

DNSSEC @ AFRINIC

DNSSEC TRAINING

AFRINIC and RDNS

- As 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
 - Zonlets from Other RIRs
 - NS provided by Afrinic and other RIRs

Example from WHOIS DB

```
domain:          0.1.196.in-addr.arpa
descr:           AfrinIC Corporate
nserver:         ns1.afrinic.net
nserver:         ns2.afrinic.net
nserver:         ns3.mu.afrinic.net
org:             ORG-AFNC1-AFRINIC
admin-c:         TEAM-AFRINIC
tech-c:          TEAM-AFRINIC
zone-c:          TEAM-AFRINIC
mnt-by:          AFRINIC-IT-MNT
mnt-lower:       AFRINIC-IT-MNT
source:          AFRINIC
```

DNSSEC Within the RDNS

- Root, arpa, in-addr.arpa, and Ip6.arpa have been signed and chain of trust built
- No excuses for not signing RIRs managed RDNS zones
- Deploying DNSSEC within the RDNS may enable some other security mechanisms around the addressing and its uses.

DNSSEC @ Afrinic

- Signed the managed RDNS zones
- Published DNS in in-addr.arpa and ip6.arpa zones
- Accept DS from Members
 - Accept DS from zonelets from Other RIRs

DNSSEC @ Afrinic

- Fee changes to the NS setup
 - Under control
- 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 publish all the managed RDNS Zones
- HSM included in RPKI infrastructure

Questions ??