Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 15, 2010

A. Bryan

January 11, 2010

Additional Hash Algorithms for HTTP Instance Digests
draft-bryan-http-digest-algorithm-values-update-04

Abstract

The IANA registry named "Hypertext Transfer Protocol (HTTP) Digest Algorithm Values" defines values for digest algorithms used by Instance Digests in HTTP. Instance Digests in HTTP provide a digest, also known as a checksum or hash, of an entire representation of the current state of a resource. This draft adds new values to the registry and updates previous values.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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/1id-abstracts.txt.

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

This Internet-Draft will expire on July 15, 2010.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Examples 3
2. IANA Considerations 3
2.1. Previous Registrations Updated 3
2.2. New Registrations 4
3. Security Considerations 4
4. Changes compared to RFC 3230 4
5. Normative References 4
Appendix A. Acknowledgements and Contributors 5
Appendix B. Document History 5
Author's Address 5

1. Introduction

The IANA registry named "Hypertext Transfer Protocol (HTTP) Digest Algorithm Values" defines values for digest algorithms used by Instance Digests in HTTP.

Note: This is unrelated to HTTP Digest Authentication. Instance Digests in HTTP provide a digest, also known as a checksum or hash, of an entire representation of the current state of a resource.

The registry was created by [RFC3230] in 2002. This draft adds new values to the registry and updates previous values which had redundant or outdated references.

[[Discussion of this draft should take place on IETF HTTP WG mailing list at ietf-http-wg@w3.org or directly to the author.]]

1.1. Examples

Examples of Instance Digest for SHA-256:

Digest: SHA-256=MWVkMWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFhOTlmNTQwYzI2M2QwM2U2MQ==

2. IANA Considerations

This document makes use of the IANA registry named "Hypertext Transfer Protocol (HTTP) Digest Algorithm Values" specified in [RFC3230].

2.1. Previous Registrations Updated

Accordingly, IANA has updated the following registrations:

Digest Algorithm: MD5

Description: The MD5 algorithm, as specified in [RFC1321]. The output of this algorithm is encoded using the base64 encoding [RFC4648].
Reference: [RFC1321] [RFC4648]

Digest Algorithm: SHA
Description: The SHA-1 algorithm [FIPS-180-3]. The output of this algorithm is encoded using the base64 encoding [RFC4648].
Reference: [FIPS-180-3] [RFC4648]

2.2. New Registrations

Accordingly, IANA has made the following registrations:

Digest Algorithm: SHA-256
Description: The SHA-256 algorithm [FIPS-180-3]. The output of this algorithm is encoded using the base64 encoding [RFC4648].
Reference: [FIPS-180-3] [RFC4648]

Digest Algorithm: SHA-512
Description: The SHA-512 algorithm [FIPS-180-3]. The output of this algorithm is encoded using the base64 encoding [RFC4648].
Reference: [FIPS-180-3] [RFC4648]

3. Security Considerations

Same as [RFC3230].

4. Changes compared to RFC 3230

All previous values to the registry are still valid.

The reference for base64 encoding has been updated for both MD5 and SHA.

The reference for SHA has been updated.

The SHA-256 and SHA-512 algorithms have been added to the registry.

5. Normative References

[FIPS-180-3]
National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", FIPS PUB 180-3, October 2008.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC3230] Mogul, J. and A. Van Hoff, "Instance Digests in HTTP", RFC 3230, January 2002.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

Appendix A. Acknowledgements and Contributors

Thanks to Mark Nottingham, Eran Hammer-Lahav, Nils Maier, Lisa Dusseault, Alfred Hoenes, Pasi Eronen, Gonzalo Camarillo, and Radia Perlman.

Appendix B. Document History

[[to be removed by the RFC editor before publication as an RFC.]]

Known issues concerning this draft:
- None known.

-04 : December 10, 2009.
- General Area Review Team (Gen-ART) review nits.

-03 : October 21, 2009.
- Make things look a bit nicer.

-02 : October 15, 2009.
- New title.

- "Note: This is unrelated to HTTP Digest Authentication."
- Remove SHA-224 and SHA-384.
- "Changes compared to RFC 3230" section added.

-01 : October 07, 2009.
- Update previous values that are outdated.
- RFC 4648 for Base64 encoding.

-00 : September 08, 2009.
- Initial draft.

Author's Address

Anthony Bryan
Pompano Beach, FL
USA

Email: anthonybryan@gmail.com
URI: http://www.metalinker.org