Encrypted DNS Server Redirection (EDSR) -03

An update for IETF 119

Corey Mosher (Innate, Inc.), John Todd (Quad9), Tommy Jensen (Microsoft)

https://datatracker.ietf.org/doc/draft-jt-add-dns-server-redirection/

What’s new in -03

- In a nutshell: no more redirections to different domain names
  - Extensive edits, but all to remove the definition of OOR mode
  - Note: managed to miss some of the I-D references to what are now RFCs… sorry!

- … and that’s it. Now on to the -03 feedback from Ben Schwartz and Manu Bretelle (thank you both!)

Post -03 feedback

- Rephrase to accurately frame SVCB usage
  - No normative MUST NOT against following diff origin redirects is needed (because that’s not how SVCB works)

Post -03 feedback

- Clarify if/when peers need to support Delegated Credentials
  - Currently says servers MAY offer it with no requirements on client
  - This implies clients MUST be prepared to expect it, but no such guidance is given for handling the case where the server uses Delegated Credentials but the client does not

Post -03 feedback

- Clarify EDSR differences when used with a resolver originally discovered using DDR (RFC 9462)
  - Text currently says the only difference is the destination MUST be able to claim the original IP address in its SAN field
  - Should point out this, like DDR, means the server needs to handle clients not presenting an SNI

Post -03 feedback

- Don’t do TTL stretching
  - Text currently requires TTL stretching by having clients force a minimum TTL of their own choosing
  - Should instead do the opposite: ignore redirections with unacceptably short TTLs

Post -03 feedback

- What happens when the redirection target goes offline?
  - Text does not directly address this scenario
  - Sections 3.5 and 8.3 help prevent increasing weakness to outages (avoid having 3 servers all redirect to one, then be left stranded when that one goes offline), but that’s both vague and only part of this question
  - The text requires servers to live with clients not following redirections for any number of reasons, so “revert to pre-redirection” is weakly implied versus “walk back up a redirection chain” but again, nothing specific yet

Questions?

Changes will be published in a -04 following this discussion

At which point, we will request adoption again

Thank you!