Observations on Deploying New DNSSEC Cryptographic Algorithms

draft-york-deploying-dnssec-crypto-algs

Dan York – Ondrej Sury - Paul Wouters – Olafur Gudmundsson

york@isoc.org

IETF 97 - Seoul
Why can’t we get new crypto algs deployed quickly?

Overall goal is to help make it easier to deploy new DNSSEC cryptographic algorithms within DNS.
   – Today ECDSA... tomorrow EdDSA ... and then..............

Intent to document a common understanding of the typical deployment process of DNS infrastructure elements and potentially identify opportunities for improvement of operations.


See DNSOP presentation at IETF 96 in Berlin
Aspects of Deploying New Algorithms

- DNS Resolvers Performing Validation
- Signing Software
- Registries
- Registrars
- DNS Hosting Operators
- Applications
Requests

- Reviewers?

- WG adoption – thoughts?