Internet Engineering Task Force (IETF)
Request for Comments: 5843
Category: Informational
ISSN: 2070-1721

A. Bryan
April 2010

Additional Hash Algorithms for HTTP Instance Digests

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 document adds new values to the registry and updates previous values.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5843.

Table of Contents

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 This document adds new values to the registry and updates previous values that had redundant or outdated references.

1.1. Example

Example 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], this document.

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], this document.

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], this document.

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], this document.

3. Security Considerations

Same as [RFC3230].

4. Changes Compared to RFC 3230

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.

All other previous values to the registry are still valid.

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, Radia Perlman, and Jeffrey Mogul.

Author's Address

Anthony Bryan
Pompano Beach, FL
USA

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