Negative Trust Anchors
(refer to -06 version)

DNSOP WG

IETF 86

March 2013
DNSSEC Validation Is Good
Except when it fails. Then people get angry. Very angry.
NTA What!?

– Sometimes DNSSEC signing domains mess things up a bit operationally…

– Some blame the validators, and have a hard time understanding it’s an authoritative issue.
  
  • “It resolves just fine with ShinyCloudFreeDNS+ but not with you guys!”
  
  • “I’m switching to a non-validating resolver. DNSSEC stinks! No security for me!”
Open Questions

• Q: Should this be a DNSOP WG draft?
• Q: Should this be Informational or a BCP?
• Q: Should we recommend that an individual NTA be time limited?
  – “Reasonably short period of time”
  – 1 month or less
  – 1 week or less
  – 1 day or less
  – Is this a MUST or a SHOULD?
• Q: How do we (or should we) assess when critical DNSSEC deployment mass has been achieved so that this is no longer a common practice?
• Q: Is it desirable to say that NTAs should not be distributed across organizational boundaries?
For the Next Version

• Add examples in an appendix (as suggested by Warren Kumari and Rick Lamb)

• Other incremental improvements

• Address issue raised by Olafur Gudmundsson on whether a non-validatable RRSIG should be returned or not when a NTA is in place.
Anything Else?

DNSSEC

STAY COOL