

[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 (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **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 can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](#) or the [Microsoft Community Promise](#). If you would prefer a written license, or if the technologies described in this documentation 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 might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are 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 as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does 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 documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
4/3/2007	1.0	New	Version 1.0 release
5/11/2007	1.2	Minor	Version 1.2 release
6/1/2007	1.2.1	Editorial	Changed language and formatting in the technical content.
7/3/2007	1.3	Minor	Clarified the meaning of the technical content.
8/10/2007	1.3.1	Editorial	Changed language and formatting in the technical content.
9/28/2007	1.3.2	Editorial	Changed language and formatting in the technical content.
10/23/2007	1.3.3	Editorial	Changed language and formatting in the technical content.
1/25/2008	1.3.4	Editorial	Changed language and formatting in the technical content.
3/14/2008	1.3.5	Editorial	Changed language and formatting in the technical content.
6/20/2008	1.3.6	Editorial	Changed language and formatting in the technical content.
7/25/2008	1.3.7	Editorial	Changed language and formatting in the technical content.
8/29/2008	1.3.8	Editorial	Changed language and formatting in the technical content.
10/24/2008	1.3.9	Editorial	Changed language and formatting in the technical content.
12/5/2008	2.0	Major	Updated and revised the technical content.
1/16/2009	3.0	Major	Updated and revised the technical content.
2/27/2009	4.0	Major	Updated and revised the technical content.
4/10/2009	4.0.1	Editorial	Changed language and formatting in the technical content.
5/22/2009	4.0.2	Editorial	Changed language and formatting in the technical content.
7/2/2009	4.0.3	Editorial	Changed language and formatting in the technical content.
8/14/2009	4.0.4	Editorial	Changed language and formatting in the technical content.
9/25/2009	4.0.5	Editorial	Changed language and formatting in the technical content.
11/6/2009	4.0.6	Editorial	Changed language and formatting in the technical content.
12/18/2009	4.0.7	Editorial	Changed language and formatting in the technical content.
1/29/2010	4.0.8	Editorial	Changed language and formatting in the technical content.
3/12/2010	4.0.9	Editorial	Changed language and formatting in the technical content.
4/23/2010	4.0.10	Editorial	Changed language and formatting in the technical content.
6/4/2010	4.0.11	Editorial	Changed language and formatting in the technical content.
7/16/2010	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
8/27/2010	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.

Date	Revision History	Revision Class	Comments
10/8/2010	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
1/7/2011	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
2/11/2011	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	4.0.11	None	No changes to the meaning, language, or formatting of the technical content.
6/17/2011	4.1	Minor	Clarified the meaning of the technical content.
9/23/2011	4.1	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	5.0	Major	Updated and revised the technical content.
3/30/2012	6.0	Major	Updated and revised the technical content.
7/12/2012	6.0	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	6.0	None	No changes to the meaning, language, or formatting of the technical content.
1/31/2013	6.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	7.0	Major	Updated and revised the technical content.
11/14/2013	7.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	7.0	None	No changes to the meaning, language, or formatting of the technical content.
5/15/2014	7.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	8.0	Major	Significantly changed the technical content.
10/16/2015	8.0	None	No changes to the meaning, language, or formatting of the technical content.
7/14/2016	8.0	None	No changes to the meaning, language, or formatting of the technical content.

Table of 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
3.1.5.1	Handling the MAC Field While Digesting DNS Messages.....	8
3.1.5.2	Support for the HDAC-MD5 Algorithm.....	8
3.1.5.3	Signing DNS Update Response Messages	9
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.....	16

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.

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:

Message Authentication Code (MAC): A message authenticator computed through the use of a symmetric key. 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 dynamic-link library (DLL) that implements the Security Support Provider Interface (SSPI) by making one or more security packages available to applications. Each security package provides mappings between an application's SSPI function calls and an actual security model's functions. Security packages support security protocols such as Kerberos authentication and NTLM.

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.

[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>

[RFC2136] Thomson, S., Rekhter Y. and Bound, J., "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997, <http://www.ietf.org/rfc/rfc2136.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>

[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., Esibov, L., Westhead, J., and Hall, R., "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 has to 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

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 the following sections.

3.1.5.1 Handling the MAC Field While Digesting DNS Messages

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.

3.1.5.2 Support for the HDAC-MD5 Algorithm

[\[RFC2845\]](#) 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.

3.1.5.3 Signing DNS Update Response Messages

As described in [RFC2136] section 3.8, the DNS server MUST send a DNS update response back to the DNS client after processing a DNS update request. If the DNS update request is signed and includes a TSIG record, as specified in [RFC3645] and [RFC2845] section 4, then the DNS server SHOULD [<1>](#) sign the DNS update response and include the resulting TSIG record as described in [RFC3645].

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.

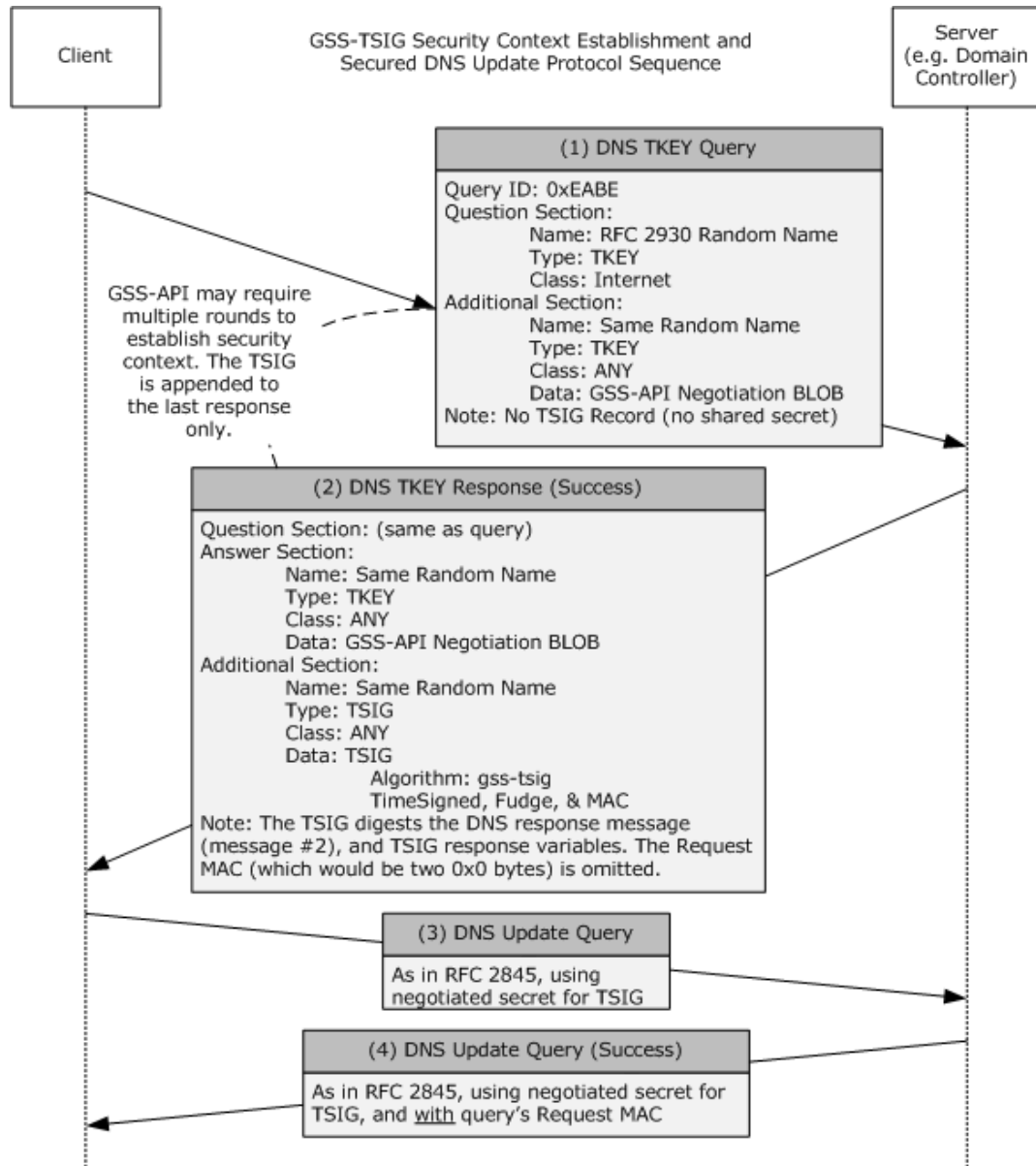


Figure 1: Example of a protocol sequence

```

- 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.

- 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
- 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 3.1.5.3](#): In the Windows implementation of the DNS server, the DNS client will find that the DNS server signed a DNS update response, as described in [\[RFC3645\]](#), only if the RCODE value in the response message is zero (indicating success).

If the RCODE value in the DNS update response message is not zero (indicating failure), the DNS client will find that the DNS server did not sign the response. Instead, the DNS server copied the DNS update request message, changed the RCODE value to the applicable nonzero error value, and sent that message back to the DNS client as the response. The message was otherwise unmodified; that is, the response message contains the same signature that was in the request message.

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

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

[Message processing](#) 8
Messages
 [overview](#) 7
 [syntax](#) 7
 [transport](#) 7

N

[Normative references](#) 5

O

Overview
 [common details](#) 8

[main](#) 6
 [Overview \(synopsis\)](#) 6

P

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

R

[References](#) 5
 [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