

New protocol elements for HTTP Status Code 451
draft-sahib-451-new-protocol-elements-01

Abstract

This draft recommends protocol updates to Hypertext Transfer Protocol (HTTP) status code 451 (defined by [RFC7725](#)) based on an examination of how the new status code is being used by parties involved in denial of Internet resources because of legal demands. Also included is an analysis of HTTP 451 from a human rights perspective using guidelines from [RFC8280](#).

Discussion of this draft is at <https://www.ietf.org/mailman/listinfo/hrpc> [1] and <https://lists.ghserv.net/mailman/listinfo/statuscode451> [2].

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 <https://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 December 31, 2018.

Copyright Notice

Copyright (c) 2018 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 (<https://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	2
2.	Requirements	3
3.	Existing Protocol Elements	3
4.	Recommendations	3
5.	Security Considerations	4
6.	IANA Considerations	4
7.	Human Rights Considerations	5
7.1.	Connectivity	5
7.2.	Privacy	5
7.3.	Content Agnosticism	5
7.4.	Security	5
7.5.	Internationalization	5
7.6.	Censorship Resistance	6
7.7.	Open Standards	6
7.8.	Heterogeneity Support	6
7.9.	Anonymity	6
7.10.	Pseudonymity	6
7.11.	Accessibility	6
7.12.	Localization	6
7.13.	Decentralization	6
7.14.	Reliability	7
7.15.	Confidentiality	7
7.16.	Integrity	7
7.17.	Authenticity	7
7.18.	Adaptability	7
7.19.	Outcome Transparency	7
	Acknowledgements	8
9.	References	8
9.1.	Normative References	8
9.2.	URIs	9
	Author's Address	9

[1.](#) Introduction

[RFC7725] was standardized by the IETF in February 2016. It defined HTTP status code 451 - to be used when a "a server operator has received a legal demand to deny access to a resource or to a set of resources".

Sahib

Expires December 31, 2018

[Page 2]

Subsequently, an effort was made to investigate usage of HTTP 451 and evaluate if it fulfills its mandate of providing "transparency in circumstances where issues of law or public policy affect server operations" [[IMPL_REPORT_DRAFT](#)]. This draft attempts to explicate the protocol recommendations arising out of that investigation. In addition, specific recommendations are made in order to disambiguate cases where the status code may or may not be used.

2. Requirements

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](#)].

3. Existing Protocol Elements

The status code as standardized by the IETF specifies the following elements [[RFC7725](#)] -

- A server can return status code 451 to indicate that it is denying access to a resource or multiple resources on account of a legal demand. Note that while the introduction of [[RFC7725](#)] mentions that the legal demand for denial of access should be related to the resource being requested, the RFC's description does not make it clear that the resource being denied access to must be directly mentioned in the legal demand.
- Responses using the status code SHOULD include an explanation in the response body of the details of the legal demand.
- Responses SHOULD include a "Link" HTTP header field [[RFC8288](#)] whose value is a URI reference [[RFC3986](#)] identifying itself. The "Link" header field MUST have a "rel" parameter whose value is "blocked-by". The intent is that the header be used to identify the entity actually implementing blockage, not any other entity mandating it.

4. Recommendations

- HTTP 451 SHOULD NOT be used by an operator to deny access to a resource on the basis of a legal demand that is not specific to the requested resource.
- HTTP 451 SHOULD NOT be used by an operator to deny access to a resource on the basis of a policy specified by the operator (as opposed to a legal demand being placed on the operator).

- In addition to the "blocked-by" header, an HTTP response with status code 451 SHOULD include another "Link" HTTP header field which has a "rel" parameter whose value is "blocking-authority". It's important to distinguish between the implementer of the block, and the authority that mandated the block in the first place. This is because these two organizations might not be the same - a government (the blocking authority) could force an Internet Service Provider (the implementer of the block) to deny access to a certain resource. [[IMPL REPORT DRAFT](#)] notes that there is confusion amongst implementors of [[RFC7725](#)] about the meaning of the term "blocked-by", perhaps in part because of the example given [[ERRATA_ID-5181](#)] - it would be useful to explicitly include space for both, as both provide essential information about the legal block.
- HTTP status code 451 is increasingly being used to deny access to resources based on geographical IP. The response SHOULD contain a provisional header with geographical scope of block. This scope SHOULD correspond to comma-separated list of alpha-2 country codes defined in [[ISO.3166-1](#)]. The rationale for keeping the geographical scope to country-level granularity is that most blocks are mandated by national governments [[IMPL REPORT DRAFT](#)]. In addition, as the serving of this status code is voluntary, there is value in not complicating the specification.

5. Security Considerations

This document does not add additional security considerations to [[RFC7725](#)].

6. IANA Considerations

The Link Relation Type Registry should be updated with the following entry:

- Relation Name: blocking-authority
- Description: Identifies the authority that has issued the block.
- Reference: this document

In addition, IANA should be updated with the following provisional header:

- Header field name: geo-scope-block
- Applicable protocol: http

- Status: provisional
- Specification document(s): this document

7. Human Rights Considerations

The use of HTTP 451 has implications for human rights, and is thus worth examining under the guidelines for developing human rights considerations for protocols [[RFC8280](#)].

7.1. Connectivity

HTTP 451 status code response can be sent by the server hosting the blocked resource (end node) or an intermediary node that implements the block. If a resource is "blocked-by" a particular ISP then the ISP will be the one serving the status code.

7.2. Privacy

HTTP 451 is used as a response when the client requests a resource that's unavailable because of legal reasons. Consequentially, there are potential privacy (and anonymity) ramifications if there is leakage of who accessed what resource.

HTTP status code 451 is cacheable by default [[RFC7725](#)]. Caching status code 451 on users' devices means that there will be a record of their attempt to access the blocked content stored on their devices. If caching is used, the software used to access the web resource should notify users that the HTTP 451 response has been received and cached.

7.3. Content Agnosticism

The scope of the blocking order may be geographical in nature. This results in an issue related to content agnosticism. This is not a protocol issue, but rather an artefact of the blocking order.

7.4. Security

Refer to [section 5](#), Security Considerations, of [[RFC7725](#)].

7.5. Internationalization

[[RFC7725](#)] does not require the use of any particular language for user-facing strings such as the response body or the value of the header fields. The header field names, however, are in English. This is a common attribute of protocol elements within the IETF [[RFC2277](#)].

[7.6.](#) Censorship Resistance

While HTTP 451 status code cannot prevent censorship, it can help make some kinds of censorship (i.e. where the censorer is interested and able to provide information about the block) more transparent and make its assessment easier by providing information about the block in a parseable manner.

[7.7.](#) Open Standards

[RFC7725] is an open standard.

[7.8.](#) Heterogeneity Support

An HTTP 451 status code response can be used for any web resource and for any software that is capable of understanding HTTP header responses.

[7.9.](#) Anonymity

HTTP 451 is an HTTP status code. If the connection between the client and the server is not over HTTPS, then there is potential for a network observer to identify what a particular user is accessing. Even with HTTPS, meta-data might be available that could be used to identify a user.

[7.10.](#) Pseudonymity

HTTP 451 does not involve pseudonyms or nicknames.

[7.11.](#) Accessibility

HTTP 451, being an HTTP status code, does not prescribe how the client should parse the information contained in the response fields. Depending on the software that is used to access the resource, there could be accessibility concerns related to understanding this information.

[7.12.](#) Localization

The values of the header fields and the response body can be localized by the blocker to suit the geographical scope of the block.

[7.13.](#) Decentralization

HTTP 451 is used to provide information about a block mandated by a (centralized) blocking authority. The status code itself does not add any additional centralization.

7.14. Reliability

HTTP 451 does not by itself prevent the misuse of the status code or wrong tagging of resources. The informational requirement as part of the protocol address this concern to some extent, but commonly it will be difficult for the end user to verify if the code has been correctly used. Objective of this draft is to increase reliability by making it clearer what a good HTTP 451 response looks like.

7.15. Confidentiality

HTTP 451 status code use implies sharing of information by the reporter that make it easier to identify where censorship is taking place. See section on Privacy and Anonymity.

7.16. Integrity

HTTP 451 does not prescribe the use of any encryption to transport it, and is thus susceptible to leakage through man-in-the-middle attacks.

7.17. Authenticity

Authenticity of the server implementing HTTP 451 is dependent on the connection being over HTTPS.

7.18. Adaptability

HTTP 451 does not have any legal or technical limitations which prevents the development of other standards / protocols.

7.19. Outcome Transparency

The assumption behind the development of the status code 451 is that transparency has a chilling effect on censorship and that transparency will allow acts of censorship to be challenged. In some countries, block orders are unevenly implemented by ISPs either because it does not serve their bottom-lines or they are resisting censorship - governments in those countries could mandate the implementation of status code 451 which will make it easier for them to monitor the implementation of their block orders. Surveillance systems in some countries could be updated to watch out for the 451 error code on unencrypted traffic making it easier to identify those trying to access prohibited content. Before the implementation of this standard there would be no uniformity in which websites would implement a block order increasing the number of false positives for any automated monitoring systems.

Acknowledgements

Thanks to Alp Toker, Christine Runnegar, Niels ten Oever, Stephane Bortzmeyer, Corinne Cath and many others on the HRPC mailing list (linked above) for reviewing and brainstorming.

9. References

9.1. Normative References

- [ERRATA_ID-5181]
Bortzmeyer, S., "[Technical Errata Reported] [RFC7725](#) (5181)", 2017,
<<https://www.rfc-editor.org/errata/eid5181>>.
- [IMPL_REPORT_DRAFT]
Abraham, S., Canales, MP., Hall, J., Khrustaleva, O., ten Oever, N., Runnegar, C., and S. Sahib, "Implementation Report for HTTP Status Code 451", 2017,
<<https://tools.ietf.org/html/draft-451-imp-report-00>>.
- [ISO.3166-1]
International Organization for Standardization, "Codes for the representation of names of countries and their subdivisions - Part 1: Country code", ISO Standard 3166-1:1997 , 1997.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997,
<<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", [BCP 18](#), [RFC 2277](#), DOI 10.17487/RFC2277, January 1998, <<https://www.rfc-editor.org/info/rfc2277>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, [RFC 3986](#), DOI 10.17487/RFC3986, January 2005,
<<https://www.rfc-editor.org/info/rfc3986>>.
- [RFC7725] Bray, T., "An HTTP Status Code to Report Legal Obstacles", [RFC 7725](#), DOI 10.17487/RFC7725, February 2016,
<<https://www.rfc-editor.org/info/rfc7725>>.
- [RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", [RFC 8280](#), DOI 10.17487/RFC8280, October 2017, <<https://www.rfc-editor.org/info/rfc8280>>.

[RFC8288] Nottingham, M., "Web Linking", [RFC 8288](#), DOI 10.17487/RFC8288, October 2017, <<https://www.rfc-editor.org/info/rfc8288>>.

9.2. URIs

- [1] <https://www.irtf.org/mailman/listinfo/hrpc>
- [2] <https://lists.ghserv.net/mailman/listinfo/statuscode451>

Author's Address

Shivan Kaul Sahib

EMail: shivankaulsahib@gmail.com