# DNSSEC@AFRINIC

*Alain P.AINA*
*DNSSEC Project Manager*

AFRINIC 16
Serekunda, The Gambia | 12-18 May 2012

# 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 RIR

# 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

# Deployment plan

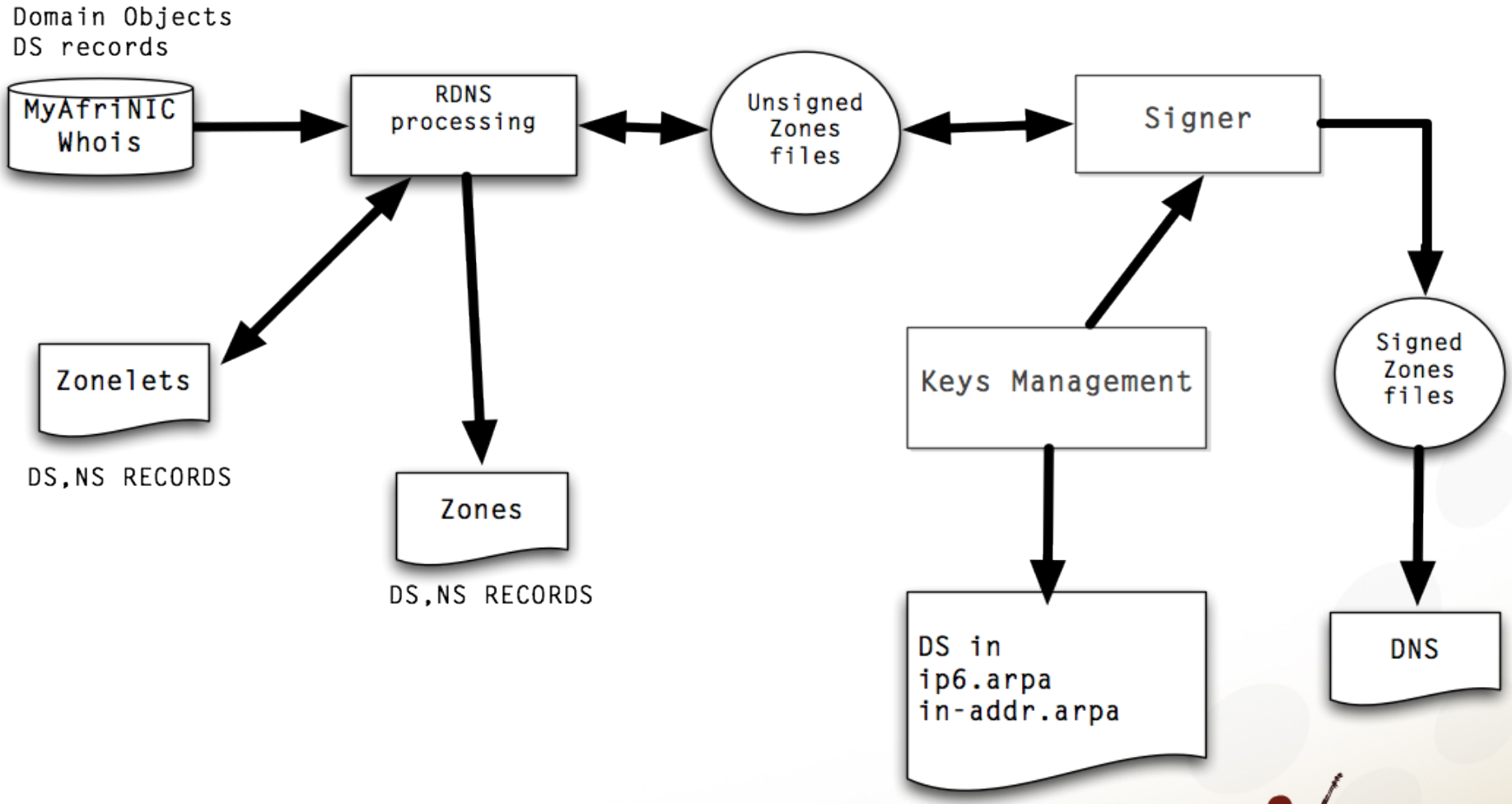
- Deployment plan adopted internally
  - Assess the RDNS provisioning system readiness
  - Deployment stages

## Multiple Phases:

- Testing Phase
- Phase 1: Unsigned zones published
- Phase 2: Signed zones published
- Phase 3:  DS publications

http://www.AFRINIC.net/index.php/en/initiatives/dnssec/690-AFRINIC-dnssec-deployment-plan

# Architecture



# DPS

KSK of 2048 bits RSA

ZSK of 1024 bits RSA

NSEC

Signatures with the SHA2-256 using RSA.

Roll ZSK monthly with a pre-publishing scheme

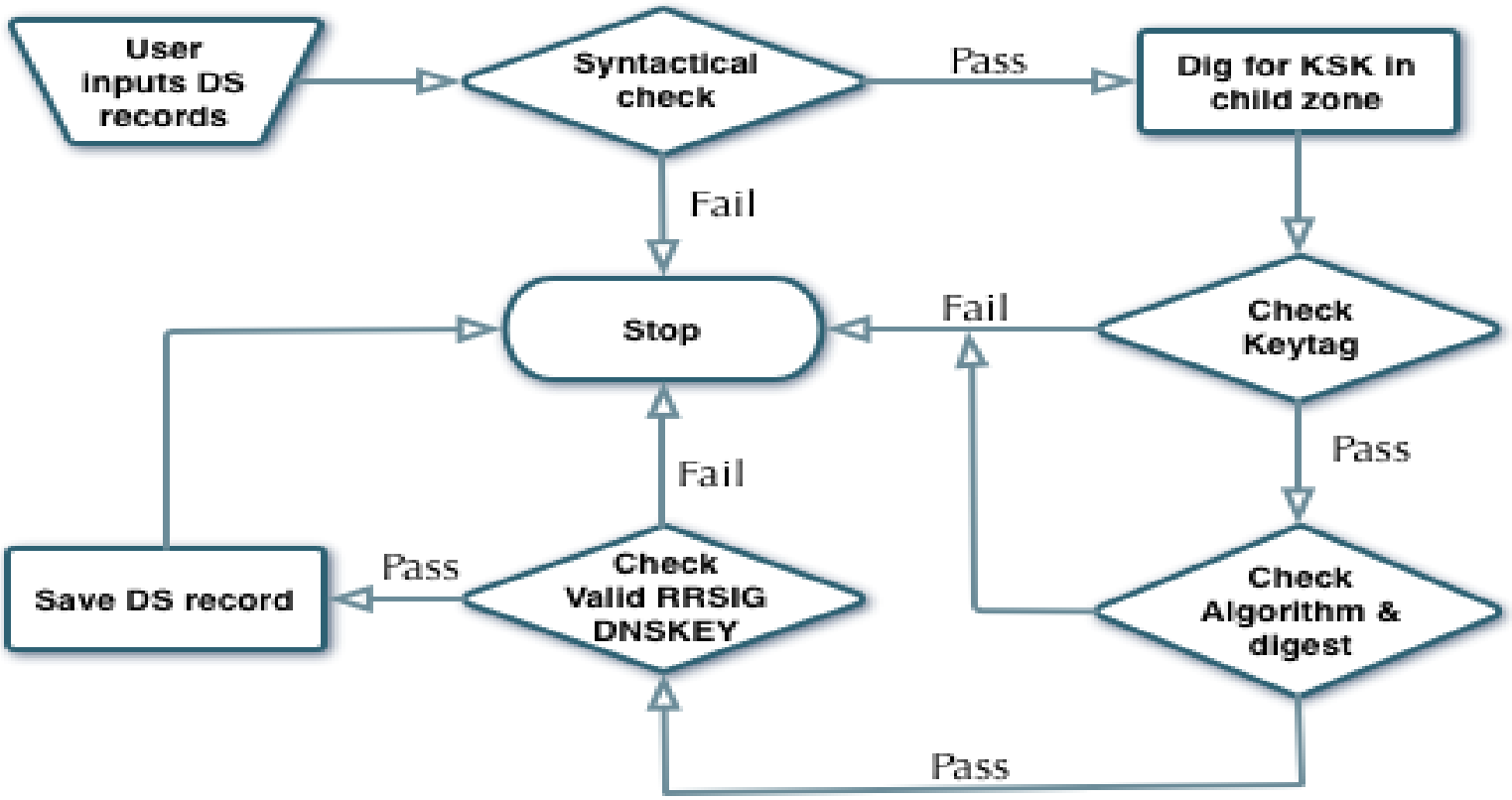
Roll KSK yearly with a double-signing scheme

Signature lifetime of 15 days.

Etc..

http://www.AFRINIC.net/index.php/en/initiatives/692-AFRINIC-dps

# DS validation



# Status

- Phase 3 implemented
  - DS into ip6.arpa and in-addr.arpa
  - Processing subdomains DS
- Accepting DS for subdomains
  - MyAFRINIC or auto-dbm
- Validating and Monitoring

# Validated DNS response

```
; <<>> DiG 9.9.0 <<>> @::1 41.in-addr.arpa TXT +dnssec

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16627

;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 8, ADDITIONAL: 17

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags: do; udp: 4096

;; QUESTION SECTION:

;41.in-addr.arpa.               IN      TXT

;; ANSWER SECTION:

41.in-addr.arpa.        172800      IN      TXT    "zone updated at 2012051677"

41.in-addr.arpa.        172800      IN      RRSIG        TXT 8 3 172800 20120531210008 20120516170009 42691
    41.in-addr.arpa. EHHXkKKc7xl912CKlZuCdukDjsgRUml2T7EOatdXlDlQcX2xXNg/TAKB
    //RGk+RZ70ulgiEhQERj8qsQaUYaPdZcaGjdEuK71P9XmlA5vOnfnc8M

    rzhF6Lo+toKJnnQAXFy1uNrEUQ23W9
```

# Communications and discussions

- Project web site
  http://www.AFRINIC.net/index.php/en/initiatives/dnssec

- Questions, comments
  - dnssec-ops@afrinic.net

- Announces and updates to various lists

AFRINIC
The Internet Numbers Registry for Africa

# Questions, Comments ???