OpenDNSSEC

Rickard Bellgrim, .SE
rickard.bellgrim@iis.se

What?

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

Why?

- The available DNSSEC tools were lacking:
  - Good key management
  - Policy handling
  - Hardware acceleration
  - Etc.
- DNSSEC should be easy to deploy
- Increase the number of DNSSEC users
- Experience from previous DNSSEC operations

Who?

NLnet Labs

nominet

.se

kirei

John A Dickinson

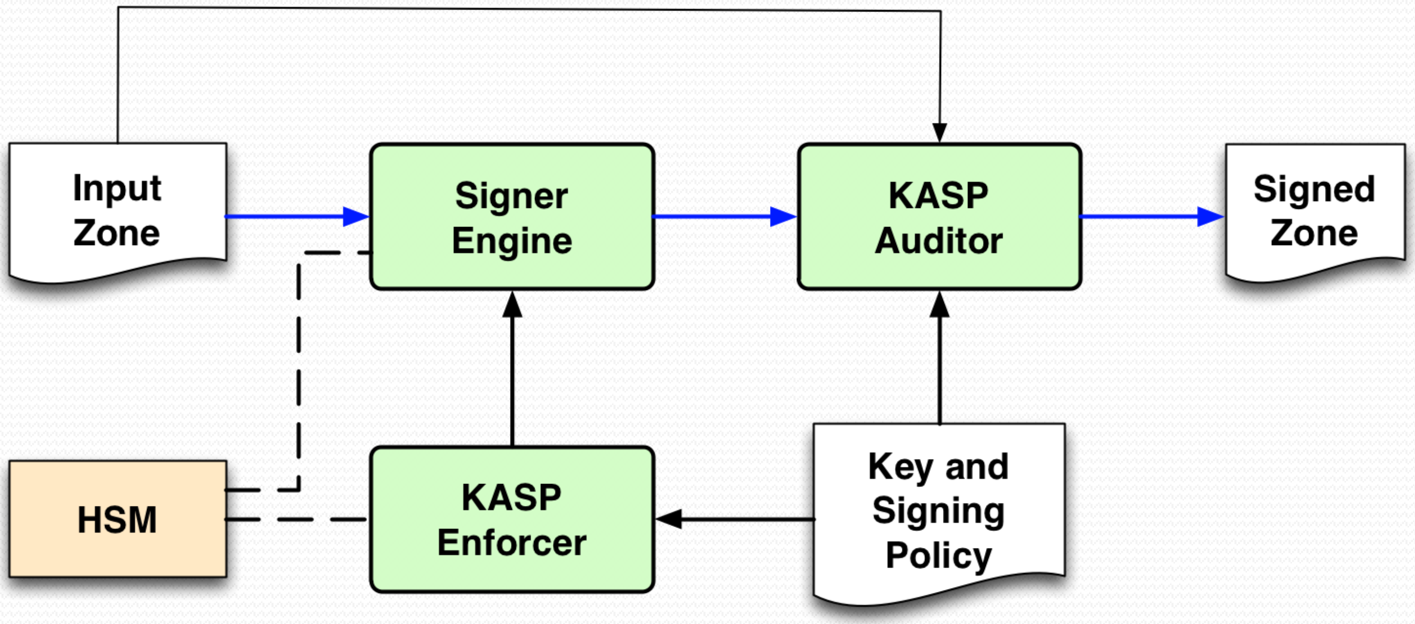
SIDN

SURF NET

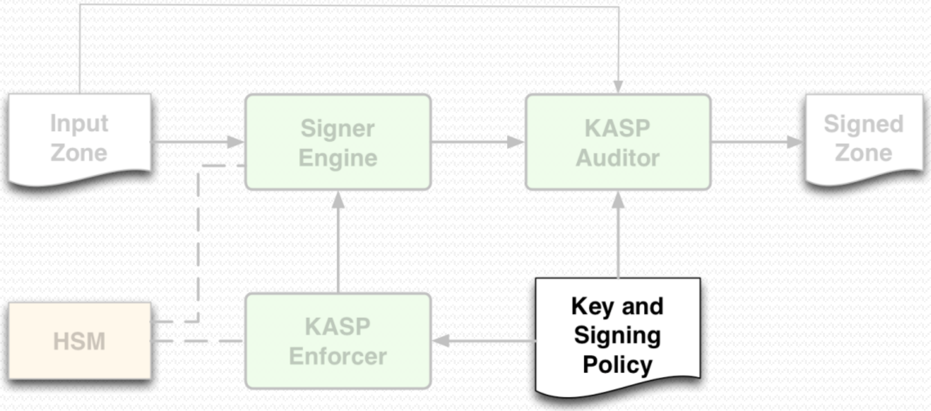
About OpenDNSSEC

- Simplifies the process of signing one or more zones
- Reducing the work load on the system administrator
- Open source software with a BSD license
- Simple to integrate into existing infrastructure
- Key storage and hardware acceleration using PKCS#11

Architecture

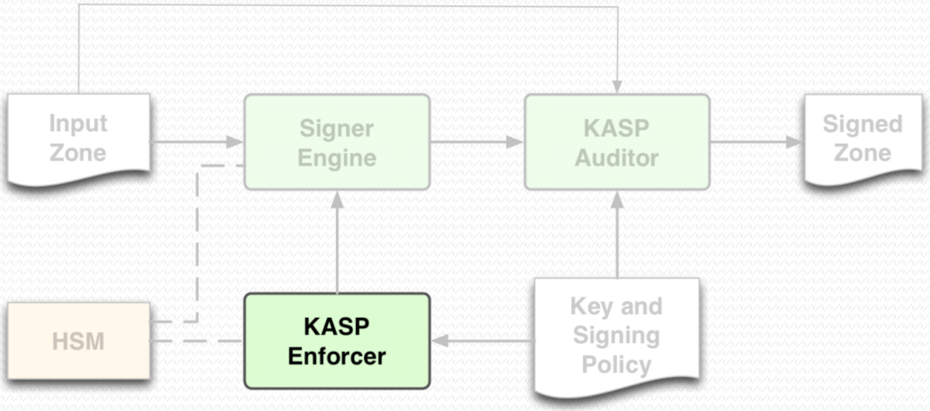


Key and Signing Policy



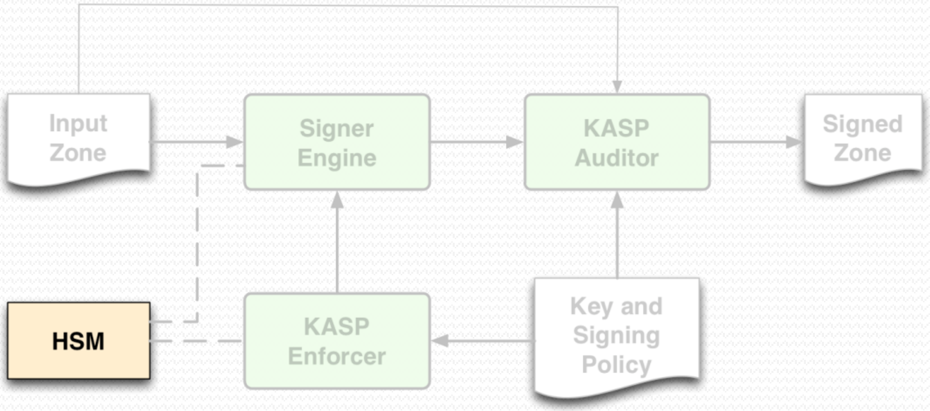
- The user creates one or more policies
- A default policy is also supplied
- The policy describes:
  - Key strengths and algorithm, key and signature lifetime, NSEC/NSEC3, etc.

KASP Enforcer



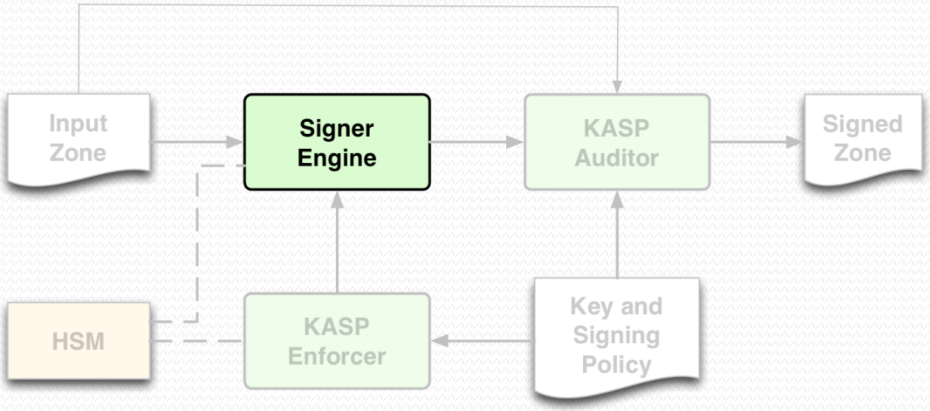
- Generate keys using one or more HSMs
- Maintains the zones according to the policies
    - Rolling keys
    - Setting TTLs, lifetimes, etc.

HSM



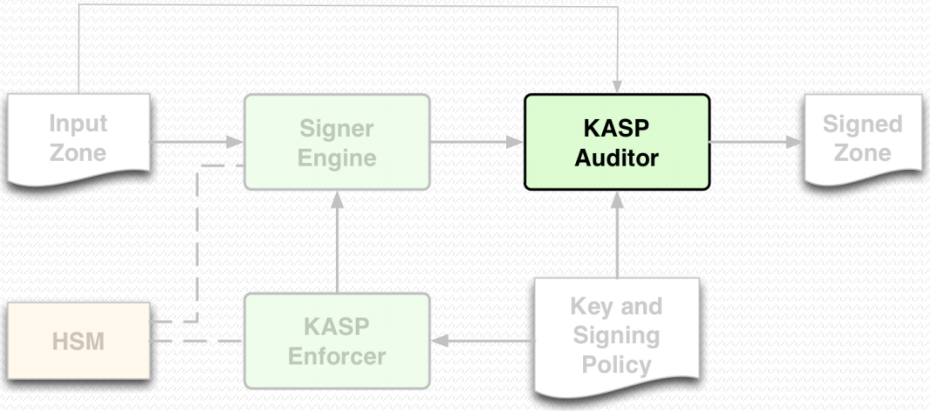
- Hardware Security Module
  - Stores the keys
  - Hardware acceleration to sign records
- Standard interface via PKCS#11 API
  - Abstracted within OpenDNSSEC into libhsm
- SoftHSM available with OpenDNSSEC
  - Software emulation of a generic HSM
  - When an HSM is not necessary or for use in a testbed

Signer Engine



- Automatic signing of the zones
    - Can reuse signatures that are not too old
    - Can spread signature expiration time over time (jitter)
- Maintains the NSEC/NSEC3 chain
- Updates SOA serial number

KASP Auditor



- Checks that the signer and enforcer work the way they are supposed to, e.g.
  - Non DNSSEC RRs are not added or removed
  - Policy is being followed
- Can stop the zone distribution if needed
- Written by a different person and in a different language (Ruby)

More about HSMs

Why should you use one?

- Security (FIPS)
    - The private keys are stored securely in the HSM
    - You know where your keys are
- Speed
    - 1 – 13,000 signatures per second

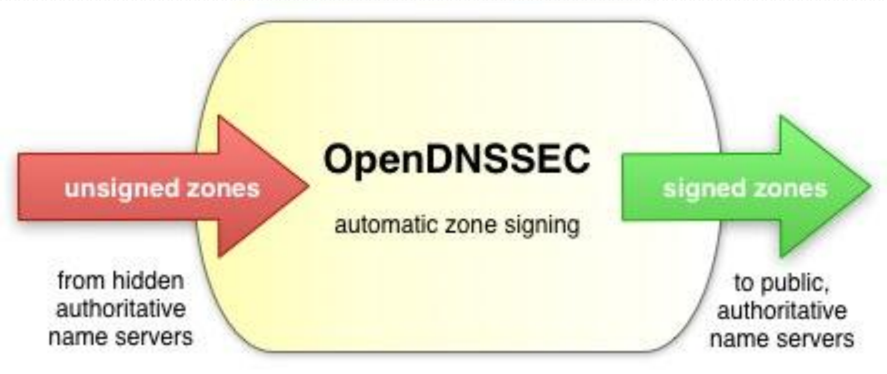
Are they expensive?

- $50 - $25,000

Remember to protect the host

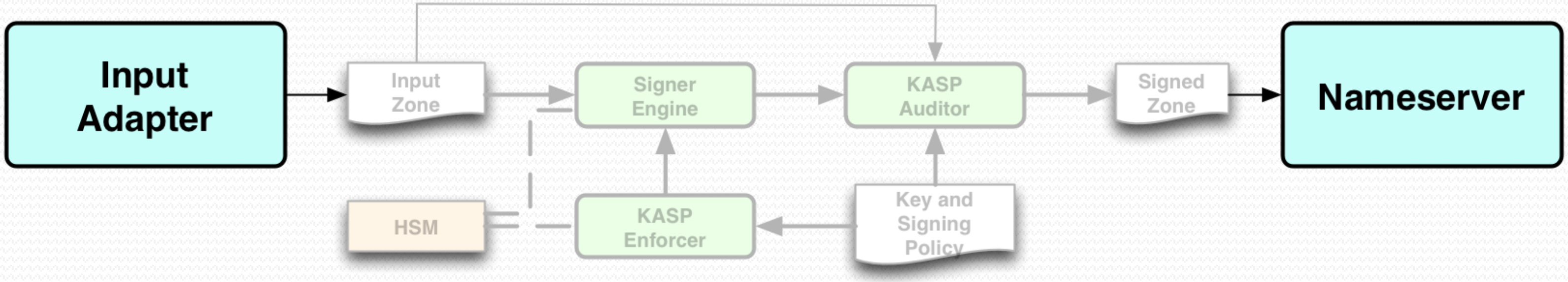
- Garbage in -> Garbage out

“Bump in the Wire”


unsigned zones
from hidden authoritative name servers
OpenDNSSEC
automatic zone signing
signed zones
to public, authoritative name servers

- In many cases, anticipate that OpenDNSSEC will be employed on a system between a hidden and public master.
- Requires additional software.

Input and Output Adapters



- Input adapter supplied as part of OpenDNSSEC - accepts AXFRs, responds to NOTIFYs.
- Output adapter not supplied - any preferred nameserver can be used (BIND, NSD, etc.)
- Can configure command to be used to reload zone.

Status

- 1.0 alpha released in July
- 1.0 beta released in October
- 1.0 expected release November 23

Thank you

- Questions?

http://www.opendnssec.org/

Open DNSSEC