Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 27 November 2026

P. Hoffman
ICANN
R. Weber
Akamai Technologies

26 May 2026

DELEG Extensions for Secure Transports
draft-hoffman-deleg-secure-transports-00

Abstract

The DELEG base protocol allows a DNS zone operator to specify servers to be used when delegating zones to other DNS nameservers. This document extends the base protocol to allow zone operators to specify secure transports for those delegations.

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 27 November 2026.

Table of Contents

1. Introduction

In the DELEG base protocol ([I-D.ietf-deleg]), a DNS zone operator uses the DELEG resource record to delegate zones to other DNS nameservers. In the base protocol, that delegation is always assumed to be using classical DNS on port 53. Some operators want to use secure transports for their name service, and want DELEG-aware resolvers to use those transports for name resolution. This document defines extensions to the DELEG record to allow such specification.

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.

2. Extensions for Secure Transports

This document defines new DelegInfo DelegInfoKey values: secure-transport, no-do53, and tlsa. The DelegInfoValue for secure-transport is an unordered collection of names of transports. There is no DelegInfoValue for no-do53. The DelegInfoValue for tlsa-desc is a string reprinting an TLSA record.

2.1. The secure-transport Key

The secure-transport DelegInfoKey lists the secure transports that are supported for a particular delegation target. It MUST only appear in a DelegInfos with a server-ipv4, server-ipv6 orserver-name DelegInfoKey. (This restriction might change if future specifications add new types of delegation targets.)

A DELEG-enabled resolver MAY use one or more of the listed values to choose a secure transport for its communications with the given delegation target. If no secure-transport key is given, the DELEG-aware resolver MUST use classical DNS over port 53 (Do53).

The values for the elements of the DelegInfoValue for the secure-transport DelegInfoKey are adot and adoq. Additional values may be defined in the future; see Section 4.2 for rules on how such values might be defined.

adot indicates that the delegation target from the server-ipv4, server-ipv6, or server-name DelegInfoKey supports DNS over TLS (DoT) [RFC7858].

adoq indicates that the delegation target from the server-ipv4, server-ipv6, or server-name DelegInfoKey supports DNS over QUIC (DoQ) [RFC9250].

Note that DNS over HTTPS (DoH) [RFC8484] is not supported by this document. This is because DoH adds no security over DoT, while adding complexity to both the client (the recursive resolver) and the server (the authoritative server). In addition, using DoH requires knowing the URI template, which would further complicate the DELEG RRset.

2.2. The no-do53 Key

The no-do53 DelegInfoKey indicates that the delegation target does not support Do53; it supports only secure transports. The no-do53 DelegInfoKey, which takes no value, MUST only appear in a DelegInfos with a secure-transport DelegInfoKey.

2.3. The tlsa Key

The tlsa DelegInfoKey indicates certificate authority (CA) and public key information that a DELEG-aware resolver MAY use for authenticating a DoT or DoQ connection. The value is a string that is a TLSA ([RFC6698]) Rdata in presentation format. It MUST only appear in a DelegInfos with a secure-transport key.

At the time that this document is written, ADoT and ADoQ servers use a variety of issuers for their TLS certificates: self-issued (often mistakenly called "self-signed"), a bespoke CA created for ADoT, and Web PKI issuers. All of these can be indicated in a tlsa value.

If there is no tlsa key, the resolver is free to choose any authentication mechanism, including accepting any certificate.

3. Examples

```
; A delegation target (IPv4 address) that is expected to respond
;   with ADoT and Do53
example. DELEG server-ipv4=192.0.2.1 secure-transport=adot

; A delegation target (server name) that is expected to respond
;   with ADoT, ADoQ, and Do53
example. DELEG server-name=ns1.xd secure-transport=adot,adoq

; A delegation target (IPv4 address) that is expected to respond
;   with ADoT but *not* over Do53
example. DELEG server-ipv4=192.0.2.1 secure-transport=adot no-do53

; A delegation with a tlsa key
example. DELEG server-name=ns1.xd secure-transport=adot (
   tlsa="0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
   7983a1d16e8a410e4561cb106618e971" }
```

4. IANA Considerations

4.1. Additions to "DELEG Delegation Information" Registry

IANA is requested to add the following values to the "DELEG Delegation Information" registry as described in [I-D.ietf-deleg].

Number: 5
Name: secure-transport
Meaning: An unordered collection of names of transports
Reference: This document
Change Controller: IETF

Number: 6
Name: no-do53
Meaning: Indicates an authoritative server does not support Do53
Reference: This document
Change Controller: IETF

Number: 6
Name: tlsa
Meaning: A TLSA Rdata associated with a secure transport
Reference: This document
Change Controller: IETF

4.2. Registry for the secure-transport Values

IANA is requested to create the "secure-transport DelegInfoKey values" registry. This is to be a sub-registry under the "DELEG Delegation Information" registry.

A registration MUST include the following fields:

Name: Unique presentation name
Meaning: A short description
Reference: Location of specification or registration source
Change Controller: Person or entity, with contact information if appropriate

To enable code reuse from SVCB parsers, the requirements for registered Name exactly copy requirements set by [RFC9460] section 14.3.1: The characters in the registered Name field entry MUST be lowercase alphanumeric or "-".

The registration policy for new entries is Expert Review ([RFC8126]). The designated expert MUST ensure that the reference is stable. The reference MAY be any individual’s Internet-Draft or a document from any other source with similar assurances of stability and availability.

Initial values for this registry are:

Name: adot
Meaning: Supports ADoT
Reference: This document
Change Controller: IETF

Name: adoq
Meaning: Supports ADoQ
Reference: This document
Change Controller: IETF

5. Security Considerations

Although this document defines an authentication mechanism Section 2.3, it does not require that DoT or DoQ sessions be authenticated. Of course, this reduces the normal level of TLS and QUIC security from "fully authenticated" to "not authenticated at all".

6. References

6.1. 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>.

[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/info/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/info/rfc8174>.

[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/info/rfc9250>.

[I-D.ietf-deleg] paek, P., Weber, R., and Lawrence, "Extensible Delegation for DNS", Work in Progress, Internet-Draft, draft-ietf-deleg-08, 16 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-deleg-08>.

6.2. Informative References

[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/info/rfc6698>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[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/info/rfc9460>.

Appendix A. Acknowledgements

Many people in the DELEG Working Group contributed early suggestions for this document.

Authors' Addresses

Paul Hoffman
ICANN
Email: paul.hoffman@icann.org

Ralf Weber
Akamai Technologies
Email: rweber@akamai.com