
# DNSSEC@AFRINIC

By
**Amreesh Phokeer**
21 June 2013

# AFRINIC and RDNS

- 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

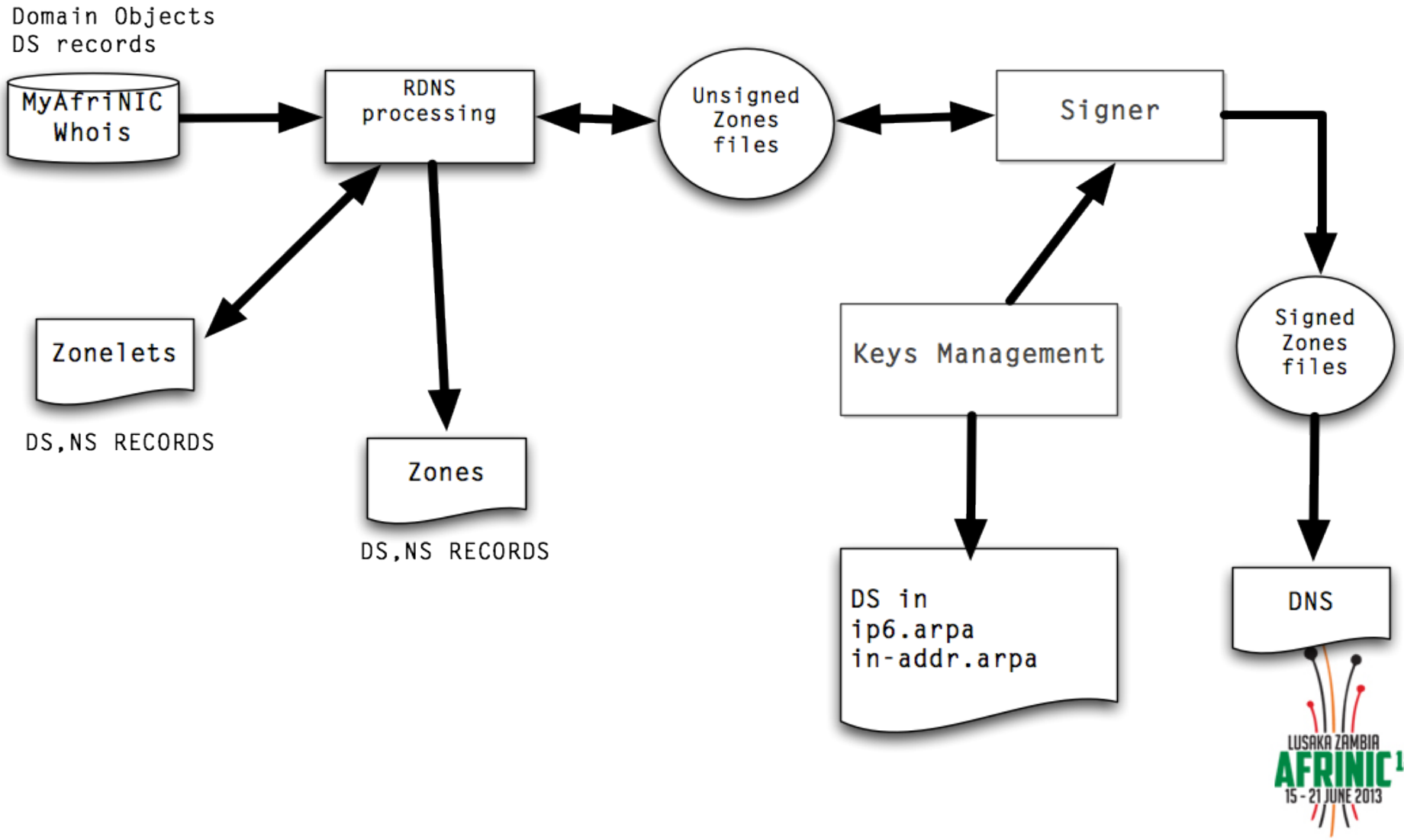
# DNSSEC within the RDNS

- Root, .arpa, .in-addr.arpa, and .ip6.arpa have been signed and chain of trust built
- Deploying DNSSEC within the RDNS enables some other security mechanisms around addressing and its uses.
- AFRINIC signing RIRs managed RDNS zones since April 2012.

# DNSSEC@AFRINIC

- Signs the managed RDNS zones
- Publishes DS in in-addr.arpa and ip6.arpa zones
- Accept DS from Members
  - process DS from zonelets from Other RIRs

# Architecture



# D-P-S

- KSK of 2048 bits RSA
- ZSK of 1024 bits RSA
- Signatures with the SHA2-256 using RSA.
- Roll ZSK monthly with a pre-publishing scheme
- Roll KSK yearly with a double-signing scheme
- …

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

# Key rollover

- Rolled over all KSKs in March 2013.
- Generated and sent new DS records to IANA for the .in-addr.arpa and .ip6.arpa zones
- Used the RESTFUL interface provided by ICANN
- Next rollover planned after deployment of hard HSM

# auto-dbm@afrinic.net

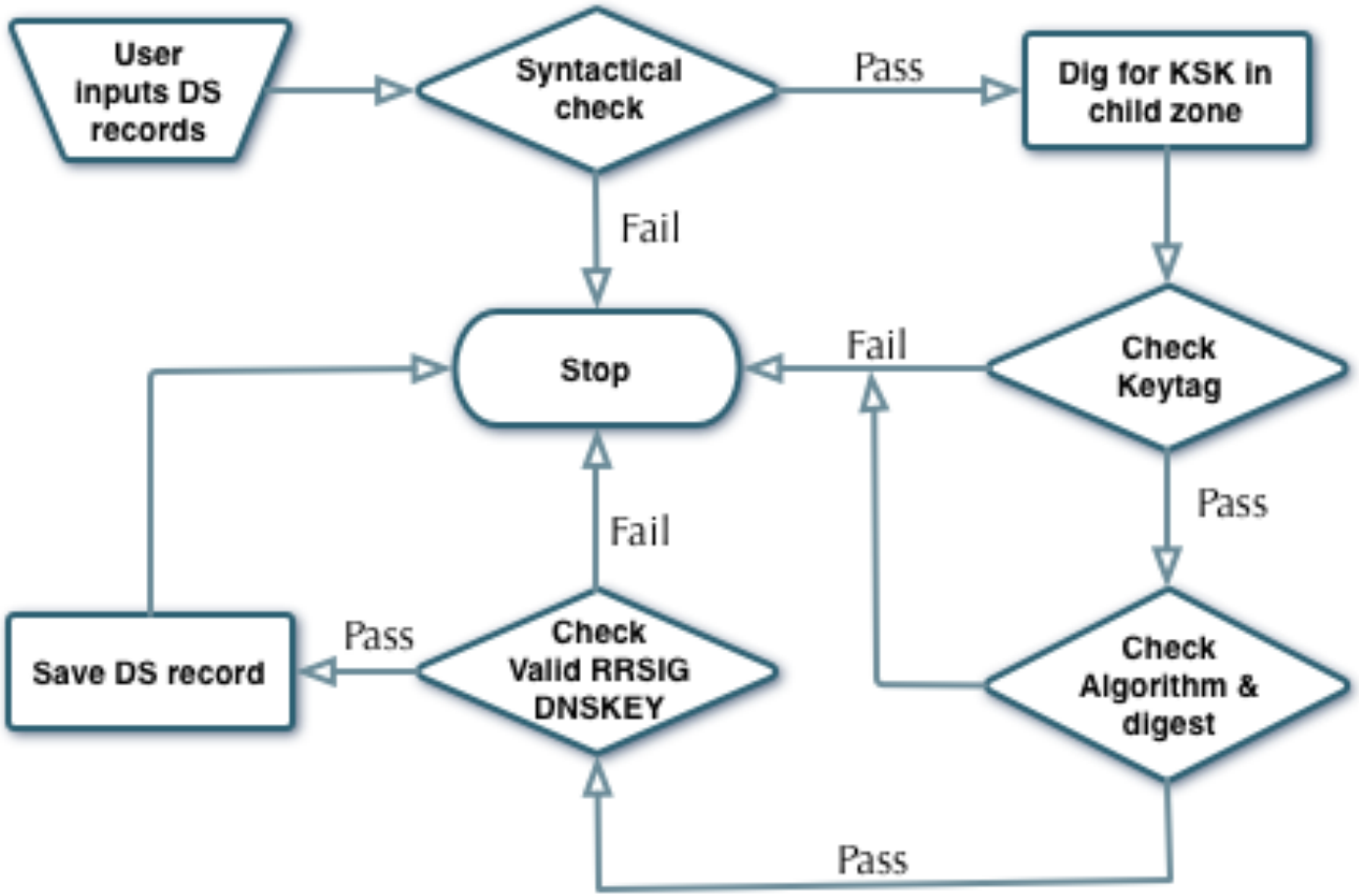
```
domain:         44.22.41.in-addr.arpa
descr:          RDNS for subnet 41.22.44.0 255.255.255.0
nserver:        ns1.toto.net
nserver:        ns2.toto.net
org:            ORG-XXX-AFRINIC
admin-c:        XXX-AFRINIC
tech-c:         XXX-AFRINIC
zone-c:         XXX-AFRINIC
mnt-by:         AFRINIC-MNT
mnt-lower:      AFRINIC-MNT
ds-rdata:       1234 5 1 7F48572A009864B2DDCCD60643EC3C255AFDB2D7
changed:        madhvi@afrinic.net 20110818
changed:        abuse@faircom.co.za 20120618
source:         AFRINIC
```

# MyAFRINIC interface

| | |
|---|---|
| **Parent:** | 196.192.112.0 - 196.192.112.255 |
| *** Reverse Zone:** | Please note that the reverse zone requested must be of the form x.y.z.in-addr.arpa (or x.y.z.ip6.arpa for IPv6) |
| *** Domain Name Servers:** | Provide the primary and secondary name servers for this reverse delegation. [Please note: we need the hostname(s) here, not the ip address(es)]<br>[More \| Less] Fields |
| **DS Records:** | Provide Delegation Signer Resource Records (RFC 4034)<br>keytag: {0-65535} ; Algorithm:{3\|5\|6\|7\|8\|10\|12\|253\|254} ; Digest type :{1-3} ; Digest:{alphanumeric}<br>[More \| Less] Fields |

LUSAKA ZAMBIA AFRINIC 18 15 - 21 JUNE 2013

# DS validation



# Some statistics

- DS records from:

| **AFRINIC** | **49** |
|---|---|
| APNIC | None |
| ARIN | None |
| LACNIC | None |
| RIPE | None |

45 DS with in-addr.arpa records

4 DS with ip6.arpa records

2 AFRINIC members so far

# 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

….

;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
+RZ70ulgiEhQERj8qsQaUYaPdZcaGjdEuK71P9XmIA5vOnfnc8M rzhF6Lo

+toKJnnQAXFy1uNrEUQ23W9

# Communications and discussions

Project web site / Statistics

http://www.AFRINIC.net/index.php/en/initiatives/dnssec

Questions, comments

– dnssec-ops@afrinic.net

# Questions, Comments ???

LUSAKA ZAMBIA
AFRINIC 18
15 - 21 JUNE 2013