OpenDNSSEC

Matthijs Mekking
NLnet Labs
DNSSEC

• Adds security to the DNS
  • Data origin authentication
  • Data integrity
• Public key cryptography
• RFC 4033 4034 4035
• Hierarchal system
2010

• The root is signed

• On new years eve 2010, 65 tld's were signed:
  
  • .ag .arpa .asia .be .bg .biz .br .bz .cat .ch .cl .cz .dk .edu .eu .fi .fr .gi .gov .gr .hn .in .info .jp .kg .la .lc .li .lk .me .mn .museum .my .na .net .nl .nu .org .pm .pr .pt .re .sc .se .tf .th .tm .uk .us .vc .wf a bunch of .xn--* zones and .yt

• More to come in 2011
What?

- Open-source turn-key solution for DNSSEC with a BSD license
- OpenDNSSEC is a zone signer that automates the process of managing DNSSEC keys and the re-signing of zones
- Bump-in-the-wire, simply to integrate into existing infrastructure
- Key storage and access through PKCS#11 API
Why?

- DNSSEC should be easy to deploy
  - OpenDNSSEC simplifies the process of signing zones, reducing the work load on the operator
- The available DNSSEC tools were lacking
  - Good key management
  - Policy handling
  - Hardware acceleration
How?

- Key management
  - DNSSEC Policy
  - HSM
  - Written in c
- Zone management
  - Signing parameters
  - Zone content
  - Half c, half Python
- Auditor
  - Audits the enforcer and signer
  - Written in Ruby
When?

- 1.0.0 was released February 2010
  - Latest release 1.1.3 in September
- This month 1.2.0 will be released (currently rc3)
  - Drops python as a dependency, new signer engine written in c
  - Lots of improvements on the KASP enforcer
New Years Resolutions

- Improve performance
  - Threaded signer, large number of zones
- More rollover scenarios
  - Algorithm rollover, Single Type Signing Scheme, Incremental transition between NSEC and NSEC3
- Other zone input and output formats (than file)
  - AXFR, IXFR, Database, Dynamic Update
- Web Interface
Who?

.se  kirei

nominet  sinodun

SIDN  NLnet Labs  SURFNET
Who else?

- Known TLD users:
  - SIDN (.nl)
  - IIS (.se)
  - Nominet UK (.uk)
  - FICORA (.fi)
  - DK Hostmaster (.dk)
  - AFNIC (.fr, .pm, .re, .tf, .wf, .yt)

- Other known users:
  - CAcert, ICANN, SURFnet, YASK (Registrar), Compricer AB (Hoster)
Want more?

- **http://www.opendnssec.org**

- **SoftHSM**
  - A Software Security Module, PKCS#11
  - Written in C++, uses Botan for cryptography
  - Cheaper than a HSM, or testing environments
  - **http://www.softhsm.org**