For confidence online

Disaster Recovery with DNSSEC

Stefan Ubbink | DNS-OARC 36 (virtual)

30 nov 2021

Agenda

1. Why this talk
2. Setup
3. Impact
4. Prevention
5. Improvements
6. Thanks
7. Questions

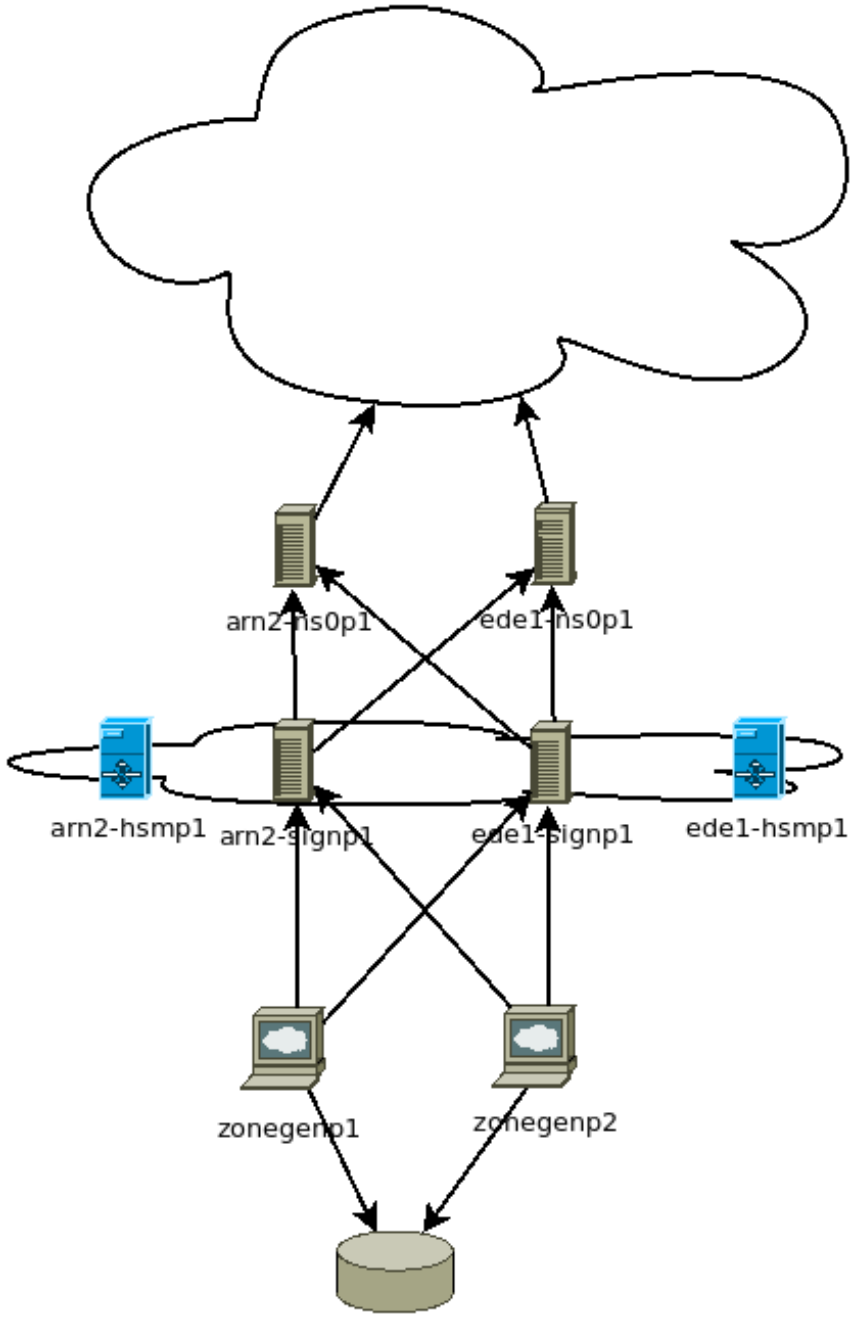
Why this talk

- HSM replacement with online KSK
- “What if…” scenarios
- Backups
- … or not

Photo by cottonbro from Pexels

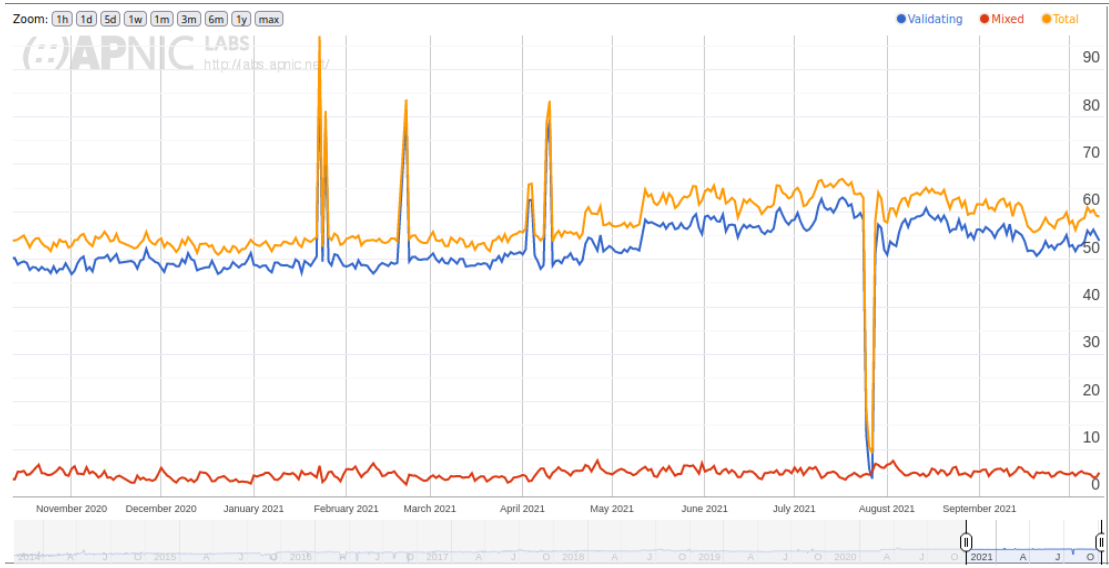
Setup

- 2 datacenters
- 1 active, 1 standby signer (hardware)
- 2 HSM's (HA, LB, networked)



Impact of lost keys

- Loss of service (no updates in the zone)
- Domains will fail when RRSIG expires
- New ZSK = DNSSEC signed zones unavailable for TTL DNSKEY+RRSIG
- ~60% validating resolvers in NL[1]



1 https://stats.labs.apnic.net/dnssec/NL

Prevention

- ~~Removing DS from parent~~
- Backups
- Fitting procedure

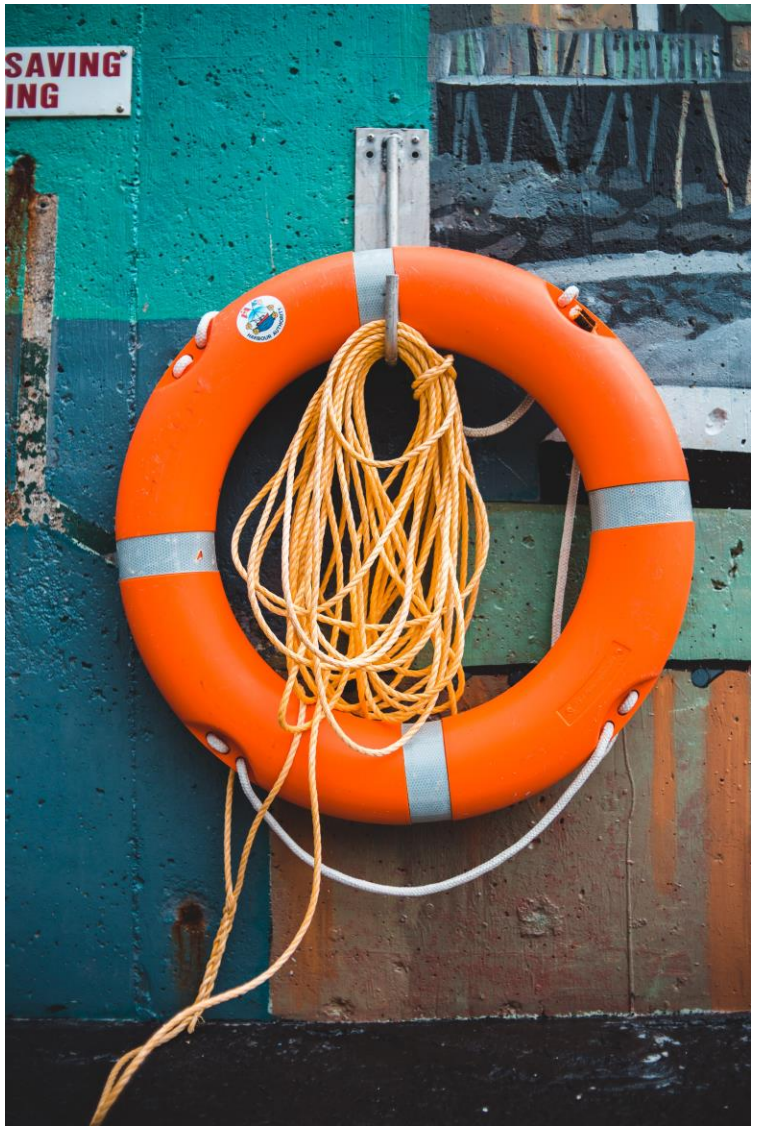


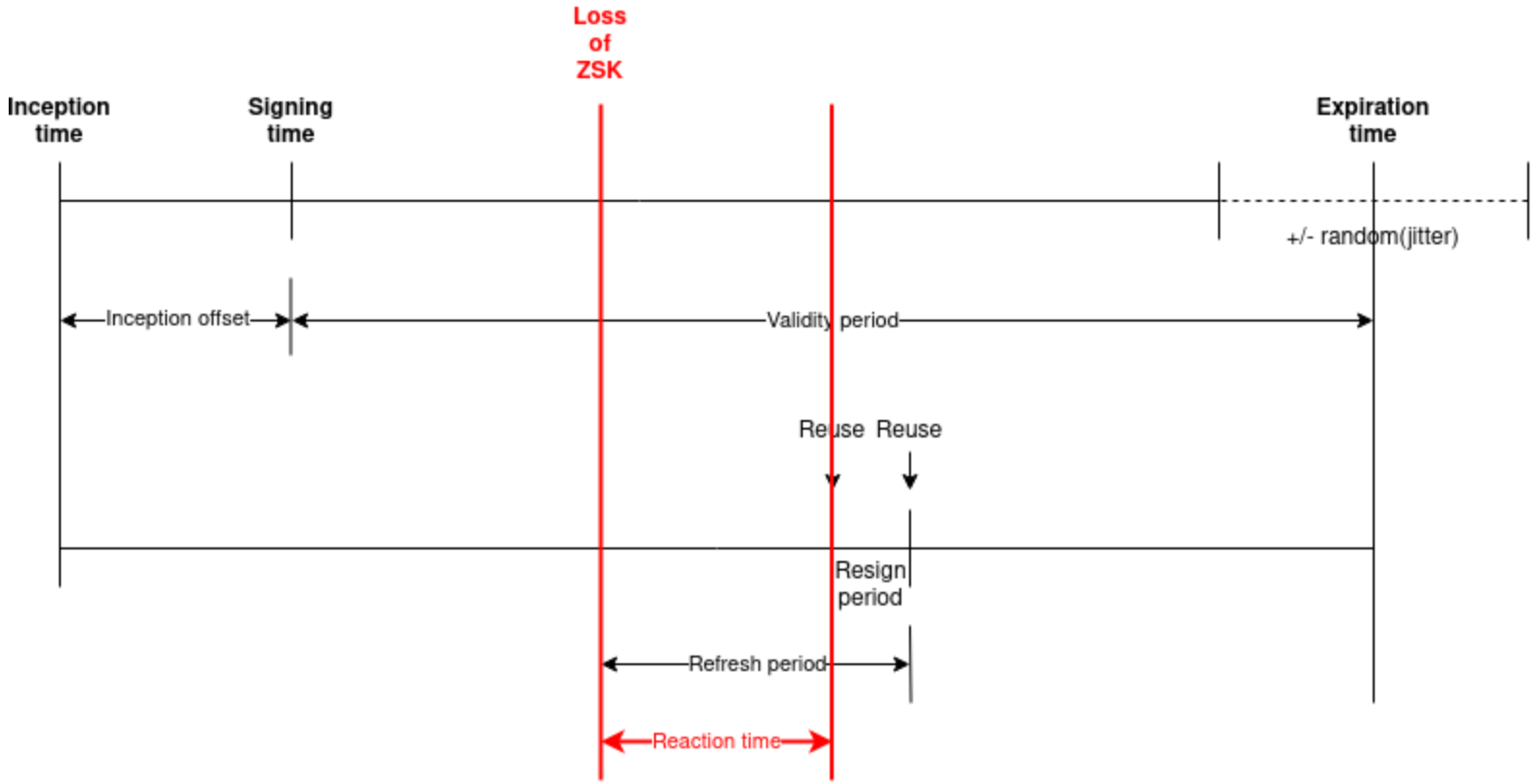
Photo by cottonbro from Pexels

Improvements

- RequireBackup setting for OpenDNSSEC
- AutomaticKeyGenerationPeriod with a good value
- Scheduled tickets for backup
- Longer Refresh time
- Shorter Resign time
- Time to react = Refresh - Resign

Photo by cottonbro from Pexels

Impact of lost keys



Thanks

- Berry van Halderen

- SIDN Colleagues

Are there any questions?

Follow us

SIDN.nl

@SIDN

SIDN

Thank you for your attention!