The New Trust Anchor and the Supply Chain

Panel – Impacts of the KSK Rollover, ICANN 58

Benno Overeinder
NLnet Labs

http://www.nlnetlabs.nl/

NLNETLABS

Root KSK Rollover and Resolver Trust Anchors

- Speaking as a software developer of Unbound
  - similar procedures are in place for Bind, Knot Resolver and PowerDNS Resolver
- Challenge to get new KSK trusted by resolver
  - SAC063, SSAC Advisory on DNSSEC Key Rollover in the Root Zone
  - RFC 5011 Rollover
  - non-RFC 5011 Rollover

RFC 5011 Rollover

- RFC 5011 is designed for active/running resolvers
- Short version
  - new KSK is signed with old KSK
  - after “hold time” new KSK is trusted
  - old KSK revoked (signed with old and new KSK)

Non-RFC 5011 Rollover

- First time installation, offline for long period, ...
- Bootstrapping the validator, priming the trust anchor
  - OS distributions and automated OS updates
  - use well publicized trust anchors with unbound-anchor

Non-RFC 5011 with Unbound-anchor

- If RFC 5011 TA update fails, use method described in RFC 7958
- Procedure
  - test if root TA works
  - if not, perform https fetch of root-anchors.xml
  - and check results (RFC 7985, IANA detached CMS signature)
  - if all checks are succesfull, update root TA

Getting the New KSK Out There

- Unbound-anchor includes new TA-tag 20326 (Unbound v1.6.1, dd. Feb 21, 2017)
- OS distributions (Debian, Redhat, *BSD) follow new Unbound releases
  - backporting new TA-tag 20326 to old/stable OS distributions?