nominet

OpenDNSSEC

Stephen Morris

stephen.morris@nominet.org.uk

What, Why, Who?

nominet

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

What, Why, Who?

nominet

- 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

OpenDNSSEC

What, Why, Who?

nominet

NLnet Labs

nominet

.se

kirei

John A Dickinson

SIDN

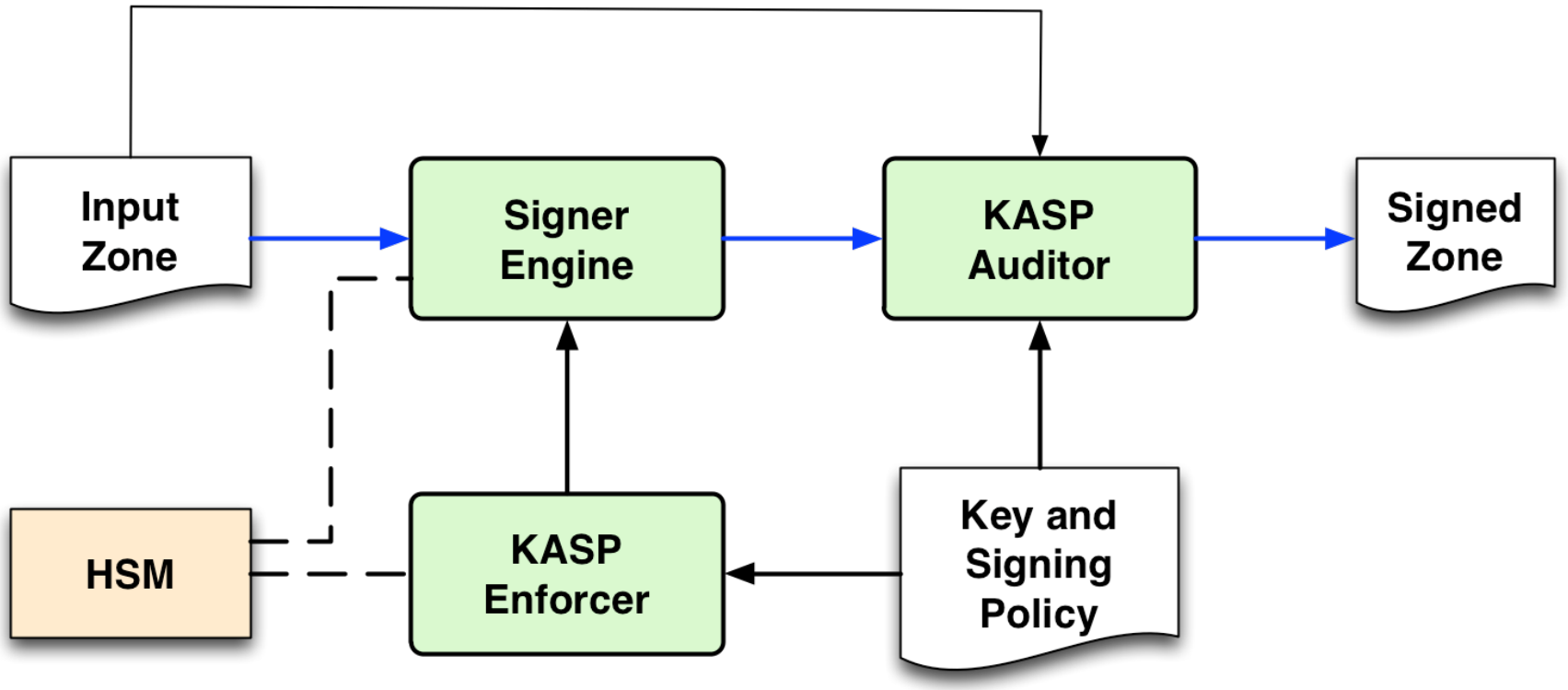
SURF NET

About OpenDNSSEC?

nominet

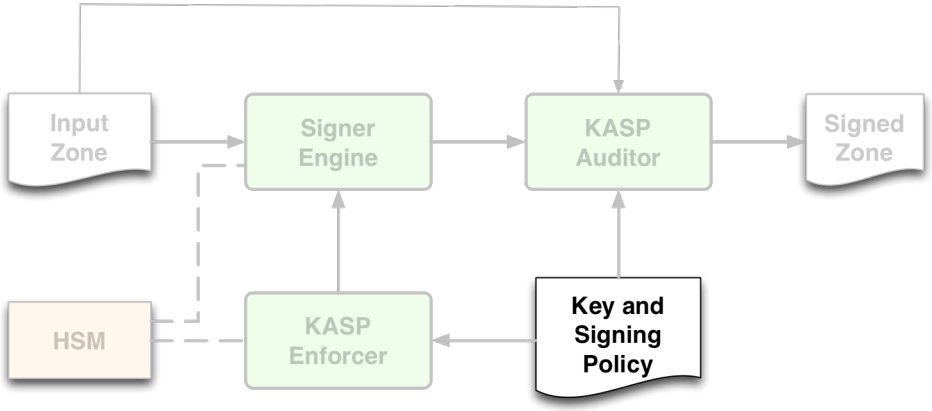
- Simplifies the process of signing one or more zones
- Key storage and hardware acceleration using HSMs
- Reduces the work load on the system administrator
- Simple to integrate into existing infrastructure
- Open source software with a BSD license

Architecture



Key and Signing Policy

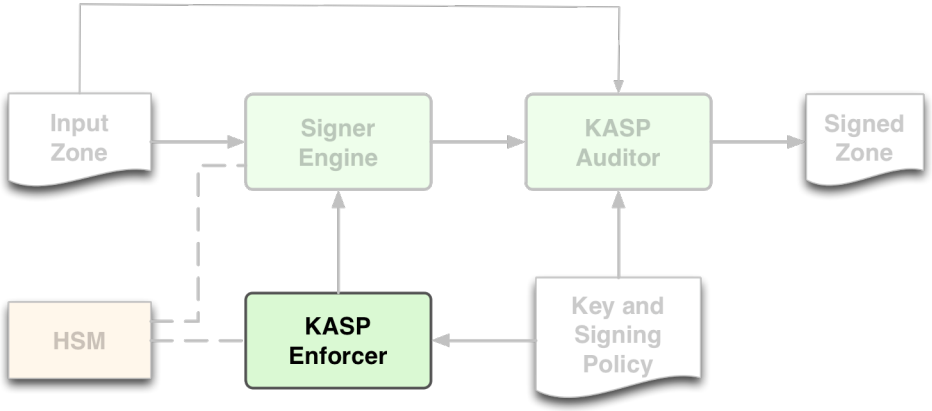
nominet



- How to sign a zone is described by a policy
- Allows choice of key strengths, algorithm, key and signature lifetimes, NSEC/NSEC3, etc.
- Can have anything between one policy for all zones to one policy per zone.

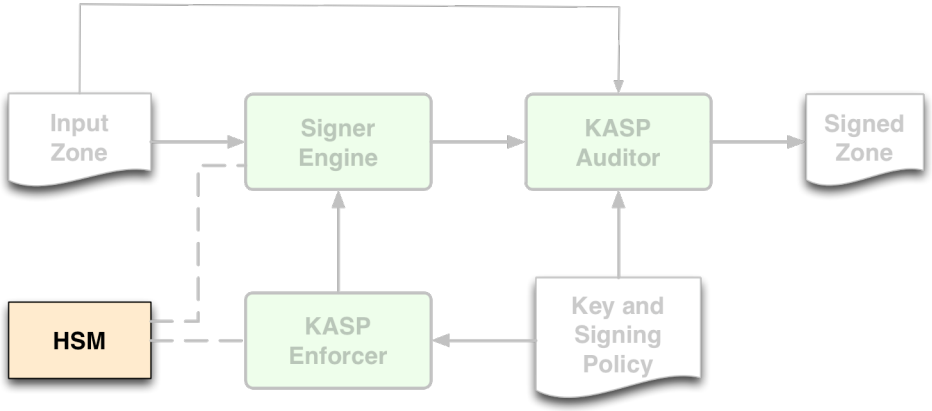
KASP Enforcer

nominet



- Handles the management of keys:
  - Key creation using HSM
  - Key rolling
- Chooses the keys used to sign the zone.

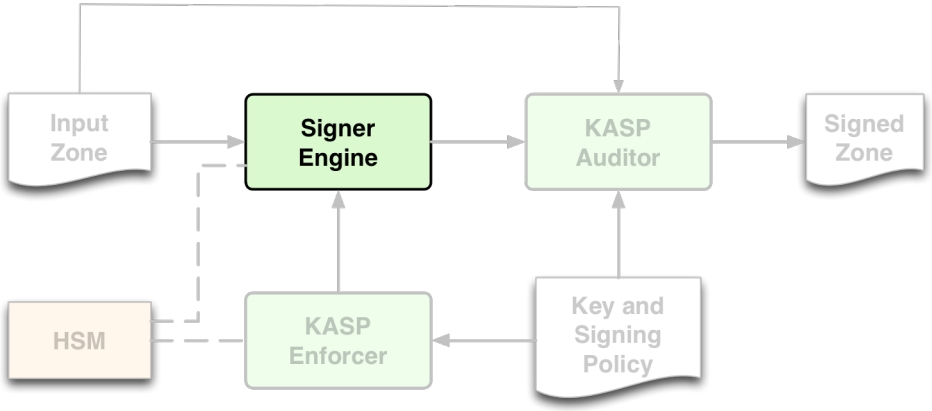
HSM



- 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 the HSM.

Signer Engine

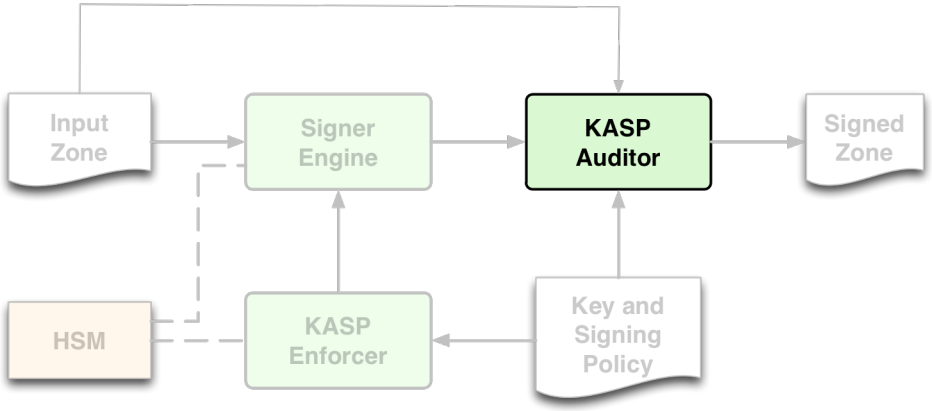
nominet



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

KASP Auditor

nominet



- 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 zone distribution if needed.
- Written by a different person and in a different language (Ruby).

OpenDNSSEC

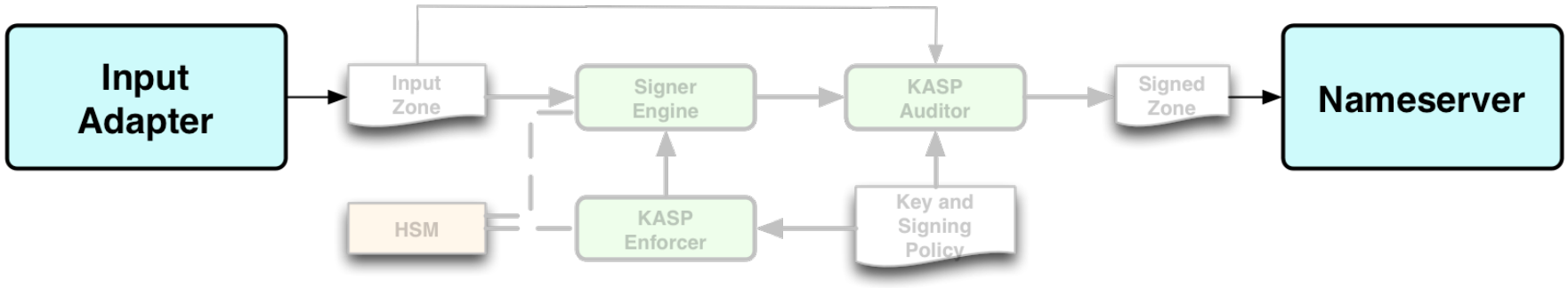
"Bump in the Wire"

nominet

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

Input and Output Adapters

nominet



- 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 late-November

Questions?

nominet

http://www.opendnssec.org