DNSSEC@AfriNIC

ICANN DNSEC Panel

ICANN 42, Dakar

Project team

AfrNIC and RDNS

○ As a RIR, AfriNIC manages and delegates RDNS subdomains to its members

  – IPv4

{ 41-196-197-102-105-154}.in-addr.arpa.

  – IPv6

{0.c.2 - 3.4.1.0.0.2 – 2.4.1.0.0.2}.ip6.arpa.

○ RDNS provisioning system includes

  – Domain objects from WHOIS database

  – Zonelets from Other RIRs

○ NS provided by AfriNIC and other RIRs

DNSSEC Within the RDNS

o Root, arpa, in-addr.arpa, and Ip6.arpa have been signed and chain of trust built

o No excuses for not signing RIRs managed RDNS zones

o Deploying DNSSEC within the RDNS may enable some other security mechanisms around addressing and its uses.

DNSSEC@AfriNIC

○ Sign the managed RDNS zones

○ Publish DS in in-addr.arpa and ip6.arpa zones

○ Accept DS from Members
  – process DS from zonelets from Other RIRs

DNSSEC@AfriNIC

- Deployment plan adopted internally
  - Assess the RDNS provisioning system readiness
  - Deployment stages

  Phase 1: Testing

  Phase 2: Signer integration into the RDNS provisioning system

  Phase 3: Unsigned zones published

  Phase 4: Signed zones published

  Phase 5: DS publication in parent zones

  Phase 6 : Members" DS publication

DNSSEC@AfriNIC

○ Few changes to the NS setup

○ RDNS provisioning system to be updated

   – Update domain object with DS attributes

   – Update on MyAfriNIC

   – DS processing

      • From domain objects

      • From zonelets

○ OpenDNSSEC as signer

   – Testbed operational

DNSSEC@AfriNIC

○ Signing policy

* ZSK is RSA 1024 key usable for 30 days

* KSK is a RSAS 2048 key usable for one Year

* Zones are signed with NSEC

* Signatures are valid for 7 Days

* Signatures are refresh 3 days

*DNSKEY TTL is the zone default TTL

*NSEC TTL is the Neg TTL of the zone

*RRSIG TTL is the Signed RRset TTL

*Zones are signed daily

○ Unsigned vs signed(at startup)

2.5M   /usr/local/var/opendnssec/unsigned/

7.4M   /usr/local/var/opendnssec/signed/

DNSSEC@AfriNIC

- Query for our signed zones ?

  Dig @dnssec.mu.afrinic.net

  We sign all the managed RDNS Zones

- We expect to update members at Afrinic-15 and hope to have good news by then :-)

- HSM discussions included in RPKI infrastructure setup.

Questions ??