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

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

18 May 2026

DNS Protocol Modifications for Delegation Extensions
draft-ietf-dnsop-delext-03

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 November 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 delegation points and describes the protocol modifications for DNS implementations that support them.

To shield implementations that do not implement these modifications, an EDNS(0) [RFC6891] flag 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, resolver or stub resolver: A client or 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

[RFC6895] establishes the allocation policy for DNS Resource Record type numbers and defines the Expert Review process governing that allocation. This section updates that policy to account for the Delegation Types subcategory introduced in Section 2 and specifies the criteria that apply to allocation requests within the ranges 0xF000-0xF1EF and 0xF1F0-0xF1FF.

2.1.1. Criteria for Delegation Type Allocation

A Resource Record type MUST be allocated as a Delegation Type, rather than as a Data Type, if and only if all of the following conditions are met:

* The RR type is intended to appear at a delegation point as authoritative data in the delegating zone, in a manner analogous to the DS record as defined in [RFC4034].

* The RR type carries information that is intended to be acted upon by a resolver during the process of following a referral. This includes information used prior to sending queries to the authoritative servers for the delegated zone, or after the referral has been followed, such as material used to authenticate a DNSKEY in the delegated zone.

* The RR type is not intended to appear as authoritative data within the delegated zone itself.

RR types that do not meet all of these criteria SHOULD be allocated from the existing Data Types range in accordance with [RFC6895] and MUST NOT be allocated from the Delegation Types range.

The fact that a record type may be useful in the context of delegation does not by itself qualify it for allocation as a Delegation Type. Record types that convey information useful to resolvers but that are intended to appear within a zone rather than at its delegation point in the delegating zone are Data Types and MUST be allocated accordingly.

2.1.2. Expert Review Procedure

Allocation requests in the range 0xF000-0xF1EF require Expert Review or Standards Action, as specified in Section 2. The Designated Experts for this range are drawn from the RFC6895 Experts Pool.

In addition to the general Expert Review criteria established by [RFC6895], the Designated Experts MUST evaluate allocation requests for Delegation Types against the criteria in Section 2.1.1. The Designated Experts SHOULD also consider:

* Whether the proposed Delegation Type requires protocol modifications beyond those defined in this document, and if so, whether those modifications have been or are being specified in an appropriate Standards Track document.

* Whether the proposed Delegation Type can be processed safely by Delegation-Extension-aware implementations that do not specifically implement the proposed type, in particular with respect to the requirements in Section 3.2 and Section 4.1.

* Whether the security properties of the proposed Delegation Type are compatible with the DNSSEC signing requirements of Section 5, and whether any additional security considerations apply.

The Designated Experts MAY approve allocation requests accompanied by a stable, publicly available specification that need not be an RFC, provided that the specification is sufficiently detailed to allow independent interoperable implementation. Allocation requests for Delegation Types that introduce new protocol behaviors or that interact with the mechanisms defined in Section 3, Section 4, or Section 5 of this document SHOULD be accompanied by, or integrated into, a Standards Track document.

2.1.3. Private Use Range

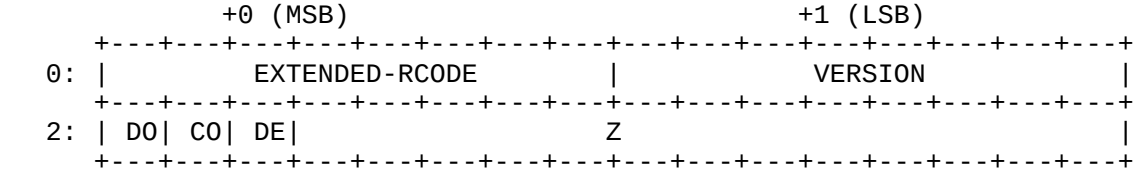
The range 0xF1F0-0xF1FF is reserved for Private Use in accordance with [RFC8126]. Values in this range MUST NOT appear in the global DNS and MUST NOT be used in any context where interoperability with implementations outside a private network is required. Private Use values are not subject to Expert Review and will not be registered by IANA.

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.

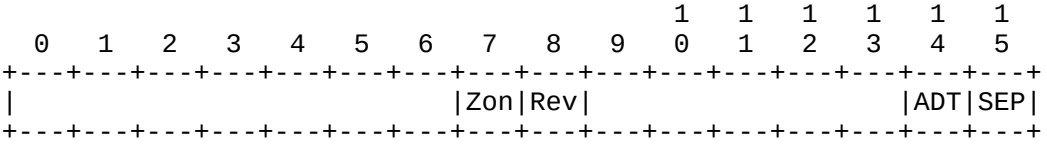
5. DNSSEC Requirements

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:



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. Operational Considerations

A Validating Stub Resolver that is Delegation-Extension-aware MUST only use security-aware resolvers that are Delegation-Extension aware. A Delegation-Extension-aware Validating Resolver that uses forwarders MUST only use Delegation-Extension-aware and security-aware forwarders. Otherwise DNSSEC-secure zones might fail to validate and DNSSEC-insecure zones might observe inconsistent answers.

7. Security Considerations

This section discusses the security properties of the mechanisms defined in this document, identifies attack surfaces, and describes the mitigations provided or required.

7.1. Threat Model

The threat model assumed by this document includes an on-path attacker capable of intercepting, modifying, dropping, and injecting DNS messages in transit between a resolver and an authoritative name server. Off-path attackers capable of response forgery (e.g., via birthday attacks on UDP) are also considered. Attackers may attempt to cause a resolver to use unencrypted transport, to resolve names incorrectly, or to be denied service entirely.

7.2. Downgrade Attacks

7.2.1. Stripping of Delegation Types from Referrals

An on-path attacker may remove Delegation Types and associated NSEC or NSEC3 records from a referral response, leaving only unsigned NS records. A resolver that accepts such a modified referral would proceed to resolve the delegated name using unencrypted transport, defeating the purpose of Delegation Types such as those indicating encrypted transport parameters.

The DNSKEY-ADT flag defined in Section 5.1 provides a mitigation against this attack for validating resolvers. When the ADT flag is set in any DNSKEY of the delegating zone's DNSKEY RRset, a validating resolver MUST verify that the referral contains NSEC or NSEC3 records proving the presence or absence of Delegation Types for the delegated name. A referral lacking this proof MUST be treated as tampered with and MUST be ignored.

This mitigation is effective only when all of the following conditions hold:

* The delegating zone is signed with DNSSEC.
* The ADT flag is set in the delegating zone's DNSKEY RRset.
* The resolver performs DNSSEC validation.
* The resolver enforces the ADT requirement as specified in Section 5.2

Operators of zones that publish Delegation Types MUST set the ADT flag in their DNSKEY RRset to ensure that validating resolvers can detect this form of tampering. Zones that have not set the ADT flag provide no cryptographic protection against this attack.

7.2.2. Stripping of the DE Flag from Queries

The DE flag is carried in the EDNS(0) OPT record of query messages sent by resolvers. An on-path attacker may remove this flag from a query before it reaches the authoritative name server. A server that receives a query with DE clear will respond without Delegation Types, returning NS records only.

However, when the ADT flag is set in the delegating zone's DNSKEY RRset, a validating resolver expects that NSEC or NSEC3 proof of Delegation Types MUST accompany any referral from that zone. This obligation is established by the DNSKEY, not negotiated per-query via the DE flag. Consequently, a referral response lacking the required NSEC or NSEC3 records MUST be rejected by a validating resolver, whether or not the DE flag was stripped from the outgoing query. In this case, the ADT mechanism defeats the DE-stripping attack.

This mitigation is subject to the same conditions as those listed in Section 7.2.1: the delegating zone must be signed, ADT must be set, and the resolver must validate. In the absence of these conditions, no cryptographic protection against DE-flag stripping is available, and the considerations in Section 7.5 apply.

7.2.3. Interaction Between Flag Stripping Attacks

The two downgrade attacks described above may be attempted in combination. An attacker who strips the DE flag from a query causes the authoritative server to respond with NS records only and no Delegation Types. Without Delegation Types in the response, the resolver cannot apply the NS-ignoring rule defined in Section 3.2, and would ordinarily follow the NS records to resolve the delegated name, potentially over unencrypted transport.

As described in Section 7.2.2, the ADT flag defeats this combined attack for validating resolvers in zones where ADT is set. The resolver’s obligation to require NSEC or NSEC3 proof derives from the previously validated DNSKEY RRset, not from the contents of the referral itself. A referral containing only NS records, with no NSEC or NSEC3 proof, will be rejected regardless of whether Delegation Types were present.

The residual risk in both Section 7.2.2 and this section therefore reduces to the same condition: zones in which ADT is not set, or in which DNSSEC is not deployed, provide no cryptographic protection against either attack. This is a deployment risk, addressed in Section 7.5.

7.3. Injection of Delegation Types

Section 3.2 specifies that when Delegation Types are present in a referral response, accompanying NS records MUST be ignored. An attacker capable of injecting or forging a referral response could exploit this rule by introducing a fabricated Delegation Type into the response, causing the resolver to ignore legitimate NS records and use only the attacker-supplied Delegation Type, which may point to an attacker-controlled server.

This attack is mitigated by DNSSEC. In a DNSSEC-signed zone, Delegation Type RRsets MUST be signed as specified in Section 5. A validating resolver will reject responses containing unsigned or incorrectly signed Delegation Types.

In unsigned zones, no cryptographic protection against this attack is available.

7.4. Denial of Service via NXDOMAIN for Legacy Resolvers

Section 4.1 specifies that when the DE flag is clear and no NS records exist for a referral, the authoritative name server SHOULD return a Name Error (NXDOMAIN) response. This behavior is intended to prevent a legacy resolver from exhausting other authoritative servers for information it cannot act upon.

An attacker may attempt to exploit this behavior by stripping the DE flag from a query directed at a zone that publishes only Delegation Types and no NS records, causing the server to return NXDOMAIN for a name that legitimately exists.

However, a resolver that set the DE flag expects NSEC or NSEC3 proof in any NXDOMAIN response, demonstrating that the queried name does not exist or that no Delegation Types are present at or above it. A bare NXDOMAIN response lacking such proof is therefore detectable by a validating resolver. When the ADT flag is set in the delegating zone's DNSKEY RRset, the resolver MUST reject an NXDOMAIN response that does not include the required NSEC or NSEC3 records, as the absence of proof indicates tampering.

As with the attacks described in Section 7.2, this mitigation depends on the delegating zone being DNSSEC-signed, ADT being set, and the resolver performing validation. In zones where these conditions do not hold, a DE-stripping attack may result in an NXDOMAIN response that the resolver cannot distinguish from a legitimate one, causing a denial of service for the queried name. This residual risk is addressed in Section 7.5.

Authoritative servers SHOULD include an Extended DNS Error [RFC8914] code in NXDOMAIN responses returned when the DE flag is clear and no NS records exist, to assist in diagnosing misconfiguration or attack.

7.5. Partial Deployment and Transition Risks

The mechanisms defined in this document are effective only when deployed end-to-end. During the transition period in which some resolvers, authoritative servers, and zones have adopted this specification and others have not, a number of residual risks apply.

The ADT flag provides protection against the downgrade attacks described in Section 7.2 only when the delegating zone is DNSSEC-signed, ADT is set in the zone's DNSKEY RRset, and the resolver performs validation. In zones that publish Delegation Types but have not set ADT, or that are not signed, no cryptographic protection against referral-stripping or DE-flag-stripping attacks is available.

Zone operators that publish Delegation Types in signed zones are REQUIRED to set the ADT flag upon deployment. Zones relying on Delegation Types for security properties such as encrypted transport MUST be DNSSEC-signed.

8. 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"

IANA is requested to assign flag 2 in the "EDNS Header Flags (16 bits)" registry in the "Domain Name System (DNS) Parameters" registry group to "DE Delegation Extensions", with this document as the Reference. This flag is described in Section 3.

IANA is requested to assign flag 14 of the 16-bit flags field in the "DNSKEY FLAGS" registry to indicate Authoritative Delegation Types, with this document as the Reference. This is described in Section 5.1.

9. Acknowledgments

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

10. References

10.1. 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>.

[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>.

[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>.

10.2. 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