OpenDNSSEC

Patrik Wallström, .SE R&D

RIPE 58, Amsterdam

Who?

nominet

NLnet Labs

.se

kirei

SURF NET

John A Dickinson

This is OpenDNSSEC

Description

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

Components

There are three major components of OpenDNSSEC:

1. **KASP -** Key and Signing Policy, a policy describing how to sign a zone. The KASP is enforced by the KASP Enforcer and communicated to the Signer with a Signer Config.

2. The **Signer -** the component that does the automatic signing of zones.

3. An **HSM -** a key store component that is either a hardware device or the software SoftHSM component supplied by OpenDNSSEC.

Additional components

There are more needed though:

4. **KASP Auditor** - monitors that the signing works the way it is supposed to.

5. **Input** and **Output adapters** - provides for AXFR, IXFR and other protocols.

6. **libhsm** - abstracts all PKCS#11 functionality.

HSMs

What is a HSM?
- Stores keys (master keys) in hardware
- Performs operations with those keys

Why use one?
- Security (FIPS)
  - Private key never allowed outside the HSM
  - You know where your keys are
- Performance
  - 1 – 14,000 signatures per second

Are they expensive?
- $50 – $50,000

SoftHSM

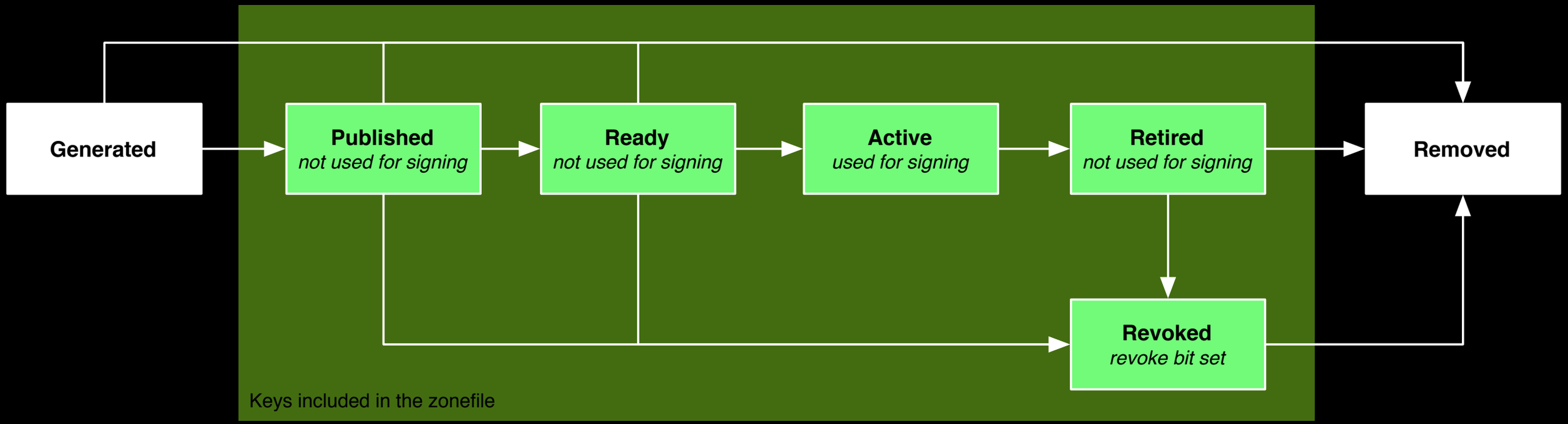
SoftHSM is an implementation of a cryptographic store accessible through a PKCS#11 interface.

You can use it to explore PKCS#11 without having a Hardware Security Module.

SoftHSM is being developed as a part of the OpenDNSSEC project. 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 states and transitions



derived from draft-morris-dnsop-dnssec-key-timing-00.txt

Key metadata in KASP

Data for the keys stored in “Metastore” are dates such as when the key was created, when it was backed up, when it was retired and so on.

Also which HSM the key is stored in.

A unique locator id is designated to all keys, which is referred to by the Locator tag in configuration files.

KASP commands

The only command that an administrator should be able to issue is **remove key**.

However, not CLI or GUI interface has not been defined yet. There is a CLI for testing purposes which lets you modify keys.

Signer Engine

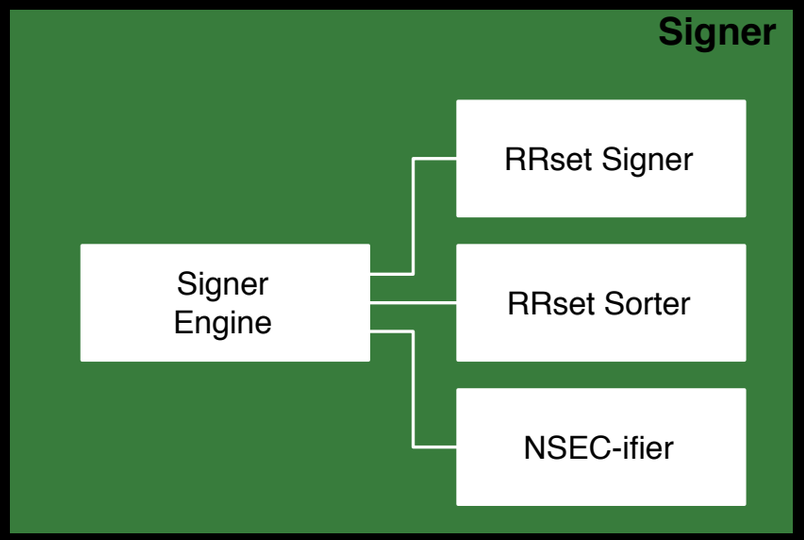
The Signer Engine does the following tasks:

Sorts RRsets

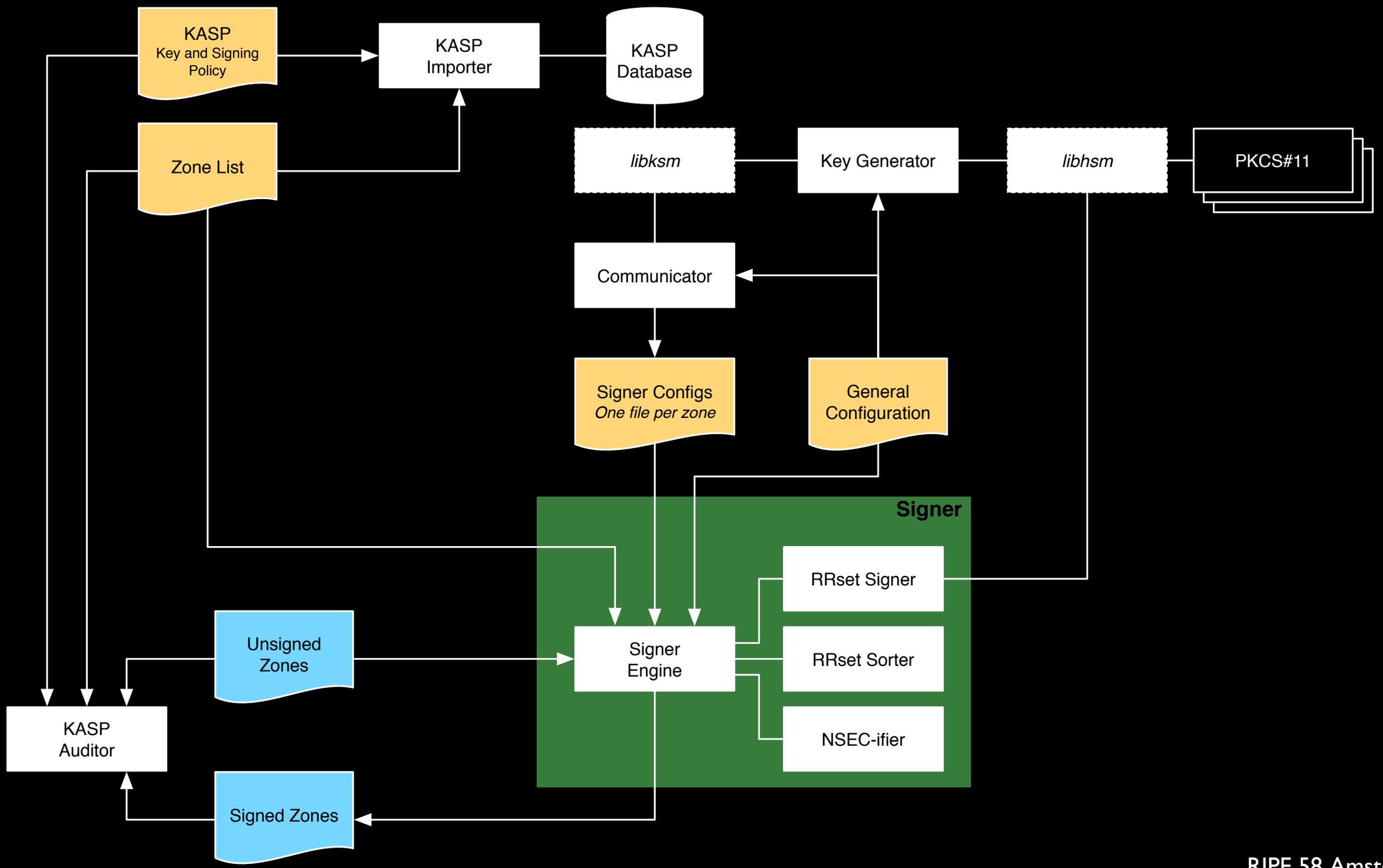
Creates NSEC-chains

Signs RRSets

Keeps the RRSIGs up to date



Architecture



Configuration

First you need a HSM. To configure SoftHSM you need to create a token like this:

softhsm --init-token /home/user/my.db --label "My token 1"

And add the token to your SoftHSM slots in softhsm.conf:

0:/home/user/my.db

conf.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>

        <RepositoryList>
                <Repository>
                        <Name>softHSM</Name>
                        <Module>/usr/local/lib/libsofthsm.so</Module>
                        <PIN>1234</PIN>
                </Repository>
        </RepositoryList>

        <Enforcer>
                <Interval>PT3600S</Interval>
                <KeygenInterval>P3M</KeygenInterval>
                <BackupDelay>P3D</BackupDelay>
        </Enforcer>

        <Signer>
                <WorkingDirectory>/var/dnssec/tmp</WorkingDirectory>
                <ZoneListFile>/var/dnssec/zonelist.xml</ZoneListFile>
                <!-- toolsdir will be removed, but is used for testing atm -->
                <ToolsDirectory>/usr/local/bin</ToolsDirectory>
        </Signer>

</Configuration>
```

kasp.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<KASP>

        <Policy name="default">
                <Description>A default policy that will amaze you and your friends</Description>
                <Signatures>
                        <Resign>PT2H</Resign>
                        <Refresh>P3D</Refresh>
                        <Validity>
                                <Default>P7D</Default>
                                <Denial>P14D</Denial>
                        </Validity>

    ...

                        <KSK>
                                <Algorithm length="2048">5</Algorithm>
                                <Lifetime>P1Y</Lifetime>
                                <Repository>softHSM</Repository>
                                <Emergency>2</Emergency>
                                <RFC5011/>
                        </KSK>

                        <ZSK>
                                <Algorithm length="1024">5</Algorithm>
                                <Lifetime>P14D</Lifetime>
                                <Repository>softHSM</Repository>
    ...
```

zonelist.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<ZoneList>
        <Zone name="opendnssec.se">
                <Policy>default</Policy>
                <SignerConfiguration>/var/opendnssec/config/opendnssec.se.xml</
    SignerConfiguration>
                <Adapters>
                        <Input>
                                <File>/var/dnssec/unsigned/opendnssec.se</File>
                        </Input>
                        <Output>
                                <File>/var/dnssec/signed/opendnssec.se</File>
                        </Output>
                </Adapters>
        </Zone>
</ZoneList>
```

opendnssec.se.xml

```
...
        <Keys>
            <TTL>PT3600S</TTL>

            <Key>
                <Flags>257</Flags>
                <Algorithm>5</Algorithm>
                <Locator>DFE7265B783F418685380AA784C2F31D</Locator>
                <KSK/>
                <Publish/>
            </Key>

            <Key>
                <Flags>256</Flags>
                <Algorithm>5</Algorithm>
                <Locator>8D76C0C49FEB4A97B8E920C7552401CE</Locator>
                <ZSK/>
                <Publish/>
            </Key>
        </Keys>

        <SOA>
            <TTL>PT3600S</TTL>
            <Minimum>PT3600S</Minimum>
            <Serial>unixtime</Serial>
        </SOA>
    ...
```

Todo

- System integration
- Install guide
- User guide
- Peer reviewing
- Make OpenDNSSEC one package
- System testing
- Performance testing
- Durability testing
- User testing

When?

Alpha version real soon now...

Version 1.0 for the IETF in Stockholm. Maybe.

http://www.opendnssec.se/

Thank you!

Questions?