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

---

Revision Summary

Date	Revision History	Revision Class	Comments
05/11/2007	0.1		MCPP 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.

Date	Revision History	Revision Class	Comments
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.

Table of 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 a Microsoft proprietary extension to GSS-TSIG.

1.1 Glossary

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.

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

There are no informative references for this document.

1.3 Protocol Overview (Synopsis)

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 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

There is no version or capability negotiation in this protocol extension.

1.8 Vendor-Extensible Fields

There are no vendor-extensible fields in this protocol extension.

1.9 Standards Assignments

There are no standards assignments for this protocol extension.

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 is 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 **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.

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

3.1.1 Abstract Data Model

This protocol extension does not require any new abstract data models.

3.1.2 Timers

This protocol extension does not define any timers.

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

This protocol extension does not expect any events that are triggered by a higher layer.

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

This protocol extension does not define any timer events.

3.1.7 Other Local Events

This protocol extension does not define any other local events.

4 Protocol Examples

This protocol extension cannot be shown in an example. See section 3.1 for information on how GSS-TSIG, as specified in [RFC3645], has been extended.

5 Security

5.1 Security Considerations for Implementers

This protocol extension does not create any new security concerns for implementers.

5.2 Index of Security Parameters

This protocol extension does not define any new security parameters.

6 Appendix A: Windows Behavior

The information in this specification is applicable to the following versions of Windows:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Windows behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that Windows does not follow the prescription.

7 Index