Upcoming Changes to Verisign-Operated Top Level Domains

Duane Wessels

DNS-OARC 26, Amsterdam
October 13, 2018
Outline

Parameters in Verisign-operated TLDs:

• ZSK Length Increase
• TTLs
• Cross-Zone Glue
ZSK Length Increase
DNSSEC Algorithms and Key Lengths used by TLDs 2018-10-08

- RSASHA1
- RSASHA1-NSEC3-SHA1
- RSASHA256
- RSASHA512
- ECDSA256
- Other
ZSK Strength Increase

- Currently, all Verisign-operated TLDs have 1024-bit RSA ZSKs
  - Root has been operating with 2048-bit ZSK since Oct 2016
- TLD ZSKs to be increased to 1280-bit RSA
  - ARPA will be increased to 2048-bit
- Rationale: 1024-bit RSA deprecated for use in DNSSEC
- Gradual rollout per platform
  - Tentatively 2018-Q4 through 2019-Q4
- For NSEC3 zones, 1280-bit keys keep us under fragmentation limits
  - See next slides
Time To Live
Time To Live Values

- Verisign-operated TLDs use 48-hour TTLs on delegation responses
- “Twas always thus”
- Implemented a feature to change delegation TTL per TLD
- Considering lower TTLs for some low-volume TLDs
- If deployed, TTLs will be changed incrementally
Cross-Zone Glue
Cross-Zone Glue

- Currently a referral for a .COM name includes .NET glue records, and vice-versa
- Most implementations ignore this cross-zone glue
  - Google Public DNS does not
- In the future, .COM and .NET referrals will not include cross-zone glue
- Rationale:
  - Cross-zone glue largely ignored
  - Slightly smaller responses
  - Allows providers to use dynamically addressed name servers in .COM and .NET
- Expected to be deployed 2018-Q4