DNSSEC – not really a success story?

Peter Koch, DENIC eG

2019-04-10 | eco KG AntiAbuse/CSA Summit | Köln
DNSSEC for DE 2ND LEVEL DOMAINS (2016-)
DNSSEC for DE 2ND LEVEL DOMAINS (2011-)

![Graph showing the increase in signed and DNSKEY-registered DE SLDs from 2012 to 2019.](image)
DNSSEC for DE 2ND LEVEL DOMAINS (2019)
METRICS?

- Is the number of signed second level domains that important?
- What relevance do the domains themselves have?
- What about subordinate infrastructure (CNAMEs into CDN land)?
- How to factor in the relying(!) parties?
Observations

• DNSSEC is not a product
• DNSSEC has no clear selling point
  • Make websites „even safer“?
  • Support DANE?
• IPv6 and RPKI have (mostly) similar problems
  • How to innovate broadly the technical core infrastructure?
• DNSSEC not well compatible with „highly dynamic“ scenarios
  • „stupid DNS tricks“

• We learned a lot about DNS during the DNSSEC journey!
IETF / Standards

- DNSSEC never gets ready!
- Too many developments in parallel (cookies, ...)
- Solves problems for „people in the room“
- Tech community reacts to lack of deployment
  - ... by producing more standards ...
Crypto is not easy, really!

- What is the threat model?
  - Multi-Provider Signing?

- KSK rollover
  - Often a pointless routine
  - RFC 5011 carries forward trust – based on which assumptions?

- HSM
  - Or everything online?
Regulation

• Remember NASA.GOV?

• Should/can trust be regulated?
  • How should OS/Applications deal with validation failures?
Concentration and Consolidation (email dejavu)

- End2end goes hop-by-hop
- Dominant players emerge
- ... and set the rules

- So, will DoH both enable DNSSEC – and render it unnecessary at the same time?
DANKE!

KONTAKT:
koch@denic.de

FRAGEN?