AFRINIC
(r)DNSSEC Infrastructure

...and how we (silently) migrated a signer

Amreesh Phokeer
amreesh@afrinic.net

R&D

ICANN-59 (28 June 2017)

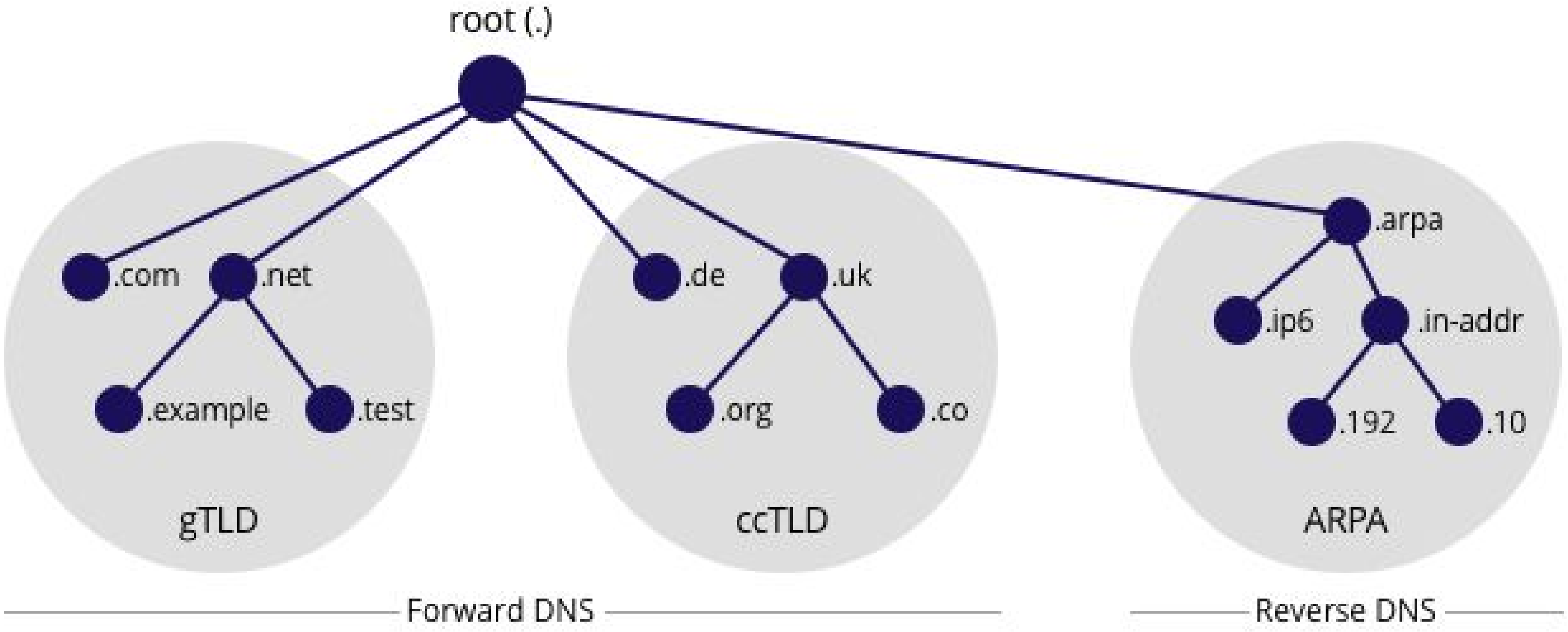
African RIR

- RIR for the African and Indian Ocean region
- Community-driven through policy discussion
- Allocation of IPv4, IPv6 and ASN
- Maintains WHOIS database
- Provides security services for resources: RPKI, IRR, DNSSEC
- Provides IPv6 and other trainings
- Since 2016 => AfriNIC Labs

AfriNIC DNS Programmes

- African Root Server Copy (AfRSCP)
- AfriNIC supported RFC5855 servers
- African DNS Support Programme (AfDSP)

RDNS



```
>$ host 192.0.32.7
7.32.0.192.in-addr.arpa domain name pointer www.icann.org.
```

DNSSEC@AfriNIC

- AfriNIC operates RDNS for its IPv4 and IPv6 zones
  - 0.c.2.ip6.arpa.
  - 3.4.1.0.0.2.ip6.arpa.
  - 2.4.1.0.0.2.ip6.arpa.
  - {41,196,197,102,105,154}.in-addr.arpa.

- Member signs their reverse zones and sends DS records to AfriNIC

DNSSEC@AfriNIC

- AfriNIC operates RDNS for its IPv4 and IPv6 zones
  - 0.c.2.ip6.arpa.
  - 3.4.1.0.0.2.ip6.arpa.
  - 2.4.1.0.0.2.ip6.arpa.
  - {41,196,197,102,105,154}.in-addr.arpa.

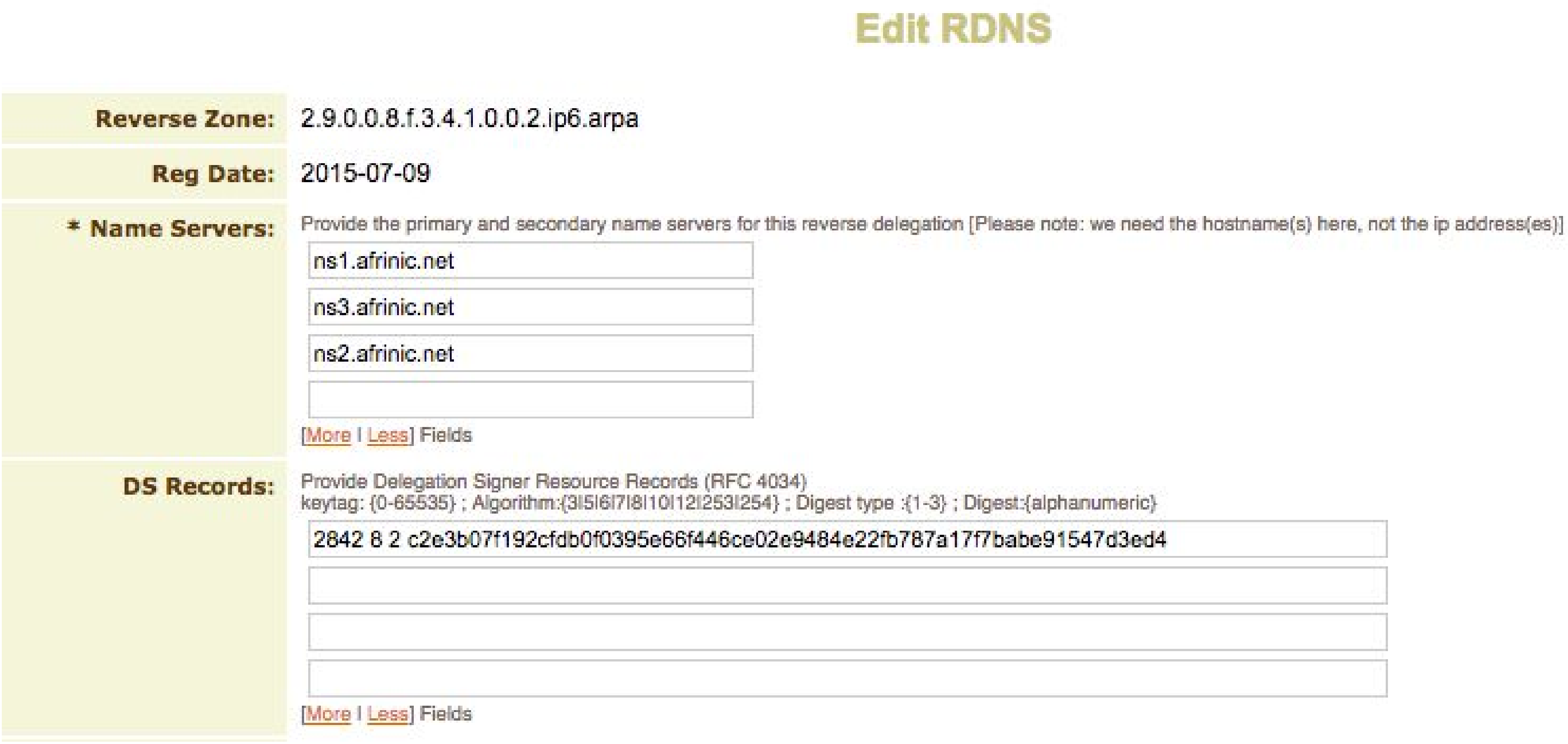
- Member signs their reverse zones and sends DS records to AfriNIC

196.216/16 ----> 216.196.in-addr.arpa

WHOIS Domain object

```
domain:          2.9.0.0.8.f.3.4.1.0.0.2.ip6.arpa
descr:           rDNS for 2001:43f8:92::/48 - AFRINIC CPT OPS
org:             ORG-AFNC1-AFRINIC
admin-c:         IT7-AFRINIC
tech-c:          IT7-AFRINIC
zone-c:          IT7-AFRINIC
nserver:         ns1.afrinic.net
nserver:         ns3.afrinic.net
nserver:         ns2.afrinic.net
ds-rdata:        2842 8 2
 c2e3b07f192cfdb0f0395e66f446ce02e9484e22fb787a17f7ba
 be91547d3ed4
remarks:         AFRINIC CPT OPS
mnt-by:          AFRINIC-IT-MNT
mnt-lower:       AFRINIC-IT-MNT
source:          AFRINIC # Filtered
```

MyAFRINIC



Edit RDNS

Reverse Zone:	2.9.0.0.8.f.3.4.1.0.0.2.ip6.arpa
Reg Date:	2015-07-09
*** 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)] ns1.afrinic.net ns3.afrinic.net ns2.afrinic.net [More | Less] Fields
DS Records:	Provide Delegation Signer Resource Records (RFC 4034) keytag: {0-65535} ; Algorithm:{3|5|6|7|8|10|12|253|254} ; Digest type :{1-3} ; Digest:{alphanumeric} 2842 8 2 c2e3b07f192cfdb0f0395e66f446ce02e9484e22fb787a17f7babe91547d3ed4 [More | Less] Fields

DNSSEC Policy

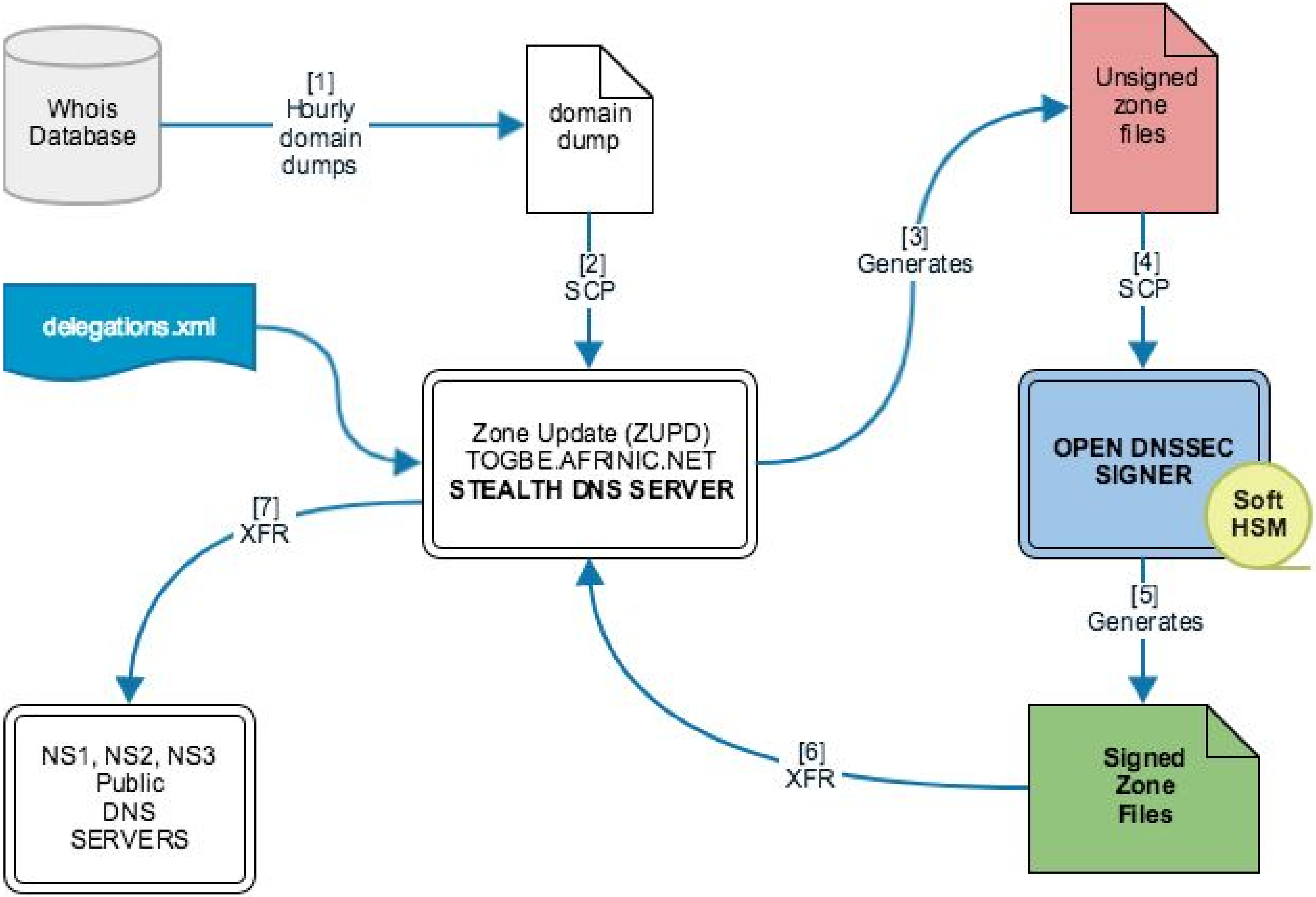
Parameter	Key Length	Algorithm
KSK	2048 bits	RSA
ZSK	1024 bits	RSA
Signature	SHA-256	RSA

- Rollover
  - ZSK: Monthly
  - KSK: Yearly

- Signature lifetime: 15 days

- TTL:
  - DNSKEY: TTL on SOA
  - NSEC: mininum of SOA
  - RRSIG: lowest TTL
  - DS: TTL on NS

Architecture



Members with DS records

- ATI - Agence Tunisienne Internet
- CBC EMEA LTD
- Posix Systems (Pty) Ltd
- RMS Powertronics CC
- Rhodes University
- AfriNIC Ltd

Adoption very very low!!!!

Signer Migration

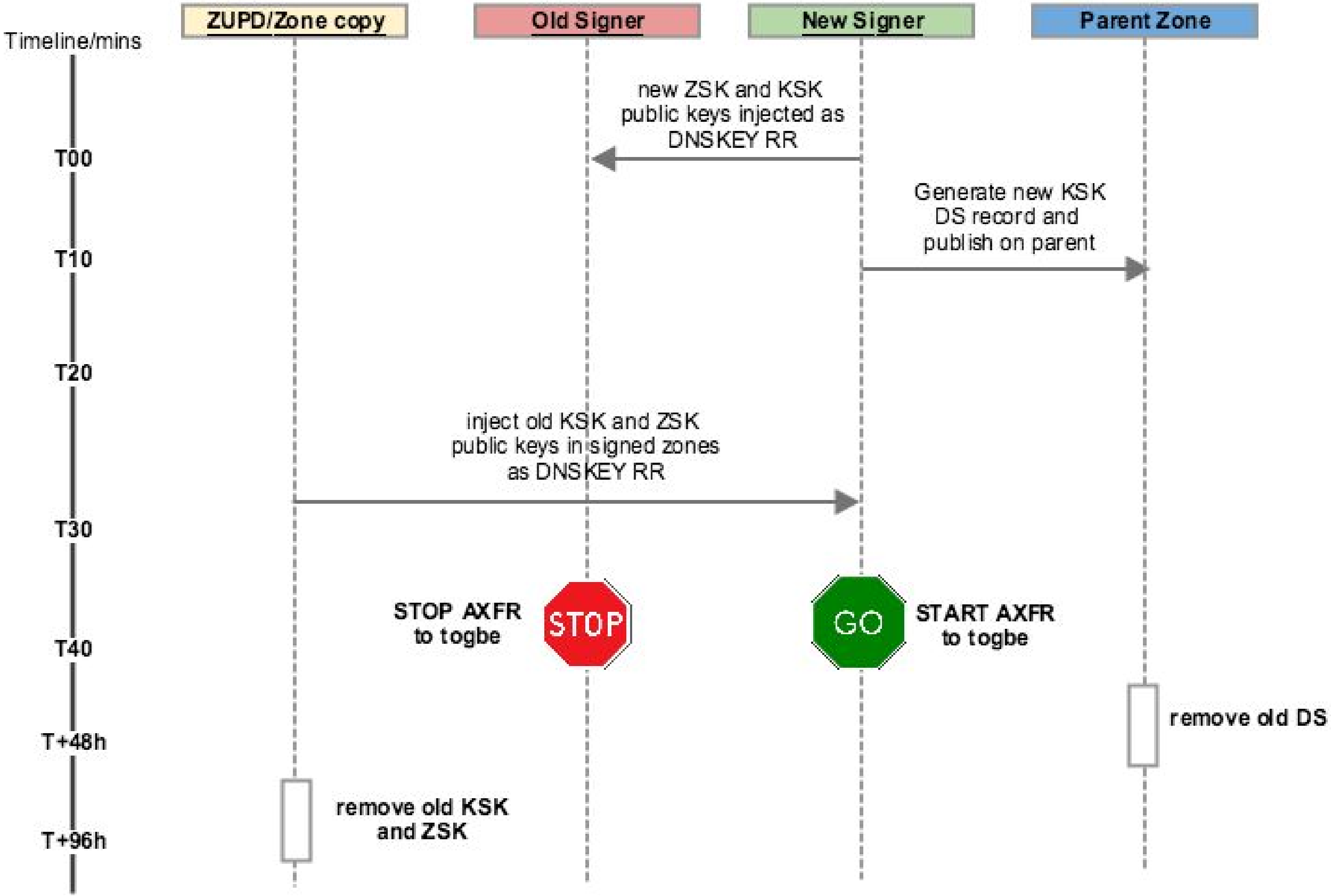
Why?

- Scalability issues with OpenDNSSEC v1.3
- Large delays for signing of zones
- The old signer was stuck into "flush mode" occasionally, leading to members to complain about time to propagate of their changes.
- Limited support for AXFR IN and OUT

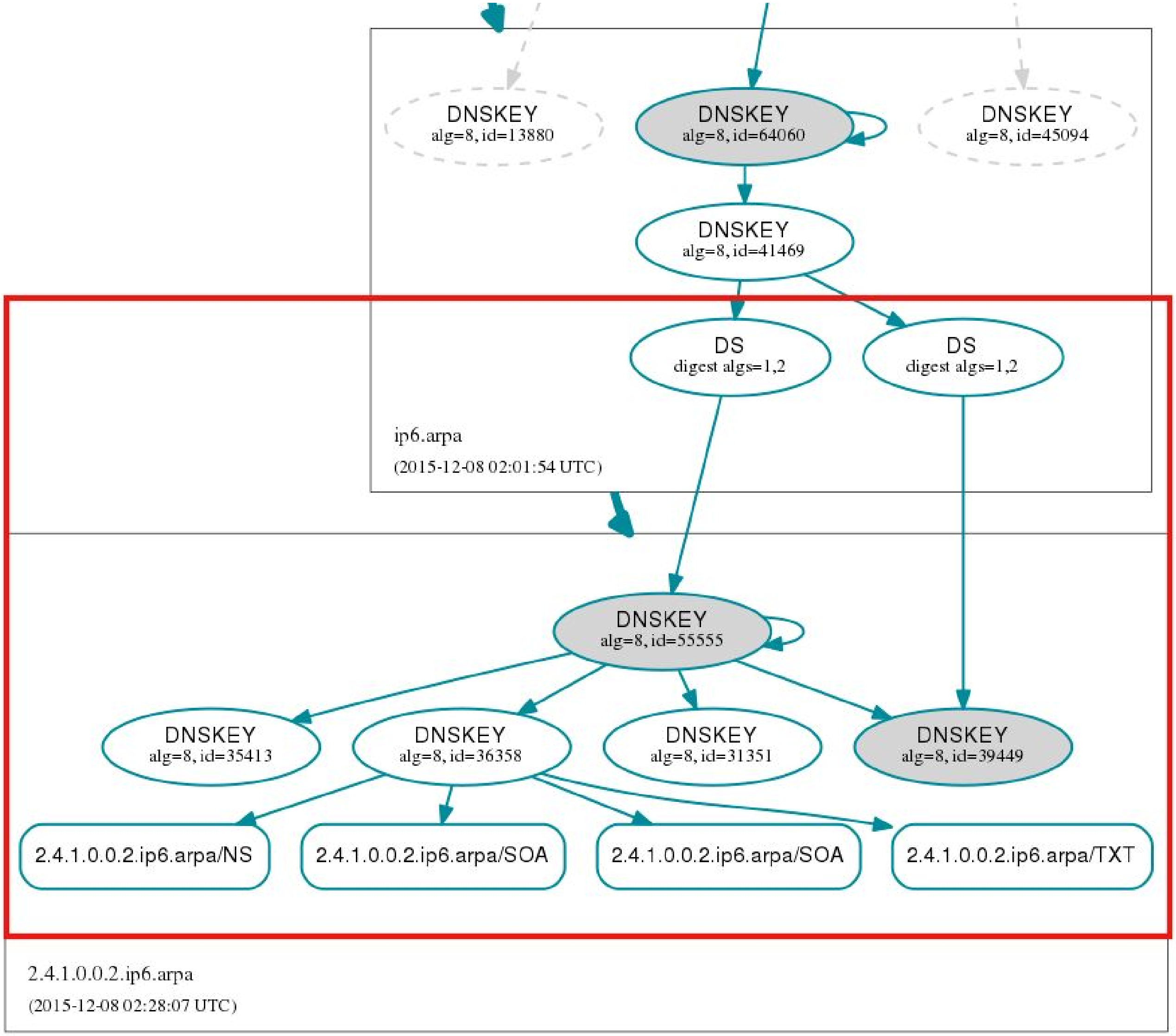
Migration Strategies

Criteria	Option 1 Export existing keys	Option 2 Key rollover	Option 3 New Keys	Option 4 Existing keys followed by rollover
Invalidity window	NO	NO	YES	NO
Key manipulation	YES	NO	NO	YES
Rollover time	None	Wait for old signatures to expire	Wait for caches to pick up new keys	-
Number of interactions with parents	0	2	1	-
DNSKEY RRset size	Same	Double	Same	Same
Exposure of private keys	YES	NO: only public keys exposed	NO	YES

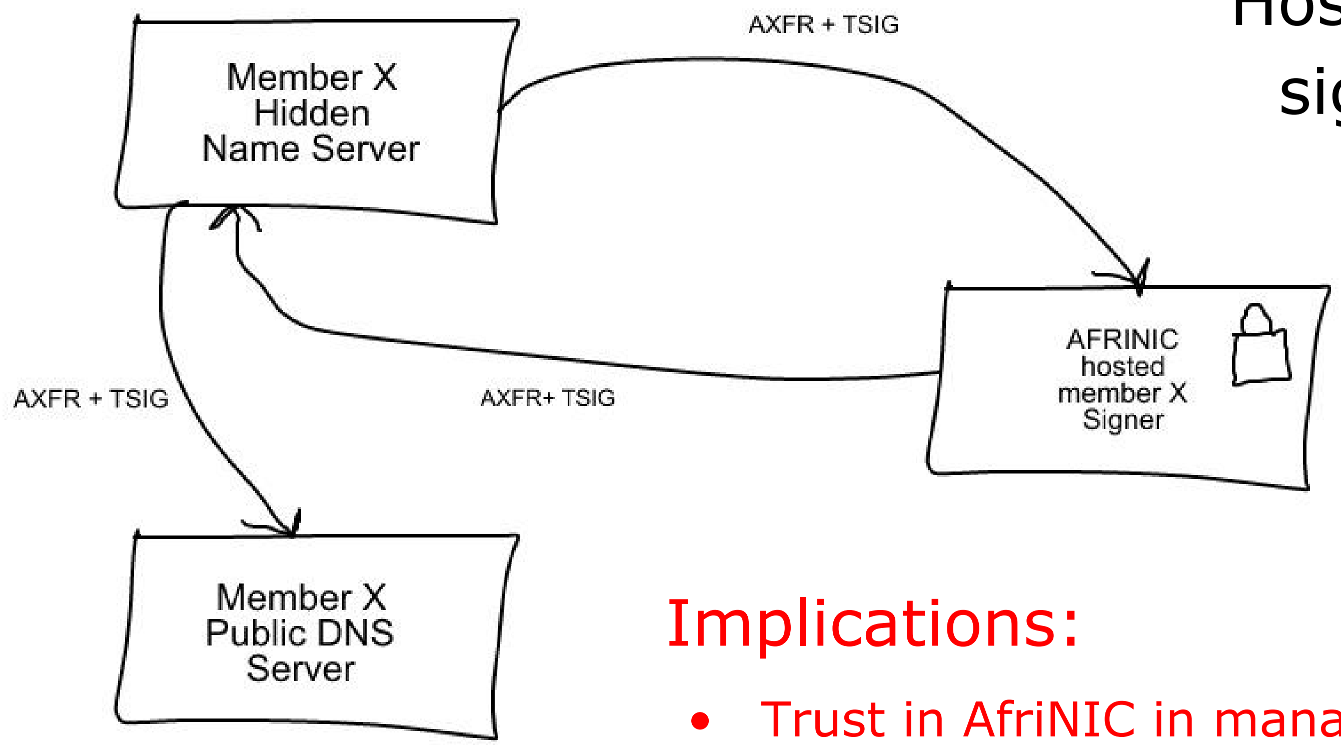
Migration timeline



Double DS


DNSKEY
alg=8, id=13880
DNSKEY
alg=8, id=64060
DNSKEY
alg=8, id=45094
DNSKEY
alg=8, id=41469
DS
digest algs=1,2
DS
digest algs=1,2
ip6.arpa
(2015-12-08 02:01:54 UTC)
DNSKEY
alg=8, id=55555
DNSKEY
alg=8, id=35413
DNSKEY
alg=8, id=36358
DNSKEY
alg=8, id=31351
DNSKEY
alg=8, id=39449
2.4.1.0.0.2.ip6.arpa/NS
2.4.1.0.0.2.ip6.arpa/SOA
2.4.1.0.0.2.ip6.arpa/SOA
2.4.1.0.0.2.ip6.arpa/TXT
2.4.1.0.0.2.ip6.arpa
(2015-12-08 02:28:07 UTC)

Future work


AXFR + TSIG
Member X Hidden Name Server
AFRINIC hosted member X Signer
AXFR + TSIG
AXFR+ TSIG
Member X Public DNS Server

Hosted DNSSEC signer engines for AFRINIC members

Implications:

- Trust in AfriNIC in managing DNSKEYs
- Uptime, SLA, etc

AFRINIC (r)DNSSEC Infrastructure

…and how we (silently) migrated a signer

Amreesh Phokeer
amreesh@afrinic.net

R&D

ICANN-59 (28 June 2017)