TLS WG
Internet-Draft
Updates: 3749, 5077, 4680, 5246, 5878, 6520, 7301 (if approved)
Intended status: Standards Track
Expires: July 6, 2017

J. Salowey
Tableau Software
S. Turner
sn3rd

January 02, 2017

D/TLS IANA Registry Updates
draft-ietf-tls-iana-registry-updates-00

Abstract

This document changes the IANA registry policy for a number of registries related to DTLS and TLS, renames some of the registries for consistency, and adds notes to many of the registries. As a result, this document updates many RFCs (see updates header).

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 http://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 July 6, 2017.

Table of Contents

1. Process Note

As the authors of this draft are also the WG chairs, the responsible Area Director has agreed to judge consensus.

RFC EDITOR: Please delete section prior to publication.

2. Introduction

This document requests that IANA make changes to a number of DTLS- and TLS-related IANA registries.

In this document, we use the term "(D)TLS" to refer to registries that apply to both TLS and DTLS.

- Add "TLS" to registries' names for consistency with other TLS-related registries.

- Change the IANA registry policy [RFC5226] for the TLS ExtensionType Values, TLS Cipher Suite, and TLS ClientCertificateType Identifiers registries. These changes register a small part of these code spaces for experimentation and private use.

- Add the designated expert intructions as a note to the TLS ExtensionType Values, TLS Cipher Suite, and TLS ClientCertificateType Identifiers registries to inform users of the registry.

- Add notes to indicate whether an extension, certain values of an extension, or an entire registry is only applicable pre-(D)TLS 1.3.

- Rename the NewSessionTicket TLS HandshakeType message registry entry [RFC5077] to new_session_ticket to match the naming nomenclature for the other Handshake type names and to match with existing implementations.

- Rename the SessionTicket TLS to session_ticket to match the nomenclature for the other extensions' names.

- Add missing entry to the TLS Alert Registry for the no_application_protocol alert defined in [RFC7301]

This document proposes no changes to the registration policies for TLS Alert [I-D.ietf-tls-tls13], TLS ContentType [I-D.ietf-tls-tls13], TLS HandshakeType, [I-D.ietf-tls-tls13] and TLS Certificate Status Types [RFC6961]; the existing policies (Standards Action for the first three; IETF Review for the last), are appropriate for these one-byte code points because of their scarcity.

This document proposes no changes to the EC Curve Type, EC Point Format, and Supported Groups Registries (see [I-D.ietf-tls-rfc4492bis]).

3. Add "TLS" to Registry Names

IANA is to update the names of the following registries to add "TLS" to for consistency with the other TLS-related extensions:

- Application-Layer Protocol Negotiation (ALPN) Protocol IDs,
- ExtensionType Values,
- Heartbeat Message Types,
- Heartbeat Modes, and
- Supported Groups.

IANA is also to add a reference to this document for the registry whose names have been updated as a result of the above change. The

remainder of this document will use the registry names with the "TLS" prefix.

4. Aligning with RFC 5226

Many of the TLS-related IANA registries were defined prior to [RFC5226] where "IETF Consensus" was used instead of the RFC5226-defined "IETF Review". To align with the new terminology, IANA is to update to use "IETF Review" in place of "IETF Consensus" in the following registries:

- TLS Authorization Data Formats
- TLS Supplemental Data Formats (SupplementalDataType)

This is not a universal change as some registries originally defined with "IETF Consensus" are undergoing other changes either as a result of this document or [I-D.ietf-tls-rfc4492bis].

5. TLS ExtensionType Values

IANA is to update the TLS ExtensionType Values registry as follows:

- Change the registry policy to:

  Values with the first byte in the range 0-254 (decimal) are assigned via Specification Required [RFC5226]. Values with the first byte 255 (decimal) are reserved for Private Use [RFC5226].

- Update the "References" to also refer to this document.

- Add the following note:

  Note: Experts are to verify that there is in fact a publicly available standard.

- Add a "Recommended" column with the contents as listed below. This table has been generated by marking Standards Track RFCs as "Yes" and all others as "No". Future extensions MUST define the value of this column. A Standards Track document [RFC5226] is required to register an extension with the value "Yes".

Extension	Recommended
server_name	Yes
max_fragment_length	Yes

client_certificate_url	Yes
trusted_ca_keys	Yes
truncated_hmac	Yes
status_request	Yes
user_mapping	Yes
client_authz	No
server_authz	No
cert_type	Yes
supported_groups	Yes
ec_point_formats	Yes
srp	No

signature_algorithms	Yes
use_srtp	Yes
heartbeat	Yes
application_layer_protocol_negotiation	Yes
status_request_v2	Yes
signed_certificate_timestamp	No
client_certificate_type	Yes
server_certificate_type	Yes
padding	Yes
encrypt_then_mac	Yes
extended_master_secret	Yes
SessionTicket TLS	Yes
renegotiation_info	Yes

6. TLS Cipher Suite Registry

IANA is to update the TLS Cipher Suite registry as follows:

- Change the registry policy to:

  Values with the first byte in the range 0-254 (decimal) are assigned via Specification Required [RFC5226]. Values with the first byte 255 (decimal) are reserved for Private Use [RFC2434].

- Add a "Recommended" column to the cipher suite registry. The cipher suites that follow in the two tables are marked as "Yes". All other cipher suites are marked as "No".

The cipher suites that follow are standards track server-authenticated (and optionally client-authenticated) cipher suites which are currently available in TLS 1.2. The notable exception are the ECDHE AES GCM cipher suites which are not yet standards track prior to the publication of this specification, but this document promotes those 4 cipher suites to standards track (see TO-DO insert reference).

Cipher Suite Name	Value
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	{0x00,0x9E}
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	{0x00,0x9F}
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2B}
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	{0xC0,0x2C}
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2F}
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	{0xC0,0x30}
TLS_DHE_RSA_WITH_AES_128_CCM	{0xC0,0x9E}
TLS_DHE_RSA_WITH_AES_256_CCM	{0xC0,0x9F}
TLS_DHE_RSA_WITH_AES_128_CCM_8	{0xC0,0xA2}
TLS_DHE_RSA_WITH_AES_256_CCM_8	{0xC0,0xA3}
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xA8}
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xA9}
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xAA}

The cipher suites that follow are standards track ephemeral pre-shared key cipher suites which are available in TLS 1.2. [RFC6655] is inconsistent with respect to the ordering of components within PSK AES CCM cipher suite names; those names are used here without modification.

Cipher Suite Name	Value
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	{0x00,0xAA}
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	{0x00,0xAB}
TLS_DHE_PSK_WITH_AES_128_CCM	{0xC0,0xA6}
TLS_DHE_PSK_WITH_AES_256_CCM	{0xC0,0xA7}
TLS_PSK_DHE_WITH_AES_128_CCM_8	{0xC0,0xAA}
TLS_PSK_DHE_WITH_AES_256_CCM_8	{0xC0,0xAB}

TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	{TBD}
TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	{TBD}
TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256	{TBD}
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	{TBD}
TLS_ECDHE_PSK_WITH_AES_256_CCM_SHA384	{TBD}
TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xAC}
TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xAD}

- Add the following:

  WARNING: Cryptographic algorithms will be broken or weakened over time. Blindly implementing cipher suites listed here is not advised. Implementers and users need to check that the cryptographic algorithms listed continue to provide the expected level of security.

  Note(1): 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 cannot it be used for TLS 1.2. Similarly, TLS 1.2 and lower cipher suites cannot be used with TLS 1.3.

  Note(2): Cipher suites marked as "Yes" are those allocated via Standards Track RFCs. Cipher suites marked as "No" are not; cipher suites marked "No" range from "good" to "bad" from a cryptographic standpoint.

  Note(3): The designated expert [RFC5226] only ensures that the specification is publically available.

7. TLS ClientCertificateType Identifiers

IANA is to update the TLS ClientCertificateType Identifiers registry as follows:

- Change the registry policy to:

  Values in the range 0-223 are assigned via Specification Required [RFC5226]. Values 224-255 are are reserved for Private Use.

- Add the following:

Note: The designated expert [RFC5226] only ensures that the specification is publically available.

8. New Session Ticket TLS Handshake Message Type

To align with TLS implementations and to align the naming nomenclature for other Handshake message types, IANA is to rename entry 4 in the TLS HandshakeType registry to "new_session_ticket (renamed from NewSessionTicket)". IANA is to also add a reference to this document in the Reference column for entry 4 in the TLS HandshakeType registry.

9. Session Ticket TLS Extension

The nomenclature for the registry entries in the TLS ExtensionType Values registry correspond to the presentation language field name except for entry 35. To ensure that the values in the registry are consistently identified in the registry, IANA is to rename entry 35 to "session_ticket (renamed from "SessionTicket TLS")".

10. TLS Exporter Label Registry

IANA is to add the following note to the TLS Exporter Label Registry:

Note: {{RFC5705}} defines keying material exporters for TLS in terms of the TLS

11. Add Missing Item to TLS Alert Registry

IANA is to add the following entry to the TLS Alert Registry (the entry was omitted from the IANA instructions in [RFC7301]):

120 no_application_protocol Y [RFC7301]

12. Orphaned Extensions

To make it clear that (D)TLS 1.3 has orphaned certain extensions (i.e., they are only applicable to version of (D)TLS prior to 1.3), IANA is to add the following to the TLS ExtensionType Values registry:

Note: The following extensions are only applicable to (D)TLS protocol vesions p

13. Orphaned Registries

To make it clear that (D)TLS 1.3 has orphaned certain registries (i.e., they are only applicable to version of (D)TLS protocol versions prior to 1.3), IANA is to:

- Add the following to the TLS Compression Method Identifiers registry [RFC3749]:

  Note: Value 0 (NULL) is the only value in this registry applicable to (D)TLS protocol version 1.3 or later.

- Add the following to the TLS Hash Algorithm [RFC5246] and TLS SignatureAlgorithm registries [RFC5246]:

  Note: The values in this registry are only applicable to (D)TLS protocol versions prior to 1.3.

- Update the "References" in the TLS Compression Method Identifiers, TLS Hash Algorithm [RFC5246] and TLS SignatureAlgorithm registries to also refer to this document.

14. Security Considerations

The authors are fairly certain that there are no security considerations for this document.

15. IANA Considerations

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

16. References

16.1. Normative References

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-18 (work in progress), October 2016.

[RFC3749] Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, DOI 10.17487/RFC3749, May 2004, <http://www.rfc-editor.org/info/rfc3749>.

[RFC4680] Santesson, S., "TLS Handshake Message for Supplemental

Data", RFC 4680, DOI 10.17487/RFC4680, October 2006, <http://www.rfc-editor.org/info/rfc4680>.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, DOI 10.17487/RFC5077, January 2008, <http://www.rfc-editor.org/info/rfc5077>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

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

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <http://www.rfc-editor.org/info/rfc5705>.

[RFC5878] Brown, M. and R. Housley, "Transport Layer Security (TLS) Authorization Extensions", RFC 5878, DOI 10.17487/RFC5878, May 2010, <http://www.rfc-editor.org/info/rfc5878>.

[RFC6520] Seggelmann, R., Tuexen, M., and M. Williams, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension", RFC 6520, DOI 10.17487/RFC6520, February 2012, <http://www.rfc-editor.org/info/rfc6520>.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, DOI 10.17487/RFC6655, July 2012, <http://www.rfc-editor.org/info/rfc6655>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <http://www.rfc-editor.org/info/rfc7301>.

16.2. Informative References

[I-D.ietf-tls-rfc4492bis]
Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", draft-ietf-tls-rfc4492bis-09 (work in progress), October 2016.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, DOI 10.17487/RFC2434, October 1998, <http://www.rfc-editor.org/info/rfc2434>.

[RFC6961] Pettersen, Y., "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", RFC 6961, DOI 10.17487/RFC6961, June 2013, <http://www.rfc-editor.org/info/rfc6961>.

Authors' Addresses

Joe Salowey
Tableau Software

Email: joe@salowey.net

Sean Turner
sn3rd

Email: sean@sn3rd.com