

INTERNET-DRAFT

HMAC-SHA TSIG Identifiers
Donald E. Eastlake 3rd
Motorola Laboratories
July 2004

Expires: December 2004

HMAC SHA TSIG Algorithm Identifiers

<[draft-eastlake-tsig-sha-03.txt](#)>

Status of This Document

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

This draft is intended to become a Proposed Standard RFC. Distribution of this document is unlimited. Comments should be sent to the author.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than a "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Abstract

Use of the TSIG DNS resource record requires specification of a cryptographic message authentication code. Currently identifiers have been specified only for the HMAC-MD5 and GSS TSIG algorithms. This document specifies identifiers for additional HMAC SHA TSIG algorithms.

INTERNET-DRAFT

HMAC-SHA TSIG Identifiers

Table of Contents

Status of This Document.....[1](#)
Abstract.....[1](#)

Table of Contents.....[2](#)

[1](#). Introduction.....[3](#)

[2](#). Algorithms and Identifiers.....[4](#)

[3](#). IANA Considerations.....[5](#)
[4](#). Security Considerations.....[5](#)
[5](#). Copyright and Disclaimer.....[5](#)
[6](#). References.....[5](#)
[6.1](#) Normative References.....[5](#)
[6.2](#) Informative References.....[6](#)

Author's Address.....[7](#)
Expiration and File Name.....[7](#)

INTERNET-DRAFT

HMAC-SHA TSIG Identifiers

1. Introduction

[RFC 2845] specifies a TSIG Resource Record that can be used to authenticate DNS queries and responses. This RR contains a domain name syntax data item which names the authentication algorithm used. [RFC 2845] defines the HMAC-MD5.SIG-ALG.REG.INT name for authentication codes using the HMAC [RFC 2104] algorithm with the MD5 [RFC 1321] hash algorithm. IANA has also registered "gss-tsig" as an identifier for TSIG authentication where the cryptographic operations are delegated to GSS [RFC 3645]. This document specifies additional names for TSIG authentication algorithms based on US NIST SHA algorithms, HMAC, and truncation.

2. Algorithms and Identifiers

TSIG Resource Records (RRs) [[RFC 2845](#)] are used to authenticate DNS queries and responses. They are intended to be efficient symmetric authentication codes based on a shared secret. (Asymmetric signatures can be provided using the SIG RR [[RFC 2931](#)]. SIG(0) can be used for transaction signatures.) Used with a strong hash function, HMAC [[RFC 2104](#)] provides a way to calculate such symmetric authentication codes. The only specified HMAC based TSIG algorithm identifier has been HMAC-MD5.SIG-ALG.REG.INT based on MD5 [[RFC 1321](#)].

The use of SHA-1 [[FIPS 180-1](#), [RFC 3174](#)], which is a 160 bit hash as compared with the 128 bits for MD5, and additional hash algorithms in the SHA family [[FIPS 180-2](#), [RFC sha224](#)] with 224, 256, 384, and 512 bits, may be preferred in some case. Use of TSIG between a DNS resolver and server is by mutual agreement. That agreement can include the support of additional algorithms.

In some cases, it is reasonable to truncate the output of HMAC and use the truncated value for authentication. Since the syntax for TSIG algorithm identifiers is that of a domain name, this is indicated in these identifiers by a leading decimal label which gives the truncated length in bits. Because the DNS protocol is byte oriented,

such truncated lengths would normally be a multiple of 8. When truncation occurs, the bits used are the initial bits, trailing bits being discarded.

For completeness in relation to HMAC based algorithms, the current HMAC-MD5.SIG-ALG.REG.INT identifier is included in the table below. [FIPS 180-2, RFC sha224]

| | |
|-------------|--------------------------|
| Mandatory | HMAC-MD5.SIG-ALG.REG.INT |
| Recommended | sha1 |
| Recommended | 96.sha1 |
| Optional | sha224 |
| Optional | 168.sha224 |
| Optional | sha256 |
| Optional | 192.sha256 |
| Optional | sha384 |
| Optional | 320.sha384 |
| Optional | sha512 |
| Optional | 448.sha512 |

3. IANA Considerations

This document, on approval by IETF Consensus [RFC 2434], registers the new TSIG algorithm identifiers listed in Section 2 with IANA.

4. Security Considerations

For all of the message authentication code algorithms listed herein, those producing longer values are believed to be stronger.

See Security Considerations section of [RFC 2845].

[5.](#) Copyright and Disclaimer

Copyright (C) The Internet Society 2004. This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

[6.](#) References

[6.1](#) Normative References

[FIPS 180-2] - Secure Hash Standard, (SHA-1/256/384/512) US Federal Information Processing Standard, Draft, 1 August 2002.

[RFC 1321] - The MD5 Message-Digest Algorithm, R. Rivest, April 1992.

[RFC 2104] - HMAC: Keyed-Hashing for Message Authentication, H. Krawczyk, M. Bellare, R. Canetti, February 1997.

[RFC 2434] - Guidelines for Writing an IANA Considerations Section in RFCs, T. Narten, H. Alvestrand, October 1998.

[RFC 2845] - Secret Key Transaction Authentication for DNS (TSIG), P.

D. Eastlake 3rd

[Page 5]

INTERNET-DRAFT

HMAC-SHA TSIG Identifiers

Vixie, O. Gudmundsson, D. Eastlake, B. Wellington, May 2000.

[RFC sha224] - "A 224-bit One-way Hash Function: SHA-224", R. Housley, December 2003, [draft-ietf-pkix-sha224-*.txt](#).

[6.2](#) Informative References.

[FIPS 180-1] - Secure Hash Standard, (SHA-1) US Federal Information Processing Standard, 17 April 1995.

[RFC 3174] - US Secure Hash Algorithm 1 (SHA1), D. Eastlake, 3rd, P. Jones, September 2001.

[RFC 2931] - DNS Request and Transaction Signatures (SIG(0)s), D. Eastlake. September 2000.

[RFC 3645] - Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG), S. Kwan, P. Garg, J. Gilroy, L. Esibov, J. Westhead, R. Hall, October 2003.

Author's Address

Donald E. Eastlake 3rd
Motorola Laboratories
155 Beaver Street
Milford, MA 01757 USA

Telephone: +1-508-786-7554 (w)
+1-508-634-2066 (h)
EMail: Donald.Eastlake@motorola.com

Expiration and File Name

This draft expires in December 2004.

Its file name is [draft-eastlake-tsig-sha-03.txt](#)

