Stream: Internet Engineering Task Force (IETF)
RFC: 8996
BCP: 195
Obsoletes: 5469, 7507
Updates:
3261, 3329, 3436, 3470, 3501, 3552, 3568, 3656, 3749, 3767, 3856, 3871, 3887, 3903, 3943, 3983, 4097, 4111, 4162, 4168, 4217,
6750, 7030, 7465, 7525, 7562, 7568, 8261, 8422
Category: Best Current Practice
Published: March 2021
ISSN: 2070-1721
Authors: K. Moriarty, *Dell EMC*
S. Farrell, *Trinity College Dublin*

RFC 8996
Deprecating TLS 1.0 and TLS 1.1

Abstract

This document formally deprecates Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346). Accordingly, those documents have been moved to Historic status. These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. TLS version 1.2 became the recommended version for IETF protocols in 2008 (subsequently being obsoleted by TLS version 1.3 in 2018), providing sufficient time to transition away from older versions. Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance.

This document also deprecates Datagram TLS (DTLS) version 1.0 (RFC 4347) but not DTLS version 1.2, and there is no DTLS version 1.1.

This document updates many RFCs that normatively refer to TLS version 1.0 or TLS version 1.1, as described herein. This document also updates the best practices for TLS usage in RFC 7525; hence, it is part of BCP 195.

Status of This Memo

This memo documents an Internet Best Current Practice.

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 BCPs 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/rfc8996.

Copyright Notice

Table of Contents

1. Introduction
   1.1. RFCs Updated
   1.2. Terminology
2. Support for Deprecation
3. SHA-1 Usage Problematic in TLS 1.0 and TLS 1.1
4. Do Not Use TLS 1.0
5. Do Not Use TLS 1.1
6. Updates to RFC 7525
7. Operational Considerations
8. Security Considerations
9. IANA Considerations
10. References
   10.1. Normative References
   10.2. Informative References

Acknowledgements

Authors' Addresses

1. Introduction

Transport Layer Security (TLS) versions 1.0 [RFC2246] and 1.1 [RFC4346] were superseded by TLS 1.2 [RFC5246] in 2008, which has now itself been superseded by TLS 1.3 [RFC8446]. Datagram Transport Layer Security (DTLS) version 1.0 [RFC4347] was superseded by DTLS 1.2 [RFC6347] in 2012. Therefore, it is timely to further deprecate TLS 1.0, TLS 1.1, and DTLS 1.0. Accordingly, the aforementioned documents have been moved to Historic status.

Technical reasons for deprecating these versions include:

- They require the implementation of older cipher suites that are no longer desirable for cryptographic reasons, e.g., TLS 1.0 makes TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA mandatory to implement.
- There is a lack of support for current recommended cipher suites, especially authenticated encryption with associated data (AEAD) ciphers, which were not supported prior to TLS 1.2. Note that registry entries for no-longer-desirable ciphersuites remain in the registries, but many TLS registries are being updated through [RFC8447], which indicates that such entries are not recommended by the IETF.
- The integrity of the handshake depends on SHA-1 hash.
- The authentication of the peers depends on SHA-1 signatures.
- Support for four TLS protocol versions increases the likelihood of misconfiguration.
- At least one widely used library has plans to drop TLS 1.1 and TLS 1.0 support in upcoming releases; products using such libraries would need to use older versions of the libraries to support TLS 1.0 and TLS 1.1, which is clearly undesirable.

Deprecation of these versions is intended to assist developers as additional justification to no longer support older (D)TLS versions and to migrate to a minimum of (D)TLS 1.2. Deprecation also assists product teams with phasing out support for the older versions, to reduce the attack surface and the scope of maintenance for protocols in their offerings.

1.1. RFCs Updated

This document updates the following RFCs that normatively reference TLS 1.0, TLS 1.1, or DTLS 1.0. The update is to obsolete usage of these older versions. Fallback to these versions is prohibited through this update. Specific references to mandatory minimum protocol versions of TLS 1.0 or TLS 1.1 are replaced by TLS 1.2, and references to minimum protocol version DTLS 1.0 are replaced by DTLS 1.2. Statements that "TLS 1.0 is the most widely deployed version and will provide the broadest interoperability" are removed without replacement.

[RFC8422] [RFC8261] [RFC7568] [RFC7562] [RFC7525] [RFC7465] [RFC7030] [RFC6750] [RFC6749] [RFC6739] [RFC6084] [RFC6083] [RFC6367] [RFC6353] [RFC6176] [RFC6042] [RFC6012] [RFC5878] [RFC5734] [RFC5456] [RFC5422] [RFC5415] [RFC5364] [RFC5281] [RFC5263] [RFC5238] [RFC5216] [RFC5158] [RFC5091] [RFC5054] [RFC5049] [RFC5024] [RFC5023] [RFC5019] [RFC5018] [RFC4992] [RFC4976] [RFC4975] [RFC4964] [RFC4851] [RFC4823] [RFC4791] [RFC4785] [RFC4732] [RFC4712]

[RFC4681] [RFC4680] [RFC4642] [RFC4616] [RFC4582] [RFC4540] [RFC4531] [RFC4513] [RFC4497] [RFC4279] [RFC4261] [RFC4235] [RFC4217] [RFC4168] [RFC4162] [RFC4111] [RFC4097] [RFC3983] [RFC3943] [RFC3903] [RFC3887] [RFC3871] [RFC3856] [RFC3767] [RFC3749] [RFC3656] [RFC3568] [RFC3552] [RFC3501] [RFC3470] [RFC3436] [RFC3329] [RFC3261]

The status of [RFC7562], [RFC6042], [RFC5456], [RFC5024], [RFC4540], and [RFC3656] will be updated with permission of the Independent Submissions Editor.

In addition, these RFCs normatively refer to TLS 1.0 or TLS 1.1 and have already been obsoleted; they are still listed here and marked as updated by this document in order to reiterate that any usage of the obsolete protocol should use modern TLS: [RFC5953], [RFC5101], [RFC5081], [RFC5077], [RFC4934], [RFC4572], [RFC4507], [RFC4492], [RFC4366], [RFC4347], [RFC4244], [RFC4132], [RFC3920], [RFC3734], [RFC3588], [RFC3546], [RFC3489], and [RFC3316].

Note that [RFC4642] has already been updated by [RFC8143], which makes an overlapping, but not quite identical, update as this document.

[RFC6614] has a requirement for TLS 1.1 or later, although it only makes an informative reference to [RFC4346]. This requirement is updated to be for TLS 1.2 or later.

[RFC6460], [RFC4744], and [RFC4743] are already Historic; they are still listed here and marked as updated by this document in order to reiterate that any usage of the obsolete protocol should use modern TLS.

This document updates DTLS [RFC6347]. [RFC6347] had allowed for negotiating the use of DTLS 1.0, which is now forbidden.

The DES and International Data Encryption Algorithm (IDEA) cipher suites specified in [RFC5469] were specifically removed from TLS 1.2 by [RFC5246]; since the only versions of TLS for which their usage is defined are now Historic, [RFC5469] has been moved to Historic as well.

The version-fallback Signaling Cipher Suite Value specified in [RFC7507] was defined to detect when a given client and server negotiate a lower version of (D)TLS than their highest shared version. TLS 1.3 ([RFC8446]) incorporates a different mechanism that achieves this purpose, via sentinel values in the ServerHello.Random field. With (D)TLS versions prior to 1.2 fully deprecated, the only way for (D)TLS implementations to negotiate a lower version than their highest shared version would be to negotiate (D)TLS 1.2 while supporting (D)TLS 1.3; supporting (D)TLS 1.3 implies support for the ServerHello.Random mechanism. Accordingly, the functionality from [RFC7507] has been superseded, and this document marks it as Obsolete.

1.2. 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.

2. Support for Deprecation

Specific details on attacks against TLS 1.0 and TLS 1.1, as well as their mitigations, are provided in [NIST800-52r2], [RFC7457], and other RFCs referenced therein. Although mitigations for the current known vulnerabilities have been developed, any future issues discovered in old protocol versions might not be mitigated in older library versions when newer library versions do not support those old protocols.

For example, NIST has provided the following rationale, copied with permission from Section 1.1, "History of TLS", of [NIST800-52r2]:

> TLS 1.1, specified in RFC 4346 [24], was developed to address weaknesses discovered in TLS 1.0, primarily in the areas of initialization vector selection and padding error processing. Initialization vectors were made explicit to prevent a certain class of attacks on the Cipher Block Chaining (CBC) mode of operation used by TLS. The handling of padding errors was altered to treat a padding error as a bad message authentication code rather than a decryption failure. In addition, the TLS 1.1 RFC acknowledges attacks on CBC mode that rely on the time to compute the message authentication code (MAC). The TLS 1.1 specification states that to defend against such attacks, an implementation must process records in the same manner regardless of whether padding errors exist. Further implementation considerations for CBC modes (which were not included in RFC 4346 [24]) are discussed in Section 3.3.2.
>
> TLS 1.2, specified in RFC 5246 [25], made several cryptographic enhancements, particularly in the area of hash functions, with the ability to use or specify the SHA-2 family of algorithms for hash, MAC, and Pseudorandom Function (PRF) computations. TLS 1.2 also adds authenticated encryption with associated data (AEAD) cipher suites.
>
> TLS 1.3, specified in RFC 8446 [57], represents a significant change to TLS that aims to address threats that have arisen over the years. Among the changes are a new handshake protocol, a new key derivation process that uses the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [37], and the removal of cipher suites that use RSA key transport or static Diffie-Hellman (DH) [sic] key exchanges, the CBC mode of operation, or SHA-1. Many extensions defined for use with TLS 1.2 and previous versions cannot be used with TLS 1.3.

3. SHA-1 Usage Problematic in TLS 1.0 and TLS 1.1

The integrity of both TLS 1.0 and TLS 1.1 depends on a running SHA-1 hash of the exchanged messages. This makes it possible to perform a downgrade attack on the handshake by an attacker able to perform 2^{77} operations, well below the acceptable modern security margin.

Similarly, the authentication of the handshake depends on signatures made using a SHA-1 hash or a concatenation of MD5 and SHA-1 hashes that is not appreciably stronger than a SHA-1 hash, allowing the attacker to impersonate a server when it is able to break the severely weakened SHA-1 hash.

Neither TLS 1.0 nor TLS 1.1 allows the peers to select a stronger hash for signatures in the ServerKeyExchange or CertificateVerify messages, making the only upgrade path the use of a newer protocol version.

See [Bhargavan2016] for additional details.

4. Do Not Use TLS 1.0

TLS 1.0 **MUST NOT** be used. Negotiation of TLS 1.0 from any version of TLS **MUST NOT** be permitted.

Any other version of TLS is more secure than TLS 1.0. While TLS 1.0 can be configured to prevent some types of interception, using the highest version available is preferred.

Pragmatically, clients **MUST NOT** send a ClientHello with ClientHello.client_version set to {03,01}. Similarly, servers **MUST NOT** send a ServerHello with ServerHello.server_version set to {03,01}. Any party receiving a Hello message with the protocol version set to {03,01} **MUST** respond with a "protocol_version" alert message and close the connection.

Historically, TLS specifications were not clear on what the record layer version number (TLSPlaintext.version) could contain when sending a ClientHello message. Appendix E of [RFC5246] notes that TLSPlaintext.version could be selected to maximize interoperability, though no definitive value is identified as ideal. That guidance is still applicable; therefore, TLS servers **MUST** accept any value {03,XX} (including {03,00}) as the record layer version number for ClientHello, but they **MUST NOT** negotiate TLS 1.0.

5. Do Not Use TLS 1.1

TLS 1.1 **MUST NOT** be used. Negotiation of TLS 1.1 from any version of TLS **MUST NOT** be permitted.

Pragmatically, clients **MUST NOT** send a ClientHello with ClientHello.client_version set to {03,02}. Similarly, servers **MUST NOT** send a ServerHello with ServerHello.server_version set to {03,02}. Any party receiving a Hello message with the protocol version set to {03,02} **MUST** respond with a "protocol_version" alert message and close the connection.

Any newer version of TLS is more secure than TLS 1.1. While TLS 1.1 can be configured to prevent some types of interception, using the highest version available is preferred. Support for TLS 1.1 is dwindling in libraries and will impact security going forward if mitigations for attacks cannot be easily addressed and supported in older libraries.

Historically, TLS specifications were not clear on what the record layer version number (TLSPlaintext.version) could contain when sending a ClientHello message. Appendix E of [RFC5246] notes that TLSPlaintext.version could be selected to maximize interoperability, though no definitive value is identified as ideal. That guidance is still applicable; therefore, TLS servers **MUST** accept any value {03,XX} (including {03,00}) as the record layer version number for ClientHello, but they **MUST NOT** negotiate TLS 1.1.

6. Updates to RFC 7525

"Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" [RFC7525] is BCP 195, which is the most recent Best Current Practice for implementing TLS and was based on TLS 1.2. At the time of publication, TLS 1.0 and TLS 1.1 had not yet been deprecated. As such, BCP 195 is called out specifically to update text implementing the deprecation recommendations of this document.

This document updates Section 3.1.1 of [RFC7525] by changing **SHOULD NOT** to **MUST NOT** as follows:

- Implementations **MUST NOT** negotiate TLS version 1.0 [RFC2246].

  Rationale: TLS 1.0 (published in 1999) does not support many modern, strong cipher suites. In addition, TLS 1.0 lacks a per-record Initialization Vector (IV) for CBC-based cipher suites and does not warn against common padding errors.

- Implementations **MUST NOT** negotiate TLS version 1.1 [RFC4346].

  Rationale: TLS 1.1 (published in 2006) is a security improvement over TLS 1.0 but still does not support certain stronger cipher suites.

This document updates Section 3.1.2 of [RFC7525] by changing **SHOULD NOT** to **MUST NOT** and adding a reference to RFC 6347 as follows:

- Implementations **MUST NOT** negotiate DTLS version 1.0 [RFC4347] [RFC6347].

  Version 1.0 of DTLS correlates to version 1.1 of TLS (see above).

7. Operational Considerations

This document is part of BCP 195 and, as such, reflects the understanding of the IETF (at the time of this document's publication) as to the best practices for TLS and DTLS usage.

Though TLS 1.1 has been obsolete since the publication of [RFC5246] in 2008, and DTLS 1.0 has been obsolete since the publication of [RFC6347] in 2012, there may remain some systems in operation that do not support (D)TLS 1.2 or higher. Adopting the practices recommended by this document for any systems that need to communicate with the aforementioned class of systems will cause failure to interoperate. However, disregarding the recommendations of this document in order to continue to interoperate with the aforementioned class of systems incurs some

amount of risk. The nature of the risks incurred by operating in contravention to the recommendations of this document are discussed in Sections 2 and 3, and knowledge of those risks should be used along with any potential mitigating factors and the risks inherent to updating the systems in question when deciding how quickly to adopt the recommendations specified in this document.

8. Security Considerations

This document deprecates two older TLS protocol versions and one older DTLS protocol version for security reasons already described. The attack surface is reduced when there are a smaller number of supported protocols and fallback options are removed.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. 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>.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, DOI 10.17487/RFC2246, January 1999, <https://www.rfc-editor.org/info/rfc2246>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3329] Arkko, J., Torvinen, V., Camarillo, G., Niemi, A., and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329, DOI 10.17487/RFC3329, January 2003, <https://www.rfc-editor.org/info/rfc3329>.

[RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, DOI 10.17487/RFC3436, December 2002, <https://www.rfc-editor.org/info/rfc3436>.

[RFC3470] Hollenbeck, S., Rose, M., and L. Masinter, "Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols", BCP 70, RFC 3470, DOI 10.17487/RFC3470, January 2003, <https://www.rfc-editor.org/info/rfc3470>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/info/rfc3501>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC3568] Barbir, A., Cain, B., Nair, R., and O. Spatscheck, "Known Content Network (CN) Request-Routing Mechanisms", RFC 3568, DOI 10.17487/RFC3568, July 2003, <https://www.rfc-editor.org/info/rfc3568>.

[RFC3656] Siemborski, R., "The Mailbox Update (MUPDATE) Distributed Mailbox Database Protocol", RFC 3656, DOI 10.17487/RFC3656, December 2003, <https://www.rfc-editor.org/info/rfc3656>.

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

[RFC3767] Farrell, S., Ed., "Securely Available Credentials Protocol", RFC 3767, DOI 10.17487/RFC3767, June 2004, <https://www.rfc-editor.org/info/rfc3767>.

[RFC3856] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, DOI 10.17487/RFC3856, August 2004, <https://www.rfc-editor.org/info/rfc3856>.

[RFC3871] Jones, G., Ed., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", RFC 3871, DOI 10.17487/RFC3871, September 2004, <https://www.rfc-editor.org/info/rfc3871>.

[RFC3887] Hansen, T., "Message Tracking Query Protocol", RFC 3887, DOI 10.17487/RFC3887, September 2004, <https://www.rfc-editor.org/info/rfc3887>.

[RFC3903] Niemi, A., Ed., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, DOI 10.17487/RFC3903, October 2004, <https://www.rfc-editor.org/info/rfc3903>.

[RFC3943] Friend, R., "Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)", RFC 3943, DOI 10.17487/RFC3943, November 2004, <https://www.rfc-editor.org/info/rfc3943>.

[RFC3983] Newton, A. and M. Sanz, "Using the Internet Registry Information Service (IRIS) over the Blocks Extensible Exchange Protocol (BEEP)", RFC 3983, DOI 10.17487/RFC3983, January 2005, <https://www.rfc-editor.org/info/rfc3983>.

[RFC4097] Barnes, M., Ed., "Middlebox Communications (MIDCOM) Protocol Evaluation", RFC 4097, DOI 10.17487/RFC4097, June 2005, <https://www.rfc-editor.org/info/rfc4097>.

[RFC4111] Fang, L., Ed., "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4111, DOI 10.17487/RFC4111, July 2005, <https://www.rfc-editor.org/info/rfc4111>.

[RFC4162] Lee, H.J., Yoon, J.H., and J.I. Lee, "Addition of SEED Cipher Suites to Transport Layer Security (TLS)", RFC 4162, DOI 10.17487/RFC4162, August 2005, <https://www.rfc-editor.org/info/rfc4162>.

[RFC4168] Rosenberg, J., Schulzrinne, H., and G. Camarillo, "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)", RFC 4168, DOI 10.17487/RFC4168, October 2005, <https://www.rfc-editor.org/info/rfc4168>.

[RFC4217] Ford-Hutchinson, P., "Securing FTP with TLS", RFC 4217, DOI 10.17487/RFC4217, October 2005, <https://www.rfc-editor.org/info/rfc4217>.

[RFC4235] Rosenberg, J., Schulzrinne, H., and R. Mahy, Ed., "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", RFC 4235, DOI 10.17487/RFC4235, November 2005, <https://www.rfc-editor.org/info/rfc4235>.

[RFC4261] Walker, J. and A. Kulkarni, Ed., "Common Open Policy Service (COPS) Over Transport Layer Security (TLS)", RFC 4261, DOI 10.17487/RFC4261, December 2005, <https://www.rfc-editor.org/info/rfc4261>.

[RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <https://www.rfc-editor.org/info/rfc4279>.

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

[RFC4497] Elwell, J., Derks, F., Mourot, P., and O. Rousseau, "Interworking between the Session Initiation Protocol (SIP) and QSIG", BCP 117, RFC 4497, DOI 10.17487/RFC4497, May 2006, <https://www.rfc-editor.org/info/rfc4497>.

[RFC4513] Harrison, R., Ed., "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms", RFC 4513, DOI 10.17487/RFC4513, June 2006, <https://www.rfc-editor.org/info/rfc4513>.

[RFC4531] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Turn Operation", RFC 4531, DOI 10.17487/RFC4531, June 2006, <https://www.rfc-editor.org/info/rfc4531>.

[RFC4540] Stiemerling, M., Quittek, J., and C. Cadar, "NEC's Simple Middlebox Configuration (SIMCO) Protocol Version 3.0", RFC 4540, DOI 10.17487/RFC4540, May 2006, <https://www.rfc-editor.org/info/rfc4540>.

[RFC4582] Camarillo, G., Ott, J., and K. Drage, "The Binary Floor Control Protocol (BFCP)", RFC 4582, DOI 10.17487/RFC4582, November 2006, <https://www.rfc-editor.org/info/rfc4582>.

[RFC4616] Zeilenga, K., Ed., "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism", RFC 4616, DOI 10.17487/RFC4616, August 2006, <https://www.rfc-editor.org/info/rfc4616>.

[RFC4642] Murchison, K., Vinocur, J., and C. Newman, "Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)", RFC 4642, DOI 10.17487/RFC4642, October 2006, <https://www.rfc-editor.org/info/rfc4642>.

[RFC4680] Santesson, S., "TLS Handshake Message for Supplemental Data", RFC 4680, DOI 10.17487/RFC4680, October 2006, <https://www.rfc-editor.org/info/rfc4680>.

[RFC4681] Santesson, S., Medvinsky, A., and J. Ball, "TLS User Mapping Extension", RFC 4681, DOI 10.17487/RFC4681, October 2006, <https://www.rfc-editor.org/info/rfc4681>.

[RFC4712] Siddiqui, A., Romascanu, D., Golovinsky, E., Rahman, M., and Y. Kim, "Transport Mappings for Real-time Application Quality-of-Service Monitoring (RAQMON) Protocol Data Unit (PDU)", RFC 4712, DOI 10.17487/RFC4712, October 2006, <https://www.rfc-editor.org/info/rfc4712>.

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <https://www.rfc-editor.org/info/rfc4732>.

[RFC4743] Goddard, T., "Using NETCONF over the Simple Object Access Protocol (SOAP)", RFC 4743, DOI 10.17487/RFC4743, December 2006, <https://www.rfc-editor.org/info/rfc4743>.

[RFC4744] Lear, E. and K. Crozier, "Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)", RFC 4744, DOI 10.17487/RFC4744, December 2006, <https://www.rfc-editor.org/info/rfc4744>.

[RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, DOI 10.17487/RFC4785, January 2007, <https://www.rfc-editor.org/info/rfc4785>.

[RFC4791] Daboo, C., Desruisseaux, B., and L. Dusseault, "Calendaring Extensions to WebDAV (CalDAV)", RFC 4791, DOI 10.17487/RFC4791, March 2007, <https://www.rfc-editor.org/info/rfc4791>.

[RFC4823] Harding, T. and R. Scott, "FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet", RFC 4823, DOI 10.17487/RFC4823, April 2007, <https://www.rfc-editor.org/info/rfc4823>.

[RFC4851] Cam-Winget, N., McGrew, D., Salowey, J., and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)", RFC 4851, DOI 10.17487/RFC4851, May 2007, <https://www.rfc-editor.org/info/rfc4851>.

[RFC4964] Allen, A., Ed., Holm, J., and T. Hallin, "The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular", RFC 4964, DOI 10.17487/RFC4964, September 2007, <https://www.rfc-editor.org/info/rfc4964>.

[RFC4975] Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., "The Message Session Relay Protocol (MSRP)", RFC 4975, DOI 10.17487/RFC4975, September 2007, <https://www.rfc-editor.org/info/rfc4975>.

[RFC4976] Jennings, C., Mahy, R., and A. B. Roach, "Relay Extensions for the Message Sessions Relay Protocol (MSRP)", RFC 4976, DOI 10.17487/RFC4976, September 2007, <https://www.rfc-editor.org/info/rfc4976>.

[RFC4992] Newton, A., "XML Pipelining with Chunks for the Internet Registry Information Service", RFC 4992, DOI 10.17487/RFC4992, August 2007, <https://www.rfc-editor.org/info/rfc4992>.

[RFC5018] Camarillo, G., "Connection Establishment in the Binary Floor Control Protocol (BFCP)", RFC 5018, DOI 10.17487/RFC5018, September 2007, <https://www.rfc-editor.org/info/rfc5018>.

[RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, DOI 10.17487/RFC5019, September 2007, <https://www.rfc-editor.org/info/rfc5019>.

[RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <https://www.rfc-editor.org/info/rfc5023>.

[RFC5024] Friend, I., "ODETTE File Transfer Protocol 2.0", RFC 5024, DOI 10.17487/RFC5024, November 2007, <https://www.rfc-editor.org/info/rfc5024>.

[RFC5049] Bormann, C., Liu, Z., Price, R., and G. Camarillo, Ed., "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)", RFC 5049, DOI 10.17487/RFC5049, December 2007, <https://www.rfc-editor.org/info/rfc5049>.

[RFC5054] Taylor, D., Wu, T., Mavrogiannopoulos, N., and T. Perrin, "Using the Secure Remote Password (SRP) Protocol for TLS Authentication", RFC 5054, DOI 10.17487/RFC5054, November 2007, <https://www.rfc-editor.org/info/rfc5054>.

[RFC5091] Boyen, X. and L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, DOI 10.17487/RFC5091, December 2007, <https://www.rfc-editor.org/info/rfc5091>.

[RFC5158] Huston, G., "6to4 Reverse DNS Delegation Specification", RFC 5158, DOI 10.17487/RFC5158, March 2008, <https://www.rfc-editor.org/info/rfc5158>.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI 10.17487/RFC5216, March 2008, <https://www.rfc-editor.org/info/rfc5216>.

[RFC5238] Phelan, T., "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, DOI 10.17487/RFC5238, May 2008, <https://www.rfc-editor.org/info/rfc5238>.

[RFC5263] Lonnfors, M., Costa-Requena, J., Leppanen, E., and H. Khartabil, "Session Initiation Protocol (SIP) Extension for Partial Notification of Presence Information", RFC 5263, DOI 10.17487/RFC5263, September 2008, <https://www.rfc-editor.org/info/rfc5263>.

[RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, DOI 10.17487/RFC5281, August 2008, <https://www.rfc-editor.org/info/rfc5281>.

[RFC5364] Garcia-Martin, M. and G. Camarillo, "Extensible Markup Language (XML) Format Extension for Representing Copy Control Attributes in Resource Lists", RFC 5364, DOI 10.17487/RFC5364, October 2008, <https://www.rfc-editor.org/info/rfc5364>.

[RFC5422] Cam-Winget, N., McGrew, D., Salowey, J., and H. Zhou, "Dynamic Provisioning Using Flexible Authentication via Secure Tunneling Extensible Authentication Protocol (EAP-FAST)", RFC 5422, DOI 10.17487/RFC5422, March 2009, <https://www.rfc-editor.org/info/rfc5422>.

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

[RFC5734] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport over TCP", STD 69, RFC 5734, DOI 10.17487/RFC5734, August 2009, <https://www.rfc-editor.org/info/rfc5734>.

[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>.

[RFC5953] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5953, DOI 10.17487/RFC5953, August 2010, <https://www.rfc-editor.org/info/rfc5953>.

[RFC6042] Keromytis, A., "Transport Layer Security (TLS) Authorization Using KeyNote", RFC 6042, DOI 10.17487/RFC6042, October 2010, <https://www.rfc-editor.org/info/rfc6042>.

[RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, DOI 10.17487/RFC6176, March 2011, <https://www.rfc-editor.org/info/rfc6176>.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 6353, DOI 10.17487/RFC6353, July 2011, <https://www.rfc-editor.org/info/rfc6353>.

[RFC6367] Kanno, S. and M. Kanda, "Addition of the Camellia Cipher Suites to Transport Layer Security (TLS)", RFC 6367, DOI 10.17487/RFC6367, September 2011, <https://www.rfc-editor.org/info/rfc6367>.

[RFC6739] Schulzrinne, H. and H. Tschofenig, "Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol", RFC 6739, DOI 10.17487/RFC6739, October 2012, <https://www.rfc-editor.org/info/rfc6739>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC6750] Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, DOI 10.17487/RFC6750, October 2012, <https://www.rfc-editor.org/info/rfc6750>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

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

[RFC7507] Moeller, B. and A. Langley, "TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks", RFC 7507, DOI 10.17487/RFC7507, April 2015, <https://www.rfc-editor.org/info/rfc7507>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[RFC7562] Thakore, D., "Transport Layer Security (TLS) Authorization Using Digital Transmission Content Protection (DTCP) Certificates", RFC 7562, DOI 10.17487/RFC7562, July 2015, <https://www.rfc-editor.org/info/rfc7562>.

[RFC7568] Barnes, R., Thomson, M., Pironti, A., and A. Langley, "Deprecating Secure Sockets Layer Version 3.0", RFC 7568, DOI 10.17487/RFC7568, June 2015, <https://www.rfc-editor.org/info/rfc7568>.

[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>.

[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>.

10.2. Informative References

[Bhargavan2016] Bhargavan, K. and G. Leuren, "Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH", DOI 10.14722/ndss.2016.23418, February 2016, <https://www.mitls.org/downloads/transcript-collisions.pdf>.

[NIST800-52r2] National Institute of Standards and Technology, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations NIST SP800-52r2", DOI 10.6028/NIST.SP.800-52r2, August 2019, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>.

[RFC3316] Arkko, J., Kuijpers, G., Soliman, H., Loughney, J., and J. Wiljakka, "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts", RFC 3316, DOI 10.17487/RFC3316, April 2003, <https://www.rfc-editor.org/info/rfc3316>.

[RFC3489] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, DOI 10.17487/RFC3489, March 2003, <https://www.rfc-editor.org/info/rfc3489>.

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, DOI 10.17487/RFC3546, June 2003, <https://www.rfc-editor.org/info/rfc3546>.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, DOI 10.17487/RFC3588, September 2003, <https://www.rfc-editor.org/info/rfc3588>.

[RFC3734] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport Over TCP", RFC 3734, DOI 10.17487/RFC3734, March 2004, <https://www.rfc-editor.org/info/rfc3734>.

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, DOI 10.17487/RFC3920, October 2004, <https://www.rfc-editor.org/info/rfc3920>.

[RFC4132] Moriai, S., Kato, A., and M. Kanda, "Addition of Camellia Cipher Suites to Transport Layer Security (TLS)", RFC 4132, DOI 10.17487/RFC4132, July 2005, <https://www.rfc-editor.org/info/rfc4132>.

[RFC4244] Barnes, M., Ed., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, DOI 10.17487/RFC4244, November 2005, <https://www.rfc-editor.org/info/rfc4244>.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, DOI 10.17487/RFC4347, April 2006, <https://www.rfc-editor.org/info/rfc4347>.

[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>.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, DOI 10.17487/RFC4492, May 2006, <https://www.rfc-editor.org/info/rfc4492>.

[RFC4507] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 4507, DOI 10.17487/RFC4507, May 2006, <https://www.rfc-editor.org/info/rfc4507>.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, DOI 10.17487/RFC4572, July 2006, <https://www.rfc-editor.org/info/rfc4572>.

[RFC4934] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport Over TCP", RFC 4934, DOI 10.17487/RFC4934, May 2007, <https://www.rfc-editor.org/info/rfc4934>.

[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>.

[RFC5081] Mavrogiannopoulos, N., "Using OpenPGP Keys for Transport Layer Security (TLS) Authentication", RFC 5081, DOI 10.17487/RFC5081, November 2007, <https://www.rfc-editor.org/info/rfc5081>.

[RFC5101] Claise, B., Ed., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, DOI 10.17487/RFC5101, January 2008, <https://www.rfc-editor.org/info/rfc5101>.

[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>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC5456] Spencer, M., Capouch, B., Guy, E., Ed., Miller, F., and K. Shumard, "IAX: Inter-Asterisk eXchange Version 2", RFC 5456, DOI 10.17487/RFC5456, February 2010, <https://www.rfc-editor.org/info/rfc5456>.

[RFC6012] Salowey, J., Petch, T., Gerhards, R., and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", RFC 6012, DOI 10.17487/RFC6012, October 2010, <https://www.rfc-editor.org/info/rfc6012>.

[RFC6083] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", RFC 6083, DOI 10.17487/RFC6083, January 2011, <https://www.rfc-editor.org/info/rfc6083>.

[RFC6084] Fu, X., Dickmann, C., and J. Crowcroft, "General Internet Signaling Transport (GIST) over Stream Control Transmission Protocol (SCTP) and Datagram Transport Layer Security (DTLS)", RFC 6084, DOI 10.17487/RFC6084, January 2011, <https://www.rfc-editor.org/info/rfc6084>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC6460] Salter, M. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 6460, DOI 10.17487/RFC6460, January 2012, <https://www.rfc-editor.org/info/rfc6460>.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <https://www.rfc-editor.org/info/rfc6614>.

[RFC7457] Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", RFC 7457, DOI 10.17487/RFC7457, February 2015, <https://www.rfc-editor.org/info/rfc7457>.

[RFC8143] Elie, J., "Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)", RFC 8143, DOI 10.17487/RFC8143, April 2017, <https://www.rfc-editor.org/info/rfc8143>.

[RFC8261] Tuexen, M., Stewart, R., Jesup, R., and S. Loreto, "Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets", RFC 8261, DOI 10.17487/RFC8261, November 2017, <https://www.rfc-editor.org/info/rfc8261>.

[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>.

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

Acknowledgements

Thanks to those that provided usage data and reviewed and/or improved this document, including: Michael Ackermann, David Benjamin, David Black, Deborah Brungard, Alan DeKok, Viktor Dukhovni, Julien Élie, Adrian Farrelll, Gary Gapinski, Alessandro Ghedini, Peter Gutmann, Jeremy Harris, Nick Hilliard, James Hodgkinson, Russ Housley, Hubert Kario, Benjamin Kaduk,

John Klensin, Watson Ladd, Eliot Lear, Ted Lemon, John Mattsson, Keith Moore, Tom Petch, Eric Mill, Yoav Nir, Andrei Popov, Michael Richardson, Eric Rescorla, Rich Salz, Mohit Sethi, Yaron Sheffer, Rob Sayre, Robert Sparks, Barbara Stark, Martin Thomson, Sean Turner, Loganaden Velvindron, and Jakub Wilk.

Authors' Addresses

Kathleen Moriarty
Dell EMC
176 South Street
Hopkinton,
United States of America
Email: Kathleen.Moriarty.ietf@gmail.com

Stephen Farrell
Trinity College Dublin
Dublin
2
Ireland
Phone: +353-1-896-2354
Email: stephen.farrell@cs.tcd.ie