[MS-TLSP]:

Transport Layer Security (TLS) Profile

Revision Summary

Date	Revision History	Revision Class	Comments
10/24/2008	0.1	New	Version 0.1 release
12/5/2008	0.1.1	Editorial	Changed language and formatting in the technical content.
1/16/2009	0.1.2	Editorial	Changed language and formatting in the technical content.
2/27/2009	0.2	Minor	Clarified the meaning of the technical content.
4/10/2009	1.0	Major	Updated and revised the technical content.
5/22/2009	1.0.1	Editorial	Changed language and formatting in the technical content.
7/2/2009	1.1	Minor	Clarified the meaning of the technical content.
8/14/2009	1.1.1	Editorial	Changed language and formatting in the technical content.
9/25/2009	1.2	Minor	Clarified the meaning of the technical content.
11/6/2009	1.2.1	Editorial	Changed language and formatting in the technical content.
12/18/2009	1.2.2	Editorial	Changed language and formatting in the technical content.
1/29/2010	2.0	Major	Updated and revised the technical content.
3/12/2010	2.0.1	Editorial	Changed language and formatting in the technical content.
4/23/2010	2.0.2	Editorial	Changed language and formatting in the technical content.
6/4/2010	2.0.3	Editorial	Changed language and formatting in the technical content.
7/16/2010	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
8/27/2010	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2010	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
1/7/2011	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
2/11/2011	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	2.0.3	None	No changes to the meaning, language, or formatting of the technical content.
6/17/2011	2.1	Minor	Clarified the meaning of the technical content.
9/23/2011	2.1	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	3.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
3/30/2012	3.0	None	No changes to the meaning, language, or formatting of the technical content.
7/12/2012	3.0	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	4.0	Major	Updated and revised the technical content.
1/31/2013	4.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	5.0	Major	Updated and revised the technical content.
11/14/2013	5.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	5.0	None	No changes to the meaning, language, or formatting of the technical content.
5/15/2014	6.0	Major	Updated and revised the technical content.
6/30/2015	7.0	Major	Significantly changed the technical content.
10/16/2015	8.0	Major	Significantly changed the technical content.
7/14/2016	9.0	Major	Significantly changed the technical content.
3/16/2017	10.0	Major	Significantly changed the technical content.
6/1/2017	10.0	None	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction

Support for **TLS**/**SSL** authentication is specified in [RFC5246], [RFC2246], [SSL3], and [PCT1]. Supported TLS extensions are specified in [RFC4366], [RFC3546], [RFC4681], and [RFC5077]. Additional supported **cipher** suites are defined in [RFC3268], [RFC4279], [RFC4492], [RFC5289], [RFC5487], and [IETFDRAFT-CURVE-25519-01]. This document specifies the differences in the Windows implementation from what is specified in the referenced documents, where applicable.<1>

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

ASCII: The American Standard Code for Information Interchange (ASCII) is an 8-bit character-encoding scheme based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that work with text. ASCII refers to a single 8-bit ASCII character or an array of 8-bit ASCII characters with the high bit of each character set to zero.

cipher: A cryptographic algorithm used to encrypt and decrypt files and messages.

Secure Sockets Layer (SSL): A security protocol that supports confidentiality and integrity of messages in client and server applications that communicate over open networks. SSL uses two keys to encrypt data-a public key known to everyone and a private or secret key known only to the recipient of the message. SSL supports server and, optionally, client authentication using X.509 certificates. For more information, see [X509]. The SSL protocol is precursor to **Transport Layer Security (TLS)**. The TLS version 1.0 specification is based on SSL version 3.0 [SSL3].

Transport Layer Security (TLS): A security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. **TLS** supports server and, optionally, client authentication by using X.509 certificates (as specified in [X509]). **TLS** is standardized in the IETF TLS working group.

UTF-8: A byte-oriented standard for encoding Unicode characters, defined in the Unicode standard. Unless specified otherwise, this term refers to the UTF-8 encoding form specified in [UNICODE5.0.0/2007] section 3.9.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as defined in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.

[IETFDRAFT-CURVE-25519-01] Josefsson, S., and Pegourie-Gonnard, M., "Curve25519 and Curve448 for Transport Layer Security (TLS)", draft-ietf-tls-curve25519-01, July 2015, https://tools.ietf.org/html/draft-ietf-tls-curve25519-01

[IETFDRAFT-TOKBND] Balfanz, D., Langley, A., Nystroem, M., et al., "Transport Layer Security (TLS) Extension for Token Binding Protocol Negotiation", draft-popov-tokbind-negotiation-00, May 2015, http://datatracker.ietf.org/doc/draft-popov-tokbind-negotiation

[NPN] Langley, A., "TLS Next Protocol Negotiation", May 2012, https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-04.html

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[RFC2246] Dierks, T., and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999, http://www.rfc-editor.org/rfc/rfc2246.txt

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000, http://www.rfc-editor.org/rfc/rfc2743.txt

[RFC3268] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002, http://www.ietf.org/rfc/rfc3268.txt

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and Wright, T., "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003, http://www.ietf.org/rfc/rfc3546.txt

[RFC4279] Eronen, P., and Tschofenig, H., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005, http://www.ietf.org/rfc/rfc4279.txt

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., et al., "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006, http://www.ietf.org/rfc/rfc4366.txt

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., et al., "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006, http://www.ietf.org/rfc/rfc4492.txt

[RFC4681] Ball, J., Medvinsky, A., and Santesson, S., "TLS User Mapping Extension", RFC 4681, October 2006, http://www.ietf.org/rfc/rfc4681.txt

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

[RFC5246] Dierks, T., and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, http://www.ietf.org/rfc/rfc5246.txt

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, August 2008, http://www.ietf.org/rfc/rfc5289.txt

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009, http://www.ietf.org/rfc/rfc5487.txt

[RFC7301] Friedl, S., Popov, A., Langley, A., and Stephan, E., "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, July 2014, http://tools.ietf.org/html/rfc7301

[RFC7627] Bhargaven, K., Delignat-Lavaud, A., Pironti, A., Paris-Rocquencourt, Inria, Langley, A., and Ray, M., "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", RFC 7627, September 2015, https://tools.ietf.org/html/rfc7627

1.2.2 Informative References

[PCT1] Benalogh, J., Lampson, B., Simon, D., Spies, T., and Yee, B., "The Private Communication Technology (PCT) Protocol", October 1995, http://tools.ietf.org/html/draft-benaloh-pct-00

[RFC4346] Dierks, T., and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006, http://www.ietf.org/rfc/rfc4346.txt

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August 2010, http://rfc-editor.org/rfc/rfc5890.txt

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011, http://www.rfc-editor.org/rfc/rfc6066.txt

[SSL3] Netscape, "SSL 3.0 Specification", http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00

1.3 Overview

The **SSL**/**TLS** (as specified in [RFC5246]) authentication mechanism is used to authenticate a server to a client with the option for mutual authentication.

1.4 Relationship to Other Protocols

This document is a companion to the **SSL**/**TLS** authentication standard [RFC5246].

The Transport Layer Security (TLS) Profile implements Server Name Indication (SNI) based on [RFC4366] where HostName is in **UTF-8** format. This behavior is not interoperable with SNI implementations of [RFC6066] where HostName is a byte string using **ASCII** encoding without a trailing dot to support internationalized domain names through the use of A-labels [RFC5890].

1.5 Prerequisites/Preconditions

SSL/**TLS** authentication has the same assumptions as specified in [RFC5246].

1.6 Applicability Statement

SSL/**TLS** authentication is used in environments where the client and server support specification [RFC5246].

1.7 Versioning and Capability Negotiation

Versioning and capability negotiation is handled as specified in [RFC5246].

1.8 Vendor-Extensible Fields

SSL/**TLS** authentication contains vendor-extensible fields as specified in [RFC5246].

1.9 Standards Assignments

Parameter	Value	Reference
Standard **TLS**/**SSL** parameters	N/A	http://www.iana.org/assignments/tls-parameters/
TLS extension parameters	N/A	http://www.iana.org/assignments/tls-extensiontype-values/

2 Messages

2.1 Transport

SSL/**TLS** messages SHOULD be transported as specified in [RFC5246].

2.2 Message Syntax

The **SSL**/**TLS** message syntax SHOULD<2> be as specified in [RFC5246], [RFC5077], and [RFC7301] and MAY<3> be as specified in [NPN].

2.2.1 Client and Server Hello Messages

Cipher suites and capabilities MAY<4> be negotiated as specified in [RFC4279] and [RFC5487], and SHOULD<5><6> be negotiated as specified in [RFC7627], [RFC5246], [RFC2246], [RFC4492], and [RFC3268].<7>

2.2.2 Alert Messages

The **SSL**/**TLS** alert message behavior and formatting SHOULD<8><9> be as specified in [RFC5246] section 7.2, [RFC2246] section 7.2, [RFC4366] section 4, and [RFC3546] section 4.

2.2.3 Extended Hello Messages

The **TLS** extended hello message behavior and formatting SHOULD<10> be as specified in [RFC5246] section 7.4.1.4, [RFC4366] sections 2.3 and 3.1, [RFC3546] section 2.3, [RFC4681] section 2,<11> [RFC5077],<12> [RFC7301],<13> and [IETFDRAFT-TOKBND].<14> It MAY<15> be as specified in [NPN].

2.2.4 Certificate Messages

The **SSL**/**TLS** certificate message behavior and formatting is specified in [RFC5246] sections 7.4.2 and 7.4.6, [RFC2246] sections 7.4.2 and 7.4.6, and [RFC4492] sections 5.3 and 5.6.<16><17>

2.3 Directory Service Schema Elements

None.

3 Protocol Details

3.1 Common Details

3.1.1 Abstract Data Model

The abstract data model follows what is specified in [RFC5246].

3.1.2 Timers

There are no timers except those specified in [RFC5246].

3.1.3 Initialization

There is no protocol-specific initialization except what is specified in [RFC5246].

3.1.4 Higher-Layer Triggered Events

There are no higher-layer triggered events in common to all parts of this protocol.

3.1.5 Processing Events and Sequencing Rules

The message processing events and sequencing rules SHOULD<18> be as specified in [RFC5246], [RFC5077], and [RFC7301]. It MAY<19> be as specified in [NPN]. If a client receives an extension type in ServerHello that it did not request in the associated ClientHello, it MAY abort the handshake. There MAY<20> be more than one extension of the same type.

3.1.5.1 GSS_WrapEx() Call

This call is an extension to GSS_Wrap ([RFC2743] section 2.3.3) that passes multiple buffers.

Inputs:

- context_handle CONTEXT HANDLE
- qop_req INTEGER -- 0 specifies default Quality of Protection (QOP)
- input_message ORDERED LIST of:
  - conf_req_flag BOOLEAN
  - sign BOOLEAN
  - data OCTET STRING

Outputs:

- major_status INTEGER
- minor_status INTEGER
- output_message ORDERED LIST (in same order as input_message) of:
  - conf_state BOOLEAN

- signed BOOLEAN
- data OCTET STRING

- signature OCTET STRING

This call is identical to GSS_Wrap, except that it supports multiple input buffers. Schannel's binding of GSS_WrapEx() is such that only the first input buffer will be processed and the rest ignored. Thus Schannel's binding of GSS_WrapEx() functions just as GSS_Wrap does.

3.1.5.2 GSS_UnwrapEx() Call

This call is an extension to GSS_Unwrap ([RFC2743] section 2.3.4) that passes multiple buffers.

Inputs:

- context_handle CONTEXT HANDLE
- input_message ORDERED LIST of:
  - conf_state BOOLEAN
  - signed BOOLEAN
  - data OCTET STRING
- signature OCTET STRING

Outputs:

- qop_req INTEGER, -- 0 specifies default QOP
- major_status INTEGER
- minor_status INTEGER
- output_message ORDERED LIST (in same order as input_message) of:
  - conf_state BOOLEAN
  - data OCTET STRING

This call is identical to GSS_Unwrap, except that it supports multiple input buffers. Schannel's binding of GSS_UnwrapEx() is such that only the first input buffer will be processed and the rest ignored. Thus Schannel's binding of GSS_UnwrapEx() functions just as GSS_Unwrap does.

3.1.6 Timer Events

There are no timer events except those specified in [RFC5246].

3.1.7 Other Local Events

There are no local events except those specified in [RFC5246].

4 Protocol Examples

Protocol examples can be found in [IETFDRAFT-CURVE-25519-01] section 2, [RFC5246] section 7.3, [RFC4366] section 3, [RFC4681] section 4, and [RFC4492] section 5.

5 Security

5.1 Security Considerations for Implementers

Security considerations are specified in each standard.

5.2 Index of Security Parameters

Security Parameter	Section
See Security Considerations for Implementers	5.1

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs.

- Windows XP operating system
- Windows Server 2003 operating system
- Windows Vista operating system
- Windows Server 2008 operating system
- Windows 7 operating system
- Windows Server 2008 R2 operating system
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 R2 operating system
- Windows 10 operating system
- Windows Server 2016 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

<1> Section 1: Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 implement **TLS** 1.2 as specified mainly in [RFC5246] with extensions from [RFC4366], [RFC4681], and [RFC5077], additional **cipher** suites from [RFC3268], [RFC4492], [RFC5289], TLS 1.1 from [RFC4346], and **SSL** from [SSL3].

Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 implement TLS 1.2 as specified mainly in [RFC5246] with extensions from [RFC4366] and [RFC4681], additional cipher suites from [RFC3268], [RFC4492], [RFC5289], TLS 1.1 from [RFC4346], and SSL from [SSL3].

Windows Vista and Windows Server 2008 implement TLS 1.0 as specified mainly in [RFC2246] with extensions from [RFC3546] and [RFC4681], additional cipher suites from [RFC3268] and [RFC4492], and SSL from [SSL3].

In Windows Server 2003 and Windows XP, TLS was implemented with [RFC2246] and [RFC4681], SSL from [SSL3], and PCT from [PCT1].

Windows NT operating system and Windows 2000 operating system implement SSL from [SSL3] and PCT from [PCT1].

Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012 operating system, Windows 8.1, Windows Server

2012 R2, Windows 10 v1507 operating system, and Windows 10 v1511 operating system do not support Curve25519 as defined in [IETFDRAFT-CURVE-25519-01].

<2> Section 2.2: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 do not support [RFC5077]. Windows 8 and Windows Server 2012 support only the client side of [RFC5077].

Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 do not support [RFC7301].

<3> Section 2.2: Only Windows 8.1, Windows Server 2012 R2, Windows 10 v1507, Windows 10 v1511, Windows 10 v1607 operating system, and Windows Server 2016 support [NPN].

<4> Section 2.2.1: Windows does not support DHE_PSK or RSA_PSK Key Exchange Algorithms defined in [RFC4279] and [RFC5487].

Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 v1507, and Windows 10 v1511 do not support PSK Key Exchange Algorithm [RFC4279] or PSK cipher suites [RFC5487].

<5> Section 2.2.1: Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 support [RFC4492], except for not allowing ECDH cipher suites where the number of bits used in the public key algorithm is less than the number of bits used in the signing algorithm.

<6> Section 2.2.1: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 do not support Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension [RFC7627].

<7> Section 2.2.1: Windows accepts a unified format ClientHello message even when SSL version 2 is disabled.

<8> Section 2.2.2: Windows has a decoupling of the network layer from the SSL/TLS layer and thus cannot ensure that alert messages are sent.

<9> Section 2.2.2: Windows XP and Windows Server 2003 do not support sending and receiving the Certificate Status Request extension from [RFC4366] and [RFC3546].

<10> Section 2.2.3: Windows XP and Windows Server 2003 do not support sending the Server Name Indications from [RFC4366] and [RFC3546] in the ClientHello.

Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 do not support sending and receiving the Server Name Indications.

<11> Section 2.2.3: Windows supports sending and receiving the User Mapping extension by using UPN domain hint from [RFC4681].

<12> Section 2.2.3: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 do not support [RFC5077]. Windows 8 and Windows Server 2012 support only the client side of [RFC5077].

<13> Section 2.2.3: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 do not support [RFC7301].

<14> Section 2.2.3: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2 operating system, and Windows 10 v1507 do not support Transport Layer Security (TLS) Extension for Token Binding Protocol Negotiation [IETFDRAFT-TOKBND].

<15> Section 2.2.3: Only Windows 8.1, Windows Server 2012 R2, Windows 10 v1507, Windows 10 v1511, Windows 10 v1607, and Windows Server 2016 support [NPN].

<16> Section 2.2.4: Windows does not require that the signing algorithm used by the issuer of a certificate match the algorithm in the end certificate. Windows also does not require particular key usage extension bits to be set in certificates.

<17> Section 2.2.4: Windows omits the root certificate by default when sending certificate chains.

<18> Section 3.1.5: Note the following Windows message processing:

- If a session fails during bulk data transfer, Windows does not prevent attempted resumption of the session.
- Only Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016 do not support or process extensions within the Certificate Status Request extension.
- Windows does not ignore a HelloRequest received, even in the middle of a handshake.
- Windows Server 2003 does not support fragmentation of incoming messages across frames as is allowed in [RFC5246] section 6.2.1.

<19> Section 3.1.5: Only Windows 8.1, Windows Server 2012 R2, Windows 10 v1507, Windows 10 v1511, Windows 10 v1607, and Windows Server 2016 support [NPN].

<20> Section 3.1.5: Windows ignores both unrequested and duplicate extensions in both ClientHello and ServerHello.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index