

Network Working Group	R. Fielding, Ed.	
Internet-Draft	Day Software	
Obsoletes: 2616 (if approved)	J. Gettys	
Updates: 2617 (if approved)	One Laptop per Child	
Intended status: Standards Track	J. Mogul	
Expires: August 28, 2008	HP	
	H. Frystyk	
	Microsoft	
	L. Masinter	
	Adobe Systems	
	P. Leach	
	Microsoft	
	T. Berners-Lee	
	W3C/MIT	
	Y. Lafon, Ed.	
	W3C	
	J. Reschke, Ed.	
	greenbytes	
	February 25, 2008	

[TOC](#)

HTTP/1.1, part 7: Authentication **draft-ietf-httpbis-p7-auth-02**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 August 28, 2008.

Abstract

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World Wide Web global information initiative since 1990. This document is Part 7 of the seven-part specification that defines the protocol referred to as "HTTP/1.1" and, taken together, obsoletes RFC 2616. Part 7 defines HTTP Authentication.

Editorial Note (To be removed by RFC Editor)

Discussion of this draft should take place on the HTTPBIS working group mailing list (ietf-http-wg@w3.org). The current issues list is at <http://www.tools.ietf.org/wg/httpbis/trac/report/11> and related documents (including fancy diffs) can be found at <http://www.tools.ietf.org/wg/httpbis/>.

This draft incorporates those issue resolutions that were either collected in the original RFC2616 errata list (<http://purl.org/NET/http-errata>), or which were agreed upon on the mailing list between October 2006 and November 2007 (as published in "draft-lafon-rfc2616bis-03").

Table of Contents

- [1.](#) Introduction
 - [1.1.](#) Requirements
- [2.](#) Notational Conventions and Generic Grammar
- [3.](#) Status Code Definitions
 - [3.1.](#) 401 Unauthorized
 - [3.2.](#) 407 Proxy Authentication Required
- [4.](#) Header Field Definitions
 - [4.1.](#) Authorization
 - [4.2.](#) Proxy-Authenticate
 - [4.3.](#) Proxy-Authorization
 - [4.4.](#) WWW-Authenticate
- [5.](#) IANA Considerations
- [6.](#) Security Considerations
 - [6.1.](#) Authentication Credentials and Idle Clients
- [7.](#) Acknowledgments
- [8.](#) References
 - [8.1.](#) Normative References
 - [8.2.](#) Informative References
- [Appendix A.](#) Compatibility with Previous Versions
 - [A.1.](#) Changes from RFC 2616

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

[B.1.](#) Since RFC2616

[B.2.](#) Since draft-ietf-httpbis-p7-auth-00

[B.3.](#) Since draft-ietf-httpbis-p7-auth-01

[§](#) Index

[§](#) Authors' Addresses

[§](#) Intellectual Property and Copyright Statements

1. Introduction

[TOC](#)

This document defines HTTP/1.1 access control and authentication. Right now it includes the extracted relevant sections of RFC 2616 with only minor changes. The intention is to move the general framework for HTTP authentication here, as currently specified in [\[RFC2617\] \(Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.\)](#), and allow the individual authentication mechanisms to be defined elsewhere. This introduction will be rewritten when that occurs.

HTTP provides several OPTIONAL challenge-response authentication mechanisms which can be used by a server to challenge a client request and by a client to provide authentication information. The general framework for access authentication, and the specification of "basic" and "digest" authentication, are specified in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\] \(Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.\)](#). This specification adopts the definitions of "challenge" and "credentials" from that specification.

1.1. Requirements

[TOC](#)

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\] \(Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.\)](#).

An implementation is not compliant if it fails to satisfy one or more of the MUST or REQUIRED level requirements for the protocols it implements. An implementation that satisfies all the MUST or REQUIRED level and all the SHOULD level requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the MUST

level requirements but not all the SHOULD level requirements for its protocols is said to be "conditionally compliant."

2. Notational Conventions and Generic Grammar

[TOC](#)

This specification uses the ABNF syntax defined in Section 2.1 of [\[Part1\] \(Fielding, R., Ed., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T., Lafon, Y., Ed., and J. Reschke, Ed., "HTTP/1.1, part 1: URIs, Connections, and Message Parsing," February 2008.\)](#). [\[abnf.dep\]](#) (ABNF syntax and basic rules will be adopted from RFC 5234, see <http://tools.ietf.org/wg/httpbis/trac/ticket/36>.)

The ABNF rules below are defined in other specifications:

```
challenge    = <challenge, defined in [RFC2617], Section 1.2>
credentials  = <credentials, defined in [RFC2617], Section 1.2>
```

3. Status Code Definitions

[TOC](#)

3.1. 401 Unauthorized

[TOC](#)

The request requires user authentication. The response MUST include a WWW-Authenticate header field ([Section 4.4 \(WWW-Authenticate\)](#)) containing a challenge applicable to the requested resource. The client MAY repeat the request with a suitable Authorization header field ([Section 4.1 \(Authorization\)](#)). If the request already included Authorization credentials, then the 401 response indicates that authorization has been refused for those credentials. If the 401 response contains the same challenge as the prior response, and the user agent has already attempted authentication at least once, then the user SHOULD be presented the entity that was given in the response, since that entity might include relevant diagnostic information. HTTP access authentication is explained in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\] \(Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.\)](#).

3.2. 407 Proxy Authentication Required

[TOC](#)

This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy. The proxy MUST return a Proxy-Authenticate header field ([Section 4.2 \(Proxy-Authenticate\)](#)) containing a challenge applicable to the proxy for the requested resource. The client MAY repeat the request with a suitable Proxy-Authorization header field ([Section 4.3 \(Proxy-Authorization\)](#)). HTTP access authentication is explained in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\] \(Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.\)](#).

4. Header Field Definitions

[TOC](#)

This section defines the syntax and semantics of HTTP/1.1 header fields related to authentication.

4.1. Authorization

[TOC](#)

A user agent that wishes to authenticate itself with a server--usually, but not necessarily, after receiving a 401 response--does so by including an Authorization request-header field with the request. The Authorization field value consists of credentials containing the authentication information of the user agent for the realm of the resource being requested.

Authorization = "Authorization" ":" credentials

HTTP access authentication is described in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\] \(Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.\)](#). If a request is authenticated and a realm specified, the same credentials SHOULD be valid for all other requests within this realm (assuming that the authentication scheme itself does not require otherwise, such as credentials that vary according to a challenge value or using synchronized clocks).

When a shared cache (see Section 9 of [\[Part6\] \(Fielding, R., Ed., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T., Lafon, Y., Ed., and J. Reschke, Ed., "HTTP/1.1, part 6: Caching," February 2008.\)](#)) receives a request containing an

Authorization field, it MUST NOT return the corresponding response as a reply to any other request, unless one of the following specific exceptions holds:

1. If the response includes the "s-maxage" cache-control directive, the cache MAY use that response in replying to a subsequent request. But (if the specified maximum age has passed) a proxy cache MUST first revalidate it with the origin server, using the request-headers from the new request to allow the origin server to authenticate the new request. (This is the defined behavior for s-maxage.) If the response includes "s-maxage=0", the proxy MUST always revalidate it before re-using it.
2. If the response includes the "must-revalidate" cache-control directive, the cache MAY use that response in replying to a subsequent request. But if the response is stale, all caches MUST first revalidate it with the origin server, using the request-headers from the new request to allow the origin server to authenticate the new request.
3. If the response includes the "public" cache-control directive, it MAY be returned in reply to any subsequent request.

4.2. Proxy-Authenticate

[TOC](#)

The Proxy-Authenticate response-header field MUST be included as part of a 407 (Proxy Authentication Required) response. The field value consists of a challenge that indicates the authentication scheme and parameters applicable to the proxy for this Request-URI.

Proxy-Authenticate = "Proxy-Authenticate" ":" 1#challenge

The HTTP access authentication process is described in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\]](#) (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.). Unlike WWW-Authenticate, the Proxy-Authenticate header field applies only to the current connection and SHOULD NOT be passed on to downstream clients. However, an intermediate proxy might need to obtain its own credentials by requesting them from the downstream client, which in some circumstances will appear as if the proxy is forwarding the Proxy-Authenticate header field.

4.3. Proxy-Authorization

[TOC](#)

The Proxy-Authorization request-header field allows the client to identify itself (or its user) to a proxy which requires authentication. The Proxy-Authorization field value consists of credentials containing the authentication information of the user agent for the proxy and/or realm of the resource being requested.

Proxy-Authorization = "Proxy-Authorization" ":" credentials

The HTTP access authentication process is described in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\]](#) (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.). Unlike Authorization, the Proxy-Authorization header field applies only to the next outbound proxy that demanded authentication using the Proxy-Authenticate field. When multiple proxies are used in a chain, the Proxy-Authorization header field is consumed by the first outbound proxy that was expecting to receive credentials. A proxy MAY relay the credentials from the client request to the next proxy if that is the mechanism by which the proxies cooperatively authenticate a given request.

4.4. WWW-Authenticate

[TOC](#)

The WWW-Authenticate response-header field MUST be included in 401 (Unauthorized) response messages. The field value consists of at least one challenge that indicates the authentication scheme(s) and parameters applicable to the Request-URI.

WWW-Authenticate = "WWW-Authenticate" ":" 1#challenge

The HTTP access authentication process is described in "HTTP Authentication: Basic and Digest Access Authentication" [\[RFC2617\]](#) (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.). User agents are advised to take special care in parsing the WWW-Authenticate field value as it might contain more than one challenge, or if more than one WWW-Authenticate header field is provided, the contents of a challenge itself can contain a comma-separated list of authentication parameters.

[TOC](#)

5. IANA Considerations

[\[anchor2\]](#) (TBD.)

6. Security Considerations

[TOC](#)

This section is meant to inform application developers, information providers, and users of the security limitations in HTTP/1.1 as described by this document. The discussion does not include definitive solutions to the problems revealed, though it does make some suggestions for reducing security risks.

6.1. Authentication Credentials and Idle Clients

[TOC](#)

Existing HTTP clients and user agents typically retain authentication information indefinitely. HTTP/1.1 does not provide a method for a server to direct clients to discard these cached credentials. This is a significant defect that requires further extensions to HTTP. Circumstances under which credential caching can interfere with the application's security model include but are not limited to:

- *Clients which have been idle for an extended period following which the server might wish to cause the client to reprompt the user for credentials.

- *Applications which include a session termination indication (such as a 'logout' or 'commit' button on a page) after which the server side of the application 'knows' that there is no further reason for the client to retain the credentials.

This is currently under separate study. There are a number of work-arounds to parts of this problem, and we encourage the use of password protection in screen savers, idle time-outs, and other methods which mitigate the security problems inherent in this problem. In particular, user agents which cache credentials are encouraged to provide a readily accessible mechanism for discarding cached credentials under user control.

7. Acknowledgments

[TOC](#)

TBD.

8. References

[TOC](#)

8.1. Normative References

[TOC](#)

[Part1]	Fielding, R., Ed., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T., Lafon, Y., Ed., and J. Reschke, Ed., "HTTP/1.1, part 1: URIs, Connections, and Message Parsing," draft-ietf-httpbis-p1-messaging-02 (work in progress), February 2008.
[Part6]	Fielding, R., Ed., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T., Lafon, Y., Ed., and J. Reschke, Ed., "HTTP/1.1, part 6: Caching," draft-ietf-httpbis-p6-cache-02 (work in progress), February 2008.
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997.
[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.

8.2. Informative References

[TOC](#)

[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," RFC 2616, June 1999.
-----------	--

Appendix A. Compatibility with Previous Versions

[TOC](#)

A.1. Changes from RFC 2616

[TOC](#)

[TOC](#)

Appendix B. Change Log (to be removed by RFC Editor before publication)

B.1. Since RFC2616

[TOC](#)

Extracted relevant partitions from [\[RFC2616\]](#) (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.).

B.2. Since draft-ietf-httpbis-p7-auth-00

[TOC](#)

Closed issues:

*<http://www3.tools.ietf.org/wg/httpbis/trac/ticket/35>: "Normative and Informative references"

B.3. Since draft-ietf-httpbis-p7-auth-01

[TOC](#)

Ongoing work on ABNF conversion (<http://www3.tools.ietf.org/wg/httpbis/trac/ticket/36>):

*Explicitly import BNF rules for "challenge" and "credentials" from RFC2617.

*Add explicit references to BNF syntax and rules imported from other parts of the specification.

Index

[TOC](#)

4	
	401 Unauthorized (status code)
	407 Proxy Authentication Required (status code)
A	
	Authorization header
G	
	Grammar
	Authorization

	challenge
	credentials
	Proxy-Authenticate
	Proxy-Authorization
	WWW-Authenticate
H	
	Headers
	Authorization
	Proxy-Authenticate
	Proxy-Authorization
	WWW-Authenticate
P	
	Proxy-Authenticate header
	Proxy-Authorization header
S	
	Status Codes
	401 Unauthorized
	407 Proxy Authentication Required
W	
	WWW-Authenticate header

Authors' Addresses

[TOC](#)

	Roy T. Fielding (editor)
	Day Software
	23 Corporate Plaza DR, Suite 280
	Newport Beach, CA 92660
	USA
Phone:	+1-949-706-5300
Fax:	+1-949-706-5305
Email:	fielding@gbiv.com
URI:	http://roy.gbiv.com/
	Jim Gettys
	One Laptop per Child
	21 Oak Knoll Road
	Carlisle, MA 01741
	USA
Email:	jg@laptop.org
URI:	http://www.laptop.org/
	Jeffrey C. Mogul
	Hewlett-Packard Company
	HP Labs, Large Scale Systems Group
	1501 Page Mill Road, MS 1177

	Palo Alto, CA 94304
	USA
Email:	JeffMogul@acm.org
	Henrik Frystyk Nielsen
	Microsoft Corporation
	1 Microsoft Way
	Redmond, WA 98052
	USA
Email:	henrikn@microsoft.com
	Larry Masinter
	Adobe Systems, Incorporated
	345 Park Ave
	San Jose, CA 95110
	USA
Email:	LMM@acm.org
URI:	http://larry.masinter.net/
	Paul J. Leach
	Microsoft Corporation
	1 Microsoft Way
	Redmond, WA 98052
Email:	paulle@microsoft.com
	Tim Berners-Lee
	World Wide Web Consortium
	MIT Computer Science and Artificial Intelligence Laboratory
	The Stata Center, Building 32
	32 Vassar Street
	Cambridge, MA 02139
	USA
Email:	timbl@w3.org
URI:	http://www.w3.org/People/Berners-Lee/
	Yves Lafon (editor)
	World Wide Web Consortium
	W3C / ERCIM
	2004, rte des Lucioles
	Sophia-Antipolis, AM 06902
	France
Email:	ylafon@w3.org
URI:	http://www.raubacapeu.net/people/yves/
	Julian F. Reschke (editor)
	greenbytes GmbH
	Hafenweg 16

	Muenster, NW 48155
	Germany
Phone:	+49 251 2807760
Fax:	+49 251 2807761
Email:	julian.reschke@greenbytes.de
URI:	http://greenbytes.de/tech/webdav/

Full Copyright Statement

[TOC](#)

Copyright © The IETF Trust (2008).

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, THE IETF TRUST 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.