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

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>0.1.196.in-addr.arpa</td>
</tr>
<tr>
<td>descr</td>
<td>AfriNIC Corporate</td>
</tr>
<tr>
<td>nservers</td>
<td>ns1.afrinic.net, ns2.afrinic.net, ns3.mu.afrinic.net</td>
</tr>
<tr>
<td>org</td>
<td>ORG-AFNC1-AFRINIC</td>
</tr>
<tr>
<td>admin-c</td>
<td>TEAM-AFRINIC</td>
</tr>
<tr>
<td>tech-c</td>
<td>TEAM-AFRINIC</td>
</tr>
<tr>
<td>zone-c</td>
<td>TEAM-AFRINIC</td>
</tr>
<tr>
<td>mnt-by</td>
<td>AFRINIC-IT-MNT</td>
</tr>
<tr>
<td>mnt-lower</td>
<td>AFRINIC-IT-MNT</td>
</tr>
<tr>
<td>source</td>
<td>AFRINIC</td>
</tr>
</tbody>
</table>
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
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
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 ??