deleg
Internet-Draft
Intended status: Standards Track
Expires: 20 March 2026

R. Arends
ICANN
P. van Dijk
PowerDNS
P. paek
ISC

16 September 2025

DNS Protocol Modifications for Extended Delegation Type
draft-ppr-dd-auth-delegation-types-01

Abstract

The Domain Name System (DNS) protocol permits Delegation Signer (DS) records at delegation points. This document describes modifications to the Domain Name System (DNS) protocol to permit a range of resource record types at delegation points. These modifications are designed to maintain compatibility with existing DNS resolution mechanisms and provide a secure method for processing these records at delegation points.

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 20 March 2026.

Copyright Notice

Table of Contents

1. Introduction

[RFC4034] defines the Delegation Signer (DS) resource record as having a unique property: it resides at a delegation as authoritative data. Discussions and drafts within the DPRIVE, DNSOP, and DELEG working groups have highlighted interest in allowing additional types of data to be present at delegation points. This document reserves a range of Resource Record (RR) types allowed at delegations points and describes the protocol modifications for DNS implementations that support them.

To shield implementations that do not implement these modifications, a new EDNS(0) [RFC6891] option is introduced to indicate support for this range of RR types.

To protect against downgrade attacks, a new DNSKEY flag is introduced.

1.1. Conventions and Definitions

The term Extended Delegation types designates the set of RR types consisting of the range of RR types reserved in Section 2 of this document.

* Extended Delegation-aware name server or resolver: A server that implements this specification

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.

1.2. Relationship with the DELEG draft

The DELEG draft specifies a new resource record type (DELEG) that is authoritative at a delegation point and proposes protocol modifications to support DELEG.

The sole purpose of this document is to make sure that the protocol modifications are generic for a range of types instead of just a single record.

If the Working Group decides to separate the DELEG type specification from the protocol modifications needed to support Extended Delegations, we will incorporate all the necessary parts in this document.

If the Working Group decides to adopt the changes proposed in this specification into the DELEG draft, it is expected that these will be integrated in the DELEG specifications.

1.3. Relationship with NS and DS records

The use of DS and delegation point NS records is orthogonal to the use of Extended Delegation records. Both types MAY co-exist with Extended Delegation types.

1.4. Services Provided by Extended Delegation Types

Services provided by Extended Delegation types consist of information useful to a resolver when connecting to servers responsible for the delegated namespace. This can range from, but is not limited to, secure transport parameters, policy information about zones, DNSSEC security parameters, etc.

2. Extended Delegation Types

[RFC6895] contains three subcategories of RR type numbers: Data Types, Q-Types, and Meta-Types. This specification adds a fourth subcategory: Extended Delegation Types.

Considerations for the allocation of Extended Delegation Types are as follows:

Decimal	Hexadecimal	Registration Procedure
512-751	0x0200-0x02EF	Expert Review or Standards Action
752-767	0x02F0-0x02FF	Private Use

2.1. Updates to allocation policy

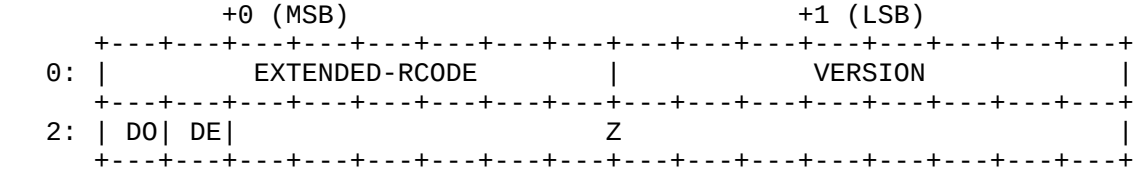
This section is to be written with guidance from the RFC6895 Experts Pool.

3. Resolver Requirements

To indicate Extended Delegation support, the resolver sets the Delegation Extensions (DE) flag in the EDNS(0) Flags field when sending a DNS request message.

3.1. The EDNS(0) DE Flag

The DE flag is carried in the OPT RR TTL field.



3.2. Referrals

Extended Delegation types in the authority section of a DNS response message indicate that the response contains a referral. Extended Delegation types are expected to contain all the information needed for a resolver to act on. Therefore, NS records that appear in addition to Extended Delegation types MUST be ignored. These NS records MUST NOT be validated or cached.

The purpose of this restriction is to avoid leakage of DNS messages over unencrypted transport when servers, indicated by Extended Delegation types, fail to respond.

When no Extended Delegation types exist, the resolver can use NS records. Note that the use of DNSSEC can prove the presence and absence of Extended Delegation types for a delegation.

4. Name Server Requirements

Extended Delegation-aware name servers MUST copy the value of the EDNS(0) DE flag from the request to the response.

4.1. Including Extended Delegation Types in a Referral Response

When the DE flag is set, the server includes Extended Delegation types in referrals and ignores NS types. When there are no Extended Delegation types for a referral, it includes NS types. The proof of existence of types for the delegated name MUST be included.

When the DE flag is clear, and no NS records exist for a referral, there is no facility for the resolver to continue resolving the delegated namespace. A name error SHOULD be returned in this case. While this may seem counterintuitive, since the name does exist, it is the only response code that stops the resolver from asking other authoritative name servers for the same information. Authoritative servers SHOULD include an Extended DNS Error [RFC8914] to clarify the reason.

4.2. Explicit queries for Extended Delegation Types

When the DE flag is set, a query for an Extended Delegation type SHOULD result in an authoritative answer when the Extended Delegation type exists, or a NODATA response (AA flag set, RCODE=0, empty answer section).

When the DE flag is clear, a query for an Extended Delegation type SHOULD result in an authoritative answer when the Extended Delegation type exists; in a referral with NS types when NS types exist, or in a NODATA response when other Extended Delegation types exist.

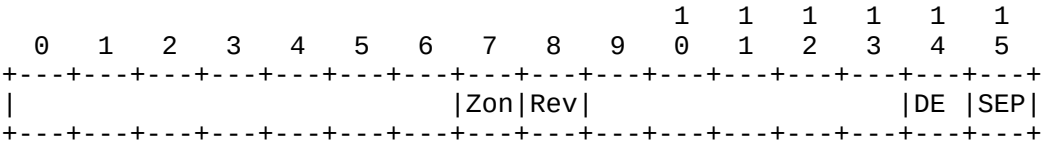
5. DNSSEC Requirements

In a DNSSEC signed zone, Extended Delegation RRsets MUST be signed.

To avoid a downgrade attack, where the Extended Delegation types and NSEC (or NSEC3) records can be replaced by unsigned NS records to cause the resolver to use unencrypted transport, a secure signal in the form of a DNSKEY flag is introduced. This secure signal indicates that NSEC or NSEC3 records MUST be present in a referral response.

5.1. The DNSKEY-DE flag

The DNSKEY Flags field consists of 16 bits:



Bit 14 is the Delegation Extension (DE) flag. It indicates to a validator that a referral MUST contain an NSEC or NSEC3 record to prove presence or absence of types for the delegated name.

5.2. Validating a Referral

When the DNSKEY-DE flag is set in any DNSKEY from the DNSKEY RRset of the delegating zone, the validator MUST check the Extended Delegation types in the authority section of the referral against the Type Bit Maps of the NSEC or NSEC3 record that matches the delegated name. If any are absent, the referral MUST be considered tampered with, and the response MUST be ignored.

6. Security Considerations

This section discusses security considerations, including downgrade attacks and resolver behavior. Further details will be added.

7. IANA Considerations

IANA is requested to change reservations in the DNS Parameters RR types registry, with this document as the Reference.

* Range 0x0200-0x02EF to Registration Procedure "Expert Review or Standards Action"
* Range 0x02F0-0x02FF to Registration Procedure "Private Use"

8. Acknowledgments

This idea was initially proposed by Petr Spacek, and independently by Paul Wouters.

9. References

9.1. 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>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC6895] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 6895, DOI 10.17487/RFC6895, April 2013, <https://www.rfc-editor.org/info/rfc6895>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

9.2. Informative References

[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>.

Authors' Addresses

Roy Arends
ICANN
Guernsey

Email: roy.arends@icann.org

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

Petr paek
ISC
Brno
Czech Republic
Email: pspacek@isc.org