dh	N
4	dss_fixed_dh	N
5	rsa_ephemeral_dh_RESERVED	D
6	dss_ephemeral_dh_RESERVED	D
20	fortezza_dms_RESERVED	D
64	ecdsa_sign	Y
65	rsa_fixed_ecdh	N
66	ecdsa_fixed_ecdh	N
67	gost_sign256	N
68	gost_sign512	N

Table 6

- Added a note on the "Recommended" column with text in Section 3.1.

12. TLS PskKeyExchangeMode Registry

In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS PskKeyExchangeMode" registry as follows:

- Updated the registration procedure to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].

- Added a reference to this document under the reference heading.
- Entries kept their existing "Recommended" column "Y" and "N" entries.
- Updated note on the "Recommended" column with text in Section 3.1.

13. TLS SignatureScheme Registry

In order to reflect the changes in the "Recommended" column allocation, IANA has updated the "TLS SignatureScheme" registry as follows:

- Updated the registration procedure to include:

  Setting a value to "Y" or "D" or transitioning the value from "Y" or "D" in the "Recommended" column requires IETF Standards Action with Expert Review or IESG Approval [RFC8126].

- Added a reference to this document under the reference heading.
- Entries kept their existing "Recommended" column "Y" and "N" entries.
- Updated note on the "Recommended" column with text in Section 3.1.

14. Adding "Comment" Column

IANA has added a "Comment" column to the following registries:

- TLS ExtensionType Values
- TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs
- TLS CachedInformationType Values
- TLS Certificate Compression Algorithm IDs
- TLS ClientCertificateType Identifiers
- TLS Cipher Suites
- TLS ContentType
- TLS EC Point Formats
- TLS EC Curve Types
- TLS Supplemental Data Formats (SupplementalDataType)
- TLS UserMappingType Values
- TLS SignatureAlgorithm

- TLS HashAlgorithm
- TLS Authorization Data Formats
- TLS Heartbeat Message Types
- TLS Heartbeat Modes
- TLS SignatureScheme
- TLS PskKeyExchangeMode
- TLS KDF Identifiers
- TLS SSLKEYLOGFILE Labels

This list of registries is all registries that do not already have a "Comment" or "Note" column or that were not orphaned by TLS 1.3.

IANA has renamed the "Note" column to "Comment" in the "TLS Exporter Labels" registry.

15. Expert Review of Current and Potential IETF and IRTF Documents

The intent of the Specification Required choice for TLS codepoints is to allow for easy registration for codepoints associated with protocols and algorithms that are not being actively developed inside the IETF or IRTF. When TLS-based technologies are being developed inside the IETF or IRTF, they should be done in coordination with the TLS WG in order to provide appropriate review. For this reason, unless the TLS WG Chairs indicate otherwise via email, designated experts should decline codepoint registrations for documents that have already been adopted or are being proposed for adoption by IETF working groups or IRTF research groups.

16. Registration Requests

Registration requests **MUST** be submitted in one of two ways:

1. By sending email to iana@iana.org; this email **SHOULD** use an appropriate subject (e.g., "Request to register value in TLS bar registry").
2. Using the online form at https://www.iana.org/form/protocol-assignment.

Specification Required [RFC8126] registry requests are registered after a three-week review period on the advice of one or more designated experts. However, to allow for the allocation of values prior to publication, the designated experts may approve registration once they are satisfied that such a specification will be published.

17. Security Considerations

Recommended algorithms are regarded as secure for general use at the time of registration; however, cryptographic algorithms and parameters will be broken or weakened over time. It is possible that the "Recommended" status in the registry lags behind the most recent advances in cryptanalysis. Implementers and users need to check that the cryptographic algorithms listed continue to provide the expected level of security.

Designated experts ensure the specification is publicly available. They may provide more in-depth reviews. Their review should not be taken as an endorsement of the cipher suite, extension, supported group, etc.

18. IANA Considerations

This document is entirely about changes to TLS-related IANA registries.

IANA has modified the note applied to all TLS Specification Required registries instructing where to send registration requests as follows:

> Note: Requests for registration in the "Specification Required" [RFC8126] range should be sent to iana@iana.org or submitted via IANA's application form, per [RFC 9847]. IANA will forward the request to the expert mailing list described in [RFC8447], Section 17 and track its progress. See the registration procedure table below for more information.

19. 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/info/rfc2119>.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, DOI 10.17487/RFC4346, April 2006, <https://www.rfc-editor.org/info/rfc4346>.

[RFC5469] Eronen, P., Ed., "DES and IDEA Cipher Suites for Transport Layer Security (TLS)", RFC 5469, DOI 10.17487/RFC5469, February 2009, <https://www.rfc-editor.org/info/rfc5469>.

[RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <https://www.rfc-editor.org/info/rfc7465>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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/info/rfc8174>.

[RFC8447] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 8447, DOI 10.17487/RFC8447, August 2018, <https://www.rfc-editor.org/info/rfc8447>.

[RFC8996] Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, DOI 10.17487/RFC8996, March 2021, <https://www.rfc-editor.org/info/rfc8996>.

[RFC9155] Velvindron, L., Moriarty, K., and A. Ghedini, "Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2", RFC 9155, DOI 10.17487/RFC9155, December 2021, <https://www.rfc-editor.org/info/rfc9155>.

Authors' Addresses

Joe Salowey
Venafi
Email: joe@salowey.net

Sean Turner
sn3rd
Email: sean@sn3rd.com