

draft-crocker-dnssec-algo-signal-03

DNSEXT WG Meeting
75th IETF
Stockholm Sweden
July 29th, 2009

Purpose of the draft

- New EDNS option: Algorithm Understand (AU)
 - Client can signal what cryptographic algorithm(s) they understand and prefer
- Two benefits
 - Track the deployment of client code that understands new algorithms
 - Smaller response sizes for some clients

Latest Version

- Change AU ALG-CODE value to be a list of algorithm codes understood by client.
- Changes some of the background and proposal reasoning text
- Clarification on role recommendations
 - Mainly the recommendations for forwarders

On the “To Do” list

- Request to become a WG draft
- Need reviewers!
 - Especially the cache/middlebox recommendations
 - Security Considerations