

HTTPbis Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 3, 2015

J. Reschke
greenbytes
January 30, 2015

The Hypertext Transfer Protocol (HTTP) Authentication-Info and Proxy-
Authentication-Info Response Header Fields
draft-ietf-httpbis-auth-info-00

Abstract

This specification defines the "Authentication-Info" and "Proxy-Authentication-Info" response header fields for use in HTTP authentication schemes which need to return additional information during or after authentication.

Editorial Note (To be removed by RFC Editor)

Discussion of this draft takes place on the HTTPBIS working group mailing list (ietf-http-wg@w3.org), which is archived at <https://lists.w3.org/Archives/Public/ietf-http-wg/>.

Working Group information can be found at <https://tools.ietf.org/wg/httpbis/> and <http://httpwg.github.io/>; source code and issues list for this draft can be found at <https://github.com/httpwg/http-extensions>.

The changes in this draft are summarized in [Appendix A](#).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on August 3, 2015.

Copyright Notice

Internet-Draft

HTTP Authentication-Info

January 2015

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

| | | |
|-----------------------------|---|-------------------|
| 1. | Introduction | 3 |
| 2. | Notational Conventions | 3 |
| 3. | The Authentication-Info Response Header Field | 3 |
| 3.1. | Parameter Value Format | 3 |
| 4. | The Proxy-Authentication-Info Response Header Field | 4 |
| 5. | Security Considerations | 4 |
| 6. | IANA Considerations | 4 |
| 7. | Acknowledgements | 5 |
| 8. | References | 5 |
| 8.1. | Normative References | 5 |
| 8.2. | Informative References | 5 |
| Appendix A. | Change Log (to be removed by RFC Editor before publication) | 5 |
| A.1. | draft-reschke-httpauth-auth-info-00 | 5 |

1. Introduction

This specification defines the "Authentication-Info" and "Proxy-Authentication-Info" response header fields for use in HTTP authentication schemes ([\[RFC7235\]](#)) which need to return additional information during or after authentication.

Both were previously defined in [Section 3 of \[RFC2617\]](#), defining the HTTP "Digest" authentication scheme. This document generalizes the description for use not only in "Digest" ([\[DIGEST\]](#)), but also other future schemes that might have the same requirements for carrying additional information during authentication.

2. Notational Conventions

This specification uses the Augmented Backus-Naur Form (ABNF) notation of [\[RFC5234\]](#) with a list extension, defined in [Section 7 of \[RFC7230\]](#), that allows for compact definition of comma-separated lists using a '#' operator (similar to how the '*' operator indicates repetition). The ABNF production for "auth-param" is defined in [Section 2.1 of \[RFC7235\]](#).

3. The Authentication-Info Response Header Field

HTTP authentication schemes can use the Authentication-Info response header field to return additional information applicable to the authentication currently in use.

The field value is a list of parameters (name/value pairs), using the "auth-param" syntax defined in [Section 2.1 of \[RFC7235\]](#). This specification only describes the generic format; authentication schemes using "Authentication-Info" will define the individual parameters. The "Digest" Authentication Scheme, for instance, defines multiple parameters in [Section 3.5.1 of \[DIGEST\]](#).

Authentication-Info = #auth-param

The Authentication-Info header field can be used in any HTTP response, independently of request method and status code. Its semantics are defined by the applicable authentication scheme. Intermediaries are not allowed to modify the field value in any way. Authentication-Info can be used inside trailers ([\[RFC7230\]](#), [Section 4.1.2](#)).

[3.1.](#) Parameter Value Format

Parameter values can be expressed either as "token" or as "quoted-string" ([Section 3.2.6 of \[RFC7230\]](#)).

Authentication scheme definitions need to allow both notations, both for senders and recipients. This allows recipients to use generic parsing components, independent of the authentication scheme in use.

For backwards compatibility, authentication scheme definitions can restrict the format for senders to one of the two variants. This can be important when it is known that deployed implementations will fail when encountering one of the two formats.

[4.](#) The Proxy-Authentication-Info Response Header Field

The Proxy-Authentication-Info response header field is equivalent to Authentication-Info, except that it applies to proxy authentication ([\[RFC7235\]](#)):

```
Proxy-Authentication-Info = #auth-param
```

[5.](#) Security Considerations

Adding information to HTTP responses that are sent over an unencrypted channel can affect security and privacy. The presence of the header fields alone indicates that HTTP authentication is in use. Additional information could be exposed by the contents of the authentication-scheme specific parameters; this will have to be considered in the definitions of these schemes.

[6.](#) IANA Considerations

HTTP header fields are registered within the "Message Headers" registry located at <http://www.iana.org/assignments/message-headers>, as defined by [BCP90].

This document updates the definitions of the "Authentication-Info" and "Proxy-Authentication-Info" header fields, so the "Permanent Message Header Field Names" registry shall be updated accordingly:

| Header Field Name | Protocol | Status | Reference |
|---------------------------|----------|----------|--|
| Authentication-Info | http | standard | Section 3 of this document |
| Proxy-Authentication-Info | http | standard | Section 4 of this document |

[7.](#) Acknowledgements

This document is based on the header field definitions in RFCs 2069 and 2617, whose authors are: John Franks, Phillip M. Hallam-Baker, Jeffery L. Hostetler, Scott D. Lawrence, Paul J. Leach, Ari Luotonen, Eric W. Sink, and Lawrence C. Stewart.

Additional thanks go to the members of the HTTPAuth and HTTPbis Working Groups, namely Amos Jeffries, Benjamin Kaduk, Alexey Melnikov, Yutaka Oiwa, Rifaat Shekh-Yusef, and Martin Thomson.

[8.](#) References

[8.1.](#) Normative References

- [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), January 2008.
- [RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), June 2014.

[RFC7235] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", [RFC 7235](#), June 2014.

[8.2.](#) Informative References

[BCP90] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", [BCP 90](#), [RFC 3864](#), September 2004.

[DIGEST] Shekh-Yusef, R., Ed., Ahrens, D., and S. Bremer, "HTTP Digest Access Authentication", [draft-ietf-httpauth-digest-12](#) (work in progress), January 2015.

[RFC2617] 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.

[Appendix A.](#) Change Log (to be removed by RFC Editor before publication)

[A.1.](#) [draft-reschke-httpauth-auth-info-00](#)

Changed boilerplate to make this an HTTPbis WG draft. Added Acknowledgements.

Reschke

Expires August 3, 2015

[Page 5]

Internet-Draft

HTTP Authentication-Info

January 2015

In the Security Considerations, remind people that those apply to unencrypted channels.

Make it clearer that these are really just response header fields.

Author's Address

Julian F. Reschke
greenbytes GmbH
Hafenweg 16
Muenster, NW 48155
Germany

EMail: julian.reschke@greenbytes.de

URI: <http://greenbytes.de/tech/webdav/>

