DNSSEC, Where does AfriNIC stand

AfriNIC-13
Johannesburg, 25/11/2010

Alain P. AINA
RPKI Projects Manager
DNSSEC Project manager/Spokesman

AfriNIC

AfriNIC and DNS

- Provides RDNS services for v4 and v6 spaces
- For v4, manages zones:
  - 41.in-addr.arpa.
  - 196.in-addr.arpa.
  - 197.in-addr.arpa.
  - 105.in-addr.arpa.

  Participates in the inter-RIRs ERX space RDNS management system
- For v6, manages zones:
  - 0.c.2.ip6.arpa.
  - 2.4.1.0.0.2.ip6.arpa.
  - 3.4.1.0.0.2.ip6.arpa.

AfriNIC

DNSSEC at AFRINIC
ToDo

- Sign the zones we manage

- Send DS records to parent zones ip6.arpa. and in-addr.arpa.

- Change to the provisioning systems to accept DS from members on domain objects
  - Through MyAFRINIC portal
  - Domain objects update through e-mail

- Update the Inter-RIRs ERX RDNS system to collect and send DS records from/to majority RIR

AfriNIC

DNSSEC at AFRINIC
New domain object

domain: [mandatory] [single] [primary/look-up key]
descr: [mandatory] [multiple] [ ]
org: [optional] [multiple] [inverse key]
admin-c: [mandatory] [multiple] [inverse key]
tech-c: [mandatory] [multiple] [inverse key]
zone-c: [mandatory] [multiple] [inverse key]
nserver: [optional] [multiple] [inverse key]
ds-rdata: [optional] [multiple] [inverse key]
sub-dom: [optional] [multiple] [inverse key]
dom-net: [optional] [multiple] [ ]
remarks: [optional] [multiple] [ ]
notify: [optional] [multiple] [inverse key]
mnt-by: [mandatory] [multiple] [inverse key]
mnt-lower: [optional] [multiple] [inverse key]
refer: [optional] [single] [ ]
changed: [mandatory] [multiple] [ ]
source: [mandatory] [single] [ ]

Add a DS attribute to the domain object

AfriNIC

DNSSEC at AFRINIC
DS-rdata attribute

ds-rdata

DS records for this domain.

<Keytag> | <Algorithm> | <Digest type> | <Digest> | ; <Comment>

Keytag is represented by an unsigned decimal integer (0-65535).

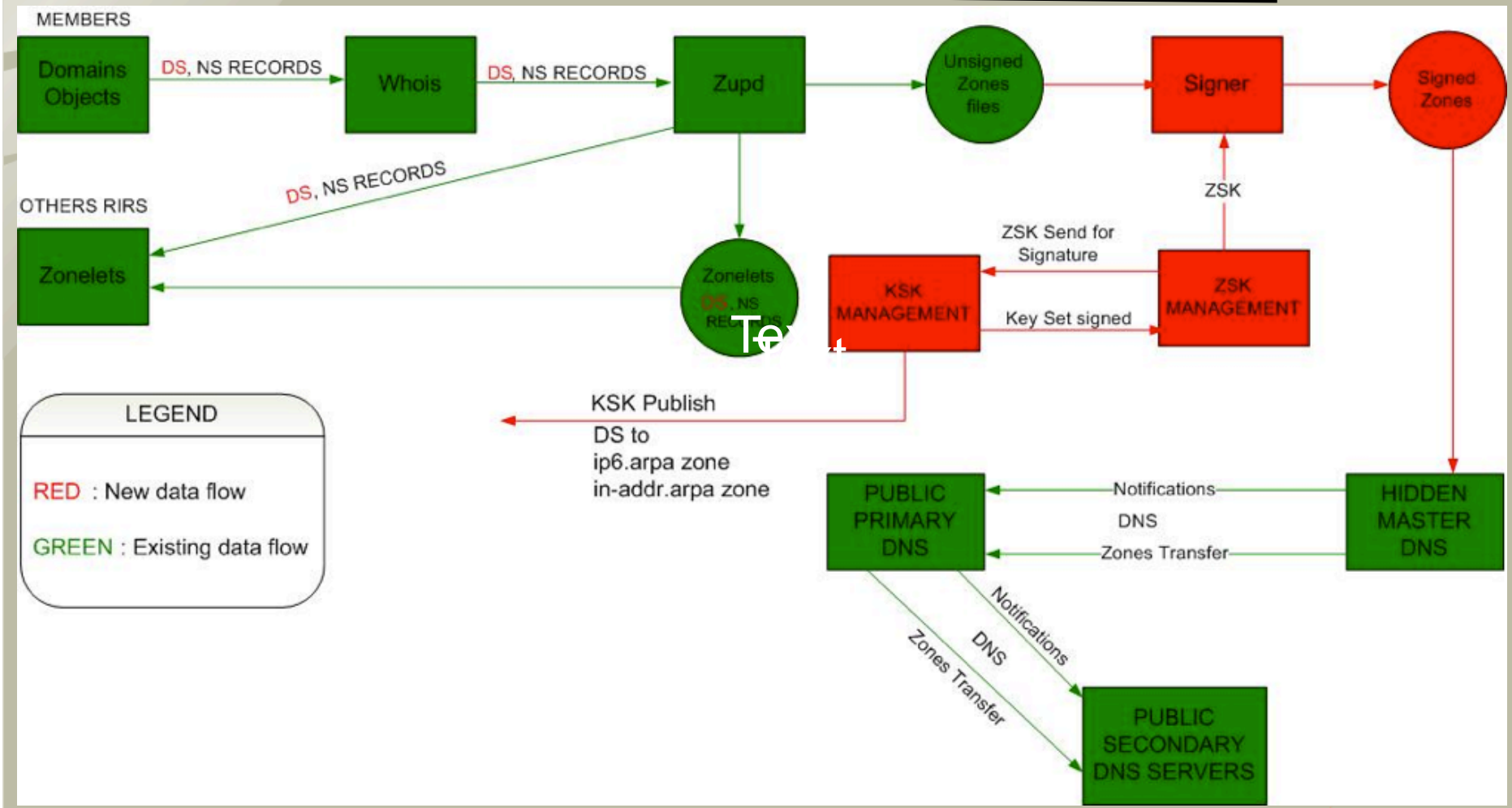
Algorithm is represented by an unsigned decimal integer (0-255) or one of the following mnemonics:
RSAMD5, DH, DSA, ECC, RSASHA1, INDIRECT, PRIVATEDNS, PRIVATEOID.

Digest type may be represented by a unsigned decimal integer (0-255) and is usually 1, which stands for SHA-1.

Digest is a digest in hexadecimal representation (case insensitive). Its length varies for various digest types.
For digest type SHA-1 digest is represented by 20 octets (40 characters, plus possible spaces).
For more details, see RFC4034.

AfriNIC

DNSSEC at AFRINIC Architecture



DNSSEC at AFRINIC
Key Management

HSM

AfriNIC

Parent zones situation

- .arpa is signed, but DS is not published in root zone. key is DLV registry
- ip6.arpa. is signed and has DS in .arpa. zone
- in-addr.arpa. not signed

AfriNIC

AFRINIC's Roadmap for DNSSEC

- **End of December 2010** – Adopt the project document and deployment plan

- **End of March 2011**- Ready to accept DS from members

Will you be the first to send DS to our RDNS zones ?

Questions ?

AfriNIC