nominet

OpenDNSSEC

Roy Arends

ICANN 37 Nairobi

nominet

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

HSMs

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

nominet

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.

KASP

- Key and Signing Policy
- Decides when zones are resigned
- Decides when keys are rolled
- Decides which keys are used.

Signer Engine

nominet

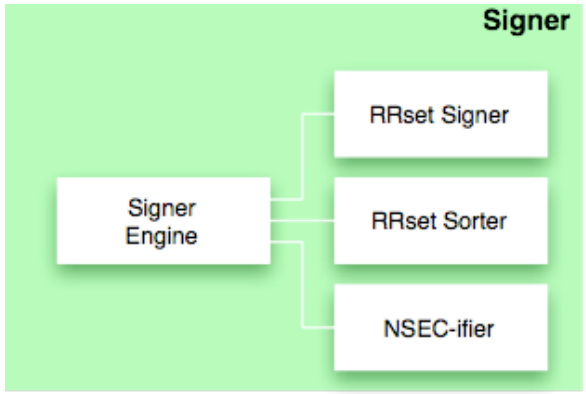
The Signer Engine does the following tasks:

Sorts RRsets

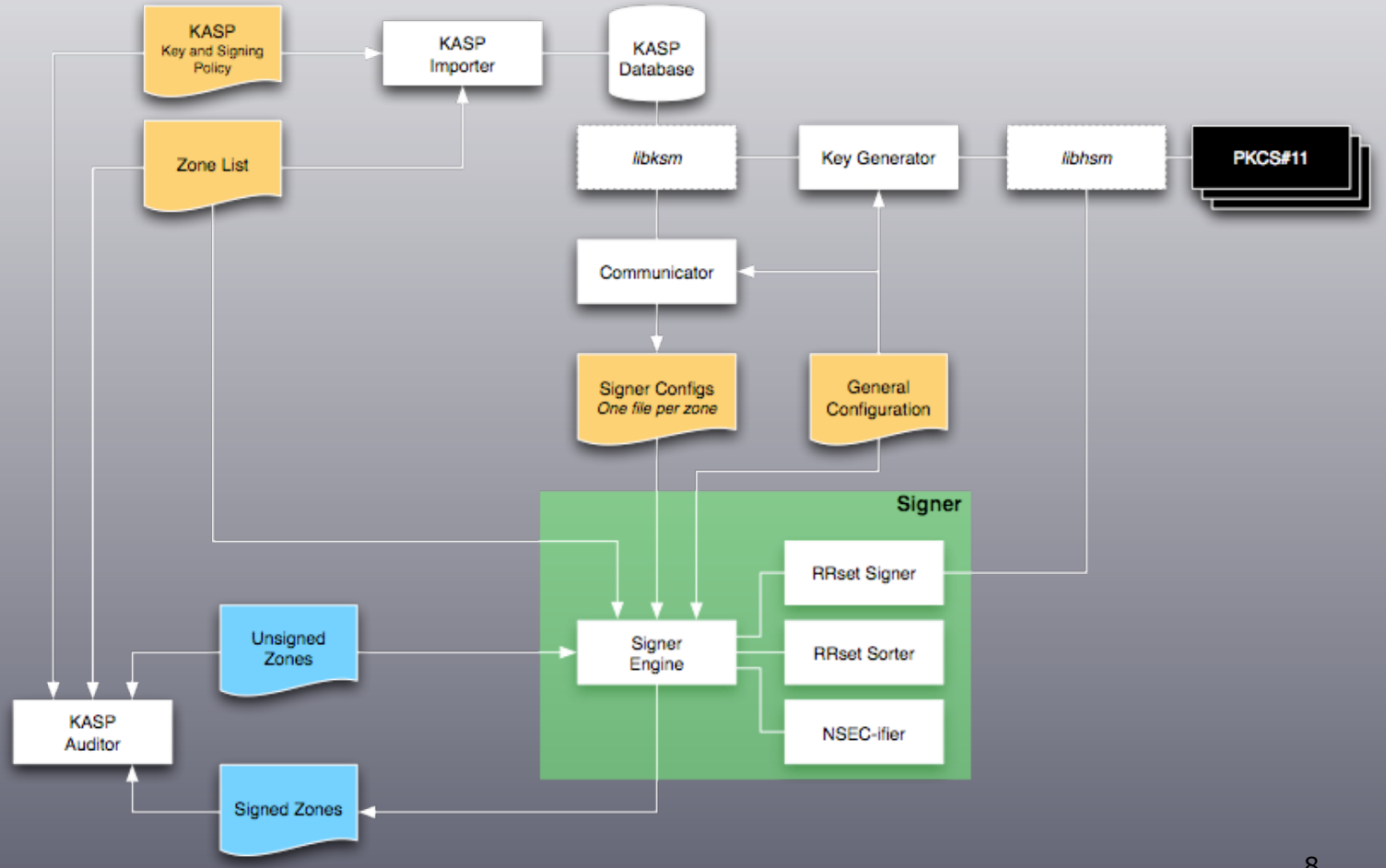
Creates NSEC(3)-chains

Signs RRSets

Keeps the RRSIGs up to date



Architecture



Who?

nominet®

NLnet Labs

.se

kirei

SURF NET

John A Dickinson

SIDN

When?

Version 1.0 released

Working hard on Version 2

Questions?

- Interested? Go to www.opendnssec.org
- Talk to us, tell us your needs