Workgroup: Transport Layer Security
Internet-Draft: draft-ietf-tls-rfc8447bis-08
Updates: 3749, 5077, 4680, 5246, 5705, 5878,
6520, 7301, 8447 (if approved)
Published: 23 January 2024
Intended Status: Standards Track
Expires: 26 July 2024
Authors: J. Salowey S. Turner
Venafi sn3rd

IANA Registry Updates for TLS and DTLS

Abstract

This document updates the changes to 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.

This document updates the following RFCs: 3749, 5077, 4680, 5246, 5705, 5878, 6520, 7301, and 8447.

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-rfc8447bis/.

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/rfc8447bis.

Status of This Memo

This Internet-Draft will expire on 26 July 2024.

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].

NOTE for IANA: This document specifies changes to the registry to update the changes made in [RFC8447].

This specification updates the "Recommended" column in TLS registries to define a third value "D" for items that are discouraged.

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. Adding "Recommended" Column

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 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 it 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. Implementers **SHOULD** consult the linked references associated with the item to determine the conditions under which it **SHOULD NOT** or **MUST NOT** be used.

Setting a value to "Y" or "D" in the "Recommended" column requires IETF Standards Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval. 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" vaue as follows:

Note: If "Recommended" column is set to "N", it does not necessarily mean that it is flawed; rather, it indicates that the item either 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.

4. TLS ExtensionType Values

In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS ExtensionType Values registry as follows:

*Change the registration procedure to:

Values with the first byte in the range 0-254 (decimal) are assigned via Specification Required [RFC8126]. Values with the first byte 255 (decimal) are reserved for Private Use [RFC8126]. Setting a "Recommended" column value to "Y" or "D" requires Standards Action [Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Update the "Recommended" column with the changes as listed below. Entries keep their existing "Y" and "N" entries except for the entries in following table. A reference to this document **SHALL** be added to these entries.

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

Table 1

*Update note on the recommended column with text in Section 3.1.

5. TLS Cipher Suites Registry

Several categories of ciphersuites are discouraged for general use and are maked as "D".

Ciphersuites that use NULL encryption do not provide the confidentiality normally expected of TLS. Protocols and applications

are often designed to require confidentialy as a security property. These ciphersuites **MUST NOT** be used in those cases.

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

Cipher suites maked as anon do not provide any authentication and are vulnerable to man-in-the-middle attacks and are deprecated in TLS 1.1 [RFC4346].

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

DES and IDEA are not considered secure for general use and are deprecated in [RFC5469].

In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS ExtensionType Values registry as follows:

*Change the registration procedure to:

Values with the first byte in the range 0-254 (decimal) are assigned via Specification Required [RFC8126]. Values with the first byte 255 (decimal) are reserved for Private Use [RFC8126]. Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Update the "Recommended" column with the changes as listed below. Entries keep their existing "Y" and "N" entries except for the entries in following table. A reference to this document **SHALL** be added to these entries. This document does not make any changes to the DTLS-OK column.

Value	Cipher Suite Name	Recommeded
0x00,0x01	TLS_RSA_WITH_NULL_MD5	D
0x00,0x02	TLS_RSA_WITH_NULL_SHA	D
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5	D
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5	D
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA	D
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	D
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA	D
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	D
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA	D
0x00,0x0B	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	D
0x00,0x0C	TLS_DH_DSS_WITH_DES_CBC_SHA	D
0x00,0x0E	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	D
0x00,0x0F	TLS_DH_RSA_WITH_DES_CBC_SHA	D

Value	Cipher Suite Name	Recommeded
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	D
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA	D
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	D
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA	D
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	D
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5	D
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	D
0x00,0x1A	TLS_DH_anon_WITH_DES_CBC_SHA	D
0x00,0x1B	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	D
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
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
0x00,0x2D	TLS_DHE_PSK_WITH_NULL_SHA	D
0x00,0x2E	TLS_RSA_PSK_WITH_NULL_SHA	D
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA	D
0x00,0x3A	TLS_DH_anon_WITH_AES_256_CBC_SHA	D
0x00,0x3B	TLS_RSA_WITH_NULL_SHA256	D
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	D
0x00,0x6C	TLS_DH_anon_WITH_AES_128_CBC_SHA256	D
0x00,0x6D	TLS_DH_anon_WITH_AES_256_CBC_SHA256	D
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	D
0x00,0x8A	TLS_PSK_WITH_RC4_128_SHA	D
0x00,0x8E	TLS_DHE_PSK_WITH_RC4_128_SHA	D
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA	D
0x00,0x9B	TLS_DH_anon_WITH_SEED_CBC_SHA	D
0x00,0xA6	TLS_DH_anon_WITH_AES_128_GCM_SHA256	D
0x00,0xA7	TLS_DH_anon_WITH_AES_256_GCM_SHA384	D
0x00,0xB0	TLS_PSK_WITH_NULL_SHA256	D
0x00,0xB1	TLS_PSK_WITH_NULL_SHA384	D
0x00,0xB4	TLS_DHE_PSK_WITH_NULL_SHA256	D
0x00,0xB5	TLS_DHE_PSK_WITH_NULL_SHA384	D
0x00,0xB8	TLS_RSA_PSK_WITH_NULL_SHA256	D
0x00,0xB9	TLS_RSA_PSK_WITH_NULL_SHA384	D
0x00,0xBF	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	D
0x00,0xC5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	D

Value	Cipher Suite Name	Recommeded
0xC0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA	D
0xC0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	D
0xC0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA	D
0xC0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	D
0xC0,0x0B	TLS_ECDH_RSA_WITH_NULL_SHA	D
0xC0,0x0C	TLS_ECDH_RSA_WITH_RC4_128_SHA	D
0xC0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA	D
0xC0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA	D
0xC0,0x15	TLS_ECDH_anon_WITH_NULL_SHA	D
0xC0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA	D
0xC0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	D
0xC0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	D
0xC0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_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
0xC0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256	D
0xC0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384	D
0xC0,0x5A	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256	D
0xC0,0x5B	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384	D
0xC0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256	D
0xC0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384	D
0xC0,0xB4	TLS_SHA256_SHA256	D
0xC0,0xB5	TLS_SHA384_SHA384	D

Table 2

*Update note on the recommended column with text in Section 3.1.

6. TLS Supported Groups

In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS Supported Groups registry as follows:

*Update the registration policy to include:

Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Update the "Recommended" column with the changes as listed below. Entries keep their existing "Y" and "N" entries except for the entries in following table. A reference to this document **SHALL** be added to these entries.

Value	Curve	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
21	secp224r1	D

Table 3

*Update note on the recommended column with text in Section 3.1.

7. TLS Exporter Labels Registry

This document updates the registration procedure for the TLS Exporter registry and updates the Recommended column allocation. IANA **SHALL** update the TLS Exporter Labels Registry as follows:

*Change the registration procedure from Specification Required to Expert Review and update it to include:

Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Entries keep their existing Recommended column "Y" and "N" entries

*Update note on the recommended column with text in Section 3.1.

*update the note on the role of the expert reviewer as follows.

Note: The role of the designated expert is described in [RFC8447]. 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. are 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.

8. TLS Certificate Types

In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the the TLS Certificate Types registry as follows:

*Change the registration procedure to:

Values in the range 0-223 (decimal) are assigned via Specification Required [RFC8126]. Values in the range 224-255 (decimal) are reserved for Private Use [RFC8126]. Setting a "Recommended" column value to "Y" or "D" requires Standards Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Entries keep their existing Recommended column "Y" and "N" entries.

*Update note on the recommended column with text in Section 3.1.

9. TLS HashAlgorithm Registry

Though TLS 1.0 and TLS 1.1 were deprecated [RFC8996], TLS 1.2 will be in use for some time. In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS HashAlgorithm Registry registry as follows:

*Update the registration procedure to include:

Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Update the TLS HashAlgorithm registry to add a "Recommended" column as follows:

Value	Descsription	Recommended
0	none	Y
1	md5	D
2	sha1	D

Value	Descsription	Recommended
3	sha224	D
4	sha256	Y
5	sha384	Y
6	sha512	Y
8	Intrinsic	Y

Table 4

*Add note on the recommended column with text in Section 3.1.

10. TLS SignatureAlgorithm registry

Though TLS 1.0 and TLS 1.1 were deprecated [RFC8996], TLS 1.2 will be in use for some time. In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS SignatureAlgorithm registry registry as follows:

*Update the registration procedure to include:

Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Update the TLS SignatureAlgorithm registry to add a "Recommended" column as follows:

Value	Descsription	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

*Add note on the recommended column with text in Section 3.1.

11. TLS ClientCertificateTypes registry

Though TLS 1.0 and TLS 1.1 were deprecated [RFC8996], TLS 1.2 will be in use for some time. In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS ClientCertificateTypes registry as follows:

*Update the registration procedure to include:

Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Update the TLS ClientCertificateTypes registry to add a "Recommended" column as follows:

Value	Descsription	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

*Add note on the recommended column with text in Section 3.1.

12. TLS PskKeyExchangeMode registry

In order to refect the changes in the Recommended column allocation, IANA **SHALL** update the TLS PskKeyExchangeMode registry as follows:

*Update the registration procedure to include:

Setting a "Recommended" column value to "Y" or "D" requires Standard Action [RFC8126]. Any state transition to or from a "Y" or "D" value requires IESG Approval.

*Add a reference to this document under the reference heading.

*Entries keep their existing recommended column "Y" and "N" entries.

*Update note on the recommended column with text in Section 3.1.

13. TLS SignatureScheme registry

IANA is requested to add a reference to this document under the reference heading.

14. Adding "Comment" Column

IANA is requested to add 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 Cipher Suites
- *TLS ContentType
- *TLS EC Point Formats
- *TLS EC Curve Types
- *TLS Supplemental Data Formats (SupplementalDataType)
- *TLS UserMappingType Values
- *TLS Authorization Data Formats
- *TLS Heartbeat Message Types
- *TLS Heartbeat Modes
- *TLS SignatureScheme
- *TLS PskKeyExchangeMode
- *TLS KDF Identifiers

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

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

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

16. Security Considerations

The change to Specification Required from IETF Review lowers the amount of review provided by the WG for cipher suites and supported groups. This change reflects reality in that the WG essentially provided no cryptographic review of the cipher suites or supported groups. This was especially true of national cipher suites.

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.

17. IANA Considerations

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

18. 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>.

[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/rfc/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/rfc/rfc5469>.

[RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc8996>.

Authors' Addresses

Joe Salowey
Venafi

Email: joe@salowey.net

Sean Turner
sn3rd

Email: sean@sn3rd.com