

Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 20, 2016

M. Nottingham
February 17, 2016

The application/proxy-explanation+json media type
draft-nottingham-proxy-explanation-00

Abstract

This specification defines the application/proxy-explanation+json media type, to allow HTTP proxies to explain to clients why a request is unsuccessful.

Note to Readers

The issues list for this draft can be found at <https://github.com/mnot/I-D/labels/proxy-explanation> .

The most recent (often, unpublished) draft is at <https://mnot.github.io/I-D/proxy-explanation/> .

Recent changes are listed at <https://github.com/mnot/I-D/commits/gh-pages/proxy-explanation> .

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 20, 2016.

Copyright Notice

Copyright (c) 2016 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	2
1.1.	Notational Conventions	3
2.	The application/proxy-explanation+json Media Type	3
2.1.	Example	4
3.	IANA Considerations	4
4.	Security Considerations	5
5.	References	6
5.1.	Normative References	6
5.2.	URIs	7
Appendix A.	Acknowledgements	7
	Author's Address	7

[1.](#) Introduction

HTTP requests [[RFC7230](#)] to a proxy might not succeed variety of reasons; the request itself might violate a policy, or the requested content might be deemed unacceptable (e.g., it contains a virus, or itself violate a policy being imposed by the proxy).

For HTTP URLs, information about the reason is often injected into the HTTP response, so that the user understands what has happened, even if the message is only an HTML "Access Denied." This practice is problematic, because both users and non-browser clients can become confused about the source of the information, mistaking content from the proxy as being from the origin.

Furthermore, for HTTPS URLs, there is no way for the proxy to inform the end user about its actions. Proxies could provide HTML content in a 403 (Forbidden) response, but browsers are unwilling to show this to end users, since doing so would subject them to a potential man-in-the-middle attack.

This specification defines a new response format with a constrained vocabulary, so that proxies can communicate basic information about why a request has not succeeded, and browsers can provide that

information to users without risking it being mistaken for an authoritative response from the origin server.

[1.1](#). Notational Conventions

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](#)].

[2](#). The application/proxy-explanation+json Media Type

The "application/proxy-explanation+json" media type denotes a JSON [[RFC7159](#)] format whose root is an object containing the following members:

- o `*name*` - A short string identifying the party operating the proxy
- o `*title*` - A short string title for the explanation
- o `*description*` - A string explaining why the request wasn't successful
- o `*moreinfo*` - A string containing an absolute URL [[RFC3986](#)] which the user can find relevant information.

The "name" and "title" members MUST be present; all other members are OPTIONAL.

This media type MUST NOT be generated by origin servers and gateway servers (i.e., "reverse proxies" and "content delivery networks"); it is only intended to be generated by proxies. It MAY be generated by interception proxies (so-called "transparent proxies"), although as per below, it might be ignored by clients in this case.

It MUST NOT be used with a 2xx or 3xx status code, and clients MUST ignore its presence on them. Typical status codes that it will be

used with include 403 (Forbidden), 451 (Unavailable For Legal Reasons), 502 (Bad Gateway), and 504 (Gateway Timeout).

Proxies SHOULD carefully consider what caching metadata [[RFC7234](#)] is appropriate to include in such responses.

Clients MAY selectively support this media type. For example, an implementation might deem it only useful (or safe) in CONNECT requests.

Clients SHOULD indicate that they support this media type by including it in the field-value of the Accept request header field [[RFC7231](#)] of all supported requests.

[2.1.](#) Example

For example:

```
CONNECT www.example.net:80 HTTP/1.1
Host: www.example.net
Accept: application/proxy-explanation+json
Accept-Language: en-us

HTTP/1.1 403 Forbidden
Content-Type: application/proxy-explanation+json
Cache-Control: no-cache

{
  "name": "Acme Networks"
  "title": "Policy Violation"
  "description": "This content is above your pay grade."
  "moreinfo": "https://acme.example.com/why"
}
```

A browser might display this to the end user in a manner similar to this:

Policy Violation

The proxy "Acme Networks" says:

This content is above your pay grade.

For more information, see:

"https://acme.example.com/why?https://www.example.net"

3. IANA Considerations

This specification defines a new Internet Media Type [[RFC6838](#)]:

- o Type name: application
- o Subtype name: proxy-explanation+json
- o Required parameters: None
- o Optional parameters: None; unrecognised parameters should be ignored

Nottingham

Expires August 20, 2016

[Page 4]

Internet-Draft

Proxy Explanations

February 2016

- o Encoding considerations: Same as [[RFC7159](#)]
- o Security considerations: See [Section 4](#)
- o Interoperability considerations: None
- o Published specification: [this document]
- o Applications that use this media type: HTTP
- o Fragment identifier considerations: Same as [[RFC7159](#)]
- o Additional information:
 - * Deprecated alias names for this type: N/A
 - * Magic number(s): N/A
 - * File extension(s): N/A
 - * Macintosh file type code(s): N/A

- o Person & email address to contact for further information: Mark Nottingham mnot@mnot.net [4]
- o Intended usage: COMMON
- o Restrictions on usage: N/A
- o Author: Mark Nottingham mnot@mnot.net [5]
- o Change controller: IESG

4. Security Considerations

The approach taken in this specification precludes a proxy presenting itself as the origin, provided that, when presented to the user, the information is sufficiently contextualised as being from the proxy.

This approach does not preclude an origin server presenting itself as a the proxy, in cases where the client supports the media type on requests other than CONNECT.

Likewise, it does not prevent a man-in-the-middle from presenting itself as a proxy, in cases where the connection is unencrypted.

Because the payload can contain a URL, it could be used by an attacker (either a hostile origin or MitM, as above) to direct users

to an origin under their control. For example, an attacker could convince users that they need to provide payment before the network is available.

An attacker could also include a URL in the textual content of its message (e.g., in the "description" member), to encourage the user to copy the link and follow it.

However, both origins and cleartext MitMs can misrepresent their identities on the Web currently, without the benefit of this mechanism. These risks are introduced only when users trust the "proxy" interface more than they would trust a "normal" Web site.

They can be mitigated in a few ways:

- o Not displaying the "moreinfo" member in situations when this is possible (i.e., on any response other than that to a CONNECT on an encrypted connection).
- o Not supporting the "application/proxy-connection+json" media type when the method is not CONNECT and the connection is not encrypted.
- o Cautioning the user that the content might not be trustworthy.

5. References

5.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [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, <<http://www.rfc-editor.org/info/rfc3986>>.
- [RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", [BCP 13](#), [RFC 6838](#), DOI 10.17487/RFC6838, January 2013, <<http://www.rfc-editor.org/info/rfc6838>>.
- [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", [RFC 7159](#), DOI 10.17487/RFC7159, March 2014, <<http://www.rfc-editor.org/info/rfc7159>>.

- [RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), DOI 10.17487/RFC7230, June 2014, <<http://www.rfc-editor.org/info/rfc7230>>.
- [RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", [RFC 7231](#), DOI 10.17487/RFC7231, June 2014,

<<http://www.rfc-editor.org/info/rfc7231>>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", [RFC 7234](#), DOI 10.17487/RFC7234, June 2014, <<http://www.rfc-editor.org/info/rfc7234>>.

[5.2.](#) URIs

[1] <mailto:mnot@mnot.net>

[2] <mailto:mnot@mnot.net>

[Appendix A.](#) Acknowledgements

Thanks to Thomas Mangin for his suggestions.

Author's Address

Mark Nottingham

Email: mnot@mnot.net

URI: <https://www.mnot.net/>