Workgroup: Network Working Group
Internet-Draft: draft-proxied-svcb-headers-00
Published: 19 February 2021
Intended Status: Standards Track
Expires: 23 August 2021
Authors: T. Pauly
Apple, Inc.

HTTP Header Fields for Proxied SVCB Metadata

Abstract

This document defines HTTP header fields for the passing Service Binding (SVCB) DNS metadata in HTTP responses.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/tfpauly/privacy-proxy.

Status of This Memo

This Internet-Draft will expire on 23 August 2021.

Copyright Notice

Table of Contents

1. Introduction

CONNECT [RFC7231] and CONNECT-UDP [I-D.ietf-masque-connect-udp] are HTTP methods that clients may use to establish TCP or UDP flows to target servers. Once proxy servers establish these flows, proxy servers treat allocated flows as opaque byte or datagram streams respectively. Clients specify the target in authority-form (Section 5.3 of [RFC7230]), including the name or IP address of the server along with a port number. When using a name instead of an IP address, the proxy server locally resolves the name to an IPv4 or IPv6 address with A or AAAA queries. The client does not see these A or AAAA answers, as they are only relevant to the proxy in establishing a connection to the target.

In some circumstances, some DNS metadata may be useful to clients. This is especially true for information contained in Service Binding (SVCB or HTTPS) records [I-D.ietf-dnsop-svcb-https]. These records can influence client behavior even when clients are not directly interacting with target IP addresses. The records can be used to determine which application-level protocols are supported by an endpoint. These records also can include a TLS Encrypted Client Hello [I-D.ietf-tls-esni] configuration, which can be used in protecting the end-to-end TLS handshake.

This document specifies HTTP header fields that proxy servers may use to relay information retrieved from SVCB records from proxy servers to clients when using CONNECT or CONNECT-UDP.

1.1. Requirements

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.

2. SVCB Request Header Field

Clients can request SVCB parameters with the Structured Header [RFC8941] "DNS-SVCB-Keys". Its value MUST be an sf-list whose members are sf-integer items that MUST NOT contain parameters. Its ABNF is:

```
DNS-SVCB-Keys = sf-list
```

Each list member corresponds to the numeric version of an SvcParamKey.

For example, a client wanting to receive ALPN and ECH Config parameters would send a request for 1 (alpn) and 5 (echconfig):

```
HEADERS
:method = CONNECT
:authority = svc.example.com:443
dns-svcb-keys = 1, 5
```

3. SVCB Response Header Fields

A proxy server that receives a request with "DNS-SVCB-Keys" MAY respond with the Structured Header "DNS-SVCB-Params" response header fields. The value of "DNS-SVCB-Params" MUST be an sf-list whose members are sf-string, each of which MUST contain parameters.

```
DNS-SVCB-Params = sf-list
```

Each list member is an sf-string that represents the TargetName of a single received SVCB or HTTPS record. The Parameters associated with each list member correspond to the SvcParam key-value pairs for that record, the priority of the record, and the TTL of the record.

The priority of the record MUST be a parameter with the key "priority", and a value as an sf-integer. Alias forms, with priority 0, MUST NOT be included.

The TTL of the record MUST be a parameter with the key "ttl", and a value as an sf-integer.

Each SvcParam that matches a key requested by the client is a parameters with a key that is the character "p" followed by the numeric version of the SvcParamKey. For example, the ALPN SvcParamKey, with the numeric value 1, would have a parameter key "p1". The value of each parameter MUST be an sf-binary item that contains the bytes of the SvcParamValue.

Proxy servers MUST NOT include the "DNS-SVCB-Params" response header field if the corresponding request did not include a "DNS-SVCB-Keys". Servers MAY include specific SvcParamKey values that were not requested. Specifically, servers SHOULD include the "mandatory" parameter if present, which would be presented as "p0", along with any parameters that are defined as mandatory for that record.

As an example, assume that the server received the following "svc.example.com" SVCB records:

```
svc.example.com. 3600 IN HTTPS 1 svc2.example.com. alpn=h2,h3 echconf
svc.example.com. 3600 IN HTTPS 2 . alpn=h2 echconfig="abc..."
```

A successful CONNECT response would include the following headers, if the client requested both "alpn" and "echconfig":

```
HEADERS
:method = CONNECT
:status = 200
dns-svcb-params = "svc2.example.com.";priority=1;ttl=3600;p1=:aDIsaDM=:;
                  "svc.example.com.";priority=2;ttl=3600;p1=:aDI=:;p5=:Y
```

4. IANA Considerations

4.1. HTTP Headers

This document registers the "DNS-SVCB-Keys" and "DNS-SVCB-Params", headers in the "Permanent Message Header Field Names" <https://www.iana.org/assignments/message-headers>.

Header Field Name	Protocol	Status	Reference
DNS-SVCB-Keys	http	exp	This document
DNS-SVCB-Params	http	exp	This document

5. Security Considerations

The "DNS-SVCB-Params" header in Section 3 does not include any DNSSEC information. Clients that depend on the contents of the SVCB record being DNSSEC-validated MUST NOT use this metadata without otherwise fetching the record and its corresponding RRSIG record and locally verifying its contents.

6. Normative References

[I-D.ietf-dnsop-svcb-https]

Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-02, 2 November 2020, <http://www.ietf.org/internet-drafts/draft-ietf-dnsop-svcb-https-02.txt>.

[I-D.ietf-masque-connect-udp] Schinazi, D., "The CONNECT-UDP HTTP Method", Work in Progress, Internet-Draft, draft-ietf-masque-connect-udp-03, 5 January 2021, <http://www.ietf.org/internet-drafts/draft-ietf-masque-connect-udp-03.txt>.

[I-D.ietf-tls-esni] Rescorla, E., Oku, K., Sullivan, N., and C. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-09, 16 December 2020, <http://www.ietf.org/internet-drafts/draft-ietf-tls-esni-09.txt>.

[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>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc7231>.

[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>.

[RFC8941] Nottingham, M. and P-H. Kamp, "Structured Field Values for HTTP", RFC 8941, DOI 10.17487/RFC8941, February 2021, <https://www.rfc-editor.org/info/rfc8941>.

Author's Address

Tommy Pauly
Apple, Inc.

Email: tpauly@apple.com