

DNS Access Denied Error page

[draft-reddy-dnsop-error-page-06](#)

IETF 110

March 2021

T. Reddy (McAfee)

N. Cook (Open-Xchange)

D. Wing (Citrix)

M. Boucadair (Orange)

Agenda

- Comments raised by the WG and changes to address these comments
 - Comment #1: Why not use EXTRA-TEXT field in the EDE option ?
 - Comment #2: What is the need for signature field in Error URI page EDNS0 Option ?

Comment#1

- Limitations of EXTRA-TEXT
 - EDE option does not offer authenticated information.
 - It can be displayed in a language not understood by the user.
 - Forwarded EXTRA-TEXT displays the source of the error and not the cause of the error.
 - Fragmentation
 - Easily spoofed

Comment#2

- Error URI page EDNS0 Option MUST NOT be propagated and processed over an unauthenticated and unencrypted connection.
- Forwarding the Error URI page EDNS0 Option is implementation dependent.
 - Mandatory to validate and re-generate the signature for validation by client.
 - If signature validation fails, EDNS0 Option is rejected by client.
 - ERROR-PAGE-URI MUST NOT be modified by the forwarder.

Comment#2

- If DNS forwarder does not recognize the URI page EDNS0 Option and forwards to the client
 - It will be rejected by the client due to signature validation failure.

draft-reddy-dnsop-error-page-06

- All received comments were handled
- Consider WG adoption
- Comments and suggestions are welcome

Thank you