[MS-TLSP]:
Transport Layer Security (TLS) Profile

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Copyright © 2011 Microsoft Corporation.

Revision Summary

Date	Revision History	Revision Class	Comments
10/24/2008	0.1		Initial Availability
12/05/2008	0.1.1	Editorial	Revised and edited the technical content.
01/16/2009	0.1.2	Editorial	Revised and edited the technical content.
02/27/2009	0.2	Minor	Updated the technical content.
04/10/2009	1.0	Major	Updated and revised the technical content.
05/22/2009	1.0.1	Editorial	Revised and edited the technical content.
07/02/2009	1.1	Minor	Updated the technical content.
08/14/2009	1.1.1	Editorial	Revised and edited the technical content.
09/25/2009	1.2	Minor	Updated the technical content.
11/06/2009	1.2.1	Editorial	Revised and edited the technical content.
12/18/2009	1.2.2	Editorial	Revised and edited the technical content.
01/29/2010	2.0	Major	Updated and revised the technical content.
03/12/2010	2.0.1	Editorial	Revised and edited the technical content.
04/23/2010	2.0.2	Editorial	Revised and edited the technical content.
06/04/2010	2.0.3	Editorial	Revised and edited the technical content.
07/16/2010	2.0.3	No change	No changes to the meaning, language, or formatting of the technical content.
08/27/2010	2.0.3	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	2.0.3	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	2.0.3	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	2.0.3	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	2.0.3	No change	No changes to the meaning, language, or formatting of the technical content.

Copyright © 2011 Microsoft Corporation.

Contents

Copyright © 2011 Microsoft Corporation.

1 Introduction

Support for **TLS**/**SSL** authentication is as specified in [RFC5246], [RFC2246], [SSL3], and [PCT1]. Supported TLS extensions are specified in [RFC4366], [RFC3546], and [RFC4681]. Additional supported **cipher** suites are defined in [RFC3268], [RFC4492], and [RFC5289]. This document will call out the differences in Microsoft's implementation from what is specified in the referenced documents, where applicable.<1>

1.1 Glossary

The following terms are defined in [MS-GLOS]:

cipher
SSL
TLS

The following terms are specific to this document:

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

1.2 References

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. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

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

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

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000, http://www.ietf.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., et al., "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003, http://www.ietf.org/rfc/rfc3546.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

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

Copyright © 2011 Microsoft Corporation.

[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

[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

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[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

If you have any trouble finding [PCT1], please check here.

[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

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

If you have any trouble finding [SSL3], please check here.

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].

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].

Copyright © 2011 Microsoft Corporation.

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/

Copyright © 2011 Microsoft Corporation.

2 Messages

2.1 Transport

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

2.2 Message Syntax

The SSL/TLS message syntax is the same as specified in [RFC5246].

2.2.1 Client and Server Hello Messages

Cipher suites and capabilities are negotiated as specified in [RFC5246], [RFC2246], [RFC4492], and [RFC3268].<2><3><4>

2.2.2 Alert Messages

The SSL/TLS alert message behavior and formatting is specified in [RFC5246] section 7.2, [RFC2246] section 7.2, [RFC4366] section 4, and [RFC3546] section 4.<5>

2.2.3 Extended Hello Messages

The TLS extended hello message behavior and formatting is as specified in [RFC5246] section 7.4.1.4, [RFC4366] section 2.3, [RFC3546] section 2.3, and [RFC4681] section 2.<6><7><8>

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. <9><10> <11>

2.3 Directory Service Schema Elements

None.

Copyright © 2011 Microsoft Corporation.

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 are as specified in [RFC5246].<12><13><14> 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 be more than one extension of the same type.<15>

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

Output:

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

Copyright © 2011 Microsoft Corporation.

- 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].

Copyright © 2011 Microsoft Corporation.

4 Protocol Examples

Protocol examples can be found in [RFC5246] section 7.3, [RFC4366] section 3, [RFC4681] section 4, and [RFC4492] section 5.

Copyright © 2011 Microsoft Corporation.

5 Security

5.1 Security Considerations for Implementers

Security considerations are specified in each standard, including [RFC5246] section 11, [RFC4366] section 6, [RFC3268], [RFC3546] section 6, [RFC4681] section 5, and [RFC4492] section 7.

5.2 Index of Security Parameters

Security Parameter	Section
See Security Considerations for Implementers	5.1

Copyright © 2011 Microsoft Corporation.

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:

- Microsoft Windows NT® operating system
- Microsoft Windows® 2000 operating system
- Windows® XP operating system
- Windows Server® 2003 operating system
- Windows Server® 2003 operating system with Service Pack 1 (SP1)
- Windows Server® 2003 R2 operating system
- Windows Vista® operating system
- Windows Server® 2008 operating system
- Windows® 7 operating system
- Windows Server® 2008 R2 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 7 and Windows Server 2008 R2 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 and Windows 2000 implement SSL from [SSL3] and PCT from [PCT1].

<2> Section 2.2.1: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 support [RFC4492] except for ECDH cipher suites.

<3> Section 2.2.1: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 support [RFC4492] except for not allowing 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.

<4> Section 2.2.1: Windows accepts a unified format Client Hello message even when SSL version 2 is disabled.

<5> Section 2.2.2: Windows has a decoupling of the network layer from the SSL/TLS layer and thus will not be able to ensure alert messages are sent.

Copyright © 2011 Microsoft Corporation.

<6> Section 2.2.3: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 support sending and receiving the Certificate Status Request extension from [RFC4366] and [RFC3546].

<7> Section 2.2.3: Windows supports sending and receiving the User Mapping extension using UPN domain hint from [RFC4681].

<8> Section 2.2.3: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 support sending the Server Name Indication extension from [RFC4366] and [RFC3546] in the ClientHello.

<9> 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.

<10> Section 2.2.4: Windows does not require particular key usage extension bits to be set in certificates.

<11> Section 2.2.4: Windows omits the root certificate by default when sending certificate chains.

<12> Section 3.1.5: If a session fails during bulk data transfer, Windows does not prevent attempted resumption of the session.

<13> Section 3.1.5: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 do not support or process extensions within the Certificate Status Request extension.

<14> Section 3.1.5: Windows does not ignore a HelloRequest received even in the middle of a handshake.

<15> Section 3.1.5: Windows ignores both unrequested and duplicate extensions in both ClientHello and ServerHello.

Copyright © 2011 Microsoft Corporation.

7 Change Tracking

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

Copyright © 2011 Microsoft Corporation.

8 Index

Copyright © 2011 Microsoft Corporation.