Looking at TLD DNSSEC Practices

Developers vs. Operators - Plenary followup

Edward Lewis
Neustar

At RIPE 64, DNS WG
Wednesday, April 18, 2012

Survey Results Todate

- As of April 15
  - 82 out of 303 TLDs sign (27%)
- "Most common" choices (not universal):
  - RSA SHA-1 "old guard", RSA-SHA-256 "newbies"
  - 1024 bit ZSK, 2048 bit KSK
  - One ZSK and one KSK active and present
  - ZSK is changed monthly, KSK can't tell
  - NSEC3 with 1 iteration, 4 byte (8 hex char) salts, rarely/never changed
  - DS record added 3 weeks after DNSKEY appears

Outliers

- I don't want to name names, but I am curious about some of the patterns I see
- I'd like to talk to operators if...
  - all of your signature expiration times are the same
  - salt changes more frequently than once a month
  - there's no registered a DS record with IANA (unless the zone was "only recently" signed)
  - signature durations "flap" wildly (1w to 4w and back)
  - you have questions or want to see what I see
- I'm here (RIPE64) and the email below works