

ADD
Internet-Draft
Updates: [8484](#) (if approved)
Intended status: Standards Track
Expires: October 19, 2020

M. Boucadair
Orange
N. Cook
Open-Xchange
T. Reddy
McAfee
D. Wing
Citrix
April 17, 2020

**Supporting Redirect Responses in DNS Queries over HTTPS (DoH)
draft-btw-add-rfc8484-clarification-01**

Abstract

This document clarifies whether DNS-over-HTTPS (DoH) redirection is allowed and specifies how redirection is thus performed.

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 October 19, 2020.

Copyright Notice

Copyright (c) 2020 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.	Terminology	2
3.	Discussion	2
4.	RFC8484 Update	4
5.	Resolving the Redirect Domain	4
6.	Applicability to DoH Server Redirect	5
7.	Security Considerations	7
8.	IANA Considerations	7
9.	Acknowledgements	7
10.	References	7
10.1.	Normative References	7
10.2.	Informative References	8
Appendix A.	Server Push	8
	Authors' Addresses	9

[1.](#) Introduction

This document clarifies the intent of DNS-over-HTTPS (DoH) [[RFC8484](#)] whether redirection is allowed ([Section 4](#)), and subsequently specifies how redirection is performed ([Section 5](#)).

This document adheres to Section 4.3 of [[I-D.ietf-httpbis-bcp56bis](#)] which discusses the need for protocols using HTTP to specify redirect handling to avoid interoperability problems.

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)][[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

"A/AAAA" is used to refer to "A and/or AAAA records".

[3.](#) Discussion

[[RFC8484](#)] indicates that the support of HTTP redirection is one of DoH design goals ([Section 1](#)):

"The described approach is more than a tunnel over HTTP. It establishes default media formatting types for requests and responses but uses normal HTTP content negotiation mechanisms for

selecting alternatives that endpoints may prefer in anticipation of serving new use cases. In addition to this media type negotiation, it aligns itself with HTTP features such as caching, redirection, proxying, authentication, and compression.

The integration with HTTP provides a transport suitable for both existing DNS clients and native web applications seeking access to the DNS."

Nevertheless, [Section 3 of \[RFC8484\]](#) indicates the following:

"This specification does not extend DNS resolution privileges to URIs that are not recognized by the DoH client as configured URIs."

This looks like an internal inconsistency of [\[RFC8484\]](#) that is worth the clarification: is redirection allowed or not?

Also, [Section 3 of \[RFC8484\]](#) indicates that:

"A DoH client MUST NOT use a different URI simply because it was discovered outside of the client's configuration (such as through HTTP/2 server push) or because a server offers an unsolicited response that appears to be a valid answer to a DNS query."

Nevertheless, [\[RFC8484\]](#) does not:

- o specify under which conditions a discovered different URI can be used.
- o describe how a different URI can be discovered using HTTP/2 server push. The only available example in the mailing list archives clarifies that server push is an example of unsolicited responses.

The text was updated late in the publication process to address this comment: https://mailarchive.ietf.org/arch/msg/doh/f_V-tBgB-KRsLZhttX9tGt75cps/. The example provided in the thread (server push) is related to the second part of the above excerpt.

- o clarify that unsolicited messages from a trusted DoH server should be excluded.

A clarification is proposed in [Section 4](#). This clarification focuses on a "different URI" that might be discovered while communicating with an HTTP server.

Additionally, assuming that redirection is allowed, this specification recommends how it is achieved, specifically regarding

inline resolution of any domain name in the redirect URI. This is required because redirection to a domain-based URI requires DNS resolution of that domain name, which creates a potential bootstrapping problem (e.g., If DoH server is the only configured DNS server, redirecting the client to a new server by presenting a name will fail).

4. [RFC8484](#) Update

OLD:

A DoH client MUST NOT use a different URI simply because it was discovered outside of the client's configuration (such as through HTTP/2 server push) or because a server offers an unsolicited response that appears to be a valid answer to a DNS query.

NEW

A DoH client MUST NOT use a different URI that was discovered outside of the client's configuration when communicating with HTTP servers except via HTTP redirection from a configured URI ([Section 6.4 of \[RFC7231\]](#)).

Also, a DoH client MUST ignore an unsolicited response (such as through HTTP/2 server push) that appears to be a valid answer to a DNS query unless that response comes from a configured URI (as described in [Section 5.3](#)).

5. Resolving the Redirect Domain

Redirection in DoH is slightly different from "regular" HTTP redirection, in that the DoH server may be the only configured DNS resolver for the client (e.g., as per [Section 7.1 of \[RFC8310\]](#)). In that case, and assuming the redirect URI uses a domain name, the client will be unable to contact the URI returned in the redirect response unless the DoH server provides the resolution information for that domain as part of the response. Even if a DoH client has a plaintext DNS resolver configured, using that resolver is considered as a minimal privacy leakage [[RFC8310](#)].

Servers supporting DoH redirect MUST support returning the redirect response body mechanism described hereafter.

Note: "MUST" is used here because resolving the redirect name using Do53 (especially for the redirection discussion in [Section 6](#)) will fail in some configurations, e.g., https://wiki.mozilla.org/Trusted_Recursive_Resolver (network.trr.mode=3).

Concretely, the DoH server returns in the response body a DNS response with an 'application/dns-message' media type as specified in [Section 6 of \[RFC8484\]](#), containing any A and AAAA records for the domain name in the redirect URI, including any CNAMEs.

For example, if the redirect URI contains the domain name "redirect.example.com", and "redirect.example.com" is a CNAME pointing to "real.example.com", then an example response body would contain:

- o A CNAME record for "redirect.example.com"
- o Any A records for "real.example.com"
- o Any AAAA records for "real.example.com"

This approach is simple; no client or server support of server push is required, and it is also more efficient in terms of the amount of data transmitted.

An early version of this document considered the use of server push to provide the client with the required A/AAAA information (Appendix A). Nevertheless, such proposal has issues as discussed in Section 4.14 of [[I-D.ietf-httpbis-bcp56bis](#)].

6. Applicability to DoH Server Redirect

This section specifies how DoH server redirection can be safely used to present a different URI to a requesting DoH client ([Section 4](#)). To that aim, the DoH server may use HTTP redirection ([Section 6.4 in \[RFC7231\]](#) or [[RFC7538](#)]) and the mechanism discussed in [Section 5](#) to inform the client about the new URI and location of the DoH server.

The mechanism discussed in [[RFC7838](#)] MAY be implemented by a DoH server if the DoH service is authoritatively available at a separate network location. This mechanism requires the alternative service to present a certificate for the origin's host name. Nevertheless, [[RFC7838](#)] is not an option for some redirection scenarios (e.g., Section 7 of [[I-D.btw-add-home](#)]). Additional complications arise to provide redirection for the latter scenarios:

1. Every GET request with a new query name will require redirection, which is suboptimal. Indeed, a redirect will only affect a request and the DoH client will need to contact the base server for every request and get redirected. Also, permanent redirects for all these queries would also bloat the client's HTTP cache.

2. Using POST would solve the issue. Nevertheless POST responses are not widely cached as per [Section 4.2.3 of \[RFC7231\]](#).
3. What about relaxing [\[RFC7838\]](#) so that the alternate service presents a certificate of a sub-domain of the Origin?
4. A solution that provides the same benefits as POST but without the caching issues is needed. Such solution must then rely upon HTTP GET method. A candidate solution using GET is described hereafter.
5. At bootstrap, the DoH client sends a GET request against a well-known URI (can also be used to retrieve the URI Templates [\[I-D.ietf-dnsop-resolver-information\]](#)). The server can redirect the client to an alternate server. The server's response will include: the Authentication Domain Name (ADN) of the redirect server, a list of IP addresses to locate the redirect server, a list of URI Templates (e.g., `https://cpe123.example.net/dns-query{?dns}`), CNAME, etc. Subsequent queries will be sent to the redirected server.

An example of such response is depicted in Figure 1. The structure of the response is inspired by [Section 4.4.2 of \[RFC7975\]](#).

```
{
  "associated-resolvers": {
    "adn": [
      {
        "name": "cpe123.example.net",
        "uri-template": [
          "https://cpe123.example.net/dns-query{?dns}"
        ],
        "a": [
          "192.0.2.1",
          "192.0.2.2"
        ],
        "aaaa": [
          "2001:db8::1",
          "2001:db8::2"
        ],
        "ttl": 3600
      }
    ]
  }
}
```

Figure 1: Response Example

Unlike the GET discussed in the first bullet, this approach does not bloat the cache.

7. Security Considerations

DoH-related security considerations are discussed in [Section 9 of \[RFC8484\]](#).

[Section 9 of \[RFC7838\]](#) describes security considerations related to the use of alternate services.

DNS clients that ignore authentication failures and accept spoofed certificates will be subject to attacks (e.g., redirect to malicious servers, intercept sensitive data).

8. IANA Considerations

This document does not request any action from IANA.

9. Acknowledgements

Many thanks to Christian Jacquenet, Philippe Fouquart, and Ben Schwartz for the comments.

10. References

10.1. 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, <<https://www.rfc-editor.org/info/rfc2119>>.
- [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, <<https://www.rfc-editor.org/info/rfc7231>>.
- [RFC7538] Reschke, J., "The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)", [RFC 7538](#), DOI 10.17487/RFC7538, April 2015, <<https://www.rfc-editor.org/info/rfc7538>>.
- [RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", [RFC 7540](#), DOI 10.17487/RFC7540, May 2015, <<https://www.rfc-editor.org/info/rfc7540>>.

- [RFC7838] Nottingham, M., McManus, P., and J. Reschke, "HTTP Alternative Services", [RFC 7838](#), DOI 10.17487/RFC7838, April 2016, <<https://www.rfc-editor.org/info/rfc7838>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", [RFC 8310](#), DOI 10.17487/RFC8310, March 2018, <<https://www.rfc-editor.org/info/rfc8310>>.
- [RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", [RFC 8484](#), DOI 10.17487/RFC8484, October 2018, <<https://www.rfc-editor.org/info/rfc8484>>.

[10.2.](#) Informative References

- [I-D.btw-add-home]
Boucadair, M., Reddy, K. T., Wing, D., and N. Cook, "DNS-over-HTTPS and DNS-over-TLS Server Discovery and Deployment Considerations for Home Networks", [draft-btw-add-home-05](#) (work in progress), April 2020.
- [I-D.ietf-dnsop-resolver-information]
Sood, P., Arends, R., and P. Hoffman, "DNS Resolver Information Self-publication", [draft-ietf-dnsop-resolver-information-01](#) (work in progress), February 2020.
- [I-D.ietf-httpbis-bcp56bis]
Nottingham, M., "Building Protocols with HTTP", [draft-ietf-httpbis-bcp56bis-09](#) (work in progress), November 2019.
- [RFC7975] Niven-Jenkins, B., Ed. and R. van Brandenburg, Ed., "Request Routing Redirection Interface for Content Delivery Network (CDN) Interconnection", [RFC 7975](#), DOI 10.17487/RFC7975, October 2016, <<https://www.rfc-editor.org/info/rfc7975>>.

[Appendix A.](#) Server Push

The DoH specification allows the use of server push to send DNS responses ([Section 5.3 of \[RFC8484\]](#)). The typical use case for server push is when the server knows that the client will need to make a request for a resource, and so provides the answer to that request via the server push mechanism. Sending answers to queries

implies that the DoH server performs those queries itself, or retrieves them from its cache.

In this case, the DoH server knows that the DoH client will need to resolve the domain returned in the redirect URI. Therefore, after receiving the initial request which would lead to a redirect response, but before returning the response, the server sends a push promise frame ([Section 8.2.1 of \[RFC7540\]](#)) request URL to retrieve the A/AAAA resource records for the domain in the redirect response (for example, if the domain has both A and AAAA records, two push promise frames would be sent). Any intermediate CNAME records would result in additional push promise frames. Promise requests cannot contain a request body as specified in [Section 8.2.1 of \[RFC7540\]](#), thus they use the GET method specified in Sections [4.1](#) and [6](#) of [\[RFC8484\]](#). The A/AAAA responses are then sent in separate streams as specified in [Section 8.2.2 of \[RFC7540\]](#). Finally, the redirect response itself is sent.

An example of the use of server push for redirection is shown in Figure 2.

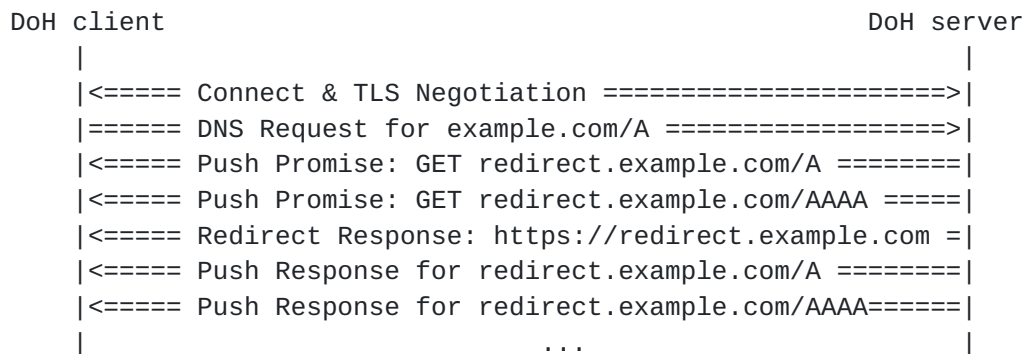


Figure 2: Redirect using Server Push

The advantage of using server push to provide the DNS resolution information of the redirect domain is that, assuming that the DoH client already supports unsolicited server push messages, then this approach should work without any changes.

Disadvantages include the possibility that DoH clients do not support server push.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Neil Cook
Open-Xchange
UK

Email: neil.cook@noware.co.uk

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: TirumaleswarReddy_Konda@McAfee.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com

