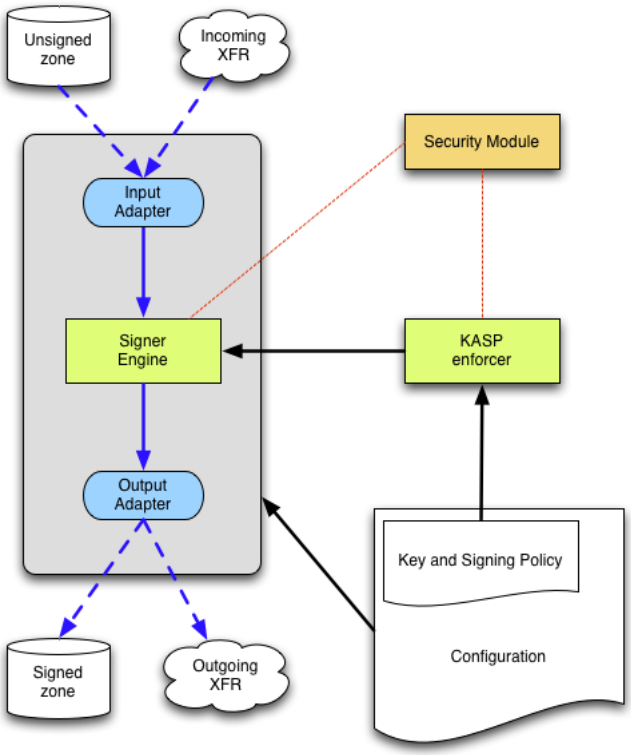
Overview of OpenDNSSEC

OpenDNSSEC is a system to manage zones. It takes in unsigned zones and policies and produces and maintains DNSSEC signed zones. OpenDNSSEC is responsible for signing, resigning, key generation, and fetching/distributing zones to and from nameservers.

The policies are defined in the KASP (Key And Signing Policies). These describe the configuration for DNSSEC such as key lengths and lifetimes.

Components

A OpenDNSSEC instance has 3 main components: HSM, Enforcer, and Signer.



HSM

The HSM (Hardware Security Module) provides storage of crypotographic keys. Whenever data needs to be signed by one of its keys, that data is transferred to the HSM, signed, and the signature transferred back. This way the private key material never needs to leave the device. OpenDNSSEC communicates with the HSM via PKCS#11 and should be compatible with any device implementing that interface. The OpenDNSSEC project provides SoftHSM which is an entirely software implementation of a HSM via the same interface. If set up correct a real HSM will provide better security and performance. If neither is critical SoftHSM is a good alternative.

Enforcer

The KASP Enforcer component manages the zones and their policies. It makes sure the needed keys are available on the HSM and precisely instructs the signer how to sign the zones. It is responsible for all timing related concepts in DNSSEC. It dictates when and in what order key rollovers happen. It is unaware of the contents of the zones but very aware of their state.

Signer

The signer handles the actual data of a zone. It will obtain unsigned zones either through files or over the network via XFR. Then it will sign the zones and when necessary refresh signatures on a regular basis. Signed zones are then output as a file or via XFR to a nameserver.

Files

OpenDNSSEC manages various information on disk which includes the following

- Configuration files, xml files that specify the settings for the system
- Zone files, unsigned and signed copies of the zones
- Working files, temporary files used by the system to exchange information between components and track internal state information
- Database, when using an SQLite database backend.

Configuration Files

By default OpenDNSSECs configuration files are stored in `/etc/opendnssec/`.

conf.xml

Daemon specific settings such as HSM configuration, logging, database location, and working directories. This file is read by both the Signer and the Enforcer.

kasp.xml

Contains a list of user defined policies. These policies describe how often keys need to be rolled, which algorithms to use, what different timing parameters are etc. This file is read exclusively by the Enforcer.

addns.xml

Specifies the input and output adapters which describe to the Signer how to acquire unsigned zones and where to store signed zonefiles. This can either be the simple file adapters (read and write zones to a file) or the more complex DNS adapters that transfer zones to and from DNS servers.

Zone Files

In case the File input adapter is used OpenDNSSEC expects to find the unsigned zonefile in `/var/opendnssec/unsigned`. Likewise for the File output adapter `/var/opendnssec/signed` is the location where the Signer will write its signed zonefiles to. These locations are not used when the DNS adapters are selected.

Working Files

`/var/opendnssec/enforcer/zones.xml`, list of zones configured in OpenDNSSEC. Produced by the Enforcer and consumed by the signer. This file links zones to the adapters for the signer.

`/var/opendnssec/signconf/`, for every zone the enforcer writes a signing configuration here. Instructing the signer which keys to publish and use for signing.

`/var/opendnssec/signer/`, this is where the signer keeps its state. Signatures are cached here and information about zone versions for IXFR.

`/var/opendnssec/kasp.db`, In case of SQLite as database backend this file contains the enforcer state. Which keys are in use and at what time records where published.