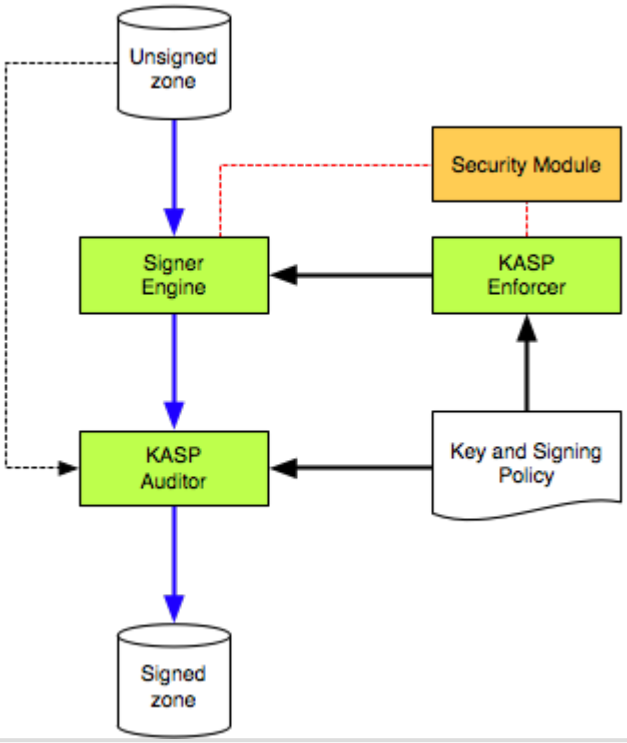
Overview of OpenDNSSEC

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:

- Generate, publish and retire keys held in an HSM according to policy. See the full key lifecycle in the Key States guide.
- Automatically (re-)sign zones according to policy.
- Audit the signed zones against policy (if configured).
- Receive unsigned zones from and provide signed zones to nameservers via AXFR (if configured).

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.
- Signed zones can be audited against policy.

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?

- **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.
- **Auditor** - performs an independent check of the signed zone before it is published. It does this by checking the zone against the KSAP database using a different implementation of the audit logic to that used by the signer.

A HSM is also required for key management and storage.