DNSSEC@AfriNIC

AfriNIC-15

Yaounde, 23rd November 2011

Alain P.AINA

AfriNIC and RDNS

- As a RIR, AfriNIC manages and delegates RDNS subdomains to its members
  - IPv4

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

    ERX Space from /8 administered by other RIRs
  - 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

- 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 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

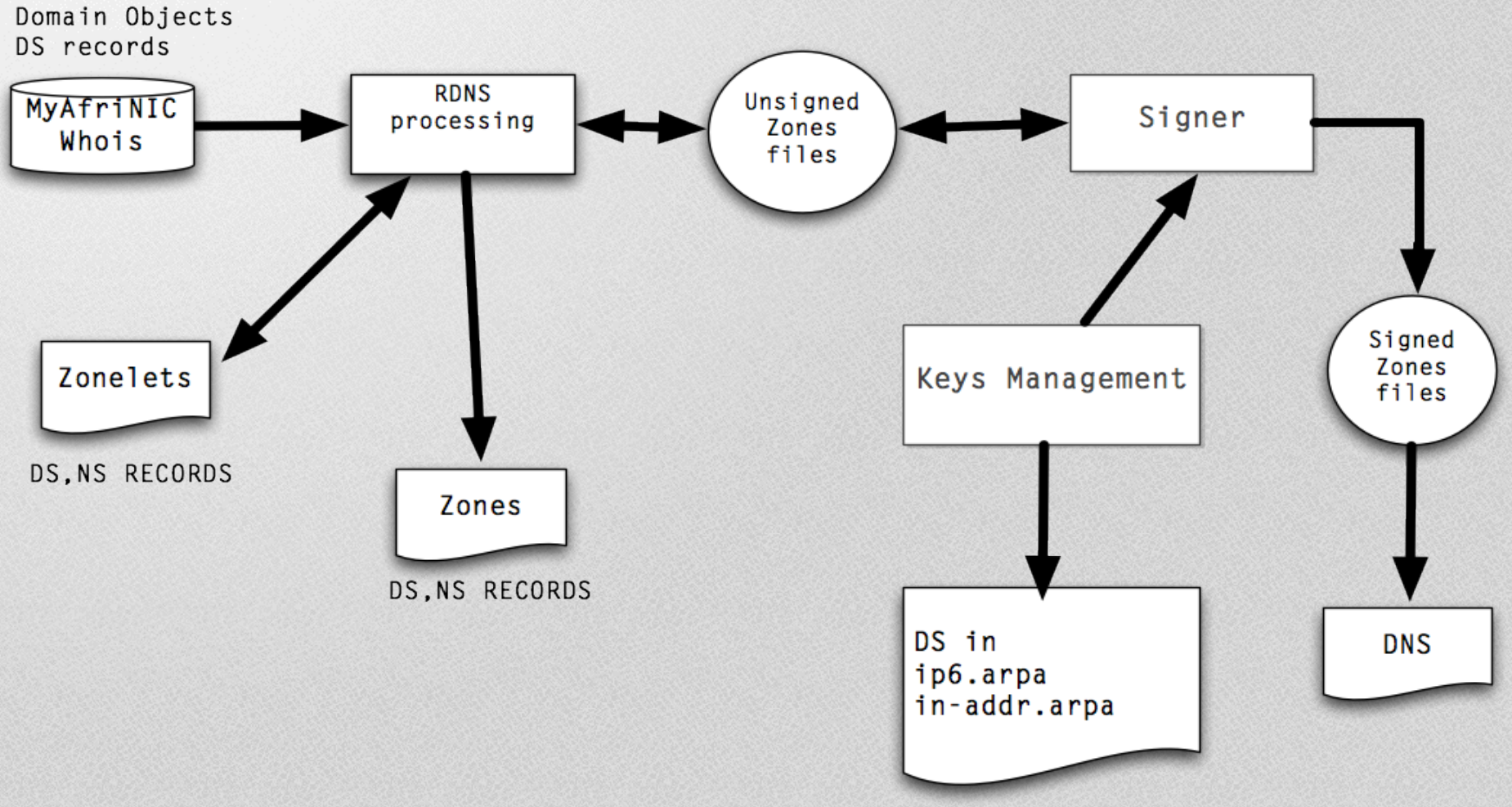
Phase 5: DS publication in parent zones

Phase 6 : Members" DS publication

DNSSEC@AfriNIC

- Few changes to the NS setup
- RDNS provisioning system to be updated
  - Update domain objects with DS attributes
  - Update on MyAfriNIC
  - DS processing
    - From domain objects/MyAfriNIC
    - From zonelets
  - Publish DS in signed zones
- OpenDNSSEC as signer
  - Testbed operational

DNSSEC@AfriNIC



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/

- HSM discussions included in RPKI infrastructure setup.

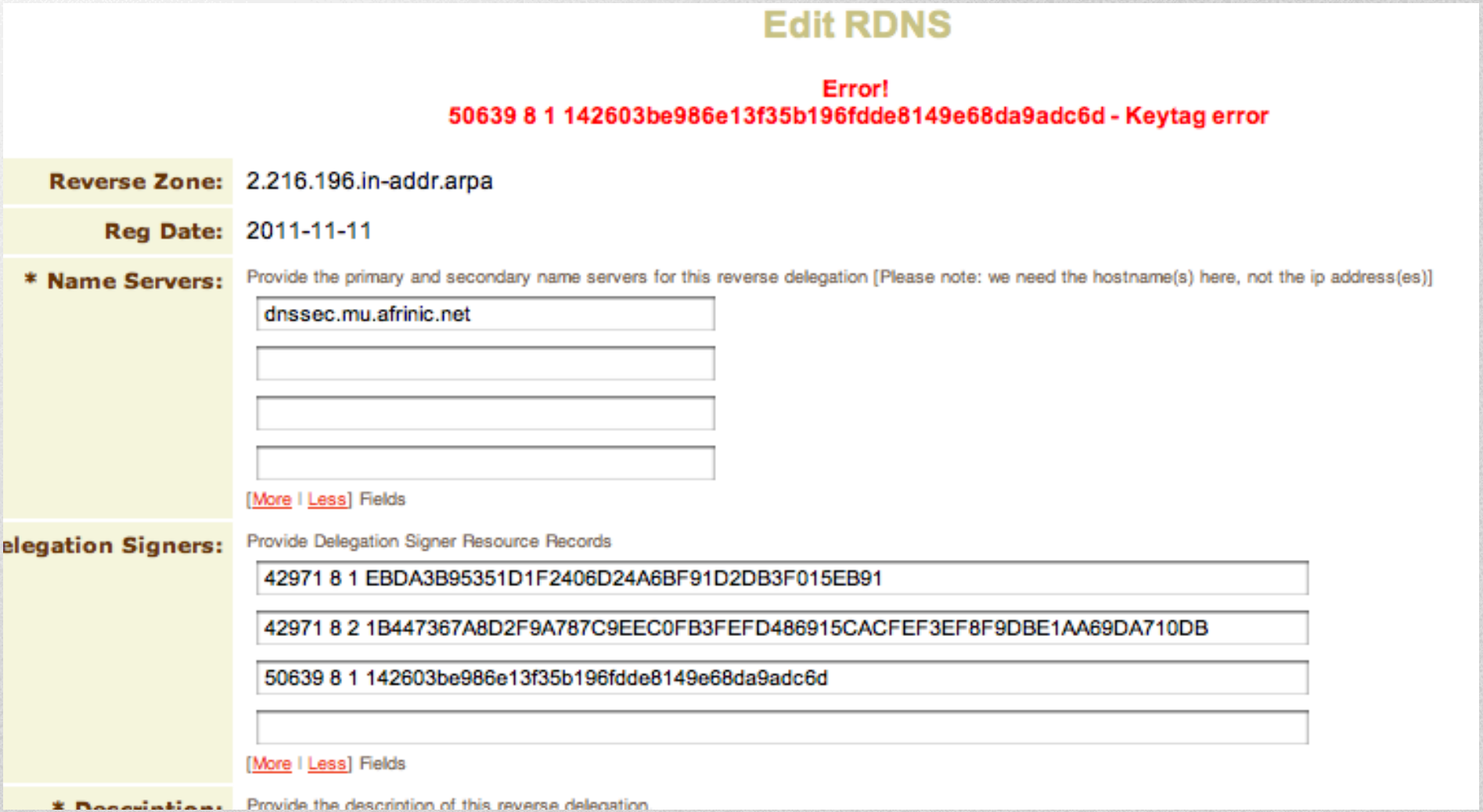
DNSSEC@AfriNIC

```
[root@dnssec ~]# ods-hsmutil list
Listing keys in all repositories.
28 keys found.

Repository              ID                                Type
----------              --                                ----
SoftHSM                 e733653681950f05ca9fc53a12a6f306  RSA/1024
SoftHSM                 58e1a5a3ccd5f31514f3f1c35af85817  RSA/1024
SoftHSM                 93dd7e4ca13798082269096058dcfca9  RSA/1024
SoftHSM                 37e5cb4fb6f10896b3deb42673798ff0  RSA/1024
SoftHSM                 52826c91605435d25b2eac9d9da198c6  RSA/1024
SoftHSM                 53ccd0ce5077ec53b58e1352875aa984  RSA/2048
SoftHSM                 2f99f4de8100158e845a5d5bb7f4f02a  RSA/1024
SoftHSM                 701c01a6df0d210ebe7c401f7e2eb153  RSA/2048
SoftHSM                 013b8fc18b325ac5362de94db751f61f  RSA/1024
SoftHSM                 36cfa8c0e6b2216a8a548cbddec44acd  RSA/1024
SoftHSM                 7d7ad3265eb05da9bd9c975718f52c12  RSA/1024
SoftHSM                 6b889934954e401e6d5b28a727c78a04  RSA/1024
SoftHSM                 0fa3d4e13440b8d226cfd9470acd58de  RSA/1024
SoftHSM                 dce5de9640d5c3b5248cea9ec9bad197  RSA/1024
SoftHSM                 55e2bdb75d3d91a4a777b48f10f1d632  RSA/1024
SoftHSM                 dedc233842c3aec5f0b66f13c0503a80  RSA/1024
SoftHSM                 10aebbd8dd987ad5b69d6762b56633bf  RSA/1024
SoftHSM                 4109ae6dc1a752b00ad9209a67cf935a  RSA/1024
SoftHSM                 dc09b65ee00f8213cff62a2caac61b22  RSA/2048
SoftHSM                 645e314e52c7f4ea458e5155425ec36f  RSA/2048
SoftHSM                 568193cec534fb0c260870492c53e172  RSA/2048
SoftHSM                 bc8b9b9002cdc8f898c6f6cac85a48b1  RSA/2048
SoftHSM                 5eb7cc88cb31944f0063710b3156d692  RSA/2048
SoftHSM                 489e06b317b2dc5bdc074648c5d2e8d9  RSA/2048
SoftHSM                 6e2155598907 9be76a22555560082c78 RSA/2048
SoftHSM                 69acd4ea8b9c32f06ceaf27469e1e191  RSA/2048
SoftHSM                 b04ddef434a3f3162152d845e2b3053e  RSA/2048
SoftHSM                 f8f1bef33d946d6b20df998df1b4f17e  RSA/2048
```

DNSSEC@AfriNIC

```
[root@dnssec ~]# ods-signer queue
It is now Wed Nov 23 01:07:25 2011
Working with task [audit] on zone 196.in-addr.arpa
Working with task [audit] on zone 41.in-addr.arpa
Working with task [audit] on zone 197.in-addr.arpa

I have 9 tasks scheduled.
On Wed Nov 23 01:07:30 2011 I will [read] zone example.com
On Wed Nov 23 01:11:17 2011 I will [sign] zone 2.216.196.in-addr.arpa
On Wed Nov 23 03:00:05 2011 I will [sign] zone 102.in-addr.arpa
On Wed Nov 23 03:00:06 2011 I will [sign] zone 2.4.1.0.0.2.ip6.arpa
On Wed Nov 23 03:00:07 2011 I will [sign] zone 3.4.1.0.0.2.ip6.arpa
On Wed Nov 23 03:00:08 2011 I will [sign] zone 154.in-addr.arpa
On Wed Nov 23 03:00:09 2011 I will [sign] zone 105.in-addr.arpa
On Wed Nov 23 03:00:11 2011 I will [sign] zone 0.c.2.ip6.arpa
On Wed Nov 23 03:00:14 2011 I will [sign] zone afrinic.net
```

DNSSEC@AfriNIC



DNSSEC@AfriNIC

- Query for our signed zones ?
  - *dig @dnssec.mu.afrinic.net +dnssec .....*
- System will be open to members very soon
  - We will publish your DS in our Signed zones
  - We will push your DS to zones managed and signed par other RIRs
- Prepare your DS

Questions ??