

## The HMAC-MD5 and HMAC-SHA-1 HTTP Digest Algorithms Tokens

### Status of this Memo

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

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/ietf/lid-abstracts.txt>](http://www.ietf.org/ietf/lid-abstracts.txt).

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

This Internet-Draft will expire in November 2004.

### Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

### Abstract

[RFC 3230](#) sets out a process for registering HTTP Digest algorithm values with IANA. This document registers the tokens "hmac-md5" and "hmac-sha-1".

### 1. Introduction.

[RFC 3230](#) [1] sets out a process for registering HTTP digest [2] algorithm values with IANA. This document registers two new values

in the IANA registry created by [RFC 3230](#).

## [2.](#) Newly registered Digest Algorithms.

The following are to be considered http digest algorithm tokens, as per [Section 4.1.1. of RFC 3230](#) [1].

HMAC-MD5	The HMAC-MD5 algorithm, as specified in <a href="#">RFC 2104</a> [3].
	The output of this algorithm is encoded using the base64 encoding [4].

HMAC-SHA-1	The HMAC-SHA-1 algorithm, as specified in <a href="#">RFC 2104</a> [3].
	The output of this algorithm is encoded using the base64 encoding [4].

## [3.](#) IANA Considerations.

The IANA is requested to insert the new values into the HTTP digest algorithm registry.

## [4.](#) Security Considerations.

In general, the registration of algorithm names and the association of those names with identifiable specifications helps ensure that all parties to a communication share a common understanding of the algorithm.

Note that the two algorithms registered by this action are keyed digests, and that they are appropriately used only in cases where the two parties can securely share the key. Because [RFC 3230](#) does not include a "parameters" field in the Digest: or Want-Digest: header (e.g. Want-Digest: hmac-md5;keyid=17), usage scenarios must not require the headers to indicate which key is in use through such a method.

## [5.](#) Normative References

- [1] Mogul, J. and Van Hoff, A. "Instance Digests in HTTP". [RFC 3230](#). January 2002.
- [2] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", [RFC 2617](#), June 1999.
- [3] Krawczyk, H., Bellare M., and Canetti, R. "HMAC: Keyed-Hashing for Message Authentication". [RFC 2140](#). February 1997.

- [4] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", [RFC 2045](#), November 1996.

## 6. Non-Normative References

None.

## 7. Acknowledgements.

AC Mahendran and Jun Wang originally suggested that these values be registered. Jeff Mogul was kind enough to review the first draft of this document and to suggest updated text for the Security Considerations section.

## 8. Author's Address

Ted Hardie Qualcomm, Inc. 675 Campbell Technology Parkway Suite 200  
Campbell, CA U.S.A.

EMail: [hardie@qualcomm.com](mailto:hardie@qualcomm.com)

## Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

#### Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.