OpenDNSSEC & CreDNS

Plans & Roadmap 2019–2020

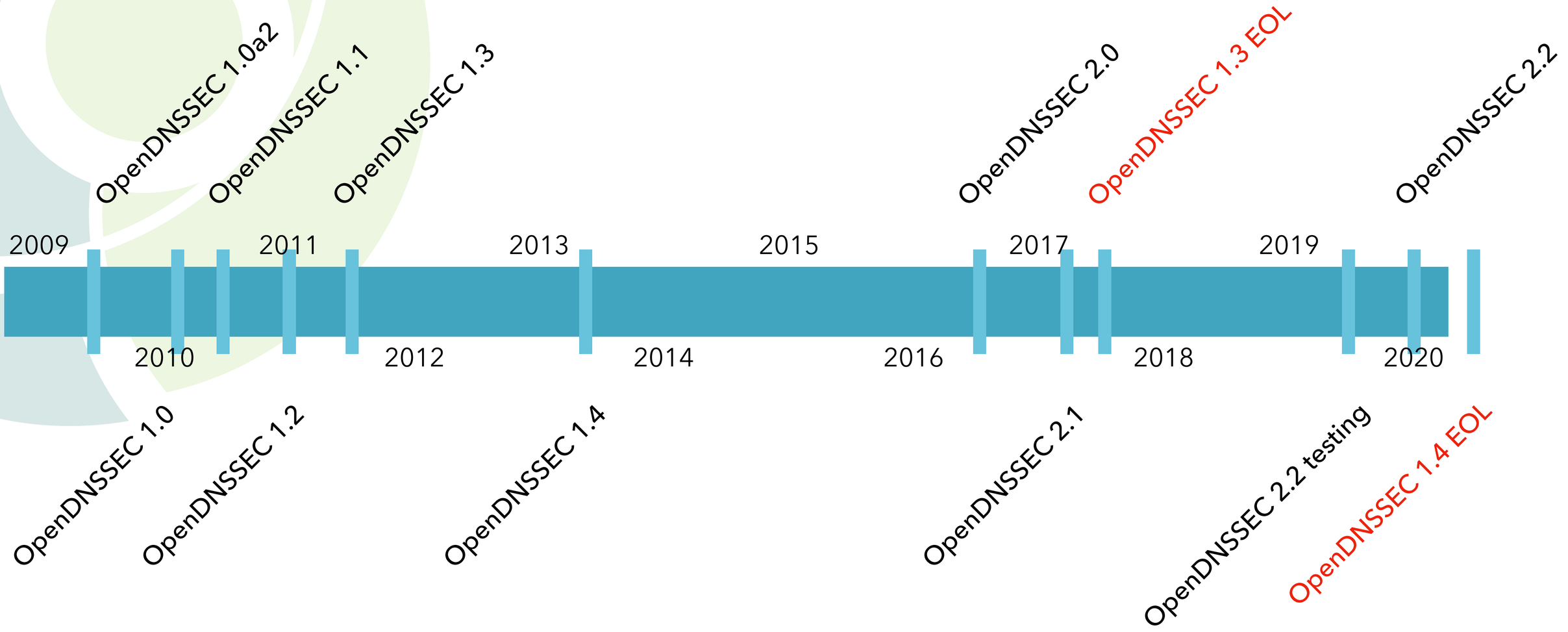
13 October 2019, Rotterdam

NLNETLABS

OpenDNSSEC: Status & Roadmap

NLNETLABS

OpenDNSSEC 2009–2019 Timeline



OpenDNSSEC 1.4 → 2.1

- OpenDNSSEC 1.4
  - rigid
    - key rollover continues although going bogus
    - no emergency rollover
- OpenDNSSEC 2.1
  - redesign of Enforcer component
    - no procedural rollover, but goal-driven towards desired state
    - see paper “Flexible and Robust Key Rollover in DNSSEC”, *Proceedings of SATIN*, March 2012

OpenDNSSEC 2.1 Key Features

- Redesign Enforcer component
  - performance
  - support for multiple key rollover mechanisms
  - support for algorithm rollover
  - support for CSK—combined signing key
  - support for unsigned zones (real bump in the wire)
- Additional cryptography algorithms
  - ECDSA P-256, P-384

OpenDNSSEC 2.2

- Fast updates in OpenDNSSEC
  - redesign of Signer component
  - already concurrent signing of multiple zones, but … signing of a zone is sequential
  - aim to improve responsiveness of the signer when new zone data is offered
  - proper handling inbound/outbound IXFRs, with IXFR history storage
- web-based ReSTful interface
- Blog post with OpenDNSSEC 2.2 details
  - https://www.nlnetlabs.nl/news/2019/Jul/30/progressing-opendnssec/

OpenDNSSEC 2.2.x

- Other features on roadmap of ODS 2.2.x
  - offline KSK/key set signing and (stand-by) key pools
  - CDS/CDNSKEY
  - monitoring, ease of use, reporting
  - …

High-Availability in OpenDNSSEC

- In 2020 start to work on high-availability in OpenDNSSEC
- High-availability scenarios
  - signing already resilient to outages
    - requires manual intervention
  - step 1: automated switchover to hot standby
    - host outage, not network outage
    - signer instances are completely independent

High-Availability in OpenDNSSEC (2)

- High-availability scenarios continued
  - step 2: active-active setup
    - multiple operational ODS signing instances
    - producing identical signed output
    - no switch-over needed, no state transfer between signers needed
    - subminute synchronisation between signers (zone update input and signature resign)

OpenDNSSEC Sneak Peek

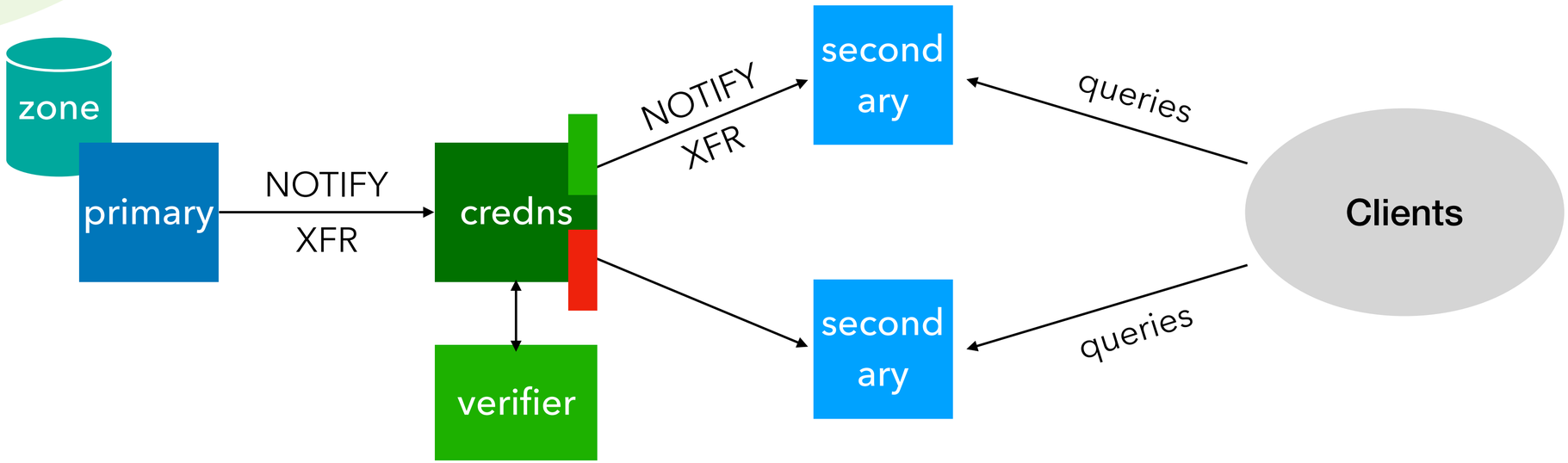
- Three modes of OpenDNSSEC operation
  - stand-alone ODS signer
  - ODS signer with specified/procedural zone signing key rollover
  - OSD signer with automated key management (Enforcer)

CreDNS Zone Verification: Project Plan

NLNETLABS

CreDNS Retrospective

- CreDNS zone verification, released in 2012
  - proxy server between signing server and publication of DNSSEC signed zone
  - prevent publication of bogus zones



CreDNS until 2019

- Latest official release CreDNS is based on NSD 3.2.12
  - maintained unofficial CreDNS up to NSD 3.2.22
- CreDNS positioned as a separate product
  - shared code base, but different release cycles
  - CreDNS and NSD 4 diverged
- CreDNS AXFR/IXFR in, **AXFR out**
  - full zone verification using, e.g., ldns-verify-zone or validns

CreDNS from 2019

- CreDNS as a module of NSD 4
  - integral part of NSD 4 releases
  - can be run in conjunction with NSD 4 (part of XFR daemon), or
  - can be configured as proxy/bump-in-the-wire
- Current limitations
  - IXFR in, AXFR out
  - full zone verification

CreDNS from 2019 (cont'd)

- Roadmap plans for late 2019, early 2020
  - NSD 4 IXFR-out
  - CreDNS incremental zone verification
    - best effort *vs* strict
- CreDNS live-validation tool, phase 1
  - IXFR-in, IXFR-out
  - best effort incremental zone verification w/ resolver (Unbound, BIND, Knot Resolver, PowerDNS Recursor)
- CreDNS live-validation tool, phase 2 (optional)
  - strict incremental zone verification and signature expiration signalling

Wrapping Up

NLNETLABS

Concluding

- OpenDNSSEC
  - ODS 1.4 to 2.1 migration: please contact us
  - ODS 2.2 testing in operational environment: please contact us
  - ODS high-availability: please contact us
- CreDNS
  - interested, use-cases, and/or requirements: please contact us
- By the by
  - SoftHSM v2: please contact us

contact email:
labs@NLnetLabs.nl