

[MS-GSSA]: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension

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 [Open Specification Promise](#) or the [Community Promise](#). 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.

Revision Summary

Date	Revision History	Revision Class	Comments
05/11/2007	0.1		MCPD Milestone 4 Initial Availability
08/10/2007	0.1.1	Editorial	Revised and edited the technical content.
09/28/2007	0.1.2	Editorial	Revised and edited the technical content.
10/23/2007	0.1.3	Editorial	Revised and edited the technical content.
11/30/2007	0.1.4	Editorial	Revised and edited the technical content.
01/25/2008	0.1.5	Editorial	Revised and edited the technical content.
03/14/2008	0.1.6	Editorial	Revised and edited the technical content.
05/16/2008	0.1.7	Editorial	Revised and edited the technical content.
06/20/2008	0.1.8	Editorial	Revised and edited the technical content.
07/25/2008	0.1.9	Editorial	Revised and edited the technical content.
08/29/2008	0.1.10	Editorial	Revised and edited the technical content.
10/24/2008	0.1.11	Editorial	Revised and edited the technical content.
12/05/2008	1.0	Major	Updated and revised the technical content.
01/16/2009	2.0	Major	Updated and revised the technical content.
02/27/2009	3.0	Major	Updated and revised the technical content.
04/10/2009	3.0.1	Editorial	Revised and edited the technical content.
05/22/2009	3.0.2	Editorial	Revised and edited the technical content.
07/02/2009	3.0.3	Editorial	Revised and edited the technical content.
08/14/2009	3.0.4	Editorial	Revised and edited the technical content.
09/25/2009	3.0.5	Editorial	Revised and edited the technical content.
11/06/2009	3.0.6	Editorial	Revised and edited the technical content.
12/18/2009	3.0.7	Editorial	Revised and edited the technical content.
01/29/2010	3.0.8	Editorial	Revised and edited the technical content.
03/12/2010	3.0.9	Editorial	Revised and edited the technical content.
04/23/2010	3.0.10	Editorial	Revised and edited the technical content.
06/04/2010	3.0.11	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
07/16/2010	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
08/27/2010	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
03/25/2011	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
05/06/2011	3.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
06/17/2011	3.1	Minor	Clarified the meaning of the technical content.

Contents

1	Introduction	5
1.1	Glossary	5
1.2	References.....	5
1.2.1	Normative References.....	5
1.2.2	Informative References	6
1.3	Overview	6
1.4	Relationship to Other Protocols.....	6
1.5	Prerequisites/Preconditions	6
1.6	Applicability Statement.....	6
1.7	Versioning and Capability Negotiation.....	6
1.8	Vendor-Extensible Fields.....	6
1.9	Standards Assignments	6
2	Messages.....	7
2.1	Transport.....	7
2.2	Message Syntax	7
3	Protocol Details	8
3.1	Common Details	8
3.1.1	Abstract Data Model	8
3.1.2	Timers	8
3.1.3	Initialization	8
3.1.4	Higher-Layer Triggered Events.....	8
3.1.5	Message Processing Events and Sequencing Rules.....	8
3.1.6	Timer Events	9
3.1.7	Other Local Events	9
4	Protocol Examples.....	10
5	Security.....	13
5.1	Security Considerations for Implementers.....	13
5.2	Index of Security Parameters	13
6	Appendix A: Product Behavior.....	14
7	Change Tracking.....	15
8	Index	17

1 Introduction

Secret Key Transaction Authentication for DNS (TSIG), as specified in [\[RFC2845\]](#), provides extensible transaction level authentication for DNS. The Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG), as specified in [\[RFC3645\]](#), identifies one possible extension to TSIG based on the Generic Security Service Application Program Interface (GSS-API), as specified in [\[RFC2743\]](#).

This document specifies an extension to GSS-TSIG.

1.1 Glossary

The following terms are specific to this document:

message authentication code (MAC): A relatively short sequence of bytes that is used to authenticate a message. A **MAC** algorithm accepts a secret key and a data buffer, and outputs a **MAC**. The data and **MAC** can then be sent to another party, which can verify the integrity and authenticity of the data by using the same secret key and the same **MAC** algorithm.

security support provider (SSP): A library that implements one or more security protocols that can be accessed programmatically.

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

References to Microsoft Open Specification documents do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

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.rfc-editor.org/rfc/rfc2119.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>

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake III, D., and Wellington, B., "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000, <http://www.ietf.org/rfc/rfc2845.txt>

[RFC2930] Eastlake III, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000, <http://www.ietf.org/rfc/rfc2930.txt>

[RFC3645] Kwan, S., Garg, P., Gilroy, J., et al., "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)", RFC 3645, October 2003, <http://www.ietf.org/rfc/rfc3645.txt>

1.2.2 Informative References

None.

1.3 Overview

Secret Key Transaction Authentication for DNS (TSIG), as specified in [RFC2845], is an extensible protocol by which DNS messages can be authenticated and validated. The Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG), as specified in [RFC3645], defines an algorithm for use with TSIG, which is based on the Generic Security Service Application Program Interface, as specified in [RFC2743].

In [RFC3645] section 2.2, GSS-TSIG specifies that the final transaction key (TKEY) response indicating successful negotiation must be signed. In [RFC2845] section 3.4, TSIG specifies which data is to be digested when generating or verifying the contents of a TSIG record. This protocol extension defines an alternate method of building the digest that is used to sign the last message in the GSS-TSIG TKEY negotiation.

1.4 Relationship to Other Protocols

This specification defines an extension to GSS-TSIG, as specified in [RFC3645]. The relationship of GSS-TSIG to other protocols is not changed by this protocol extension.

1.5 Prerequisites/Preconditions

All prerequisites and preconditions applicable to GSS-TSIG, as specified in [RFC3645], apply to this protocol extension.

1.6 Applicability Statement

This protocol extension does not change the way in which GSS-TSIG, as specified in [RFC3645], is used.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

This protocol extension does not change the format of messages defined by GSS-TSIG, as specified in [\[RFC3645\]](#). The format of messages remains the same, although the contents of the TSIG record attached to the final TKEY response in the negotiation are changed.

2.1 Transport

This protocol extension does not change the base transport used by GSS-TSIG, as specified in [\[RFC3645\]](#).

2.2 Message Syntax

This document does not specify any new messages.

3 Protocol Details

3.1 Common Details

GSS-TSIG, as specified in [\[RFC3645\]](#), specifies how the client and server exchange tokens obtained from GSS-API calls (as specified in [\[RFC2743\]](#)). The tokens are contained in DNS TKEY records, as specified in [\[RFC2930\]](#). In [\[RFC3645\]](#) section 4.1.3, GSS-TSIG specifies that the server MUST sign the final TKEY response in GSS-TSIG negotiation.

In [\[RFC2845\]](#) section 3.4.3, TSIG specifies that the request **message authentication code (MAC)** is to be included in the digest when generating or validating a DNS message. However, because the final TKEY response in the GSS-TSIG is the first DNS message in the exchange that has been signed, there is no request MAC that can be included when performing the digest operation.

When there is no request MAC, the most obvious interpretation of [\[RFC2845\]](#) section 3.4.3 is that the 2-byte MAC length with a value of zero be included in the digest to indicate that no MAC data bytes are being included in the digest. This protocol extension specifies that when building the digest for this message, the request MAC MUST be completely omitted. In other words, the request MAC length and request MAC data fields MUST NOT be included in the digest, so the only components of the digest will be the DNS response message and TSIG response variables.

After GSS-TSIG negotiation is complete, the digesting of further DNS messages MUST include the request MAC, as specified in [\[RFC2845\]](#) section 3.4.

[\[RFC2845\]](#) section 2.2 specifies that TSIG MUST support the "HMAC-MD5" algorithm. GSS-API does not explicitly define the MAC formats supported. Instead it relies on the **security support provider (SSP)** that is exposed by the operating system. Implementations of this protocol extension MUST NOT support the "HMAC-MD5.SIG-ALG.REG.INT" algorithm in [\[RFC2845\]](#) section 7. Implementations of this protocol extension MUST support the "gss-tsig" algorithm, as specified in [\[RFC3645\]](#) section 3.1.2.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

This protocol extension does not require any initialization that is not already required by GSS-TSIG, as specified in [\[RFC3645\]](#).

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

This protocol extension does not change message processing events or sequencing rules of messages defined by GSS-TSIG, as specified in [\[RFC3645\]](#), beyond the changes described in section [3.1](#).

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

4 Protocol Examples

Examples that clarify the difference between a strict interpretation of the relevant RFCs and the Microsoft implementation are included in the figures in this section.

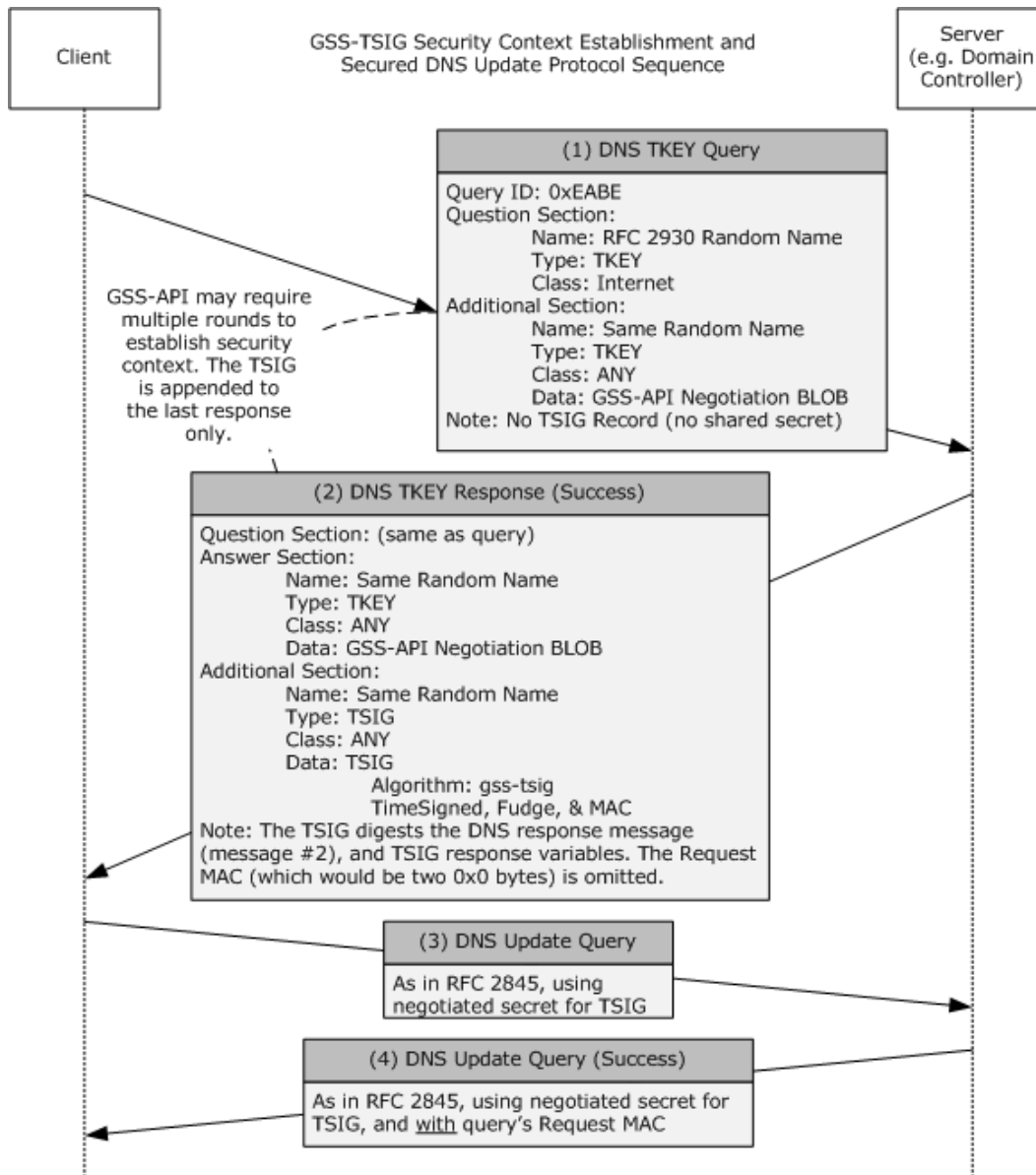


Figure 1: Example of a protocol sequence

```

- Request-MAC (Not included in Microsoft implementation, despite RFC 2845 §4.4.2)
  MACSize: 0 (0x0)
- DNS Response Message:
  QueryIdentifier: 60094 (0xEABE)
  - Flags:
    QR: (1.....) Response
    Opcode: (.0000.....) QUERY (Standard query) 0
    AA: (.....0.....) Not authoritative
    TC: (.....0.....) Not truncated
    RD: (.....0.....) Recursion not desired
    RA: (.....0.....) Recursive query support not available
    Zero: (.....0.....) 0
    AuthenticatedData: (.....0.....) Not AuthenticatedData
    CheckingDisabled: (.....0.....) Not CheckingDisabled
    Rcode: (.....0000) Success 0
  QuestionCount: 1 (0x1)
  AnswerCount: 1 (0x1)
  NameServerCount: 0 (0x0)
  AdditionalCount: 0 (0x0) (This is the response before adding the TSIG RR)
  - QRecord:
    QuestionName: 1184-ms-7.93-ba98458.06282df7-e7e7-11dd-25bc-000ffed6cffd
    QuestionType: TKEY, 249(0xf9)
    QuestionClass: Internet, 1(0x1)
  - ARecord:
    ResourceName: 1184-ms-7.93-ba98458.06282df7-e7e7-11dd-25bc-000ffed6cffd
    ResourceType: TKEY, 249(0xf9)
    ResourceClass: Any, 255(0xff)
    TimeToLive: 0 (0x0)
    ResourceDataLength: 211 (0xD3)
  - TKEYRData:
    Algorithm: gss-tsig
    Inception: 01/24/2009, 12:32:09 AM .0000 UTC
    Expiration: 01/25/2009, 12:32:09 AM .0000 UTC
    Mode: GSS-API negotiation 3
    Error: No Error 0
    KeySize: 185 (0xB9)
    + KeyData: Binary Large Object (185 Bytes)
    OtherSize: 0 (0x0)
  - TSIG Variables: (As specified in RFC 2845 §3.4.2)
    ResourceName: 1184-ms-7.93-ba98458.06282df7-e7e7-11dd-25bc-000ffed6cffd
    ResourceClass: Any, 255(0xff)
    TimeToLive: 0 (0x0)
    AlgorithmName: gss-tsig
    TimeSigned: 1232757129 (0x497A6189)
    Fudge: 36000 (0x8CA0)
    Error: 0 (0x0)
    OtherLen: 0 (0x0)
    OtherData:

```

Figure 2: Example of Message #2 input to the GSS_GetMIC TSIG generation function

```

- dns:
  QueryIdentifier: 60094 (0xEABE)
- Flags:
  QR: (1.....) Response
  Opcode: (.0000.....) QUERY (Standard query) 0
  AA: (....0.....) Not authoritative
  TC: (.....0.....) Not truncated
  RD: (.....0.....) Recursion not desired
  RA: (.....0.....) Recursive query support not available
  Zero: (.....0.....) 0
  AuthenticatedData: (.....0.....) Not AuthenticatedData
  CheckingDisabled: (.....0.....) Not CheckingDisabled
  Rcode: (.....0000) Success 0
  QuestionCount: 1 (0x1)
  AnswerCount: 1 (0x1)
  NameServerCount: 0 (0x0)
  AdditionalCount: 1 (0x1)
- QRecord:
  QuestionName: 1184-ms-7.93-ba98458.06282df7-e7e7-11dd-25bc-000ffed6cffd
  QuestionType: TKEY, 249(0xf9)
  QuestionClass: Internet, 1(0x1)
- ARecord:
  ResourceName: 1184-ms-7.93-ba98458.06282df7-e7e7-11dd-25bc-000ffed6cffd
  ResourceType: TKEY, 249(0xf9)
  ResourceClass: Any, 255(0xff)
  TimeToLive: 0 (0x0)
  ResourceDataLength: 211 (0xD3)
- TKEYRData:
  Algorithm: gss-tsig
  Inception: 01/24/2009, 12:32:09 AM .0000 UTC
  Expiration: 01/25/2009, 12:32:09 AM .0000 UTC
  Mode: GSS-API negotiation 3
  Error: No Error 0
  KeySize: 185 (0xB9)
+ KeyData: Binary Large Object (185 Bytes)
  OtherSize: 0 (0x0)
- AdditionalRecord:
  ResourceName: 1184-ms-7.93-ba98458.06282df7-e7e7-11dd-25bc-000ffed6cffd
  ResourceType: TSIG, Transaction Signature, 250(0xfa)
  ResourceClass: Any, 255(0xff)
  TimeToLive: 0 (0x0)
  ResourceDataLength: 54 (0x36)
- TSIGRData:
  AlgorithmName: gss-tsig
  TimeSigned: 1232757129 (0x497A6189)
  Fudge: 36000 (0x8CA0)
  MACSize: 28 (0x1C)
  MAC: (Binary Data)
  OriginalID: 60094 (0xEABE)
  Error: 0 (0x0)
  OtherLen: 0 (0x0)
  OtherData:

```

Figure 3: Example of Message #2, as it appears on the wire

5 Security

5.1 Security Considerations for Implementers

None.

5.2 Index of Security Parameters

None.

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® 2000 operating system
- 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

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.

7 Change Tracking

This section identifies changes that were made to the [MS-GSSA] protocol document between the May 2011 and June 2011 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1.2 References	Added explanatory statement regarding the removal of the publishing year from Microsoft Open Specification document references.	N	Content updated.

8 Index

A

[Abstract data model](#) 8
[Applicability](#) 6

C

[Capability negotiation](#) 6
[Change tracking](#) 15
[Common details](#) 8

D

[Data model - abstract](#) 8
[Details - common](#) 8

E

[Examples](#) 10

F

[Fields - vendor-extensible](#) 6

G

[Glossary](#) 5

H

[Higher-layer triggered events](#) 8

I

[Implementer - security considerations](#) 13
[Index of security parameters](#) 13
[Informative references](#) 6
[Initialization](#) 8
[Introduction](#) 5

L

[Local events](#) 9

M

[MAC \(Message Authentication Code\) described](#) 5
[Message Authentication Code \(MAC\) described](#) 5
[Message processing](#) 8
Messages
 [overview](#) 7
 [syntax](#) 7
 [transport](#) 7

N

[Normative references](#) 5

O

Overview
 [common details](#) 8
 [main](#) 6

P

[Parameters - security index](#) 13
[Preconditions](#) 6
[Prerequisites](#) 6
[Product behavior](#) 14

R

References
 [informative](#) 6
 [normative](#) 5
 [Relationship to other protocols](#) 6

S

[Secret Key Transaction Authentication for DNS \(TSIG\) described](#) 6
Security
 [implementer considerations](#) 13
 [parameter index](#) 13
 [Sequencing rules](#) 8
 [Standards assignments](#) 6
 [Syntax](#) 7

T

[Timer events](#) 9
[Timers](#) 8
[Tracking changes](#) 15
[Transport](#) 7
[Triggered events - higher-layer](#) 8

V

[Vendor-extensible fields](#) 6
[Versioning](#) 6