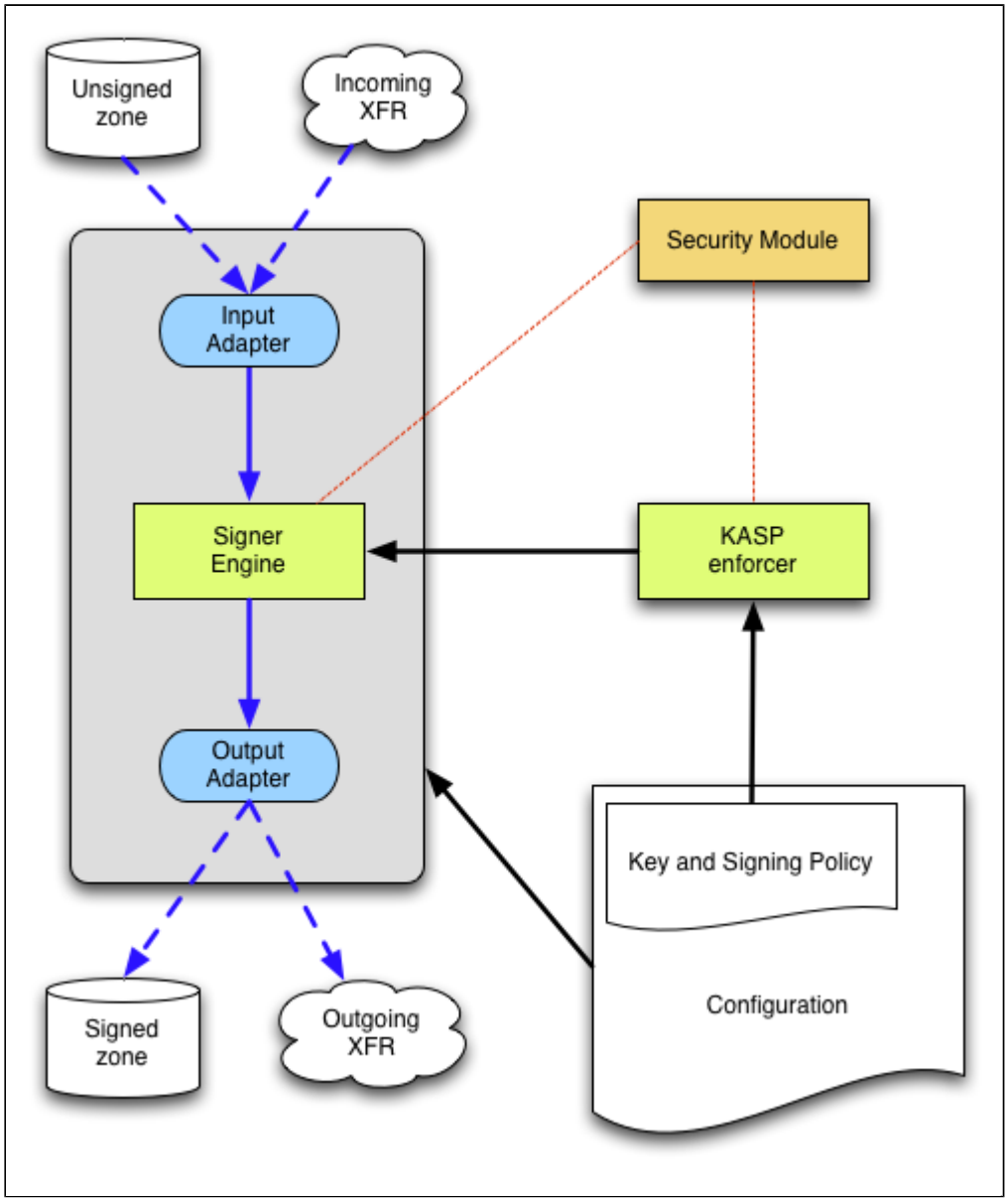
Overview of OpenDNSSEC

OpenDNSSEC takes in unsigned zones, adds the signatures and other records for DNSSEC and passes the zones on to the authoritative name servers for that zones.

It does this according to a Key and Signing Policy (KASP) that describes how an organisation wants their DNSSEC configured.



On this Page

What does OpenDNSSEC do automatically?

Once installed, configured and running OpenDNSSEC will do the following:

- Receive unsigned zones from file or through XFR.
- Key Rollover: Generate, publish and retire keys held in an HSM according to policy. See the full key lifecycle in the Key States guide.
- Signing and re-signing of zones according to policy, including the reuse of signatures.
- Provide signed zones to file or to name servers via XFR.

What can be done manually?

- Zones can be added, updated and removed.
- Keys can be backup and exported or managed manually.
- Manual key rollovers can be performed to cater for emergencies.
- The Key and Signing policy can be updated.

See the Running OpenDNSSEC guide for more details

What must be done manually?

Uploading the Trust Anchor to the parent and notifying OpenDNSSEC that this has been done is a manual operation.

What are the key components of OpenDNSSEC?

- **Configuration including:**
  - *KASP* - is the set of user defined policies to be used for signing and maintaining zones managed by this system.
- **Enforcer** - is responsible for enforcing the policy by managing the keys and orchestrating zone signing.
- **Signer** - is responsible for performing zone signing according to the instructions from the Enforcer. Is is also responsible for ensuring that the zone is secure i.e. it will validate correctly.
  - *Input/Output Adapters* - are responsible for managing the input and output of zones via the specified mechanism (file, AXFR/IXFR).

- A HSM is also required for key management and storage.