Documenting Validator Requirements

An advertisement for *draft-mglt-dnsop-dnssec-validator-requirements-07*

Edward Lewis
ICANN

FOSDEM 2019/DNS Developer Room
3 February 2019

Seeking support for an IETF Internet Draft

- The goal of this talk is to stir interest of developers in an IETF draft on DNSSEC validation
  - The goal of the document is to explain what is needed to perform validation
  - DNSSEC validation is already defined in other documents, and there is no thought of changing that
  - This document is about making validation manageable

- The goal is not to just again "ask developers to participate in the IETF process"!

Why Bring This Topic Up in the Venue?

- A document of this kind should reflect reality
  - Coder's reality, not Protocol Engineer's reality
  - Be positioned to help the Operator's reality

- The intent is a document useful when code is updated, created or even specified for procurement
  - For coder's: is this addressing what is considered implementation history?
  - A question for later: Is the related code "all done" and not likely to be updated?

Document History

- This document has been in existence since February 2014 (5 years!)
- Personal history – added as an author in March 2017
  - Motivated by experience in the DNSSEC root KSK Rollover
  - I haven't been to an IETF since 2016
- The document was presented to the IETF DNSOP WG in March 2017
  - Not adopted, and seems to be flirting with the edges of working group's interest
- This document lives (or dies) based on developer interest
  - Does it have straw for the camel? Maybe, maybe not

Topics in the Draft

- Time information
- Trust Anchor Datastore/database
- Key Revocation Capabilities
- Cryptographic Code Management
- Reporting

Time Reporting

- Not all devices have access to wall-clock time, or perhaps accurate wall-clock time

- Accurate, secure, wall-clock time is important to DNSSEC validation
  - Signature records contain "valid from" to "valid to" time stamps
  - The reason is to prevent replay attacks

Trust Anchor Datastore/database

- Trust Anchor management was greatly improved during the KSK Rollover planning and execution
  - Improved tooling to allow operators to list the trust anchors, for instance
- Realization that the data structure for trust anchors, although simple, needs to accommodate inspection and changes by authorized actors
- Constant desire for remote inspection too
  - Operators has asked "what trust anchors do I have?"

Key Revocation Capabilities

- This section covers situations in which a key is abruptly discredited
  - Corrupt key ("cracked")
  - Changed in a "botched" emergency roll
- Negative Trust Anchors
  - Known-bad keys
- Revoking data sets validation due to key "gone bad"

Cryptographic Code Management

- Determine whether a DNSSEC signer/server supports cryptographic algorithms of interest to the validator

Reporting

- When DNSSEC validations fail
  - More than discarding the data is needed

- Who to tell/notify
  - Perhaps to install a Negative Trust Anchor
  - To address a larger issue (could be a network cut)

Comment Request

- Read, comment (email or at an IETF meeting)
- Authors Email addresses:
  - daniel.migault@ericsson.com
  - edward.lewis@icann.org
  - york@isoc.org
- Is this draft "too late" or "helpful" for validators in development
- Will this help organize improvements to current code bases?
- Title: "DNSSEC Validator Requirements"
  - https://tools.ietf.org/html/draft-mglt-dnsop-dnssec-validator-requirements-07

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: edward.lewis@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg