DNSSEC Signer Switchover experience

Alain Patrick AINA

Former: AFRINIC
NOW: WACREN

Alain.Aina@wacren.net

Disclaimer

This switchover was done at AFRINIC

https://www.afrinic.net/en/initiatives/dnssec

https://afrinic.net/blog/67-migrating-an-opendnssec-signer

Context

- ✓ Old signer on Opendnssec
  - ✓ Keys in SoftHSM
  - ✓ KSK/ZSK, NSEC
  - ✓ RSASHA256
  - ✓ Sqlite database
- ✓ Zone signing issues noted
  - ✓ Workarounds until migration

Motivations

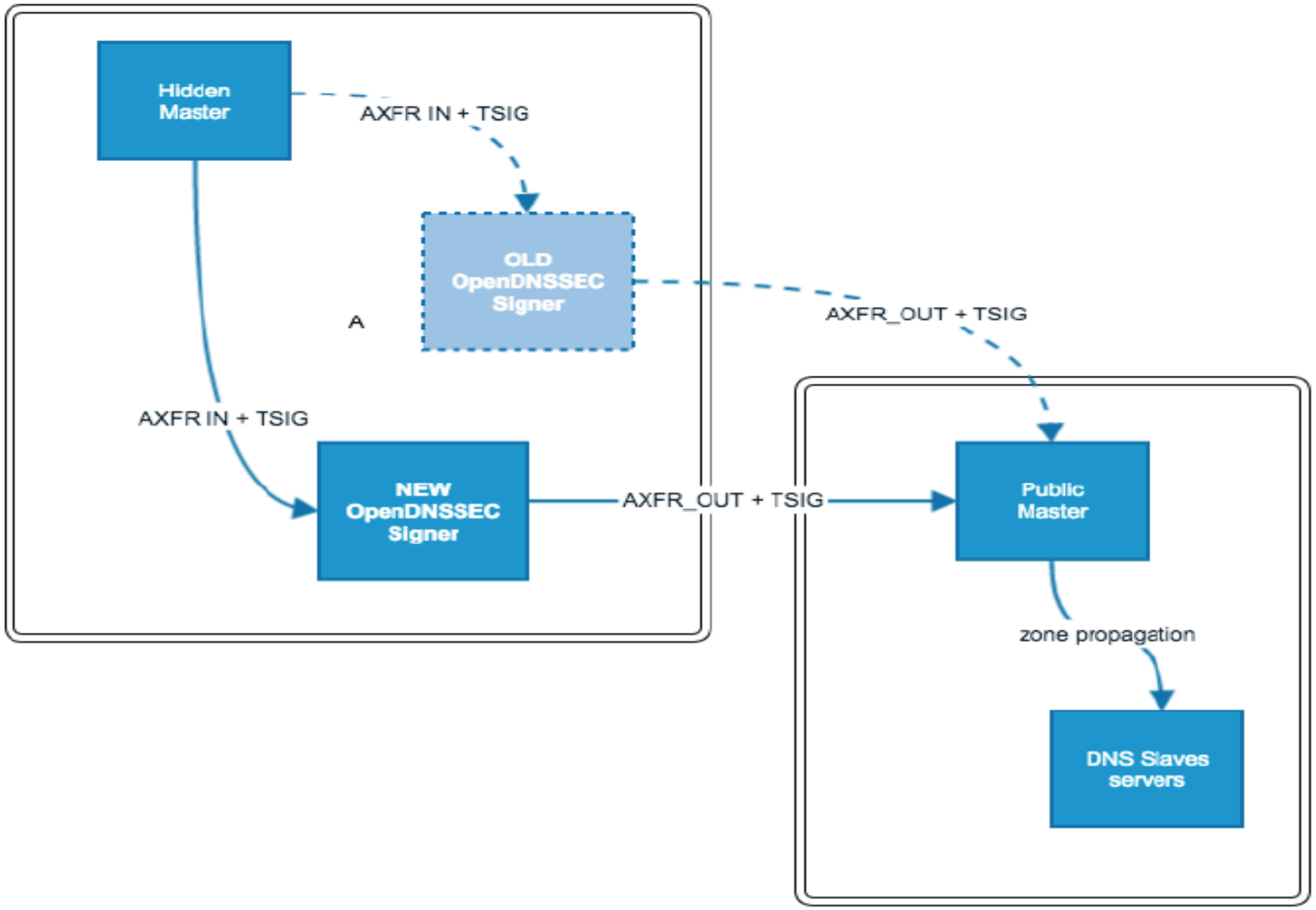
- ✓ Migrate to a newer version which is more stable, secure and scalable with :
  - ✓ MySql database
  - ✓ New version of SoftHSM
  - ✓ Keys in SoftHSM
  - ✓ Same key algorithms and size
  - ✓ Same policies
  - ✓ Etc.

Strategy

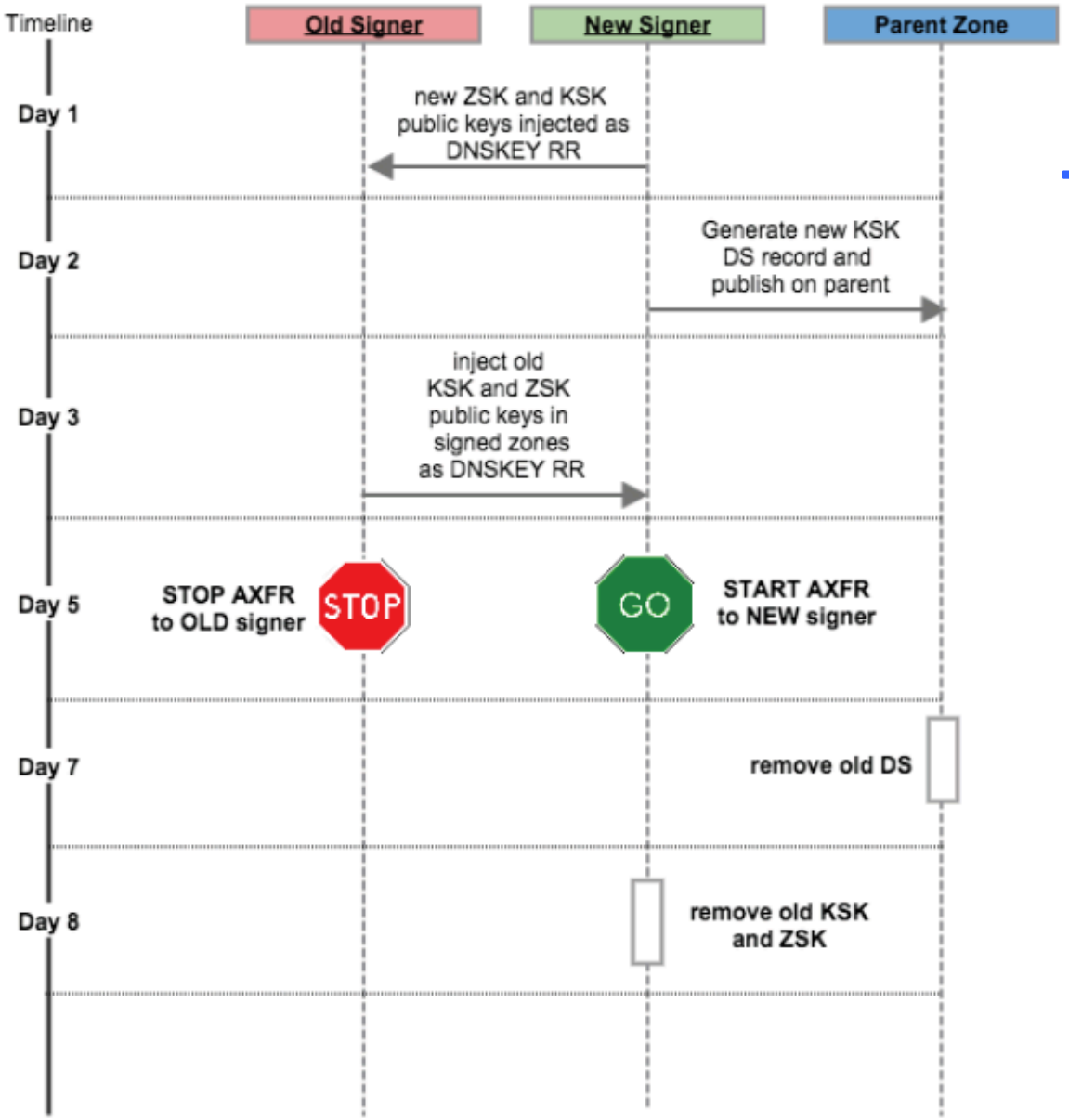
- ✓ No private key export
- ✓ No fresh start
- ✓ Keep validation state of all signed zones all the time

✓ Migrate with keys rollover

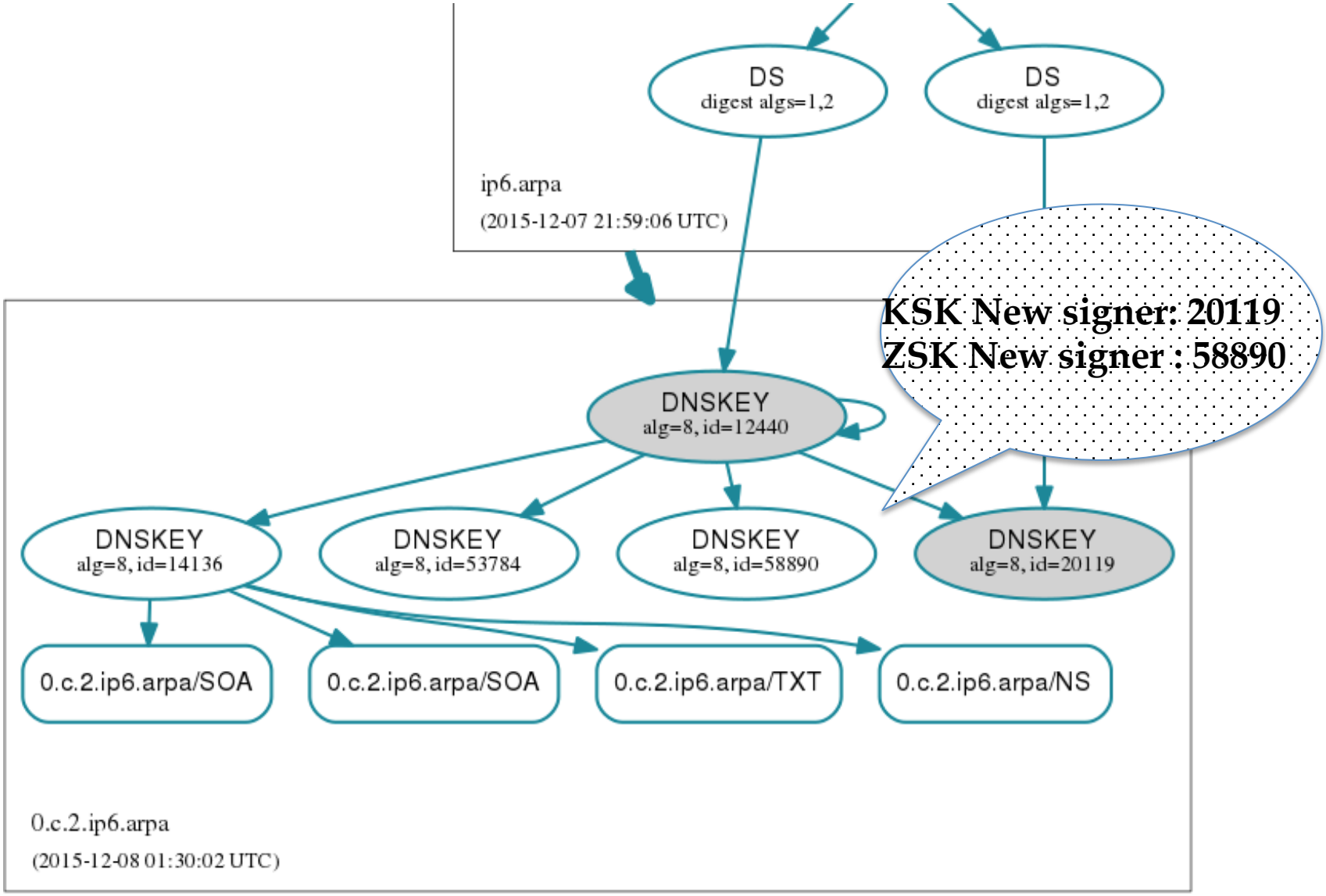
Architecture



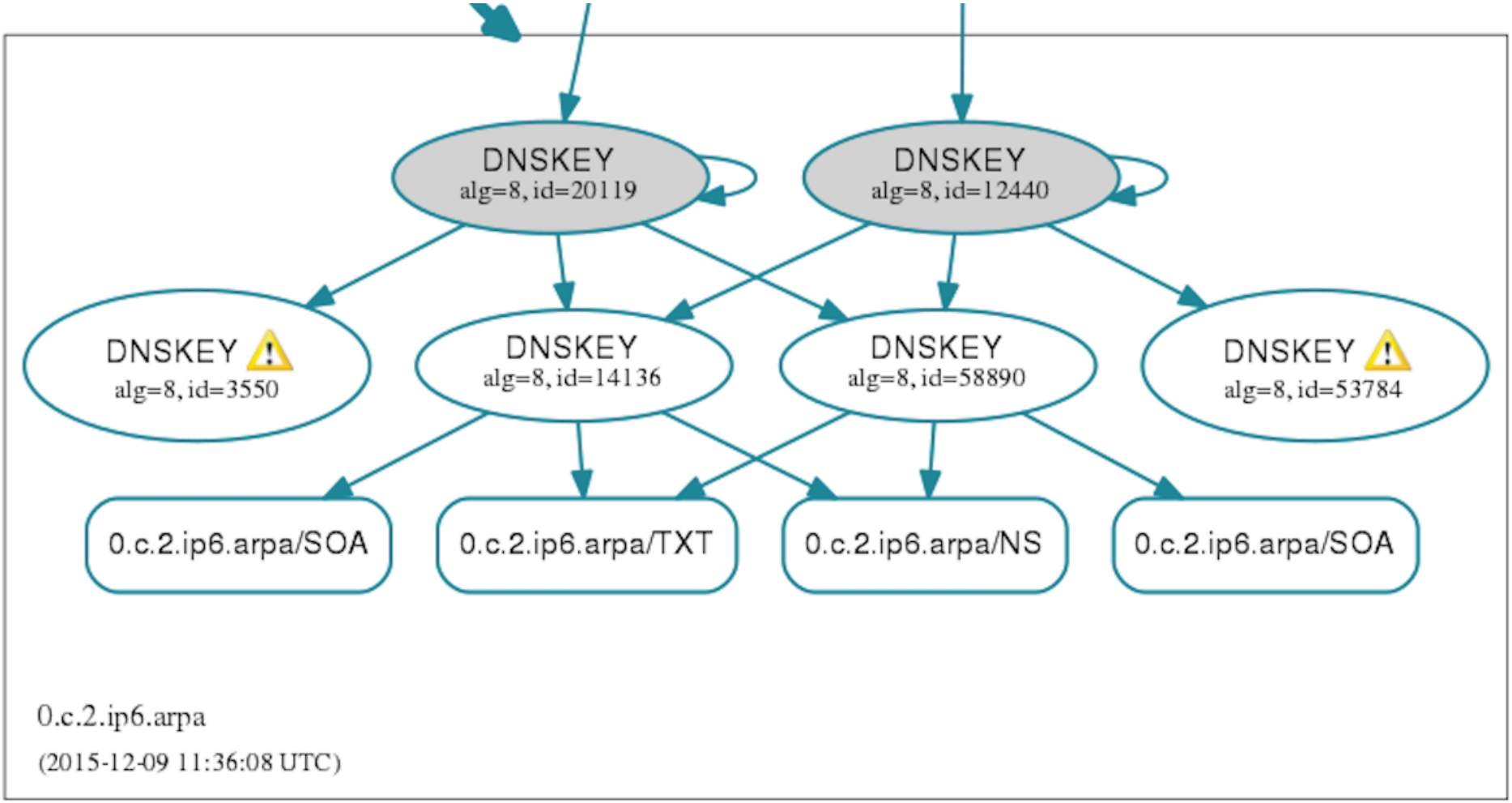
Pre publish DNSKEY & double DS



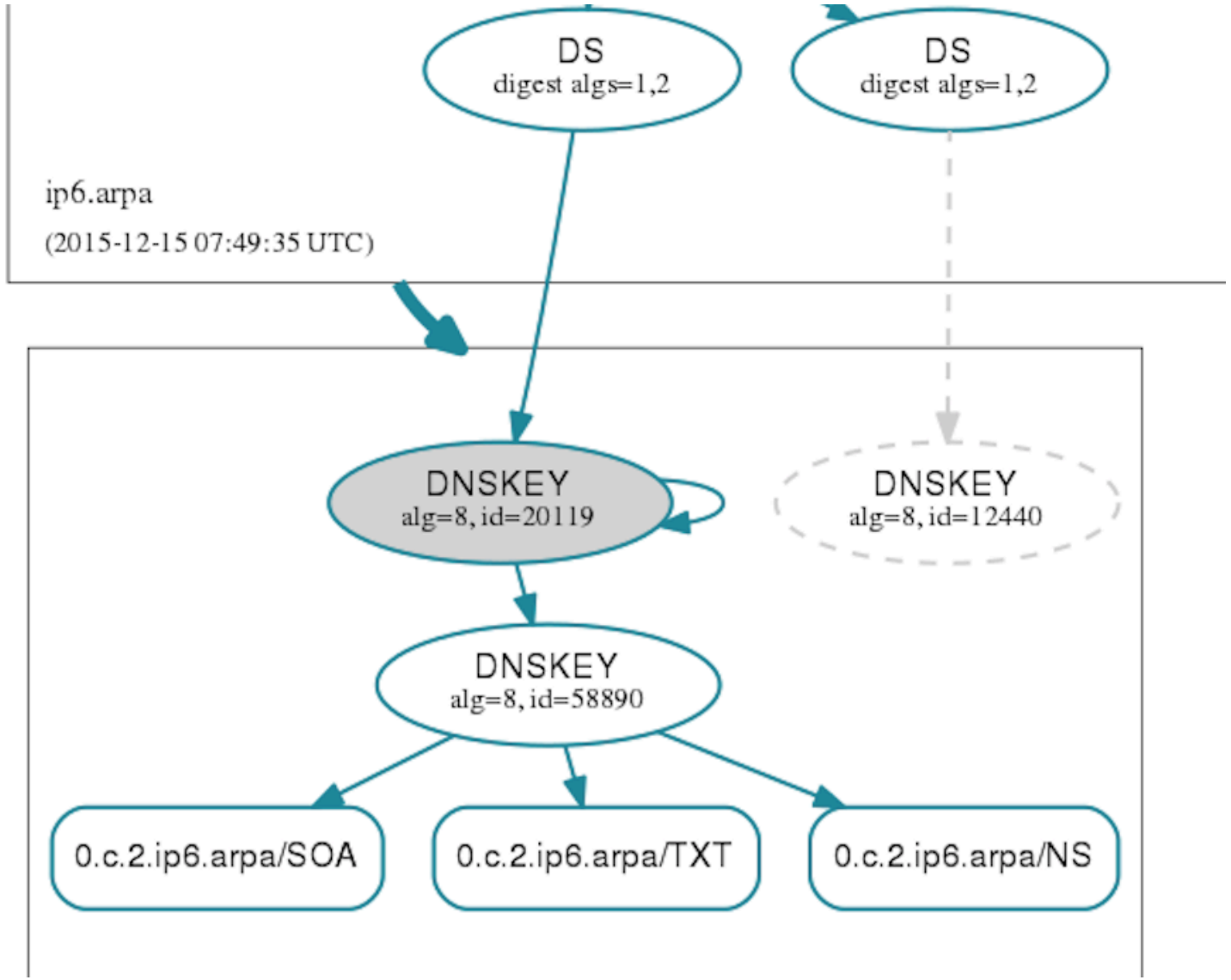
Before switchover



After switchover



Final before old DS removal



And so..

- ✓ It requires careful consideration of the planning and various timings
  - ✓ Signatures lifetime
  - ✓ TTLs
  - ✓ Keys management
  - ✓ Switchover
  - ✓ Etc..
- ✓ It works out very well
  - ✓ No crash
  - ✓ No alert

Conclusions

- ✓ **Good experience**
- ✓ **Would have been a different story with keys in HSM**
- ✓ **Will do same thing next time**
  - ✓ **Excerpt Pre-publishing KSKs**