HMAC SHA TSIG Algorithm Identifiers

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 DNSEXT working group mailing list <namedroppers@ops.ietf.org>.

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 as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-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 standardizes identifiers and implementation requirements for additional HMAC SHA TSIG algorithms and standardizes how to specify and handle the truncation of HMAC values.

Copyright Notice

Copyright (C) The Internet Society 2005. All Rights Reserved.
Table of Contents

Status of This Document.................................1
Abstract..................................................1
Copyright Notice.........................................1

Table of Contents........................................2

1. Introduction...........................................3
2. Algorithms and Identifiers............................4
3. Specifying Truncation................................5
4. TSIG Policy Provisions and Truncation Error............6
5. IANA Considerations....................................7
6. Security Considerations...............................7
7. Copyright and Disclaimer...............................7
8. Normative References................................8
9. Informative References...............................8

Author’s Address.........................................9
Expiration and File Name.................................9
1. Introduction

[RFC 2845] specifies a TSIG Resource Record (RR) 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].

In section 2, this document specifies additional names for TSIG authentication algorithms based on US NIST SHA algorithms and HMAC and specifies the implementation requirements for those algorithms.

In section 3, this document specifies the meaning of inequality between the normal output size of the specified hash function and the length of MAC (message authentication code) data given in the TSIG RR. In particular, it specifies that a shorter length field value specifies truncation and a longer length field is an error.

In section 4, policy restrictions and implications related to truncation and a new error code to indicate truncation shorter than permitted by policy are described and specified.

The use herein of MUST, SHOULD, MAY, MUST NOT, and SHOULD NOT is as defined in [RFC 2119].
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]. In particular, 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 3874] with 224, 256, 384, and 512 bits, may be preferred in some cases particularly since increasingly successful cryptanalytic attacks are being made on the shorter hashes. Use of TSIG between a DNS resolver and server is by mutual agreement. That agreement can include the support of additional algorithms and may specify policies as to which algorithms and truncations are acceptable subject to the restriction and guidelines in Section 3 and 4 below.

The current HMAC-MD5.SIG-ALG.REG.INT identifier is included in the table below for convenience. Implementations which support TSIG MUST also implement HMAC SHA1 and HMAC SHA256 and MAY implement gss-tsig and the other algorithms listed below.

<table>
<thead>
<tr>
<th>Type</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory</td>
<td>HMAC-MD5.SIG-ALG.REG.INT</td>
</tr>
<tr>
<td>Mandatory</td>
<td>hmac-sha1</td>
</tr>
<tr>
<td>Optional</td>
<td>hmac-sha224</td>
</tr>
<tr>
<td>Mandatory</td>
<td>hmac-sha256</td>
</tr>
<tr>
<td>Optional</td>
<td>hmac-sha384</td>
</tr>
<tr>
<td>Optional</td>
<td>hmac-sha512</td>
</tr>
</tbody>
</table>
3. Specifying Truncation

In some cases, it is reasonable to truncate the output of HMAC and use the truncated value for authentication. HMAC SHA-1 truncated to 96 bits is an optional available in several IETF protocols including IPSEC and TLS.

The TSIG RR [RFC 2845] includes a "MAC size" field, which gives the size of the MAC field in octets. But [RFC 2845] does not specify what to do if this MAC size differs from the length of the output of HMAC for a particular hash function.

The specification for TSIG handling is changed as follows:

1. If "MAC size" field is greater than HMAC output length:
   This case MUST NOT be generated and if received MUST cause the packet to be dropped and RCODE 1 (FORMERR) to be returned.

2. If "MAC size" field equals HMAC output length:
   Operation is as described in [RFC 2845] with the entire output HMAC output present.

3. "MAC size" field is less than the larger of 10 (octets) and half the length of the hash function in use:
   With the exception of certain TSIG error messages described in RFC 2845 section 3.2 where it is permitted that the MAC size be zero, this case MUST NOT be generated and if received MUST cause the packet to be dropped and RCODE 1 (FORMERR) to be returned. The size limit for this case can also, for the hash functions mentioned in this document, be stated as less than half the hash function length for hash functions other than MD5 and less than 10 octets for MD5.

4. "MAC size" field is less than HMAC output length but greater than that specified in case 3 above:
   This is sent when the signer has truncated the HMAC output to an allowable length, as described in RFC 2104, taking initial octets and discarding trailing octets. TSIG truncation can only be to an integral number of octets. On receipt of a packet with truncation thus indicated, the locally calculated MAC is similarly truncated and only the truncated values compared for authentication. The request MAC used when calculating the TSIG MAC for a reply is the truncated request MAC.

TSIG implementations SHOULD implement SHA-1 truncated to 96 bits (12 octets) and MAY implement any or all other truncations valid under case 4 above.
4. TSIG Policy Provisions and Truncation Error

Use of TSIG is by mutual agreement between a resolver and server. Implicit in such "agreement" are policies as to acceptable keys and algorithms and now, with the extensions in this document, truncations. In particular note the following:

Such policies MAY require the rejection of TSIGs even though they use an algorithm for which implementation is mandatory.

When a policy calls for the acceptance of a TSIG with a particular algorithm and a particular non-zero amount of truncation it SHOULD also permit the use of that algorithm with lesser truncation (a longer MAC).

Regardless of lower minimum MAC lengths specified by policy, a reply SHOULD be sent with a MAC at least as long as that in the corresponding request.

Implementations permitting policies with multiple acceptable algorithms and/or truncations SHOULD permit this list to be ordered by presumed strength and SHOULD allow different truncations for the same algorithm to be treated as separate entities in this list. When so implemented, policies SHOULD accept a presumed stronger algorithm and truncation than the minimum required by the policy.

If a TSIG is received with truncation which is permitted under Section 3 above but the MAC is too short for the policy in force, an RCODE of TBA [22 suggested](BADTRUNC) MUST be returned.
5. IANA Considerations

This document, on approval for publication as a standards track RFC, (1) registers the new TSIG algorithm identifiers listed in Section 2 with IANA and (2) allocates the BADTRUNC RCODE TBA [22 suggested].

6. Security Considerations

For all of the message authentication code algorithms listed herein, those producing longer values are believed to be stronger; however, while there are some arguments that mild truncation can strengthen a MAC by reducing the information available to an attacker, excessive truncation clearly weakens authentication by reducing the number of bits an attacker has to try to force [RFC 2104].

Significant progress has been made recently in cryptanalysis of hash function of the type used herein, all of which ultimately derive from the design of MD4. While the results so far should not effect HMAC, the stronger SHA-1 and SHA-256 algorithms are being made mandatory due to caution.

See also the Security Considerations section of [RFC 2845].

6. Copyright and Disclaimer

Copyright (C) The Internet Society 2005. 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.
7. Normative References


8. Informative References.


Author’s Address

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

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

Expiration and File Name

This draft expires in September 2005.

Its file name is draft-ietf-dnsext-tsig-sha-02.txt