TLS WG
Internet-Draft
Updates: 3749, 5077, 4680, 5246, 5705,
5878, 6520, 7301 (if approved)
Intended status: Standards Track
Expires: August 19, 2018

J. Salowey
Tableau Software
S. Turner
sn3rd

February 15, 2018

IANA Registry Updates for TLS and DTLS
draft-ietf-tls-iana-registry-updates-04

Abstract

This document describes a number of changes to (D)TLS IANA registries that range from adding notes to the registry all the way to changing the registration policy. These changes were mostly motivated by WG review of the (D)TLS-related registries undertaken as part of the TLS1.3 development process. This document updates many (D)TLS RFCs (see updates header).

Status of This Memo

Copyright Notice

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 instructs IANA to make changes to a number of (D)TLS-related IANA registries. These changes were almost entirely motivated by the development of TLS1.3 [I-D.ietf-tls-tls13].

The changes introduced by this document range from simple, e.g., adding notes, to complex, e.g., changing a registry's registration policy. Instead of listing the changes and their rationale in this,

the introductory, section each section provides rationale for the proposed change(s).

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] registries; 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.

3. 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.

4. Add "TLS" to Registry Names

For consistency amongst TLS registries, IANA [SHALL prepend/has prepended] "TLS" to the following registries:

- Application-Layer Protocol Negotiation (ALPN) Protocol IDs [RFC7301],

- ExtensionType Values,

- Heartbeat Message Types [RFC6520], and

- Heartbeat Modes [RFC6520].

IANA [SHALL update/has updated] the reference for these four registries to also refer to this document. The remainder of this document will use the registry names with the "TLS" prefix.

5. Aligning with RFC 8126

Many of the TLS-related IANA registries were defined prior to [RFC8126] where "IETF Consensus" was used instead of the RFC8126-defined "IETF Review". To align with the new terminology, IANA [SHALL update/has updated] the following registries to use "IETF Review" in place of "IETF Consensus":

- TLS Authorization Data Formats [RFC4680]

- TLS Supplemental Data Formats (SupplementalDataType) [RFC5878]

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].

IANA [SHALL update/has updated] the reference for these two registries to also refer to this document.

6. Adding Recommended Column

The instructions in this document add a Recommended column to many of the TLS registries to indicate parameters that are generally recommended for implementations to support. Adding a recommended parameter to a registry or updating a parameter to recommended status requires standards action. Not all parameters defined in standards track documents need to be marked as recommended.

If an item is marked as not recommended it does not necessarily mean that it is flawed, rather, it indicates that either the item has not been through the IETF consensus process, has limited applicability, or is intended only for specific use cases.

7. 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:

- [SHALL rename/has renamed] entry 35 to "session_ticket (renamed from "SessionTicket TLS")" [RFC5077].

- [SHALL add/has added] a reference to this document in the Reference column for entry 35.

8. TLS ExtensionType Values

Experience has shown that the IETF Review registry policy for TLS Extensions was too strict. Based on WG consensus, the decision was taken to change the registration policy to Specification Required [RFC8126] while reserving a small part of the code space for experimental and private use. Therefore, IANA [SHALL update/has updated] the TLS ExtensionType Values registry to:

- Change the registry policy 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].

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

- Add the following notes:

Note: Experts are to verify that there is in fact a publicly available standard. An Internet Draft that is posted and never published or a standard in another standards body, industry consortium, university site, etc. suffices.

Note: As specified in [RFC8126], assignments made in the Private Use space are not generally useful for broad interoperability. It is the responsibility of those making use of the Private Use range to ensure that no conflicts occur (within the intended scope of use). For widespread experiments, temporary reservations are available.

See Section 18 for additional information about the designated expert pool.

Despite wanting to "loosen" the registration policies for TLS Extensions, it is still useful to indicate in the IANA registry which extensions the WG recommends be supported. Therefore, IANA [SHALL update/has updated] the TLS ExtensionType Values registry to:

- 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 the Recommended column. In order to register an extension with the value "Yes", a Standards Track document [RFC8126] is REQUIRED. IESG action is REQUIRED for a Yes->No transition.

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
session_ticket	Yes
renegotiation_info	Yes

NOTE: The following is from [I-D.ietf-tls-tls13] and is included here to ensure aligment between these specifications.

[I-D.ietf-tls-tls13] also uses the TLS ExtensionType Registry originally created in [RFC4366]. IANA has updated it to reference this document. The registry and its allocation policy is listed below:

- IANA [SHALL update/has updated] this registry to include the "key_share", "pre_shared_key", "psk_key_exchange_modes", "early_data", "cookie", "supported_versions", "certificate_authorities", "oid_filters", "post_handshake_auth", and "signature_algorithms_certs", extensions with the values defined in this document and the Recommended value of "Yes".

- IANA [SHALL update/has updated] this registry to include a "TLS 1.3" column which lists the messages in which the extension may appear. This column [SHALL be/has been] initially populated from the table in Section 4.2 of [I-D.ietf-tls-tls13] with any extension not listed there marked as "-" to indicate that it is not used by TLS 1.3.

9. TLS Cipher Suite Registry

Experience has shown that the IETF Consensus registry policy for TLS Cipher Suites was too strict. Based on WG consensus, the decision was taken to change the TLS Cipher Suite registry's registration policy to Specification Required [RFC8126] while reserving a small part of the code space for experimental and private use. Therefore, IANA [SHALL update/has updated] the TLS Cipher Suite registry's policy as follows:

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}}.

See Section 18 for additional information about the designated expert pool.

The cipher suite registry has grown significantly and will continue to do so. To better guide those not intimately involved in TLS, IANA [shall update/has updated] the TLS Cipher Suite registry as follows:

- Add a "Recommended" column to the TLS Cipher Suite registry. The cipher suites that follow in the two tables are marked as "Yes". All other cipher suites are marked as "No". Future cipher suites MUST define the value of the Recommended column. In order to register an extension with the value "Yes, a Standards Track document [RFC8126] is REQUIRED. IESG action is REQUIRED for a Yes->No transition.

  The cipher suites that follow are standards track server-authenticated (and optionally client-authenticated) cipher suites which are currently available in TLS 1.2.

RFC EDITOR: The previous paragraph is for document reviewers and is not meant for the registry.

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_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.

RFC EDITOR: The previous paragraph is for document reviewers and is not meant for the registry.

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_ECDHE_PSK_WITH_AES_128_GCM_SHA256	{TBD}
TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	{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}

Despite the following behavior being misguided, experience has shown that some customers use the IANA registry as checklist against which to measure an implementation's completeness and some implementers blindly implement cipher suites. Therefore, IANA [SHALL add/has added] the following warning to the registry:

WARNING: Cryptographic algorithms and parameters 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.

IANA [SHALL add/has added] the following note to ensure that those that focus on IANA registries are aware that TLS 1.3 [I-D.ietf-tls-tls13] uses the same registry but defines ciphers differently:

Note: 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 be used for TLS 1.2. Similarly, TLS 1.2 and lower cipher suite values cannot be used with TLS 1.3.

IANA [SHALL add/has added] the following notes to document the rules for populating the Recommended column:

Note: 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: CCM_8 cipher suites are not marked as recommended. These cipher suites have a significantly truncated authentication tag that represents a security trade-off that may not be appropriate for general environments.

IANA [SHALL add/has added] the following notes for additional information:

Note: The designated expert [RFC8126] only ensures that the specification is publicly available. An Internet Draft that is posted and never published or a standard in another standards body, industry consortium, university site, etc. suffices.

Note: As specified in [RFC8126], assignments made in the Private Use space are not generally useful for broad interoperability. It is the responsibility of those making use of the Private Use range to ensure that no conflicts occur (within the intended scope of use). For widespread experiments, temporary reservations are available.

IANA [SHALL update/has updated] the reference for this registry to also refer to this document.

10. TLS Supported Groups

Similar to cipher suites, supported groups have proliferated over time and some use the registry to measure implementations. Therefore, IANA [SHALL add/has added] a "Recommended" column with a "Yes" for secp256r1, secp384r1, x25519, and x448 while all others are "No". These "Yes" groups are taken from Standards Track RFCs. Not all groups from [I-D.ietf-tls-rfc4492bis], which is standards track, are marked as "Yes"; these groups apply to TLS 1.3 [I-D.ietf-tls-tls13] and previous versions of TLS. Future supported groups MUST define the value of this column. In order to register an extension with the value "Yes", a Standards Track document [RFC8126] is REQUIRED. IESG action is REQUIRED for a Yes->No transition.

IANA [SHALL add/has added] the following note:

Note: Supported Groups marked as "Yes" are those allocated via Standards Track RFCs. Supported Groups marked as "No" are not; supported groups marked "No" range from "good" to "bad" from a cryptographic standpoint.

Note: The designated expert [RFC8126] only ensures that the specification is publicly available. An Internet Draft that is posted and never published or a standard in another standards body, industry consortium, university site, etc. suffices.

Despite the following behavior being misguided, experience has shown that some customers use the IANA registry as checklist against which to measure an implementation's completeness and some implementers blindly implement groups supported. Therefore, IANA [SHALL add/has added] the following warning to the registry:

WARNING: Cryptographic algorithms and parameters 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.

IANA [SHALL update/has updated] the reference for this registry to also refer to this document.

The value 0 (0x0000) is to be marked as reserved.

11. TLS ClientCertificateType Identifiers

Experience has shown that the IETF Consensus registry policy for TLS ClientCertificateType Identifiers is too strict. Based on WG consensus, the decision was taken to change registration policy to

Specification Required [RFC8126] while reserving a small part of the code space for experimental and prviate use. Therefore, IANA [SHALL update/has updated] the TLS Cipher Suite registry's policy as follows:

Values in the range 0-223 are assigned via Specification Required {{RFC8126}}. Values 224-255 are reserved for Private Use.

See Section 18 for additional information about the designated expert pool.

IANA [SHALL add/has added] the following notes:

Note: The designated expert [RFC8126] only ensures that the specification is publicly available. An Internet Draft that is posted and never published or a standard in another standards body, industry consortium, university site, etc. suffices.

Note: As specified in [RFC8126], assignments made in the Private Use space are not generally useful for broad interoperability. It is the responsibility of those making use of the Private Use range to ensure that no conflicts occur (within the intended scope of use). For widespread experiments, temporary reservations are available.

Note: ClientCertificateType Identifiers marked as "Yes" are those allocated via Standards Track RFCs. ClientCertificateTypes marked as "No" are not.

12. New Session Ticket TLS Handshake Message Type

To align with TLS implementations and to align the naming nomenclature with other Handshake message types, IANA:

- o [SHALL rename/has renamed] entry 4 in the TLS HandshakeType registry to "new_session_ticket (renamed from NewSessionTicket)" [RFC5077].

- o [SHALL add/has added] a reference to this document in the Reference column for entry 4 in the TLS HandshakeType registry.

13. TLS Exporter Label Registry

To aid those reviewers who start with the IANA registry, IANA [SHALL add/has added]:

- o The following note to the TLS Exporter Label Registry:

Note: [RFC5705] defines keying material exporters for TLS in terms of the TLS PRF. [I-D.ietf-tls-tls13] replaced the PRF with HKDF, thus requiring a new construction. The exporter interface remains the same, however the value is computed different.

- A "Recommended" column to the TLS Exporter Label registry. The table that follows has been generated by marking Standards Track RFCs as "Yes" and all others as "No". Future exporters MUST define the value of this column. In order to register an extension with the value "Yes", a Standards Track document [RFC8126] is REQUIRED. IESG action is REQUIRED for a Yes->No transition.

Exporter Value	Recommended
client finished	Yes
server finished	Yes
master secret	Yes
key expansion	Yes
client EAP encryption	Yes
ttls keying material	Yes
ttls challenge	Yes
EXTRACTOR-dtls_srtp	Yes
EXPORTER_DTLS_OVER_SCTP	Yes
EXPORTER: teap session key seed	Yes

To provide additional information for the designated experts, IANA [SHALL add/has added] the following note:

Note: The designated expert [RFC8126] ensures that the specification is publicly available. An Internet Draft that is posted and never published or a standard in another standards body, industry consortium, university site, etc. suffices. 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.

Note: Exporters Labels marked as "Yes" are those allocated via Standards Track RFCs. Exporter Labels marked as "No" are not.

IANA [SHALL update/has updated] the reference for this registry to also refer to this document.

14. Add Missing Item to TLS Alert Registry

IANA [SHALL add/has added] the following entry to the TLS Alert Registry; the entry was omitted from the IANA instructions in [RFC7301]:

```
120   no_application_protocol  Y  [RFC7301]
```

15. TLS Certificate Types

Experience has shown that the IETF Consensus registry policy for TLS Certificate Types is too strict. Based on WG consensus, the decision was taken to change registration policy to Specification Required [RFC8126] while reserving a small part of the code space for experimental and private use. Therefore, IANA [SHALL add/has added] a "Recommended" column to the registry. X.509 and Raw Public Key are "Yes". All others are "No". In order to register an extension with the value "Yes", a Standards Track document [RFC8126] is REQUIRED. Future Certificate Types MUST define the value of this column. A Standards Track document [RFC8126] is REQUIRED to register an entry with the value "Yes". IESG action is REQUIRED for a Yes->No transition.

See Section 18 for additional information about the designated expert pool.

IANA [SHALL add/has added] the following note:

Note: Certificate Types marked as "Yes" are those allocated via Standards Track RFCs. Certificate Types marked as "No" are not.

IANA [SHALL update/has updated] the reference for this registry to also refer this document.

16. Orphaned Extensions

To make it clear that (D)TLS 1.3 has orphaned certain extensions (i.e., some extensions are only applicable to version of (D)TLS prior to 1.3), IANA [SHALL add/has added] the following note to the TLS ExtensionType Values registry:

Note: The following extensions are only applicable to (D)TLS protocol versions prior to 1.3: trusted_ca_keys, truncated_hmac, user_mapping, cert_type, ec_point_formats, srp, status_request_v2, encrypt_then_mac, extended_master_secret, session_ticket, and renegotiation_info. These extensions are not applicable to (D)TLS 1.3.

17. 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:

- [SHALL add/has added] 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.

- [SHALL add/has added] the following to the TLS HashAlgorithm [RFC5246] and TLS SignatureAlgorithm registries [RFC5246]:

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

- [SHALL update/has updated] the "Reference" field in the TLS Compression Method Identifiers, TLS HashAlgorithm and TLS SignatureAlgorithm registries to also refer to this document.

- [SHALL update/has updated] the TLS HashAlgorithm Registry to list values 7-223 as "Reserved" and the TLS SignatureAlgorithm registry to list values 4-223 as "Reserved".

Despite the fact that the HashAlgorithm and SignatureAlgorithm registries are orphaned, it is still import to warn implementers of pre-TLS1.3 implementations about the dangers of blinding implementing cryptographic algorithms. Therefore, IANA [SHALL add/has added] the following warning to the HashAlgorithm and SignatureAlgorithm:

WARNING: Cryptographic algorithms and parameters 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.

18. Designated Expert Pool

Specification Required [RFC8126] registry requests are registered after a three-week review period on the tls-reg-review@ietf.org mailing list, 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.

Registration requests sent to the mailing list for review SHOULD use an appropriate subject (e.g., "Request to register value in TLS bar registry").

Within the review period, the Designated Experts will either approve or deny the registration request, communicating this decision to the review list and IANA. Denials SHOULD include an explanation and, if applicable, suggestions as to how to make the request successful. Registration requests that are undetermined for a period longer than 21 days can be brought to the IESG's attention (using the iesg@ietf.org mailing list) for resolution.

Criteria that SHOULD be applied by the Designated Experts includes determining whether the proposed registration duplicates existing functionality, whether it is likely to be of general applicability or useful only for a single application, and whether the registration description is clear.

IANA MUST only accept registry updates from the Designated Experts and SHOULD direct all requests for registration to the review mailing list.

It is suggested that multiple Designated Experts be appointed who are able to represent the perspectives of different applications using this specification, in order to enable broadly informed review of registration decisions. In cases where a registration decision could be perceived as creating a conflict of interest for a particular Expert, that Expert SHOULD defer to the judgment of the other Experts.

19. 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.

20. IANA Considerations

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

21. References

21.1. Normative References

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-23 (work in progress), January 2018.

[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>.

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

[RFC4680] Santesson, S., "TLS Handshake Message for Supplemental Data", RFC 4680, DOI 10.17487/RFC4680, October 2006, <https://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, <https://www.rfc-editor.org/info/rfc5077>.

[RFC5246] 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/info/rfc5246>.

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <https://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, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7301>.

[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>.

21.2. 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-17 (work in progress), May 2017.

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, DOI 10.17487/RFC4366, April 2006, <https://www.rfc-editor.org/info/rfc4366>.

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

Authors' Addresses

Joe Salowey
Tableau Software

Email: joe@salowey.net

Sean Turner
sn3rd

Email: sean@sn3rd.com