OpenDNSSEC

DNS Working Group @ RIPE 66

Sara Dickinson - sara@opendnssec.org
What is OpenDNSSEC?
OpenDNSSEC

- Turn-key solution for DNSSEC
- Automates zone & key management
- RFC compliant
- Open Source Software – BSD License
Key Features

- **Flexible**: policy driven (KASP)
- **Scalable**
  - many zones, many records
  - key sharing between zones
- **Secure**: PKCS#11 support
- **SoftHSM**
Organisation

OpenDNSSEC

Contributors
- Joe Abley (ICANN)
- Olaf Kolkman (NLNetLabs)
- Jacques Latour (CIRA)
- Sion Lloyd (Nominet)
- Roland van Rijswijk (SURFnet)
- Jakob Schlyter (Kirei)
- Ondřej Surý (CZ.NIC)
- Patrik Wallström (.SE) (corporate liaison)

Architecture Board
- Non-profit company
- Secure Funding for future development
- Long term software support
- Training classes
- Consultancy

Design & Architecture
Software Development
System Testing
Support and Maintenance

Project Team 🎉
Current status
OpenDNSSEC releases

- Stable releases:
  - 1.3.14 (1.3 is a Long Term Support Release)
  - 1.4.0 (Standard Release - April 2013)

- Development release:
  - 2.0 ("enforcer-ng" - Alpha available)
OpenDNSSEC 1.4

• Re-factor of signer: input & output adaptors
  • Zone file
  • AXFR/IXFR [NEW!]
    - [NOTE: changes to configuration files]

• No integrated auditor [No ruby!]
  - Use e.g. validns through credns to verify the zone after signing
OpenDNSSEC 1.4

Architecture

1.3

Signed zone

Security Module

KASP Auditor

KASP Enforcer

UnSigned zone

Signer Engine

1.4

Input Adapter

UnSigned zone

Key and Signing Policy

Signed zone

Security Module

Signer Engine

KASP enforcer

Output Adapter

Key and Signing Policy
OpenDNSSEC 1.4

- PIN storage facility. No longer have to have HSM PIN in clear text in conf.xml

- Number of enhancements to ‘ods-ksmutil’
  - more information in ‘key list’, ‘rollover list’, ‘key generate’
  - CKA_ID can be included in DSSSubmit
  - one step key backup deprecated

- Script to enable migration between SQLite and MySQL backend (recommend MySQL for production)
SoftHSM

- Stable release
  - 1.3.4 (LTS)

- Development release: 2.0
  - "Plug-able" crypto libraries (Botan & OpenSSL)
  - Improved security
  - Beta release planned in next month or two
Other news

• Versioning will reflect API changes rather than component changes

• Using jenkins for regression testing:
  - https://jenkins.opendnssec.org/

• Continuing to add to online documentation
  - https://wiki.opendnssec.org/display/DOCS
  - Quick guides & user contributions
  - Usability
## Build Queue
No builds in the queue.

<table>
<thead>
<tr>
<th>#</th>
<th>Status</th>
<th>Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Idle</td>
<td></td>
</tr>
</tbody>
</table>

## Build Executor Status

### Latest builds

<table>
<thead>
<tr>
<th>Job</th>
<th>Build</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-daily-opendnssec-1.3-mysql</td>
<td>#19</td>
<td>May 15, 2013 5:01:20 AM</td>
</tr>
<tr>
<td>test-daily-opendnssec-1.3</td>
<td>#115</td>
<td>May 15, 2013 5:01:20 AM</td>
</tr>
<tr>
<td>test-daily-opendnssec-1.3-mysql</td>
<td>#116</td>
<td>May 15, 2013 5:01:20 AM</td>
</tr>
<tr>
<td>test-daily-opendnssec-1.4</td>
<td>#19</td>
<td>May 15, 2013 5:01:20 AM</td>
</tr>
<tr>
<td>test-daily-opendnssec-trunk-mysql</td>
<td>#190</td>
<td>May 15, 2013 4:01:20 AM</td>
</tr>
<tr>
<td>test-daily-opendnssec-trunk</td>
<td>#204</td>
<td>May 15, 2013 4:01:20 AM</td>
</tr>
<tr>
<td>test-daily-opendnssec-1.3</td>
<td>#114</td>
<td>May 14, 2013 5:01:20 AM</td>
</tr>
</tbody>
</table>
OpenDNSSEC Documentation Home

Welcome

About

The OpenDNSSEC documentation gives information on how to install, configure, and run OpenDNSSEC. There might still remain some questions, so we try to reflect them in our a growing list of frequently asked questions.

Remember that you also need an HSM, which uses the PKCS#11 interface. We do provide the SoftHSM, a software-only implementation of an HSM. Read the HSM Buyer's Guide for more information and consult the list of HSM vendors.

The latest version of OpenDNSSEC is 1.4

See what is new in 1.4 - note that due to changes in the database schema a migration is required when upgrading to 1.4 from earlier versions of OpenDNSSEC.

Scope

The goal of OpenDNSSEC is to have a complete DNSSEC zone signing system which maintains stability and security of signed domains. DNSSEC adds many cryptographic concerns to DNS; OpenDNSSEC automates those to allow current DNS administrators to adopt DNSSEC. This document provides DNS administrators with the necessary information to get the system up and running with a basic configuration.
Roadmap
OpenDNSSEC 2.0

‘enforcer-ng’

• Refactoring the ‘enforcer’: Performance

Preliminary results: for illustration purposes only!

Enforcer performance - trivial case

Number of zones

0 1250 2500 3750 5000

time (s)

0 20 40 60 80

1.3 enforcer-ng
OpenDNSSEC 2.0

• Refactoring the ‘enforcer’: Functionality

  • Support for multiple key rollover mechanisms
  • Support for algorithm rollover
  • Support for CSK – Combined Signing Key
  • Support for unsigned zones
Beyond 2.0...

- More adapters:
  - Dynamic updates
  - Database input/output
- Common API for system integration
- Offline keys…
• Find us:
  • Web: www.opendnssec.org
  • Facebook: https://www.facebook.com/OpenDNSSEC
  • Twitter: https://twitter.com/opendnssec
  • In the bar (Bellini’s): 6pm tonight

Meet the OpenDNSSEC team!
OpenDNSSEC

- Find us:
  - Web: www.opendnssec.org
  - Facebook: https://www.facebook.com/OpenDNSSEC
  - Twitter: https://twitter.com/opendnssec
  - In the bar (Bellini’s): 6pm tonight

Meet the OpenDNSSEC team!

Will sign zones for beer

Wednesday, 15 May 13