Root Zone KSK Roll

Operational Gaps and Navel Gazing

Joe Abley – IETF 93 – Praha

Root Zone KSK Roll

- Long-anticipated, never quite here, in the grand tradition of DNSSEC

- Recent traction in the form of a volunteer design team convened by ICANN

  - draft findings to be published any day now

  - ICANN intends to solicit public comment through their usual process

  - Review and contributions from this audience would be extremely valuable

Potential Work for dnsop

- Two gaps stand out following the design team's work over the past several months

  - the approach and mechanism for secure trust anchor retrieval is not well-understood and arguably not well-documented

  - automatic bootstrapping of validators is done in different ways

    - in the context of root zone KSK rollover, this presents headaches and uncertainty

Possible Starting Points

- Two drafts (either expired or on deadline-rev life support) could be viable starting points:

  - draft-jabley-dnssec-trust-anchor describes the publication formats and the stable URIs used for retrieval

  - draft-jabley-validator-bootstrap describes how a validator should start up, how it should retrieve and authenticate a trust anchor set and gain an accurate sense of time before validation begins

But... ICANN, etc

- ICANN delivers what is required of it, as specified in the IANA Functions Contract, which currently references various draft specifications published on www.root-dnssec.org

- I obviously do not speak for ICANN (but others here do, and perhaps they will), but we could perhaps imagine

  - future direction for ICANN referencing RFCs rather than the current draft specs

  - ICANN deciding to implement a superset of what is required by the IANA Functions Contract and what is specified by the IETF

- Either way, there is good reason to think that effort to fill these gaps will not be wasted.

Proposal

- **Both of these gaps need stable, authoritative specifications**

- These are operational DNS matters (not DNS protocol matters) and hence on-topic for dnsop

- The two documents mentioned are reasonable starting points, since backwards compatibility with what we have is important

- **We propose that the working group adopt these two documents and own these specifications**