

deleg
Internet-Draft
Intended status: Standards Track
Expires: 19 September 2026

R. Arends
ICANN
P. van Dijk
PowerDNS
P. paek
ISC
18 March 2026

DNS Protocol Modifications for Delegation Extensions
draft-ietf-dnsop-delext-02

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 19 September 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights

and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
1.1. Conventions and Definitions	3
1.2. Relationship with the DELEG draft	3
1.3. Relationship with NS and DS records	3
1.4. Services Provided by Delegation Types	3
2. Delegation Types	3
2.1. Updates to allocation policy	4
3. Resolver Requirements	4
3.1. The EDNS(0) DE Flag	4
3.2. Referrals	4
4. Name Server Requirements	4
4.1. Including Delegation Types in a Referral Response	5
4.2. Explicit queries for Delegation Types	5
5. DNSSEC Requirements	5
5.1. The DNSKEY-ADT flag	5
5.2. Validating a Referral	6
6. Security Considerations	6
7. IANA Considerations	6
8. Acknowledgments	6
9. References	6
9.1. Normative References	6
9.2. Informative References	7
Authors' Addresses	7

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 delegation 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 Delegation Types designates the set of RR types consisting of the range of RR types reserved in Section 2 of this document.

* Delegation-Extension-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 purpose of this document is to make sure that protocol modifications are generic for a range of types.

1.3. Relationship with NS and DS records

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

1.4. Services Provided by Delegation Types

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

2. Delegation Types

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

Considerations for the allocation of Delegation Types are as follows:

Decimal	Hexadecimal	Registration Procedure
61440-61935	0xF000-0xF1EF	Expert Review or Standards Action
61936-61951	0xF1F0-0xF1FF	Private Use

2.1. Updates to allocation policy

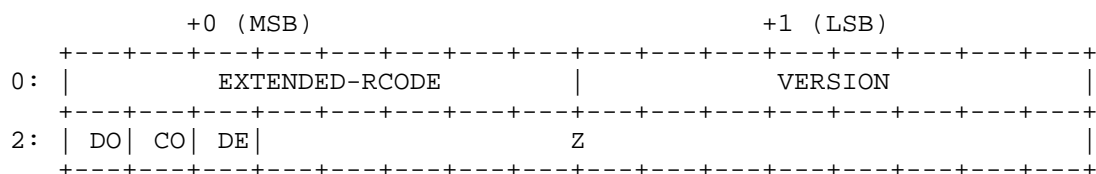
This section is to be written with guidance from the RFC6895 Experts Pool.

3. Resolver Requirements

To indicate Delegation Types 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

Delegation Types in the authority section of a DNS response message indicate that the response contains a referral. Delegation Types are expected to contain all the information needed for a resolver to act on. Therefore, NS records that appear in addition to 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 Delegation Types, fail to respond.

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

4. Name Server Requirements

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

4.1. Including Delegation Types in a Referral Response

When the DE flag is set, the server includes Delegation Types in referrals and ignores NS types. When there are no 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 Delegation Types

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

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

5. DNSSEC Requirements

In a DNSSEC-signed zone, Delegation Type RRsets **MUST** be signed.

To avoid a downgrade attack, where the Delegation Types and NSEC (or NSEC3) records can be replaced by unsigned NS records, causing 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-ADT flag

The DNSKEY Flags field consists of 16 bits:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
										Zon	Rev					ADT	SEP

Bit 14 is the Authoritative Delegation Types (ADT) 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-ADT flag is set in any DNSKEY from the DNSKEY RRset of the delegating zone, the validator MUST check the 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 0xF000-0xF1EF to Registration Procedure "Expert Review or Standards Action"
- * Range 0xF1F0-0xF1FF to Registration Procedure "Private Use"

8. Acknowledgments

This idea was initially proposed by Petr paek, 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