OpenDNSSEC

DNS Working Group @ RIPE'62

Jakob Schlyter – jakob@kirei.se

What is OpenDNSSEC?

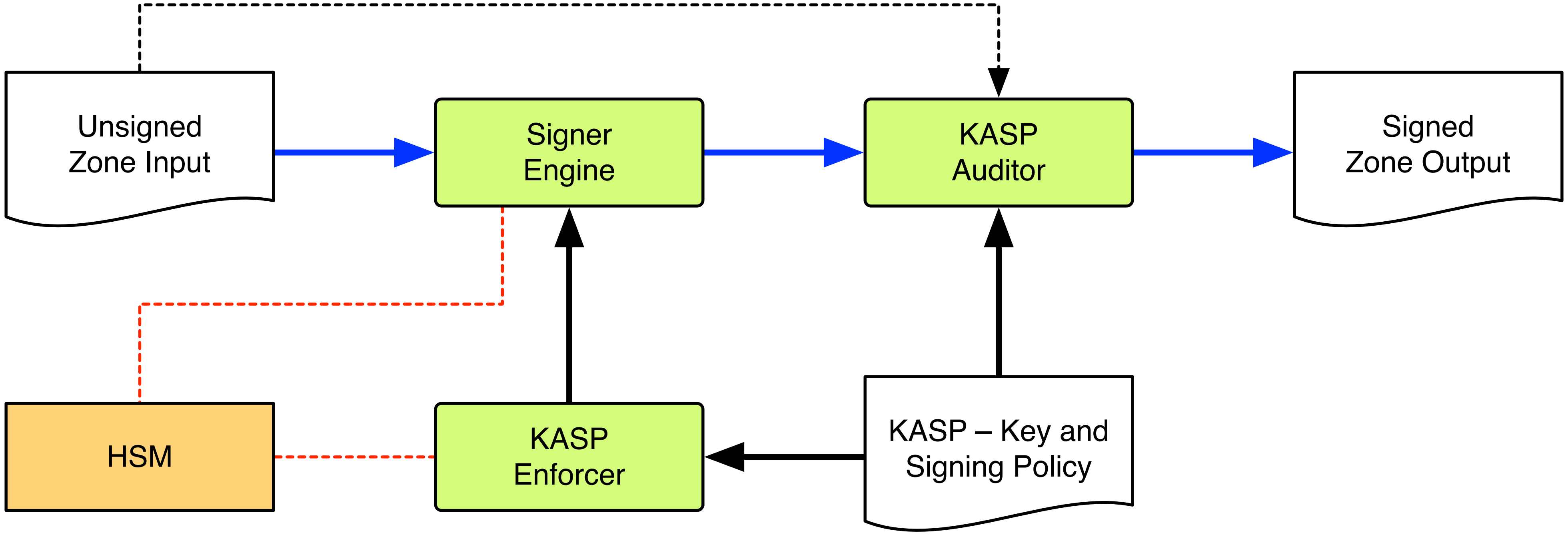
OpenDNSSEC

- Turn-key solution for DNSSEC
- Signer only – no name server included
- Open Source Software – BSD License

Key Features

- Policy driver configuration using KASP
- Out of the box support for PKCS#11
    - No dependencies on OpenSSL
- Key sharing between zones
- Scales to ≥ 50,000 zones

Architecture



Authors

NLnet Labs

nominet

.se

kirei

sinodun

SIDN

SURF NET

Organization

OpenDNSSEC AB (svb)

- Non-profit company
- Long-term support for OpenDNSSEC
  - Secure funding for future development
  - Software support
  - Training classes
  - Consulting services for system integration

OpenDNSSEC AB (svb)

- Owners (formation in process)
  - CIRA
  - Nominet
  - .SE
  - SIDN

Architecture Board

- Jakob Schlyter – Kirei
- Joe Abley – ICANN
- Olaf Kolkman – NLNetLabs
- Ondřej Surý – CZ.NIC
- Patrik Wallström – .SE
- Roland van Rijswijk – SURFnet
- Siôn Llyod – Nominet

Backtrack & Roadmap

OpenDNSSEC 1.0

Released in February 2010

- First version
- Limited performance
- Python-based signer engine

OpenDNSSEC 1.1

Released in May 2010

- Increased performance
  - Faster sorting & signing
- MySQL KASP database backend
- EPP client plugins
- Partial zone auditing

OpenDNSSEC 1.2

Released in January 2011

- New signer engine
  - Written in C – bye bye Python
- Zones are maintained in memory
  - Faster, but with requires more memory
- Improved key sharing

OpenDNSSEC 1.3

Scheduled for May 2011

- Multi-threaded signer engine
  - Old signer engine did not scale for large zones
  - Results in increased performance on some HSMs, e.g., the Sun^H^H^HOracle SCA/6000

OpenDNSSEC 1.4

Scheduled for Q2 2011

- Input and output Adapters for
  - MySQL
  - AXFR
  - IXFR
- Better connection handling for HSMs

OpenDNSSEC 1.5

Scheduled for Q3 2011

- Refactoring the Enforcer
- Support for algorithm rollover
- Incremental transition between NSEC & NSEC3
- Performance improvements for larger number of zones

SoftHSM

- Software PKCS#11 Provider
  - Can be used as a OpenDNSSEC keystore instead of a “real” HSM
- Large speed improvements in trunk – not yet
- SoftHSM 2.0 in development

Education

- OpenDNSSEC courses scheduled for May, June, September, October & November.
    - See www.OpenDNSSEC.org for exact schedule
- Lab server templates for Amazon EC2 will be available for anyone to use.

Thanks to our users

- Top Level Domains
  - .dk .fi .fr .lu .nl .pm .re .se .re .tf .uk .wf .yt
- ICANN
- SURFnet

Network HSM Evaluation

- Review of Hardware Security Modules
  - AEP Keyper
  - Safenet Luna
  - Thales nShield
  - Ultimaco CryptoServer
- Full report at http://goo.gl/05rpM

www.opendnssec.org