draft-ietf-dnsext-dnssec-bis-updates-10

Samuel Weiler

IETF77, Anaheim

24 March 2010

Changes Since -09

- Nested Trust Anchors
- Setting DO Bit on Replies
- Answering Queries with CD bit set

Path Forward

- Document History
- Last call?

Nested Trust Anchors

- Removed 2119 SHOULD.

  "Which [trust anchor selection policy] to use is a matter of implementation choice. It is possible and perhaps advisable to expose the choice of policy as a configuration option."

- Added discussion of possibilities.

Nested Trust Anchors

- Removed 2119 SHOULD.

  "Which [trust anchor selection policy] to use is a matter of implementation choice. It is possible and perhaps advisable to expose the choice of policy as a configuration option."

- Added discussion of possibilities.
- Left in a weak default recommendation:

  "As a default, we suggest that validators implement the "Accept Any Success" policy ... while exposing other policies as configuration options."

Setting DO (DNSSEC OK) Bit on Replies

- Before: Authoritative servers may copy the setting of the DO bit from query to response. Or may set it arbitrarily. (From -04, October 2006.)

Setting DO (DNSSEC OK) Bit on Replies

- Before: Authoritative servers may copy the setting of the DO bit from query to response. Or may set it arbitrarily. (From -04, October 2006.)
- Now: MUST copy, based on RFC3225.

Setting DO (DNSSEC OK) Bit on Replies

- Before: Authoritative servers may copy the setting of the DO bit from query to response. Or may set it arbitrarily. (From -04, October 2006.)
- Now: MUST copy, based on RFC3225.
- Encourage validators to accept either.

Answering Queries with CD (Checking Disabled) bit set

- Old: "When processing a request with the CD bit set, the resolver MUST set the CD bit on its upstream queries."
- What if you have a cached answer obtained w/o the CD bit?

Answering Queries with CD (Checking Disabled) bit set

- Old: "When processing a request with the CD bit set, the resolver MUST set the CD bit on its upstream queries."
- What if you have a cached answer obtained w/o the CD bit?
- That's fine!
- Unless it's a SERVFAIL.

Answering Queries with CD (Checking Disabled) bit set

- Old: "When processing a request with the CD bit set, the resolver MUST set the CD bit on its upstream queries."
- What if you have a cached answer obtained w/o the CD bit?
- That's fine!
- Unless it's a SERVFAIL.
- Which should only be cached for five minutes (RFC2308).

Answering Queries with CD (Checking Disabled) bit set

- Old: "When processing a request with the CD bit set, the resolver MUST set the CD bit on its upstream queries."
- What if you have a cached answer obtained w/o the CD bit?
- That's fine!
- Unless it's a SERVFAIL.
- Which should only be cached for five minutes (RFC2308).
- In those cases (only), query upstream with CD set.
- OK to set CD for any queries for which you have an applicable trust anchor.

Changes through time

- -10, Mar 2010: no additions. Changed CD and DO bit rules. Changed nested trust anchor guidance.
- -09, Sep 2009: editorial only.
- -08, Jan 2009: NSEC3, SHA256, AD bit, CD bit, nested trust anchors, 5155 typo.
- -07, Jul 2008: editorial.
- -06, Nov 2007: validating insecure delegations
- -05, Mar 2007: CNAME proofs, REMOVED responding to ANY queries
- -04, Oct 2006: responding to ANY queries, setting DO bit on replies
- -03, Jun 2006: editorial
- -02, Jan 2006: canonical form typecode list
- -01, May 2005: validating ANY queries

Anything else?

- Changes due to "rollover and die"?

Anything else?

- Changes due to "rollover and die"?
- Time to WGLC and publish?