

OpenDNSSEC

Jakob Schlyter

Who are we?

- .SE
- Nominet
- NLNetLabs
- John A Dickinson
- Kirei

What are we trying do?

- Gather common requirements
- Build an fully automated DNSSEC production package
 - ▶ Automatic signing
 - ▶ Automatic key management
 - ▶ Optional HSM support

The Requirements

- High performance
- High security
- Support very large zones
- Support very large amount of zones
- Fully automated key management
- Monitoring

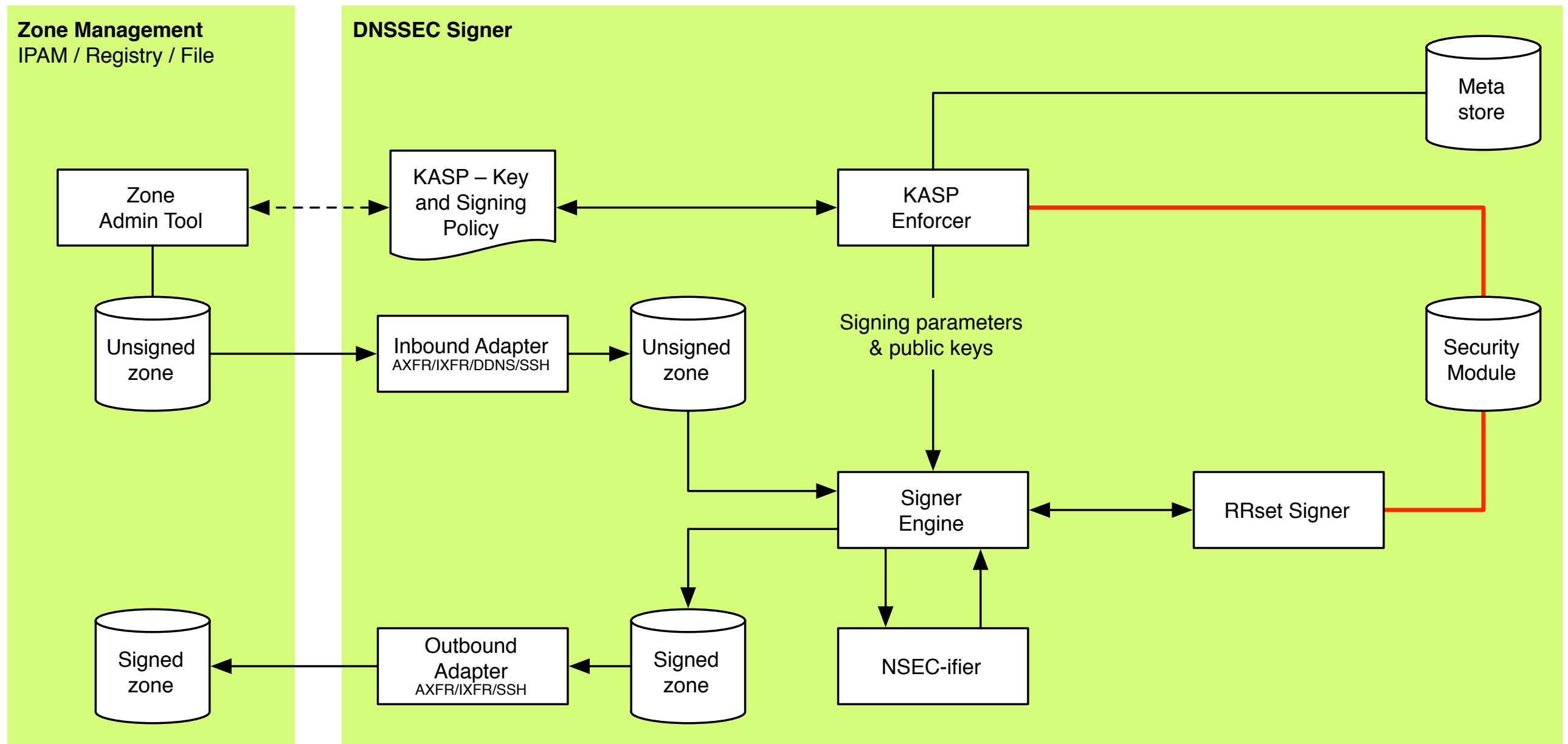
The Implementation

- Prototype – a set of loosely coupled tools, in order to test the architecture.
- Production version – an integrated, standalone, easy to install, platform independent package

The Architecture

- Policy-driven configuration
- Incremental signer with optional hardware acceleration
- Flexible input/output
 - ▶ AXFR/IXFR/DDNS/Disk

The Big Picture



The Key Management

- Uses KASP – *Key and Signing Policy*
- The *KASP* describes the policy
- The *KASP Enforcer* implements the policy
- Based on work by Nominet and John A Dickinson

What policy?

Zone Signing Policy

- Zone resigning interval
- Signature refresh, validity, jitter
- TTL
- ...

Key Policy

- Algorithm & Size
- Lifetimes
- Storage (disk/HSM/...)
- # of simultaneous keys (overlap)

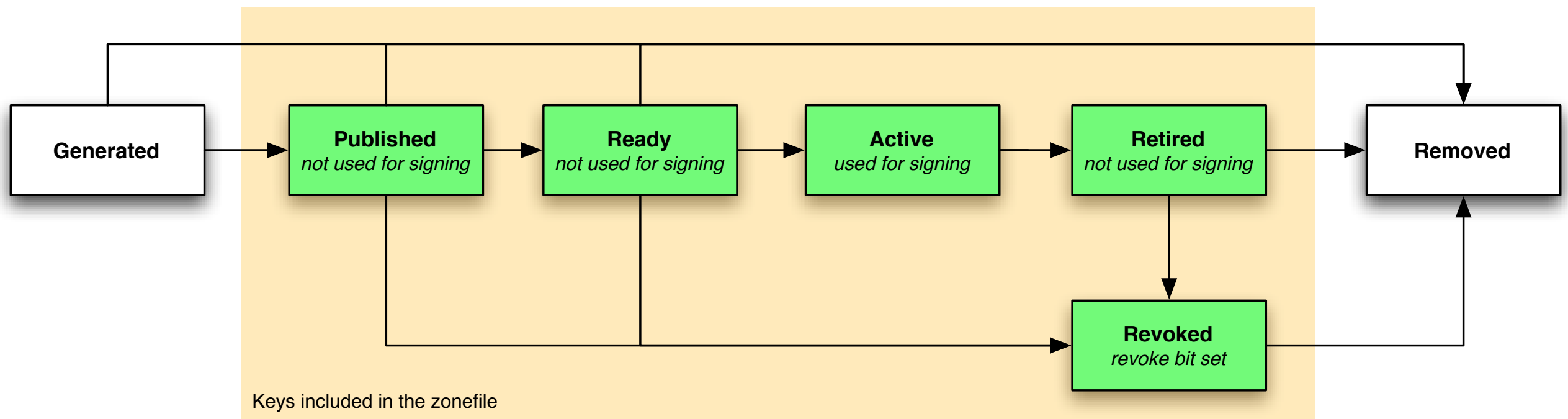
Authenticated Denial Policy

- Protocol (NSEC/NSEC3)
- NSEC3 opt-out
- NSEC3 hash algorithm, salt size, iterations
- NSEC3 re-salting interval

The KASP Enforcer

- Public keys and other parameters are stored in a *Meta Store*
- Private keys are stored in a *Security Module*
- Secure reasonable defaults included!

The life of a key...



The Signer

- Signer Engine
 - ▶ Configured by the KASP Enforcer
- NSEC/NSEC Generator (NSEC-ifier)
- RRset Signer
 - ▶ Signs RRset using the *Security Module*
 - ▶ Probably based on LDNS and PKCS#11

The Adapters

- Inbound Adapter
 - ▶ Fetches the unsigned zone using XFR/Disk
 - ▶ ... or accepts updates via DDNS
- Outbound Adapter
 - ▶ Delivers the signed zone using XFR/Disk

The Next Step

- Write a prototype implementation of the KASP Enforcer
- Teach LDNS to speak PKCS#11
- Hopefully a prototype implementation around spring, but no promises...

The WIKI

- All documentation, source code etc. is published at **www.opensssec.se**

jakob@kirei.se