

Internet Engineering Task Force (IETF)
Request for Comments: 8447
Updates: 3749, 5077, 4680, 5246, 5705,
5878, 6520, 7301
Category: Standards Track
ISSN: 2070-1721

J. Salowey
Tableau Software
S. Turner
sn3rd
August 2018

IANA Registry Updates for TLS and DTLS

Abstract

This document describes a number of changes to TLS and DTLS 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 TLS- and DTLS-related registries undertaken as part of the TLS 1.3 development process.

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

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/rfc8447>.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

| | |
|---|----|
| 1. Introduction | 3 |
| 2. Terminology | 3 |
| 3. Adding "TLS" to Registry Names | 3 |
| 4. Aligning with RFC 8126 | 4 |
| 5. Adding "Recommended" Column | 4 |
| 6. Session Ticket TLS Extension | 4 |
| 7. TLS ExtensionType Values | 5 |
| 8. TLS Cipher Suites Registry | 8 |
| 9. TLS Supported Groups | 10 |
| 10. TLS ClientCertificateType Identifiers | 11 |
| 11. New Session Ticket TLS Handshake Message Type | 12 |
| 12. TLS Exporter Labels Registry | 12 |
| 13. Adding Missing Item to TLS Alerts Registry | 13 |
| 14. TLS Certificate Types | 14 |
| 15. Orphaned Registries | 15 |
| 16. Additional Notes | 16 |
| 17. Designated Expert Pool | 16 |
| 18. Security Considerations | 17 |
| 19. IANA Considerations | 18 |
| 20. References | 18 |
| 20.1. Normative References | 18 |
| 20.2. Informative References | 19 |
| Authors' Addresses | 20 |

1. Introduction

Per this document, IANA has made changes to a number of IANA registries related to Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). These changes were almost entirely motivated by the development of TLS 1.3 [RFC8446].

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 here in the introduction, each section provides rationale for the proposed change(s).

This document proposes no changes to the registration policies for TLS Alerts [RFC8446], TLS ContentType [RFC8446], TLS HandshakeType [RFC8446], 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.

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 "TLS" to Registry Names

For consistency amongst TLS registries, IANA has prepended "TLS" to the following registries:

- o Application-Layer Protocol Negotiation (ALPN) Protocol IDs [RFC7301],
- o ExtensionType Values,
- o Heartbeat Message Types [RFC6520], and
- o Heartbeat Modes [RFC6520].

IANA 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.

4. Aligning with RFC 8126

Many of the TLS-related IANA registries had the registration procedure "IETF Consensus", which was changed to "IETF Review" by [RFC8126]. To align with the new terminology, IANA has updated the following registries to "IETF Review":

- o TLS Authorization Data Formats [RFC4680]
- o 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, [RFC8446], or [RFC8422].

IANA has updated the reference for these two registries to also refer to this document.

5. Adding "Recommended" Column

Per this document, a "Recommended" column has been added to many of the TLS registries to indicate parameters that are generally recommended for implementations to support. Adding a "Recommended" parameter (i.e., "Y") 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 not marked as "Recommended" (i.e., "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.

6. 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:

- o has renamed entry 35 to "session_ticket (renamed from "SessionTicket TLS")" [RFC5077].
- o has added a reference to this document in the "Reference" column for entry 35.

7. 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 private use. Therefore, IANA has updated the TLS ExtensionType Values registry as follows:

- o Changed 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].

- o Updated the "Reference" to also refer to this document.

See Section 17 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 has updated the TLS ExtensionType Values registry as follows:

- o Added a "Recommended" column with the contents as listed below. This table has been generated by marking Standards Track RFCs as "Y" and all others as "N". The "Recommended" column is assigned a value of "N" unless explicitly requested, and adding a value with a "Recommended" value of "Y" requires Standards Action [RFC8126]. IESG Approval is REQUIRED for a Y->N transition.

| Extension | Recommended |
|------------------------|-------------|
| server_name | Y |
| max_fragment_length | N |
| client_certificate_url | Y |
| trusted_ca_keys | Y |
| truncated_hmac | Y |
| status_request | Y |
| user_mapping | Y |

| Extension | Recommended |
|--|-------------|
| client_authz | N |
| server_authz | N |
| cert_type | N |
| supported_groups | Y |
| ec_point_formats | Y |
| srp | N |
| signature_algorithms | Y |
| use_srtp | Y |
| heartbeat | Y |
| application_layer_protocol_negotiation | Y |
| status_request_v2 | Y |
| signed_certificate_timestamp | N |
| client_certificate_type | Y |
| server_certificate_type | Y |
| padding | Y |
| encrypt_then_mac | Y |
| extended_master_secret | Y |
| cached_info | Y |
| session_ticket | Y |
| renegotiation_info | Y |

IANA has added the following notes:

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. The expert may provide more in-depth reviews, but their approval should not be taken as an endorsement of the extension.

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: If an item is not marked as "Recommended", 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.

The extensions added by [RFC8446] are omitted from the above table; additionally, `token_binding` is omitted, since [TOKBIND] specifies the value of the "Recommended" column for this extension.

[RFC8446] also uses the TLS ExtensionType Values registry originally created in [RFC4366]. The following text is from [RFC8446] and is included here to ensure alignment between these specifications.

- o IANA 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_cert" extensions with the values defined in [RFC8446] and the "Recommended" value of "Y".
- o IANA has updated this registry to include a "TLS 1.3" column that lists the messages in which the extension may appear. This column has been initially populated from the table in Section 4.2 of [RFC8446] with any extension not listed there marked as "-" to indicate that it is not used by TLS 1.3.

8. TLS Cipher Suites 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 Suites registry's registration policy to Specification Required [RFC8126] while reserving a small part of the code space for private use. Therefore, IANA has updated the TLS Cipher Suites 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 17 for additional information about the designated expert pool.

The TLS Cipher Suites registry has grown significantly and will continue to do so. To better guide those not intimately involved in TLS, IANA has updated the TLS Cipher Suites registry as follows:

- o Added a "Recommended" column to the TLS Cipher Suites registry. The cipher suites that follow in the two tables are marked as "Y". All other cipher suites are marked as "N". The "Recommended" column is assigned a value of "N" unless explicitly requested, and adding a value with a "Recommended" value of "Y" requires Standards Action [RFC8126]. IESG Approval is REQUIRED for a Y->N transition.

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

| 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 that are available in TLS 1.2.

| 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 | {0xD0,0x01} |
| TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 | {0xD0,0x02} |
| TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256 | {0xD0,0x05} |
| TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256 | {0xCC,0xAC} |
| TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256 | {0xCC,0xAD} |

The TLS 1.3 cipher suites specified by [RFC8446] are not listed here; that document provides for their "Recommended" status.

Despite the following behavior being misguided, experience has shown that some customers use the IANA registry as a checklist against which to measure an implementation's completeness, and some implementers blindly implement cipher suites. Therefore, IANA 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 has added the following note to ensure that those that focus on IANA registries are aware that TLS 1.3 [RFC8446] 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 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.

IANA has added the following notes to document the rules for populating the "Recommended" column:

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.

Note: If an item is not marked as "Recommended", 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.

IANA has added the following notes for additional information:

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. The expert may provide more in-depth reviews, but their approval should not be taken as an endorsement of the cipher suite.

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 has updated the reference for this registry to also refer to this document.

9. TLS Supported Groups

Similar to cipher suites, supported groups have proliferated over time, and some use the registry to measure implementations. Therefore, IANA has added a "Recommended" column with a "Y" for secp256r1, secp384r1, x25519, and x448, while all others are "N". These "Y" groups are taken from Standards Track RFCs; [RFC8422] elevates secp256r1 and secp384r1 to Standards Track. Not all groups from [RFC8422], which is Standards Track, are marked as "Y"; these groups apply to TLS 1.3 [RFC8446] and previous versions of TLS. The "Recommended" column is assigned a value of "N" unless explicitly requested, and adding a value with a "Recommended" value of "Y" requires Standards Action [RFC8126]. IESG Approval is REQUIRED for a Y->N transition.

IANA has added the following notes:

Note: If an item is not marked as "Recommended", 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.

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. The expert may provide more in-depth reviews, but their approval should not be taken as an endorsement of the supported group.

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

WARNING: Cryptographic algorithms and parameters will be broken or weakened over time. Blindly implementing supported groups 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 has updated the reference for this registry to also refer to this document.

The value 0 (0x0000) has been marked as reserved.

10. 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 the registration policy to Specification Required [RFC8126] while reserving some of the code space for Standards Track usage and a small part of the code space for private use. Therefore, IANA has updated the TLS ClientCertificateType Identifiers registry's policy as follows:

- Values in the range 0-63 are assigned via Standards Action.
- Values 64-223 are assigned via Specification Required [RFC8126].
- Values 224-255 are reserved for Private Use.

See Section 17 for additional information about the designated expert pool.

IANA has added the following notes:

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. The expert may provide more in-depth reviews, but their approval should not be taken as an endorsement of the identifier.

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.

11. 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 has renamed entry 4 in the TLS HandshakeType registry to "new_session_ticket (renamed from NewSessionTicket)" [RFC5077].
- o has added a reference to this document in the "Reference" column for entry 4 in the TLS HandshakeType registry.

12. TLS Exporter Labels Registry

To aid those reviewers who start with the IANA registry, IANA has added:

- o The following note to the TLS Exporter Labels registry:

Note: [RFC5705] defines keying material exporters for TLS in terms of the TLS PRF. [RFC8446] replaced the PRF with HKDF, thus requiring a new construction. The exporter interface remains the same; however, the value is computed differently.

- o A "Recommended" column to the TLS Exporter Labels registry. The table that follows has been generated by marking Standards Track RFCs as "Y" and all others as "N". The "Recommended" column is assigned a value of "N" unless explicitly requested, and adding a value with a "Recommended" value of "Y" requires Standards Action [RFC8126]. IESG Approval is REQUIRED for a Y->N transition.

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

To provide additional information for the designated experts, IANA has added the following notes:

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. 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.

Note: If an item is not marked as "Recommended", 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.

IANA has updated the reference for this registry to also refer to this document.

13. Adding Missing Item to TLS Alerts Registry

IANA has added the following entry to the TLS Alerts registry; the entry was omitted from the IANA instructions in [RFC7301]:

```
120  no_application_protocol  Y  [RFC7301] [RFC8447]
```

14. 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 private use. Therefore, IANA has changed the TLS Certificate Types registry as follows:

- o Changed the registry policy 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].

- o Added a "Recommended" column to the registry. X.509 and Raw Public Key are "Y". All others are "N". The "Recommended" column is assigned a value of "N" unless explicitly requested, and adding a value with a "Recommended" value of "Y" requires Standards Action [RFC8126]. IESG Approval is REQUIRED for a Y->N transition.

See Section 17 for additional information about the designated expert pool.

IANA has added the following notes:

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. The expert may provide more in-depth reviews, but their approval should not be taken as an endorsement of the certificate type.

Note: If an item is not marked as "Recommended", 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.

IANA has updated the reference for this registry to also refer this document.

15. 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:

- o 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.

- o 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. (D)TLS 1.3 and later versions' values are registered in the TLS SignatureScheme registry.

- o has updated the "Reference" field in the TLS Compression Method Identifiers, TLS HashAlgorithm and TLS SignatureAlgorithm registries to also refer to this document.
- o has updated the TLS HashAlgorithm registry to list values 7 and 9-223 as "Reserved" and the TLS SignatureAlgorithm registry to list values 4-6 and 9-223 as "Reserved".
- o has added the following to the TLS ClientCertificateType Identifiers registry [RFC5246]:

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

Despite the fact that the TLS HashAlgorithm and SignatureAlgorithm registries are orphaned, it is still important to warn implementers of pre-TLS1.3 implementations about the dangers of blindly implementing cryptographic algorithms. Therefore, IANA has added the following warning to the TLS HashAlgorithm and SignatureAlgorithm registries:

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

16. Additional Notes

IANA has added the following warning and note to the TLS SignatureScheme registry:

WARNING: Cryptographic algorithms and parameters will be broken or weakened over time. Blindly implementing signature schemes 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: 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 has added the following notes to the TLS PskKeyExchangeMode registry:

Note: If an item is not marked as "Recommended", 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.

Note: The role of the designated expert is described in RFC 8447. The designated expert [RFC8126] ensures that the specification is publicly available. It is sufficient to have an Internet-Draft (that is posted and never published as an RFC) or a document from another standards body, industry consortium, university site, etc. The expert may provide more in depth reviews, but their approval should not be taken as an endorsement of the key exchange mode.

17. 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.

18. 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.

19. IANA Considerations

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

20. References

20.1. 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>>.
- [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] Seggellmann, 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>>.

- [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>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.

20.2. Informative References

- [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>>.
- [RFC8422] Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", RFC 8422, DOI 10.17487/RFC8422, August 2018, <<https://www.rfc-editor.org/info/rfc8422>>.
- [TOKBIND] Popov, A., Nystrom, M., Balfanz, D., and A. Langley, "Transport Layer Security (TLS) Extension for Token Binding Protocol Negotiation", Work in Progress, draft-ietf-tokbind-negotiation-14, May 2018.

Authors' Addresses

Joe Salowey
Tableau Software

Email: joe@salowey.net

Sean Turner
sn3rd

Email: sean@sn3rd.com

