

# nominet

OpenDNSSEC

Roy Arends

ICANN 35 Sydney

## Description

---

- OpenDNSSEC is a complete DNSSEC solution
- Completely automates the process of keeping track of DNSSEC keys and the signing of zones.



# Components

---

Three major components:

HSM The key storage component

KASP Key and Signing Policy

SIGNER All things DNSSEC-protocol

## What is an HSM?

- Stores keys in hardware

- Performs cryptographic operations

## Why use one?

- Private keys will never appear outside the HSM

- Performance 1 – 14,000 signatures per second

SoftHSM is an implementation of a cryptographic store accessible through a PKCS#11 interface.

Uses Botan for its cryptographic operations and SQLite to store its key material.

SoftHSM allows OpenDNSSEC to only provide one interface for all crypto operations.

## Key and Signing Policy

Decides when zones are resigned

Decides when keys are rolled

Decides which keys are used.

# Signer Engine

---

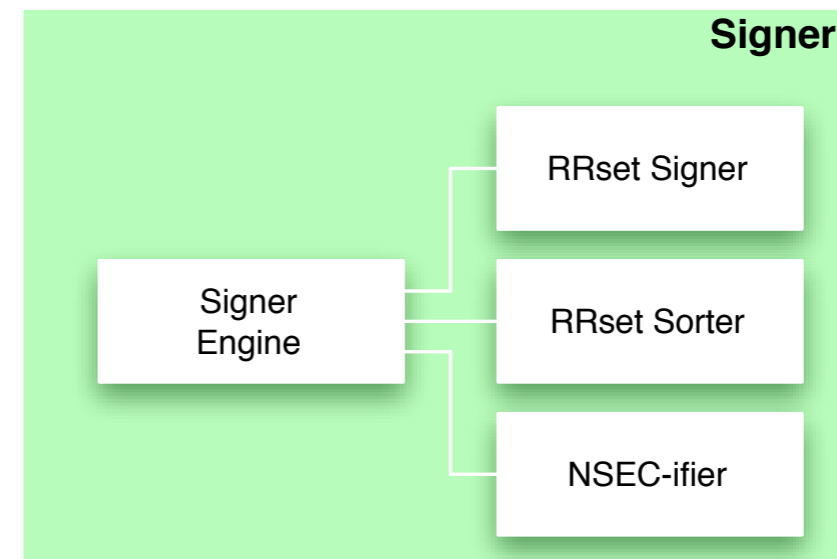
The Signer Engine does the following tasks:

Sorts RRsets

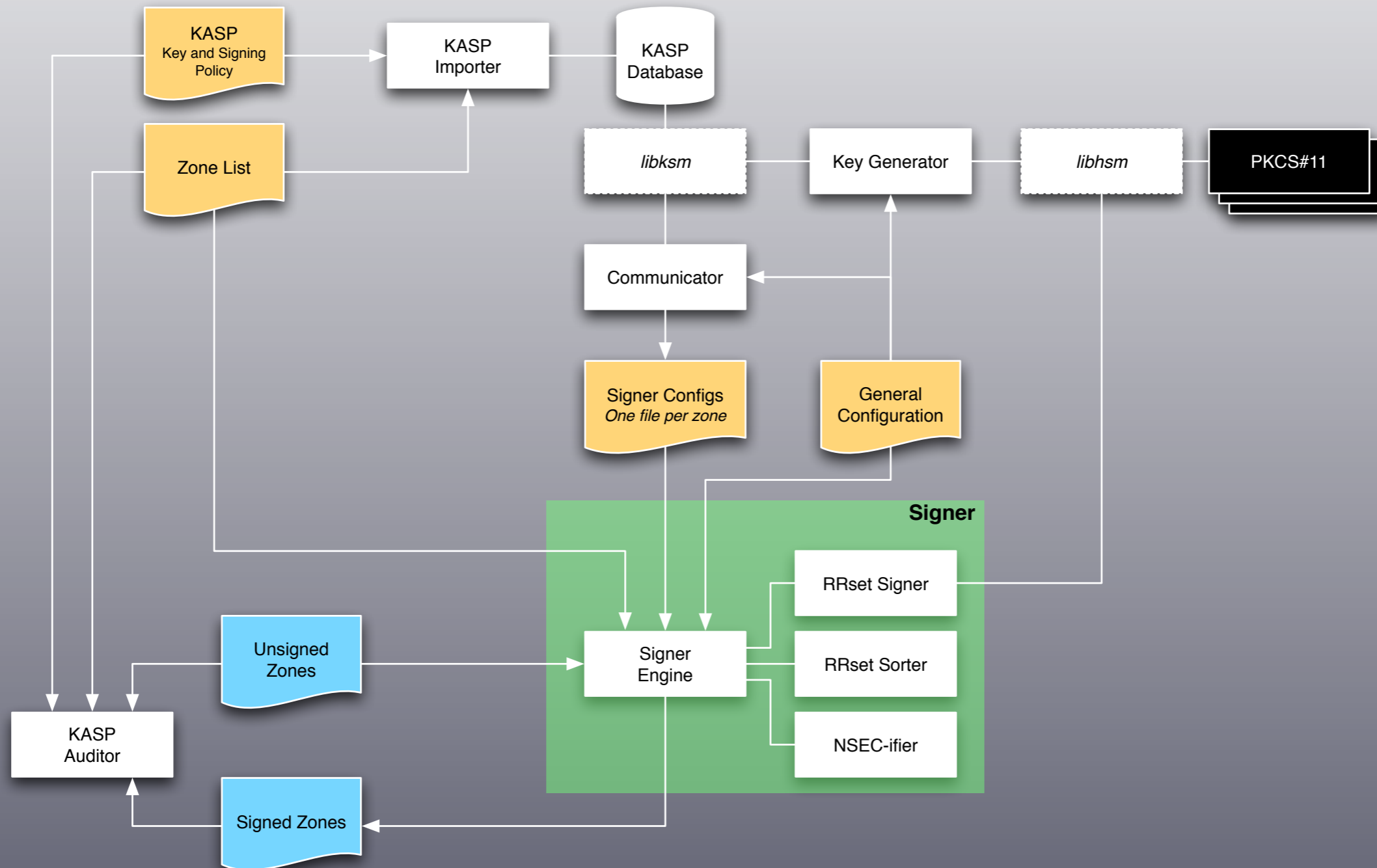
Creates NSEC(3)-chains

Signs RRsets

Keeps the RRSIGs up to date



# Architecture





# Who?

---

nominet®

NLnet  
10000 11000  
11000 11000  
10010 11000  
00111 10000  
00010 11000  
00010 11000

Labs

.se

kirei

SURF  
NET

John A  
Dickinson

When?

---

Alpha version real soon now...

Version 1.0 for the IETF in Stockholm.

## Questions?

---

- Interested? Go to [www.opendnssec.org](http://www.opendnssec.org)
- Talk to us, tell us your needs