Network Working Group
Internet-Draft
Intended status: Informational
Expires: 7 November 2025

P. Hoffman
ICANN

6 May 2025

Getting Nameservers in the New Delegation Protocol
draft-hoffman-deleg-getting-names-08

Abstract

The DELEG Working Group has chosen a base protocol that describes how resolvers will be able to get a new DNS resource record to create a new process for DNS delegation. After a resolver gets this new type of record, it needs to know how to process the record in order to get a set of nameservers for a zone. This document lists many of the considerations for that process, including many open questions for the DELEG Working Group. More considerations and open questions might be added in later versions of this draft.

Note that this draft is _not_ intended to become an RFC. It is being published so that the DELEG Working Group has a place to point its efforts about how resolvers get nameservers for a zone while it continues to work on choosing a base protocol. The work that results from this might be included in the base protocol specification, or in a new draft authored by some of the many people who have done earlier work in this area.

Table of Contents

1. Introduction

The DELEG Working Group (https://datatracker.ietf.org/group/deleg/about/) charter says that the WG is choosing a base protocol, a "specification defining the new delegation information distribution mechanism". This document specifies how that information will appear in the new resource records from the base protocol, and what resolvers that receive those records will do with them.

According to the working group charter, after it has chosen the base protocol, it will specify a "specification for how to use the new delegation information to perform aliasing of delegation information" and "new DNS authoritative signaling mechanisms for alternative DNS transports". Section 2 and Section 3 of this document gives some idea for what those extensions might include, and how they related to the mechanisms in this document. The charter does not specify whether these two specifications need to be in different standards-track documents or can be in the same document.

1.1. The Base Protocol

The WG chose [I-D.draft-ietf-deleg] as the starting point for the base protocol. It will work on fixes and clarifications for many topics that came up during the consensus process, such as for root zone priming and interactions with DNSSEC. In this document, the base protocol is called "DELEG_base".

DELEG_base uses the same display and wire format as SVCB [RFC9460] for records returned to the resolver in delegation responses. In SVCB, the first field in the RR is called the "SvcPriority", and different values cause the resolver to go into "AliasMode" or "ServiceMode". The result of using this field in resolution is a set of "alternative endpoints". The second field is called "TargetName". The third field is optional, and is called "SvcParams"; it has a lot of sub-fields, some of which are useful for the DNS delegation use cases.

In order to not confuse this with specifics that DELEG_base gives beyond the base protocol, the new record type returned in delegation responses is called "DELEG_rr" here. (Of course, the name can be whatever the WG chooses in the eventual base protocol.) DELEG_rr has different semantics from SVCB because SCVB assumed a base protocol of HTTPS. DELEG_base gives different names to values for the first field in the RR, and for sub-fields in the optional third field. Other names from DELEG_base and SVCB are renamed here for clarity; the eventual names might be completely different.

The base protocol will allow for extensions in the third field. Those extensions might reuse entries in the IANA SVCB registry (https://www.iana.org/assignments/dns-svcb/dns-svcb.xhtml), they might add new extensions to that registry, or there might be a new registry for the DELEG_rr record.

2. Getting Nameserver Names for a Zone

The goal of the DELEG Working Group effort is to give resolvers a better way create a set of nameservers for a zone when making DNS queries to authoritative servers. In DELEG_base, when a resolver makes a query that gets a delegation response, the resolver may get back one or more DELEG_rr records and NS records that it can further process to create the set of nameservers for the zone. This eventual set of nameservers can be called the "DELEG_nameservers"; this is quite different from the set of DELEG_rr records it received.

In the DELEG_rr, the first field can be thought of as indicating the _action_ to find names for the DELEG_nameservers other than the NS records that might be at the apex, using the second field as a _target_ domain name where to look. The first field can be called "DELEG_action" and the second "DELEG_target". The third field, which holds metadata about the DELEG_target, can be called "DELEG_metadata"

The rest of this section describes how a resolver processes the DELEG_rr record, based on proposals made in [I-D.wesplaap-deleg], [I-D.homburg-deleg], and various discussions in the DELEG Working Group.

The WG discussion so far has led to general agreement a DELEG_action of value 0 means an action like "find a nameserver to be included in DELEG_nameservers elsewhere based on the value in the DELEG_target", and a value of 1 means something like "the name in DELEG_target is a nameserver for DELEG_nameservers". Thus, when a resolver receives one or more DELEG_rr records with a DELEG_action of 0, it needs to do more processing to complete the DELEG_nameservers set. When it receives one or more DELEG_rr records with a DELEG_action of 1, it copies the DELEG_target from those records and puts them into the DELEG_nameservers (possibly with additional information from the DELEG_metadata, such as from Section 3).

There has been much discussion in the WG about what action a resolver take when it gets a DELEG_action of 0. Some proposals include following chains of SVCB records, with some limits to prevent loops or excessive processing; others include following CNAME records, while others include querying DELEG_target for DELEG_rr records.

2.1. Additional Considerations for the WG on Filling the DELEG_nameservers Set

The resolver [[MAY / SHOULD / SHOULD NOT / MUST / MUST NOT]] use the NS records that were returned with the query to expand the DELEG_nameservers. (If SHOULD or SHOULD NOT is chosen by the WG, the exceptions need to be listed.)

If there are DELEG_rr records but the resolver ends up with nothing in the DELEG_nameservers, does it fall back to using the NS records in the original query?

Is the addition to the DELEG_nameservers different if following a DELEG_action of 0 leads to signed vs. unsigned responses? Asked another way, if the DELEG_nameservers contains some results that were signed and some that were unsigned, does the DELEG_nameservers become an ordered list or are the unsigned results discarded?

What is the TTL of the records in DELEG_nameservers? A likely answer (but not the only possible one) is the TTL on the DELEG_rr record that had a DELEG_action of 1. If so, this could mean that different delegation records in the DELEG_nameservers for the same zone might have different TTLs.

3. Addresses and Transports When Filling the DELEG_nameservers Set

Address and transport information in the DELEG_metadata can affect the addressed added to the DELEG_nameservers. Thus, these might become part of whatever document describes filling the DELEG_nameservers set, or these might be in a separate document that is referenced from the main addressing document.

The DELEG_metadata field in the DELEG_rr record will have a subfield to indicate the IPv4 and IPv6 address(es) associated with the DELEG_target. The subfield can be called "DELEG_ips".

The DELEG_metadata field in the DELEG_rr record will have a subfield to indicate the transport(s) associated with the DELEG_target. The subfield can be called "DELEG_transports".

3.1. Addresses

Can a DELEG_rr with a DELEG_action of 0 have a DELEG_ips in the record? In SVCB they cannot, but the SVCB spec allows other specs to allow them.

Is the value for the DELEG_ips a single address or potentially a list? If the former, how are multiple DELEG_rr records with the same DELEG_action and DELEG_target combined?

What happens if some of the discovered name/address pairs have different addresses? Does that disagreement in the DELEG_nameservers cause the removal of something from the DELEG_nameservers?

3.2. Transports

Can a DELEG_rr with a DELEG_action of 0 have a DELEG_transports in the record? In SVCB they cannot, but the SVCB spec allows other specs to allow them.

Some specific DNS transports will be allowed or required with DELEG_transports. Which secure transport(s), if any, will be mandory to implement?

Does supporting both TLS and QUIC make operational or security sense?

Does supporting DOH make operational or security sense if other secure transport is allowed?

If either or both TLS and DoH are allowed, which versions of TLS are allowed?

Does Do53 need to be specified every time it is available?

3.3. Authentication of Secure Transports

How will clients deal with authenticating TLS? Should they just use the web PKI pile of CAs, or will something else be specified?

Should certificates with IP addresses be supported?

Should clients ignore PKIX Extended Key Usage settings?

If authentication fails during a lookup, should the resolver fall back to unauthenticated encrypted transport, or should it retry on Do53, or should the DELEG_rr that contained this secure transport be ignored?

4. Priming the Root Zone

The current proposal for DELEG_base cannot be used to prime the root zone because the root zone is not its own parent. Different proposals have been made informally how to make a special case of the DELEG_base protocol to allow a DELEG_rr record to be legally served by root server operators to allow the advantages of DELEG_base (can be signed; can include IP addresses and transports) to cover the root zone.

Should such proposals be considered?

5. IANA Considerations

There may be IANA considerations when the working group finishes this work.

6. Security Considerations

There will certainly be security considerations when the working group finishes this work.

7. Informative References

[I-D.draft-ietf-deleg]
April, T., paek, P., Weber, R., and Lawrence, "Extensible Delegation for DNS", Work in Progress, Internet-Draft, draft-ietf-deleg-00, 6 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-deleg-00>.

[I-D.homburg-deleg]
Homburg, P., Wicinski, T., van Zutphen, J., and W. Toorop, "Extensible Delegation for DNS", Work in Progress, Internet-Draft, draft-homburg-deleg-01, 3 April 2025, <https://datatracker.ietf.org/doc/html/draft-homburg-deleg-01>.

[I-D.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>.

[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>.

Author’s Address

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