

# DELEG Requirements Discussion

DELEG Interim meeting  
October 8, 2024

# Agenda

1. Administrivia - 15 minutes
2. Requirements discussion - 90 minutes
3. AOB - 15 minutes

# Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (<https://www.ietf.org/contact/ombudsteam/>) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- [BCP 9](#) (Internet Standards Process)
- [BCP 25](#) (Working Group processes)
- [BCP 25](#) (Anti-Harassment Procedures)
- [BCP 54](#) (Code of Conduct)
- [BCP 78](#) (Copyright)
- [BCP 79](#) (Patents, Participation)
- <https://www.ietf.org/privacy-policy/>(Privacy Policy)

# Requirements Draft

[Problem Statement and Requirements for an Improved DNS Delegation Mechanism](#)

<https://datatracker.ietf.org/doc/draft-ietf-deleg-requirements/>

<https://github.com/ietf-wg-deleg/draft-ietf-deleg-requirements>

# Requirements with no discussion

H1: DELEG must not disrupt the existing registration model of domains.

H3: DELEG must not negatively impact most DNS software.

H6: DELEG must be incrementally deployable.

H7: DELEG must allow multiple independent operators to simultaneously serve a zone.

S1: DELEG should facilitate the use of new DNS transport mechanisms.

S3: DELEG should minimize transaction cost in its usage

S5: DELEG should allow for backward compatibility to the conventional NS-based delegation mechanism.

Are these too obvious as requirements?

# Requirements with a little discussion

H4: DELEG must be able to secure delegations with DNSSEC.

- New S8: DELEG should be able to convey a security model for delegations stronger than currently exists with DNSSEC.

H5: DELEG must support updates to delegation information with the same relative ease as currently exists with NS records.

S2: DELEG should make clear all of the necessary details for contacting a ~~Service Access Point~~ service.

S4: DELEG should enable a DNS operator to manage DNS service more completely on behalf of domain administrators.

- Make this a hard requirement?

S6: DELEG should be easily extensible, ~~much like Extension Mechanisms for DNS~~

- Rephrased to avoid mention of EDNS

S7: DELEG should support an in-band means for the child to signal to the parent that parent-side records related to the child should be updated.

- Out of scope? handled by existing solutions?

# Requirements with significant discussion

H2: DELEG must be backwards compatible with the existing ecosystem.

- a better wording for the third sentence would be "Nameserver (NS) records will continue to define the delegation of authority between a parent zone and a child zone for systems that do not yet implement DELEG".
- The requirement should be that DELEG records do not replace NS records but augment them. So it should be fine to say that the presence of a parental side NS record indicates a zone cut and that any DELEG records provide additional information about the zone cut.
- There is also the rather tricky distinction between what needs to be (at least conceptually) present in a zone, and what needs to be sent over the wire to a DELEG-aware resolver.
- I don't think enforcing the presence of NS along with DELEG is a good thing for the long term
- If the child cannot override the parent, we need to make sure child operators have a provisioning interface with parent operators, where DELEG is involved.
- I get the sense that the rather central concepts of "delegation" and "authority" in the DNS are under assault...

# Other significant discussion

## Can/Should a Child Zone have DELEG Records?

- Possibilities:
  - 1) No -- child DELEG records would be an error.
  - 2a) Yes – child records have higher precedence than parent
  - 2b) Yes – resolver can choose if parent or child have precedence
- “child-centric resolution ignores the fundamental fact that the DNS is a tree/hierarchy where the child depends on the parent only. let’s keep it simple”
- “Both parent-centric and child-centric have strong proponents. So maybe it is better to keep that out of the requirements and only require that a DELEG mechanism supports both parent-centric and child-centric resolution.”
- “If a DELEG mechanism introduces new types at the parent side of a delegation then it must disallow those types at the apex of the child zone.”
- “Being able to cache and interpret both "delegation information from parent" and "delegation information from child" unambiguously feels like an advantage over what we have today.”
- “having both parent and child centric resolution cohabiting is an operational nightmare.”
- “Leaving out requirements regarding child centric would not be great for the proponents of child centric. Then an implementation could only support parent centric and meet the requirements. So it would be an uphill battle to get support for DELEG at the child back in.”
- “I’d like to have the ability to store child delegation information somewhere.”
- “It seems to me that ... we are in agreement that we don't want a new architecture to require the same RR at the same QNAME in parent and child.”
- “I think the DS record is a good example of the problems that come with parent-centric: hard to update, no control over TTL, no control over contents (the parent can decide on the hash algorithm).”

# Non-Requirements

Declared out-of-scope in draft-ietf-deleg-requirements

- Whether NS records must continue to be the primary means by which resolutions happen.
- Whether information for a new delegation mechanism is stored in at the zone name or elsewhere in the domain name hierarchy.
- (new) If a new delegation protocol is based on a DNS resource record, that record must not appear in both the parent and child with the same name and type.