draft-jabley-dnsop-validator-bootstrap

Kindly presented by Andrew Sullivan

(because apparently Joe is not adept at correlating
IETF meeting agendas with airline schedules,
and Dave is not here)

Problem Statement

- DNSSEC validators need a trust anchor
- The choice of appropriate trust anchor is not expected to be constant over time
  - e.g. accidents happen
- Not all validators can be expected to be administered competently
  - e.g. embedded devices from Costco

History

- Root-Signing documentation described the initial method of trust anchor distribution
  - see http://www.root-dnssec.org/
- Root was signed, trust anchor published
- Discussion in dnsop seeded by questions from cisco and others
- draft-jabley-dnsop-validator-bootstrap-00

Root-Zone TA

- We focus on the problem of retrieving a TA for the root zone KSK
  - other applications (e.g. for private DNS views) presumably have accompanying engineering and administration
  - DNSSEC uptake in TLDs is significant; there's little indication that large islands of trust are necessary

Observations

- Validators need an accurate sense of time
- Validators need a trusted copy of a root trust anchor
- draft-wijngaards-dnsext-trust-history seems applicable, although that proposal is not universally loved
- Opportunities for validation using vendor-supplied certificates exist in some cases

More Observations

- This proposal is based on existing arrangements and procedures for publishing trust anchors for the root zone
- Other answers are surely possible, but be aware that changing process in root zone KSK management involves work and therefore time

This Proposal

- Simple state model
  - no trust anchor, no accurate time
  - accurate time, no suitable trust anchor available
  - suitable trust anchor obtained
- You don't validate until you reach the final state (before then you might still resolve)

This Proposal

- is out-of-band (i.e. does not use DNS)
- Uses HTTP, involves XML parsing and X.509 certificate validation
- Seems (to the authors) to be fairly easy to implement in a variety of validator deployment scenarios
- Seems (to the authors) to have no significant security issues

Questions to the Room

- Is a problem that needs a solution?
- If yes, should the work on that problem happen here?
- If yes, should this document be adopted by dnsop?