



OpenDNSSEC

1.3

Matthijs Mekking
NLnet Labs



Little bit of history repeating

- Open-source turn-key solution for DNSSEC
- Version 1.0.0 'Proof of concept' (Feb 2010)
 - Critics: Dependency hell, Performance suboptimal
- Version 1.1.0 (May 2010)
 - Performance optimization for 1.0.0
- Version 1.2.0 (January 2011)
 - Remove Python related dependencies
 - Slightly faster than 1.1.0

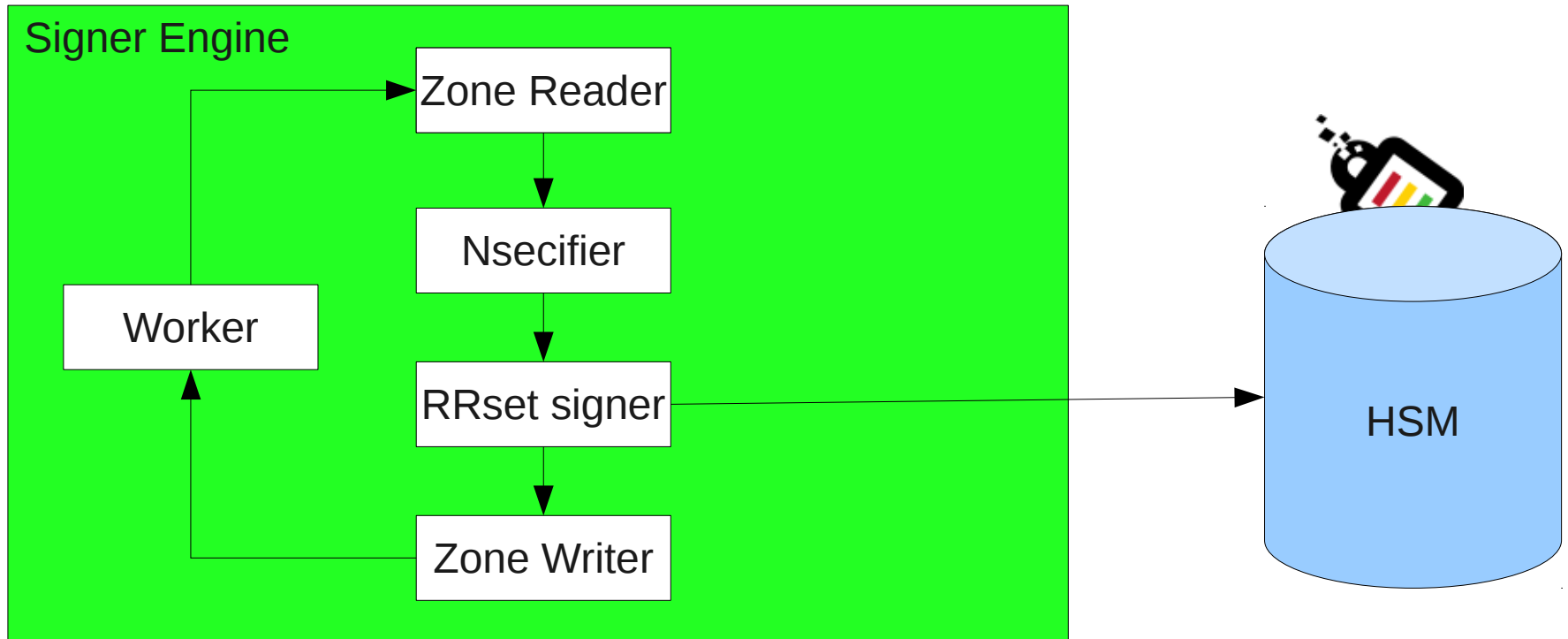


What's cooking?

- Version 1.3.0 (April 2011?)
 - Threaded signer

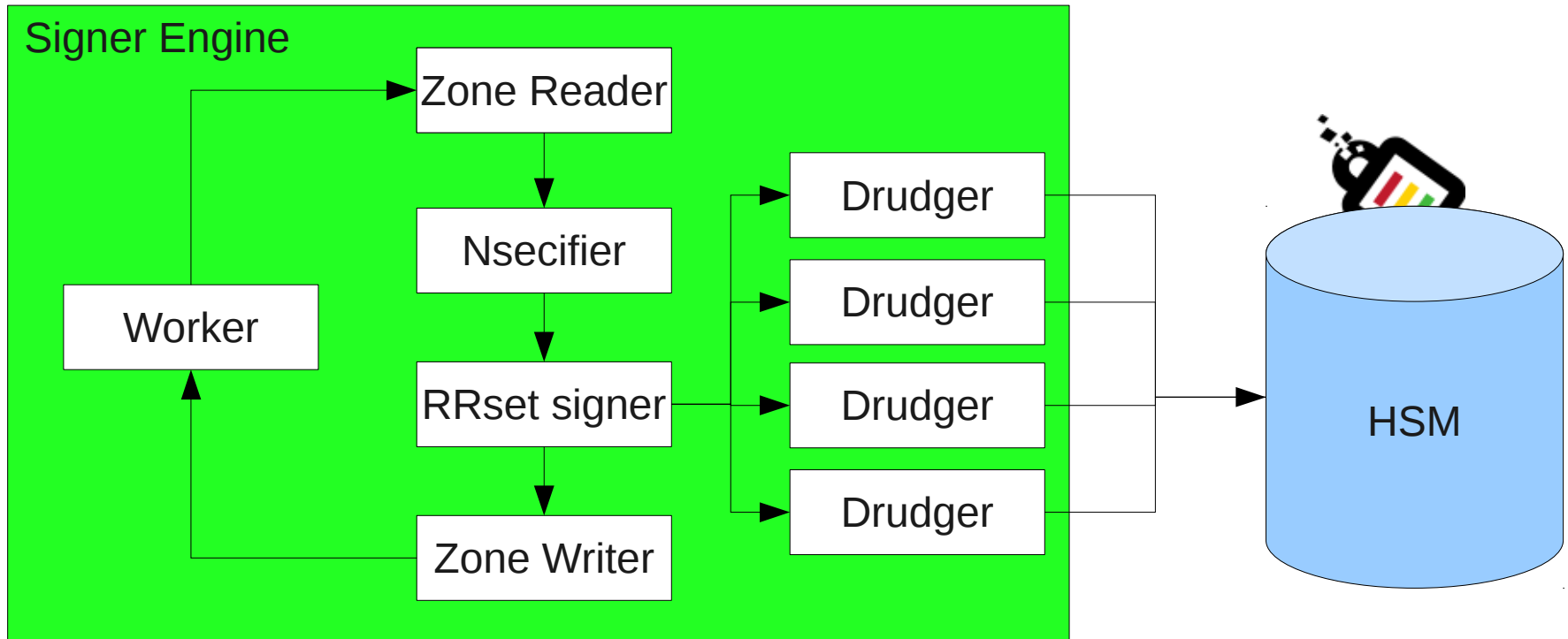


Signer 1.2.X





Signer 1.3.X





Meep, Meep!

- SCA6000 HSM
 - “Up to 13,000 RSA operations per second”
- OpenDNSSEC 1.2.X Performance
 - ~2100 RRSIG / second
- OpenDNSSEC 1.3.X Performance
 - 13552 RRSIG / second





All optimizations

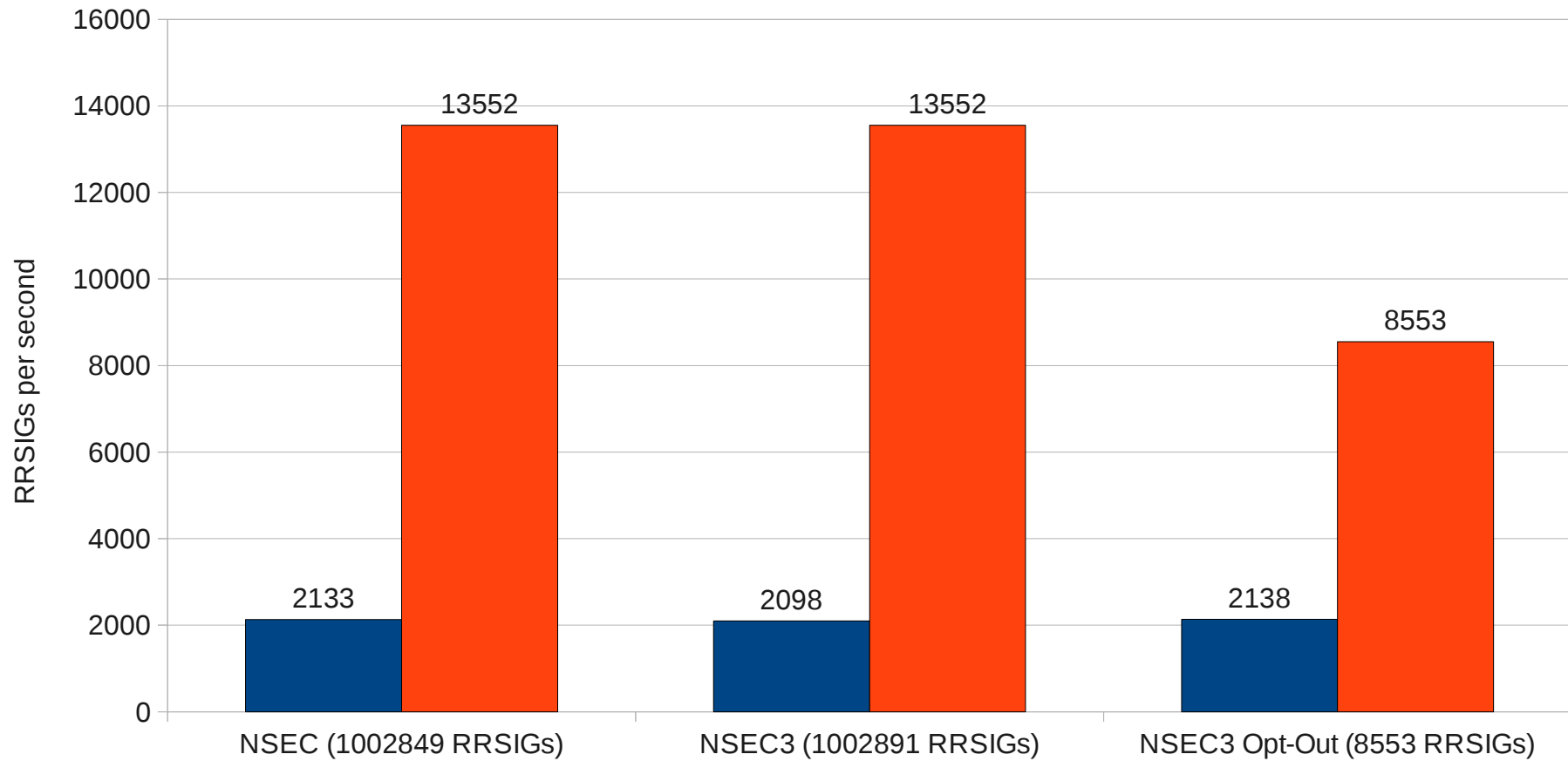
- Threaded signer
- Optimized signer core
 - Clever log level checking
 - Temperate SOA SERIAL maintenance
 - Temperate NSEC/NSEC3 maintenance
- Reasonable backup strategy



RRSIGs per second

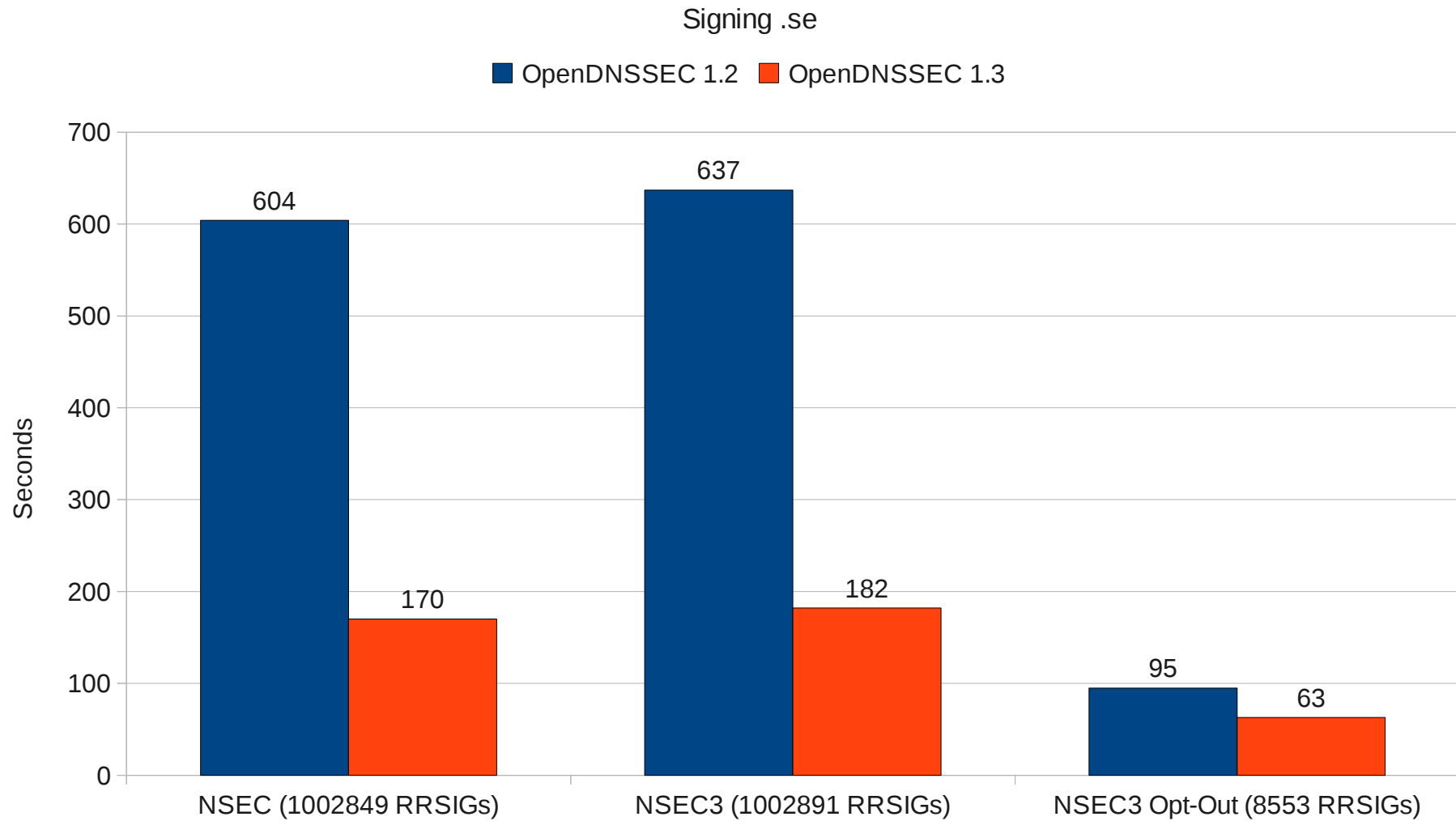
Signing .se

■ OpenDNSSEC 1.2 ■ OpenDNSSEC 1.3



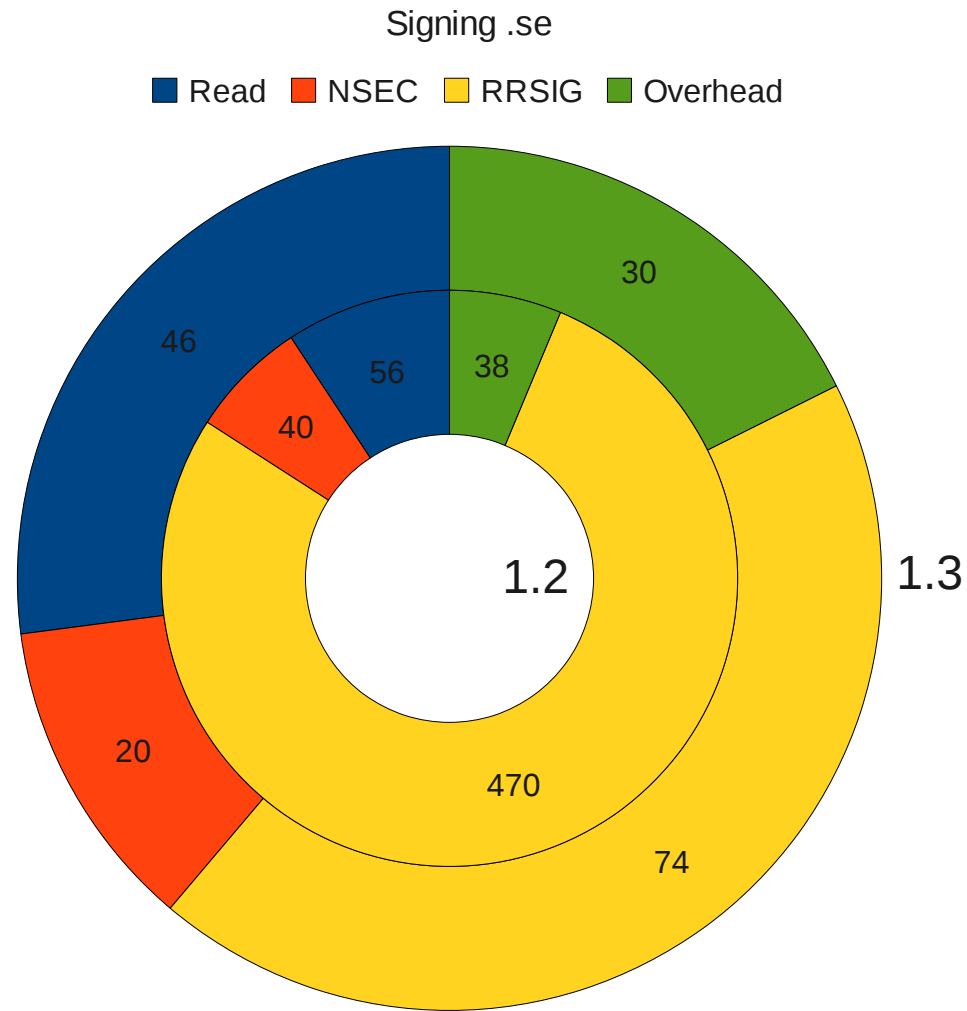


Full zone sign



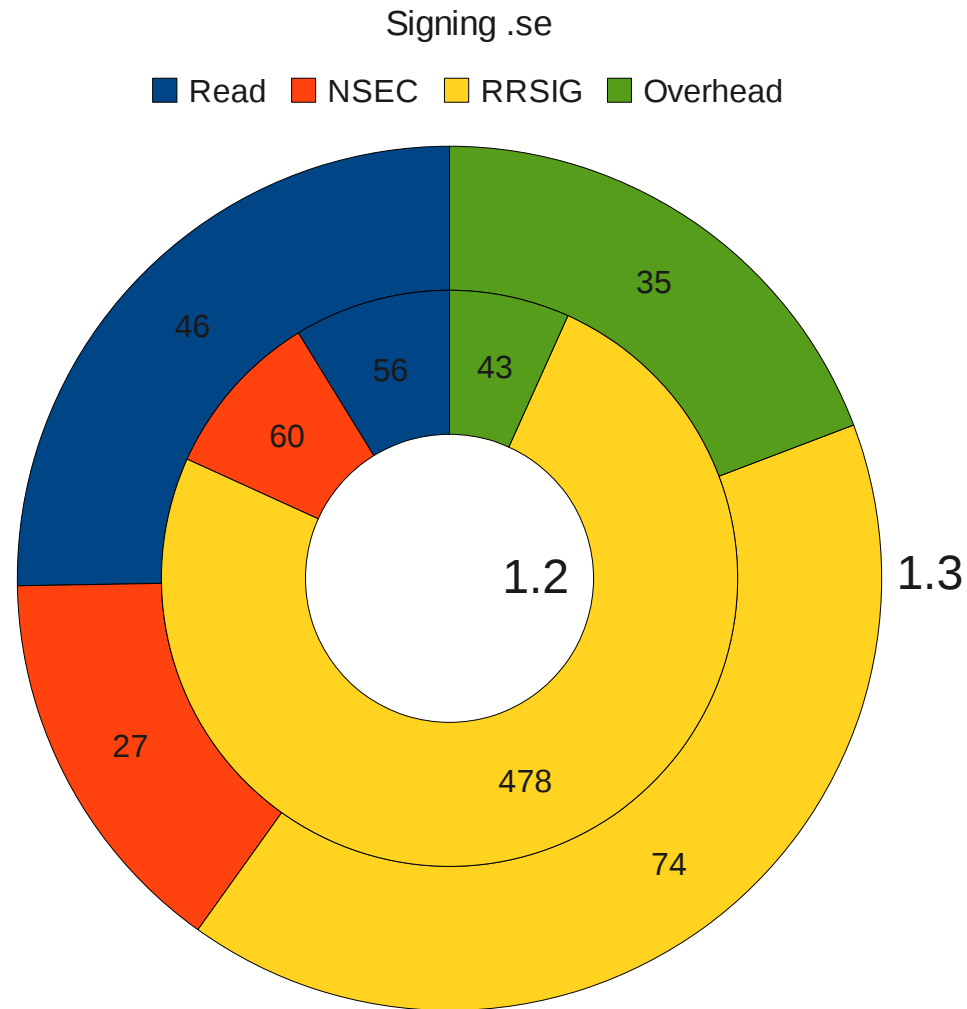


1.2 vs 1.3: NSEC



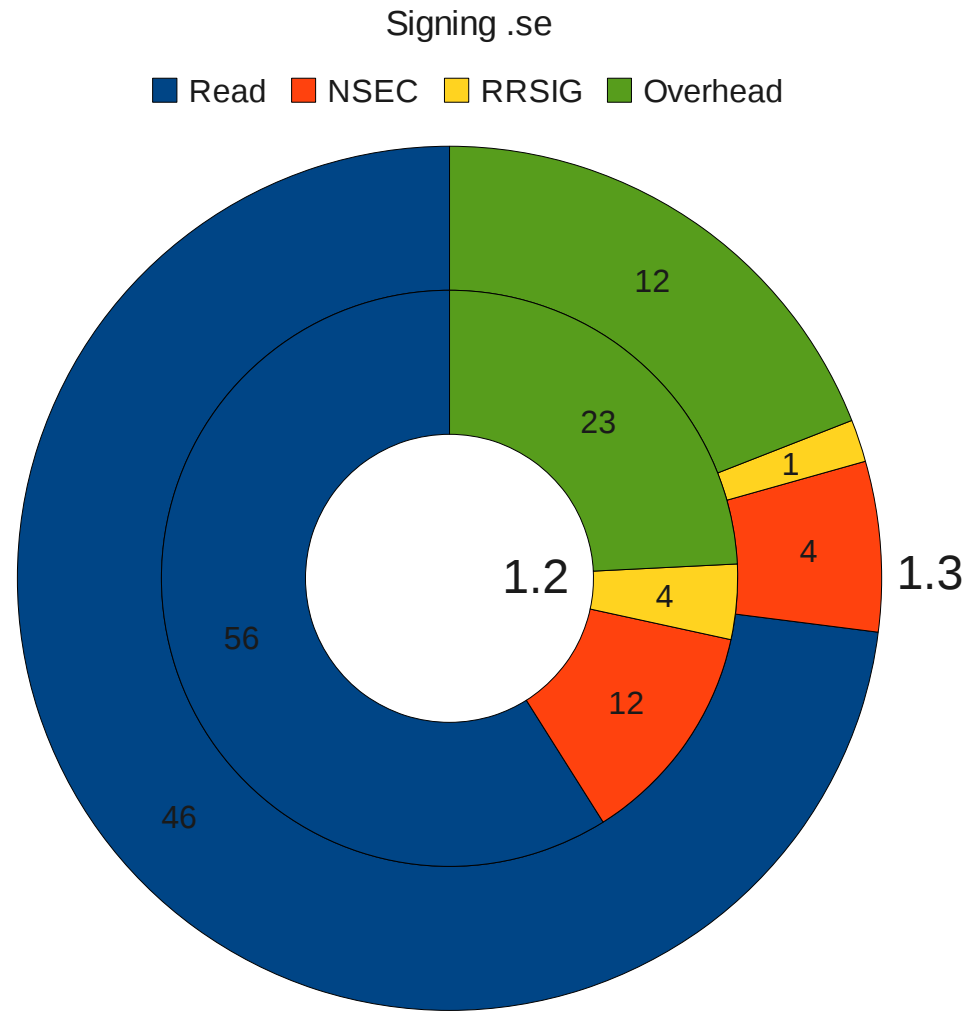


1.2 vs 1.3: NSEC3





1.2 vs 1.3: NSEC3 Opt-Out





Who?

.se

kirei

nominet

sinodun



NLnet
Labs





For more info

- <http://www.opendnssec.org>
- SoftHSM 
 - <http://www.softsm.org>