

Workgroup: dnsop
Internet-Draft:
draft-ietf-dnsop-parent-side-auth-types-00
Published: 24 September 2020
Intended Status: Standards Track
Expires: 28 March 2021
Authors: P. van Dijk P. Spacek
 PowerDNS CZNIC

Parent-side authoritative DNS records for enhanced delegation

Abstract

A DNS RRtype numeric range that behaves like DS is reserved. This means: being authoritative on the parent side of a delegation; being signed by the parent; being provided along with delegations by the parent. If this document had become an RFC five years ago, deploying new types (along the lines of NS2/NS2T, DSPKI or various other imagined things like DNS ('signed delegation NS')) would be easier to deploy and experiment with today.

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 28 March 2021.

Copyright Notice

Copyright (c) 2020 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 Simplified BSD License text as described in

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Document work](#)
- [3. Conventions and Definitions](#)
- [4. Summary](#)
- [5. Implementation](#)
 - [5.1. Authoritative server changes](#)
 - [5.2. Validating resolver changes](#)
 - [5.3. Stub resolver changes](#)
 - [5.4. Zone validator changes](#)
 - [5.5. Domain registry changes](#)
- [6. Security Considerations](#)
- [7. Implementation Status](#)
- [8. IANA Considerations](#)
- [9. Acknowledgements](#)
- [10. Normative References](#)
- [11. Informative References](#)
- [Appendix A. Document history](#)
- [Authors' Addresses](#)

1. Introduction

[[RFC4035](#)] defines the DS Resource Record, as a type with the special property that it lives at the parent side of a delegation, unlike any other record (if we can briefly ignore NSEC living on both sides of a delegation as an extra special case). In various conversations and posted drafts in DPRIVE and DNSOP, a need to publish other kinds of data parent-side has been identified. Some drafts simply proposed a new type, assuming that authoritative DNS servers and registry operations would eventually follow along; other drafts have tried to shoehorn new kinds of data into the DS record. If, when DS was defined, or at any time since then, a range of RRtype numbers would have been specified to have the same behaviour as DS, those drafts, and the experiments that need to go with figuring out the exact definition of a protocol, would have been much more feasible. This document requests that IANA allocate such a range.

2. Document work

This document lives [on GitHub](#); proposed text and editorial changes are very much welcomed there, but any functional changes should always first be discussed on the IETF DNSOP WG mailing list.

3. Conventions and Definitions

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.

4. Summary

A range of new types is allocated, but not assigned (FIXME: wording?). This range of types is defined to be handled by DNS software like the DS record is handled. Authoritative servers serve the types from the parent side of a delegation. Resolvers know to ask the parent side of a delegation.

No semantics are assigned to the numbers at this time. Having these numbers reserved with these processing rules allows for future extension of parent-side publication of data on behalf of a child, without having to wait for implementations to catch up.

5. Implementation

The subsection titles in this section attempt to follow the terminology from [[RFC8499](#)] in as far as it has suitable terms. 'Implementation' is understood to mean both 'code changes' and 'operational changes' here.

5.1. Authoritative server changes

This specification defines changes to query processing in authoritative servers.

FIXME

5.2. Validating resolver changes

This specification defines changes to query processing in resolvers.

FIXME

5.3. Stub resolver changes

This specification defines no changes to query processing in resolvers.

FIXME

5.4. Zone validator changes

This specification defines changes to zone validation in zone validators.

FIXME

5.5. Domain registry changes

Domain registries MAY decide to allow children to publish records of any type from the range defined in this document in the parent zone. Alternatively, they MAY decide to only allow such publication for types that actually get allocated a name and a semantic. Ideally, domain registries would allow anything in the experimental subrange.

6. Security Considerations

7. Implementation Status

[RFC Editor: please remove this section before publication]

8. IANA Considerations

IANA is requested to reserve a range of numbers in the Domain Name System (DNS) Parameters Resource Record (RR) TYPES, with this document as the Reference. The numbers shall get no meaningful names (but perhaps they would get some useful mnemonic, a weak proposal is PA00 through PAXX for 'parent authoritative').

IANA is also requested to mark a subset of that range as 'experimental'. The experimental numbers are expected to never be hardcoded in published, released software, and no further allocation or naming of the experimental numbers by an RFC or otherwise is expected.

9. Acknowledgements

This idea was initially proposed by Petr Spacek. His contribution is rewarded by listing him as an author so he can take equal parts credit and blame.

10. Normative References

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <<https://www.rfc-editor.org/info/rfc4035>>.

[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>>.

11. 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>>.
- [RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <<https://www.rfc-editor.org/info/rfc8499>>.

Appendix A. Document history

Authors' Addresses

Peter van Dijk
PowerDNS
Den Haag
Netherlands

Email: peter.van.dijk@powerdns.com

Petr Spacek
CZNIC
Prague
Czech Republic

Email: petr.spacek@nic.cz