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

---

---

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
04/10/2007	1.0		Version 1.0 release
05/18/2007	1.2		Version 1.2 release
06/08/2007	1.2.1	Editorial	Revised and edited the technical content.
07/10/2007	1.3	Minor	Updated the technical content.
08/17/2007	1.3.1	Editorial	Revised and edited the technical content.
09/21/2007	1.3.2	Editorial	Revised and edited the technical content.
10/26/2007	1.3.3	Editorial	Revised and edited the technical content.
01/25/2008	1.3.4	Editorial	Revised and edited the technical content.
03/14/2008	1.3.5	Editorial	Revised and edited the technical content.
06/20/2008	1.3.6	Editorial	Revised and edited the technical content.
07/25/2008	1.3.7	Editorial	Revised and edited the technical content.
08/29/2008	1.3.8	Editorial	Revised and edited the technical content.
10/24/2008	1.3.9	Editorial	Revised and edited the technical content.
12/05/2008	2.0	Major	Updated and revised the technical content.
01/16/2009	3.0	Major	Updated and revised the technical content.
02/27/2009	4.0	Major	Updated and revised the technical content.
04/10/2009	4.0.1	Editorial	Revised and edited the technical content.
05/22/2009	4.0.2	Editorial	Revised and edited the technical content.
07/02/2009	4.0.3	Editorial	Revised and edited the technical content.
08/14/2009	4.0.4	Editorial	Revised and edited the technical content.
09/25/2009	4.0.5	Editorial	Revised and edited the technical content.
11/06/2009	4.0.6	Editorial	Revised and edited the technical content.
12/18/2009	4.0.7	Editorial	Revised and edited the technical content.
01/29/2010	4.0.8	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
03/12/2010	4.0.9	Editorial	Revised and edited the technical content.
04/23/2010	4.0.10	Editorial	Revised and edited the technical content.
06/04/2010	4.0.11	Editorial	Revised and edited the technical content.
07/16/2010	4.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
08/27/2010	4.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	4.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	4.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	4.0.11	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	4.0.11	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

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

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

[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., 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 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.

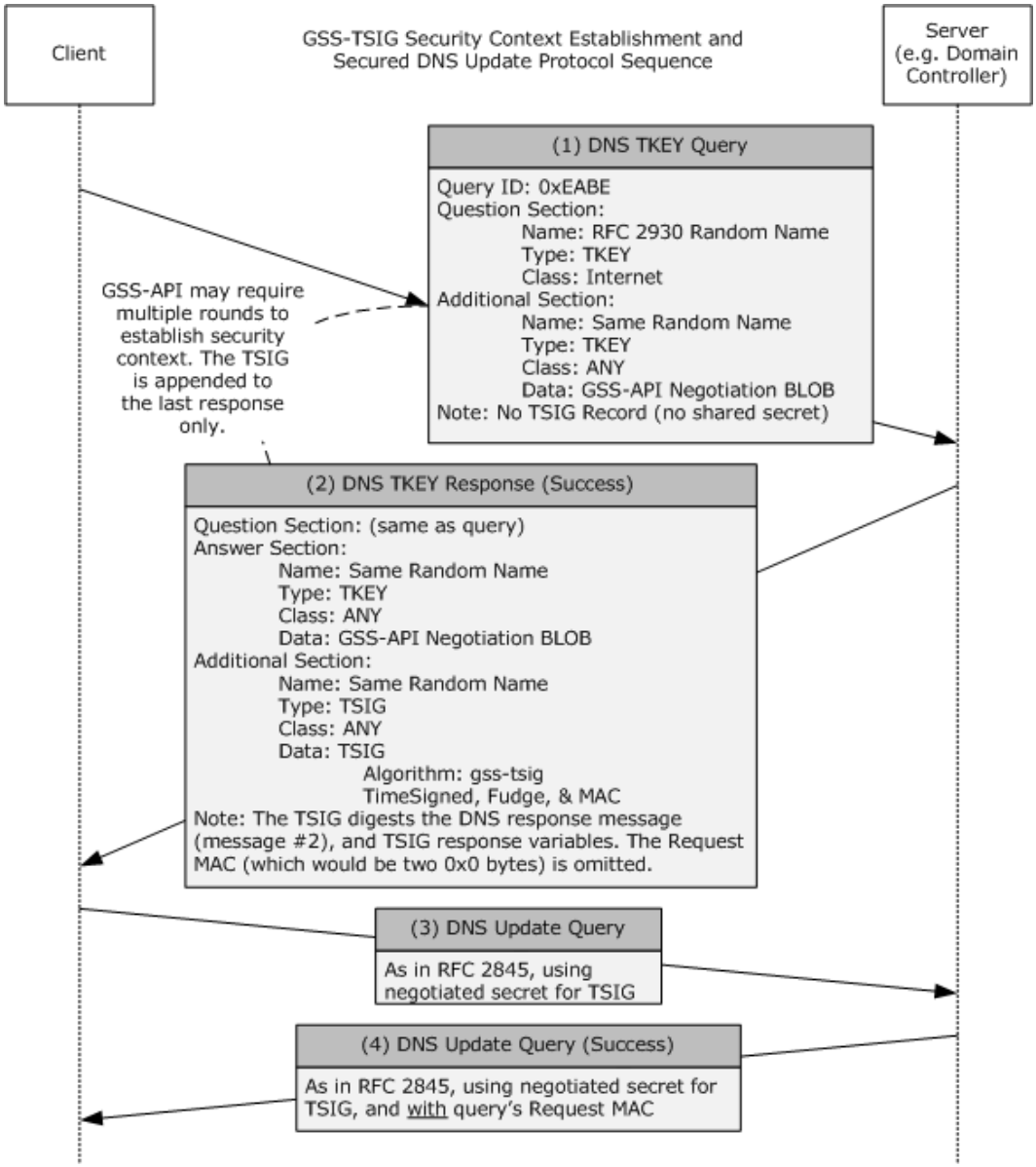

Figure 1: Example of a protocol sequence

```
- ~~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

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

8 Index