OpenDNSSEC Status Update

Matthijs Mekking

RIPE 60, Prague

What is OpenDNSSEC?

- OpenDNSSEC is a zone signer that automates the process of keeping track of DNSSEC keys and the signing of zones.

Authors

NLnet Labs

nominet

.se

kirei

sinodun

SIDN

SURF NET

SoftHSM

- Software implementation of a cryptographic store accessible through a PKCS#11 interface
- Can be used as an OpenDNSSEC keystore instead of a “real” HSM

Status update

- Technology Preview July 2009
- 1.0.0 Release February 2010
  - Prototype release. File based, including a zone fetcher
- In production use (se, uk, ICANN)
- SoftHSM steadily improving (1.1.4)

OpenDNSSEC 1.1 rc2

- Speed optimizations in zone sorting and 'nsec3ing'
- Partial Auditor (useful for large zones, dnsruby-1.46)
- EPP client (experimental)

Future

- Future version will include
  - Increased performance for large zones
  - Increased performance for many zones
  - Improved key sharing between zones
  - Continuous signing with IXFR input/output

OpenDNSSEC 1.2

- Improved key sharing between zones
- Improved performance for many zones
- Remove Python dependency

OpenDNSSEC 2.0

- Continuous signing with IXFR input/output (IXFR Adapter)
- Dynamic Update Adapter
- Database Adapter
- User Interface

SoftHSM 2.0

- Focus on enhanced security:
- Improve scalability number of keys
- Support for other crypto libraries, such as OpenSSL
- Support for GOST, 'Zerorize' memory, ...

www.opendnssec.org