DNSSEC under ARPA

DNS Working Group
RIPE 60 Prague
May 2010

Dave Knight

ARPA

- Signed in late 2009

  ‣ distributed to root server operators for internal testing

- Signed ARPA zone served since March 2010

- Test Deployment

  ‣ testing is now complete, no problems found

  ‣ ICANN will submit a test report to NTIA and propose that DNSSEC in ARPA be considered to be in full production

Children of ARPA

E164.ARPA
IN-ADDR.ARPA
IN-ADDR-SERVERS.ARPA
IP6.ARPA
IP6-SERVERS.ARPA
IRIS.ARPA
URI.ARPA
URN.ARPA

E164.ARPA

- Signed by RIPE NCC since 2007

- RIPE NCC has told us that they intend to submit a DS RRSet for inclusion in ARPA in Q3 following the next e164.arpa key roll.

IN-ADDR.ARPA

- A proposal has been submitted to NTIA to re-delegate IN-ADDR.ARPA

  ▶ away from root servers

  ▶ to servers operated by the RIRs and ICANN

- Plan has been well-coordinated with RIRs

- Proposal includes DNSSEC signing

Other Children

- Several other delegated zones are operated by ICANN as an IANA function

  ▸ IP6.ARPA

  ▸ IN-ADDR-SERVERS.ARPA, IP6-SERVERS.ARPA

  ▸ URI.ARPA, URN.ARPA, IRIS.ARPA

- Signed on 29 April 2010

Operational Details

- OpenDNSSEC operated by ICANN in a dual-site, HA configuration

  ‣ GSA class-5 secure containers

  ‣ FIPS-140 HSMs

Operational Details

- DNSSEC Parameters

  ‣ RSA/SHA256, NSEC

  ‣ 2048-bit KSK, 1024-bit ZSK

  ‣ ZSK Rollover every 3 months

  ‣ KSK Rollover annually

Trust Anchors

- ARPA

  ▸ published in the IANA ITAR since March

- ARPA Children

  ▸ DS RRSets will be inserted into ARPA following conclusion of testing

Timeline

- ARPA

  ▸ signed now

- IN-ADDR.ARPA

  ▸ to be advised; many dependencies

  ▸ expected this year, however

- IP6.ARPA and other children

  ▸ signed now, trust anchors in ARPA soon

Questions?

dave.knight@icann.org