

DNS Resolver Priming and DNSSEC

`draft-koch-dnsop-resolver-priming-00.txt`

DNSOP@IETF68 — Praha, CZ — 2007-03-19

Peter Koch

pk@DENIC.DE

Plain Old Priming

- *Hints* file may be outdated, so ...
- ...ask for the NS RRSet for the root to bootstrap/verify
- Really looking after the addresses (A and soon AAAA)
- Will probably need to advertize EDNS0 (larger UDP packets)
- Recently received attention by RSSAC/SSAC for root server AAAA:
 - <http://www.icann.org/committees/security/sac016.htm>
 - <http://www.icann.org/committees/security/sac017.htm>
- Priming has not yet been standardized/documentated in an RFC

Priming **TODO**

- Document / Recommend
- Specify Parameters for the priming queries
- Re-Priming practices
 - Honor TTLs? If yes, which?
 - Re-query early?
 - Update hints?
- Special root server requirements?

DNSSEC and Priming

- Not talking about the Trust Anchors here
- Is setting the DO bit (CD?) needed – delegations aren't signed either?
- How else would we [protect the root NS RRSet](#)?
- More important, though, are the A/AAAA RRSet

Providing the Full Trust Chain

Components needed for root server address validation, RRSIG only

- root NS RRSet
- A and AAAA RRsets (up to 26)
- ROOT-SERVERS.NET KSK and ZSK (maybe can get away with one)
- ROOT-SERVERS.NET DS
- same for NET TLD (although with KSK/ZSK split)
- root KSK and ZSK

(Remember: This is not about signing glue, it's about delivering RRSIGs in the additional section)

Issues with DNSSEC validation

- NET-related information not (readily) available to root servers
 - Rename root servers (only zones root servers are authoritative for)
 - Use a second trust anchor
- Response size: around 35 RRSIGs plus 5 or 6 DNSKEYs
 - Rename root servers (lesser zones, maybe ARPA or .)
 - Continue to use SBELT until finished
 - Use a second trust anchor

Questions

- Do we need to **specify** and **recommend** priming?
- Any known problems with/without vanilla DNS priming?
- Priming with DO bit?
- Root server address validation needed?

Thank You!