

DELEG draft version 8

Into working group last call....

Ralf Weber, IETF125 Shenzhen, 20. March 2026

Agenda

- Changes from 05 to 08
- DNSSEC clarifications
- To NS or not to NS
- TODOs

05 - 08 Changes

Overview

- No semantic changes
- No wire format changes
 - We added the mandatory parameter, but that is what params are for
- Some bike shedding
- Better structure
- More and better formulated Text (Thanks to wg participation)

05 - 08 Changes

Bike shedding

- Final names for RR Types:
 - DELEG
 - DELEGPARAM
- Naming (not in 08)
 - Delegation point
 - Delegated zone
- Clarification on appearance
 - DELEGPARAM can not be at the delegation point



05 - 08 Changes

Organisation

- Reorganized parts of the draft
 - New protocol overview section (chapter 2)
 - Record/Parameter definitions now have their own section (chapter 3)
 - New operational considerations section (chapter 6)
 - More security considerations (chapter 7)

05 - 08 Changes

Details

- Added more and better plus fixed examples (TODOs from IETF124)
 - Test vectors still missing hopefully coming to another revision soon
- Clarification on SLIST processing (SLIST is a set)
- New mandatory parameter similar to SVCB
- DELEG aware responder always has to set DE=1
- Protocol clarifications for ADT flag, AA bit, DNSSEC validator rules (more later)
- Explanation of problems with validator chains (have all to be DELEG aware)

05 - 08 Changes

DNSSEC and validation

- Clarified that behavior of the AA bit is similar to DS (set when asked in parent)
- DELEG is signed in the parent:
 - Absences of a DELEG record in a delegation MUST be proven only when the ADT is set
 - A positive DELEG delegation can be proven without the ADT bit set so validators MUST do this

To NS or not to NS

In some far distant future (6.2 and 7.3)

- With DELEG the actual delegation is signed
- With NS an attacker can fake glue and intercept traffic
- DELEG can not be expressed by NS
- Therefore we have to allow DELEG only delegations
- That could make parts of the namespace invisible to non DELEG aware clients
 - Similar to split horizon
- We mention the operational problems with that in the draft

Todo

- 7.1 Overworking attacks
 - We have a number for indirections to follow
 - This is uncommon in DNS
- Opinons?

Going forward

- Working group last call?
- Early allocation (all/partly)?
 - DELEG Delegation Information registry
 - EDNS0 DE Flag
 - DNSSEC Key Flag
 - DELEG with specific value
 - DELEGPARAM
 - EDE code point
 - Resinfo code point