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 Engine

- Zone Reader
- Nsecifier
- RRset signer
- Zone Writer

Worker

HSM
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

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of RRSIGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSEC (1002849 RRSIGs)</td>
<td>2133</td>
</tr>
<tr>
<td>NSEC3 (1002891 RRSIGs)</td>
<td>2098</td>
</tr>
<tr>
<td>NSEC3 Opt-Out (8553 RRSIGs)</td>
<td>2138</td>
</tr>
<tr>
<td></td>
<td>8553</td>
</tr>
</tbody>
</table>
Full zone sign

Signing .se

<table>
<thead>
<tr>
<th>Method</th>
<th>NSEC (1002849 RRSIGs)</th>
<th>NSEC3 (1002891 RRSIGs)</th>
<th>NSEC3 Opt-Out (8553 RRSIGs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenDNSSEC 1.2</td>
<td>604</td>
<td>637</td>
<td>95</td>
</tr>
<tr>
<td>OpenDNSSEC 1.3</td>
<td>170</td>
<td>182</td>
<td>63</td>
</tr>
</tbody>
</table>

26 Mar 2011  IEPG80, Prague
1.2 vs 1.3: NSEC

26 Mar 2011 IEPG80, Prague
1.2 vs 1.3: NSEC3

Signing .se
- Read
- NSEC
- RRSIG
- Overhead

26 Mar 2011
IEPG80, Prague
1.2 vs 1.3: NSEC3 Opt-Out

Signing .se

- Read
- NSEC
- RRSIG
- Overhead

26 Mar 2011
IEPG80, Prague
For more info

- [http://www.opendnssec.org](http://www.opendnssec.org)
- [SoftHSM](http://www.softhsm.org)