3-2-3
Provisioning DNSsec with OpenDNSsec

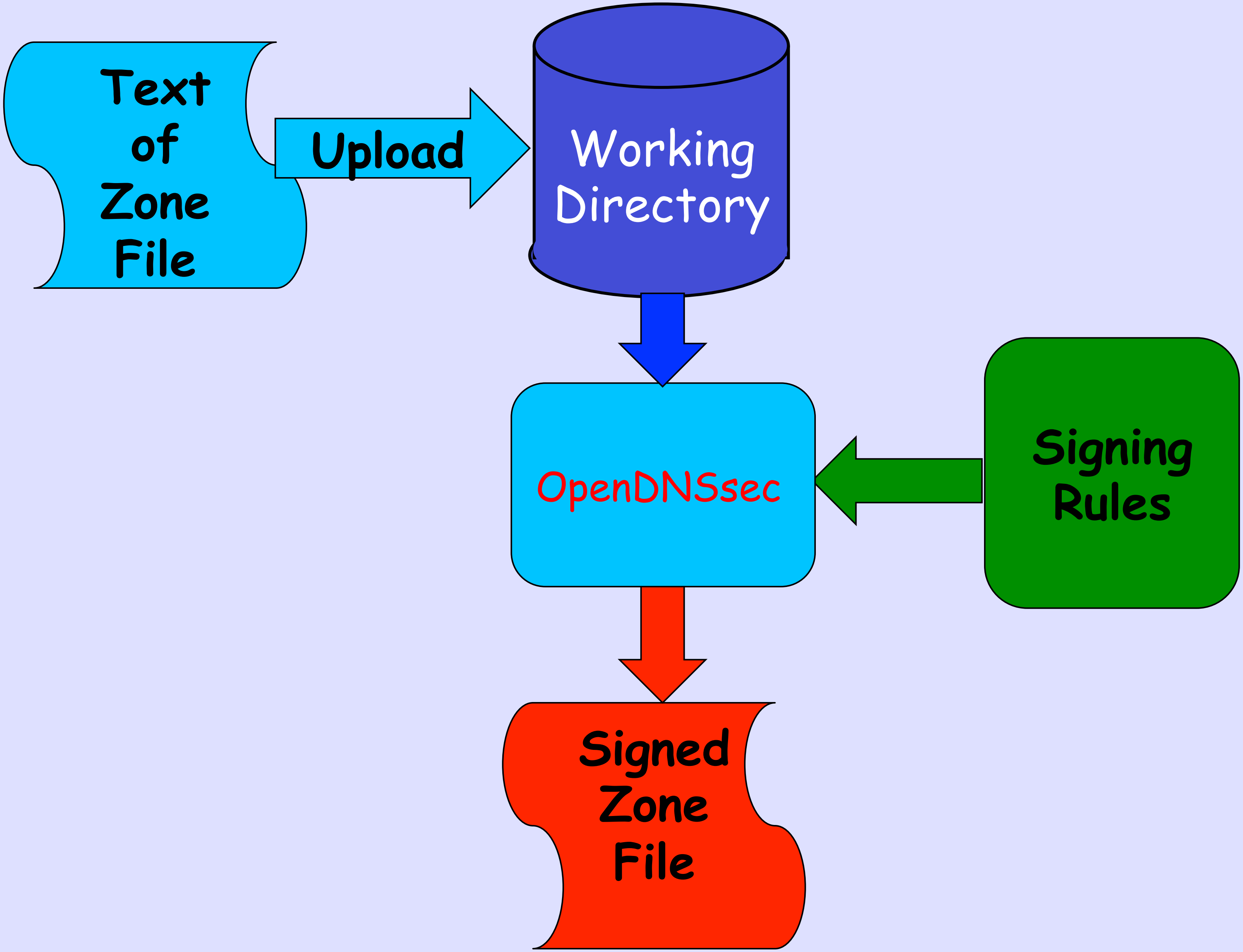
The Bad News

DNSsec Design Complex

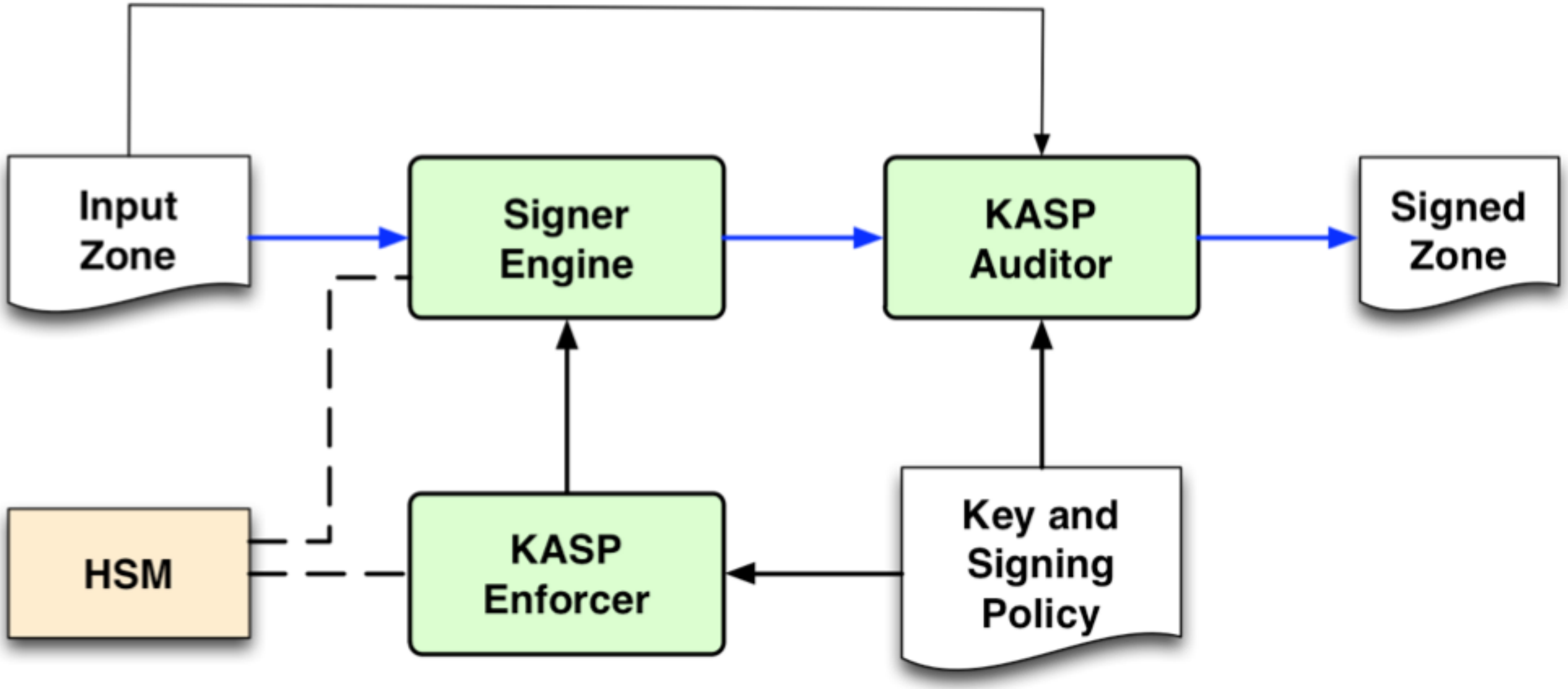
Software is Complex

The Good News

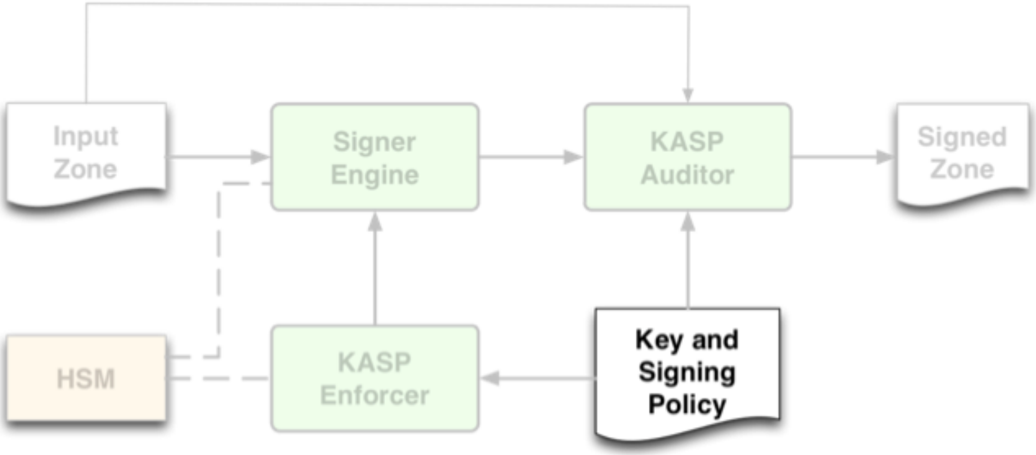
OpenDNSsec Works


Text of Zone File
Upload
Working Directory
OpenDNSsec
Signing Rules
Signed Zone File

Architecture

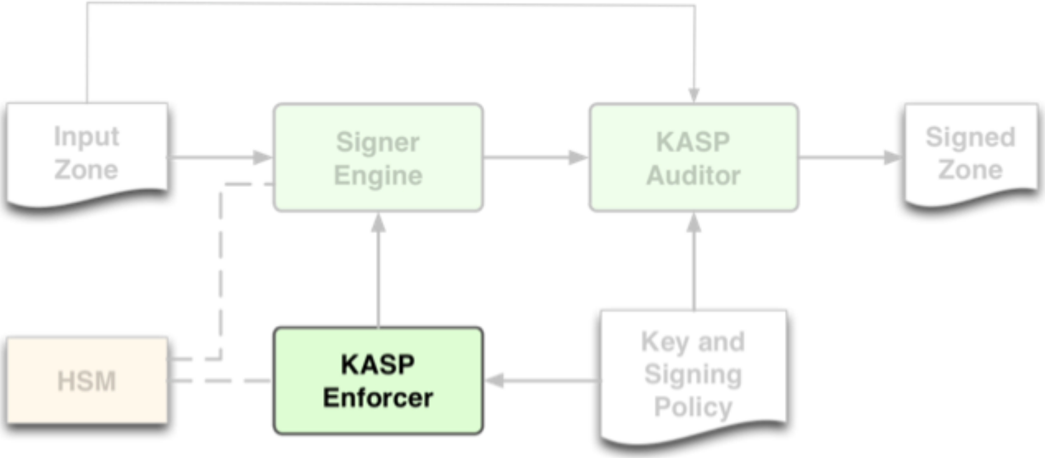


Key and Signing Policy



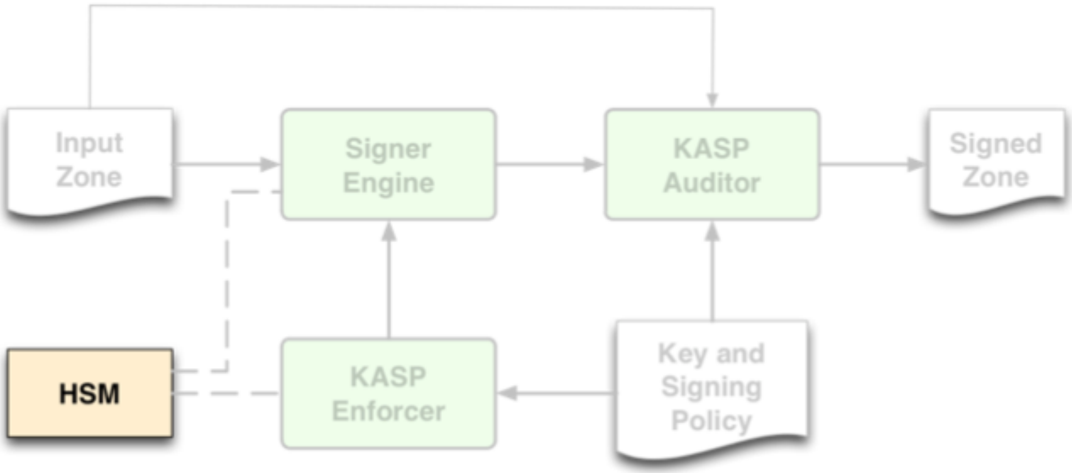
- How to sign a zone is described by a policy
- Allows choice of key strengths, algorithm, key and signature lifetimes, NSEC/NSEC3, etc.
- Can have anything between one policy for all zones to one policy per zone.

KASP Enforcer



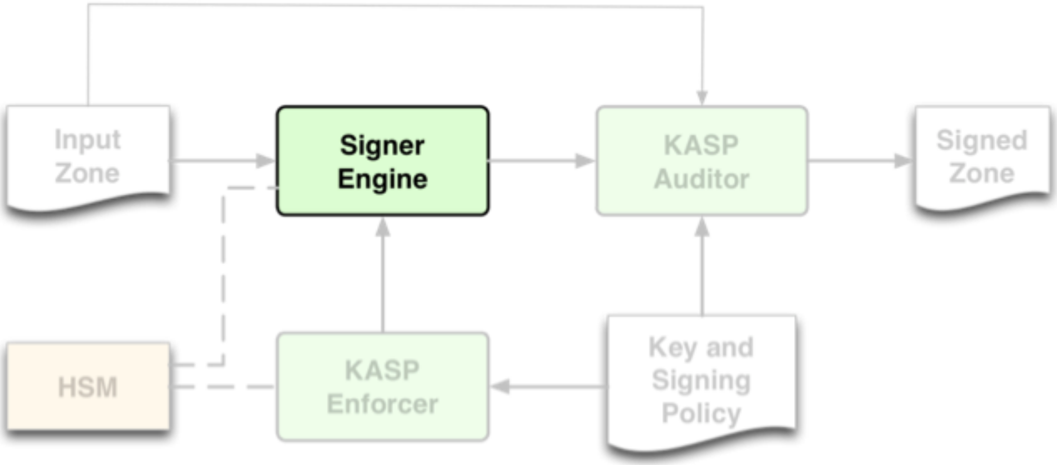
- Handles the management of keys:
  - Key creation using HSM
  - Key rolling
- Chooses the keys used to sign the zone.

HSM



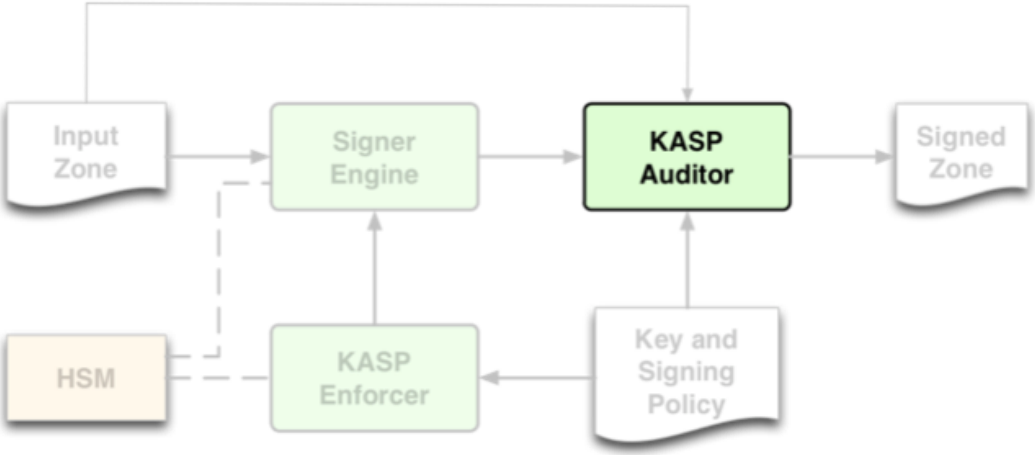
- Hardware Security Module
    - Stores the keys
    - Hardware acceleration to sign records
- Standard interface via PKCS#11 API
- SoftHSM available with OpenDNSSEC

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 in Ruby

.se