Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 4 September 2025

T. April
P. paek
ISC
R. Weber
Akamai Technologies
D. Lawrence
Salesforce
3 March 2025

Extensible Delegation for DNS using different transport protocols
draft-wesplaap-deleg-transport-00

Abstract

This document extends DELEG record, and SVCB records pointed to by DELEG record, as defined in [I-D.draft-wesplaap-deleg], with ability to specify transport protocols and authentication parameters supported by name servers.

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 4 September 2025.

Copyright Notice

Table of Contents

1. Introduction

The new delegation mechanism based on DELEG record type allows to specify attributes a resolver can use when talking to a delegated authority. This document introduces parameters specific to different transport mechanism than the default udp/53 protocol.

Legacy DNS resolvers unaware of DELEG mechanism would continue to use the NS and DS records, while resolvers that understand DELEG and its associated parameters can efficiently switch to new transports.

1.1. 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.

Terminology regarding the Domain Name System comes from [BCP219], with addition terms defined here:

* legacy transport name servers: An authoritative name server that only supports unencrypted DNS via UDP/TCP port 53

2. New DNS transports

There has been a lot of work defining new ways to transport DNS over new encrypted protocols. While most of this work was focusd on the client/stub resolver to recursive resolver connection the protocols will remain the same for an recursive to authoritative connections when iterating for a name. These are:

* DNS over TLS as defined in [RFC7858]

* DNS over HTTPS as defined in [RFC8484]

* DNS over Dedicated QUIC Connections RFC9250

While the DNS over HTTPs recommends HTTP/2 [RFC9113] as the minimum version there are no differences when using to over HTTP/3 [RFC9114].

2.1. Selecting transport protocols

The selection of the transport protocol to use to connect to an authoritative server for a delegation is done by the ALPN parameter as defined in [RFC9460].

If there is no ALPN parameter the connection MUST be established using unencrypted DNS over UDP/TCP on port 53.

If there is an ALPN parameter up to 4 protocols in the list MUST be tried to connect to the authoritative server.

The following ALPN are allowed to be used and may need the additional parameters as defined in this table: | ALPN | parameters | |-------|------------| | dot | | | doq | | | h2 | dohpath | | h3 | dohpath |

2.2. Authenticating transport protocols

As all defined transport protocols here rely on TLS the authentication for the authentication of them is identical. When no TLSA parameter is present authentication is MUST be done using the normal PKI infrastructure of the recursive resolver. The name used for the authentication is the target name of the DELEG or SVCB record. When a TLSA paramert is present the authentication MUST be done using the digests in that record

2.2.1. "TLSA" parameter

The "TLSA" SvcParamKey is a transport parameter representing a TLSA RRset [RFC6698] to be used when connecting to TargetName using a TLS-based transport.

The SvcParamValue is a non-empty value-list. The presentation and wire format of each value is the same as the presentation and wire format described for the TLSA record as defined in [RFC6698], sections 2.1 and 2.2 respectively. To avoid wasting resources in the parent zone parents MAY reject RRSets containing "tlsa" SvcParams that use matching type 0 (exact match).

2.2.2. Authentication Failures

When a resolver attempts to access nameserver delegated by a DELEG or SVCB record, if a connection error occurs, such as a certificate mismatch or unreachable server, the resolver SHOULD attempt to connect to the other nameservers delegated to until either exhausting the list or the resolver’s policy indicates that they should treat the resolution as failed.

3. Privacy Considerations

All of the information handled or transmitted by this protocol is public information published in the DNS.

4. Security Considerations

TODO: Fill this section out

5. IANA Considerations

5.1. New SvcParamKey Values

This document defines new SvcParamKey values in the "Service Binding (SVCB) Parameter Registry".

SvcParamKey	NAME	Meaning	Reference
TBD1	tlsa	TLSA RRset	(This Document)

Table 1

6. Informative References

[BCP219] Best Current Practice 219,
<https://www.rfc-editor.org/info/bcp219>.
At the time of writing, this BCP comprises the following:

Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219,
RFC 9499, DOI 10.17487/RFC9499, March 2024,
<https://www.rfc-editor.org/info/rfc9499>.

[I-D.draft-wesplaap-deleg]
April, T., paek, P., Weber, R., and Lawrence,
"Extensible Delegation for DNS", Work in Progress,
Internet-Draft, draft-wesplaap-deleg-02, 18 February 2025,
<https://datatracker.ietf.org/doc/html/draft-wesplaap-deleg-02>.

[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/rfc/rfc2119>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/rfc/rfc6698>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/rfc/rfc7858>.

[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/rfc/rfc8174>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018,
<https://www.rfc-editor.org/rfc/rfc8484>.

[RFC9113] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113,
DOI 10.17487/RFC9113, June 2022,
<https://www.rfc-editor.org/rfc/rfc9113>.

[RFC9114] Bishop, M., Ed., "HTTP/3", RFC 9114, DOI 10.17487/RFC9114,
June 2022, <https://www.rfc-editor.org/rfc/rfc9114>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/rfc/rfc9460>.

Appendix A. Acknowledgments

This draft is heavily based on past work (draft-tapril-ns2) done by Tim April and thus extends the thanks to the people helping on this which are: John Levine, Erik Nygren, Jon Reed, Ben Kaduk, Mashooq Muhaimen, Jason Moreau, Jerrod Wiesman, Billy Tiemann, Gordon Marx and Brian Wellington.

Appendix B. TODO

RFC EDITOR: PLEASE REMOVE THE THIS SECTION PRIOR TO PUBLICATION.

* Write a security considerations section

Appendix C. Change Log

RFC EDITOR: PLEASE REMOVE THE THIS SECTION PRIOR TO PUBLICATION.

~~~ 01234567890123456789012345678901234567890123456789012345678901234567891

Contributors

Christian Elmerot
Cloudflare
Email: christian@elmerot.se

Edward Lewis
ICANN
Email: edward.lewis@icann.org

Shumon Huque
Salesforce
Email: shuque@gmail.com
~~~

Klaus Darilion
nic.at
Email: klaus.darilion@nic.at

Libor Peltan
CZ.nic
Email: libor.peltan@nic.cz

Vladimr unt
CZ.nic
Email: vladimir.cunat@nic.cz

Shane Kerr
NS1
Email: shane@time-travellers.org

David Blacka
Verisign
Email: davidb@verisign.com

George Michaelson
APNIC
Email: ggm@algebras.org

Ben Schwartz
Meta
Email: bemasc@meta.com

Jan Velk
NS1
Email: jvcelak@ns1.com

Peter van Dijk
PowerDNS
Email: peter.van.dijk@powerdns.com

Philip Homburg
NLnet Labs
Email: philip@nlnetlabs.nl

Erik Nygren
Akamai Technologies
Email: erik+ietf@nygren.org

Vandan Adhvaryu
Team Internet
Email: vandan@adhvaryu.uk

Manu Bretelle
Meta
Email: chantr4@gmail.com

Authors' Addresses

Tim April
Email: ietf@tapril.net

Petr paek
ISC
Email: pspacek@isc.org

Ralf Weber
Akamai Technologies
Email: rweber@akamai.com

David C Lawrence
Salesforce
Email: tale@dd.org