Signer Engine Adapter Architecture

OpenDNSSEC 1.4 Signer Engine Architecture.

The signer is the core of this system. It drives the whole signing process by continuously keeping all zones signed as specified in the signer configuration (signconf) received from the KASP Enforcer.

The signer is responsible for:

- resigning before signatures expires
- resigning when the keys have changed
- denial of existence roll-over, NSEC3 salt roll-over
- updating the SOA serial when resigning a zone

The signer itself consists of multiple components:

- The **Signer Engine** schedules all required operations, like reading, nsecifying, signing and writing a zone.
- A set of **Workers** that execute scheduled operations.
- A set of **Drudgers** that take care of subtasks like signing a single RRset (also known als RRset Signers).
- **Zone Adapters** that convert zones in various formats from and to the Signer Engine.
- A **Command Handler** that forwards commands from the user to the Signer Engine.
- A **DNS Handler** that forwards incoming packets to the Signer Engine.
- A **XFR Handler** that handles incoming zone transfers and Dynamic Updates.

Signer Engine

When the Signer Engine is started, it reads the signer specific configuration settings from conf.xml and the zones from zonelist.xml. It may recover zones from zone specific backup files. All zones have a dedicated task to ensure that a correct, signed zone is outputted regularly.

Configuration

The signer configuration settings are stored within the <Common> and <Signer> elements in conf.xml. See conf.xml for more details.

Zonelist

The zones are listed in zonelist.xml. See zonelist.xml for more details.

Backup files

If the signer has been stopped, due to an upgrade or a crash, the Signer Engine can recover zones from created backup files. There can be up to three files per zone. For the zone example.com: example.com.xfrd, example.com.ixfr, example.com.db

- example.com.xfrd is the transferred, unsigned zone from the master (in AXFR or IXFR format). The file is not used for recovery, but may be re-read when an **`ods-signer sign example.com`** command is given.
- example.com.db is the full, signed zone, including sign configuration parameters. The file may be recovered on startup.The file may be recovered partially: If it can read the serial values, it SHOULD use these even if other backup values cannot be retrieved. This is to prevent an unwanted serial decremental.
- example.com.journal is the signed zone in IXFR format and may be served to secondaries. If it matches the backup version and time from the example.com.db file, this journal may be recovered.

Task Queue

Each zone has a corresponding task that needs to be scheduled in the task queue. The Signer Engine is responsible for that. Successfully recovered zones will be scheduled with a re-sign task, at the time provided by the backup file. Fresh zones will be scheduled with the immediate task to load the sign configuration, to determine the required signing parameters. The known tasks are: Load Sign Configuration, Read Unsigned Zone, Sign Zone and Write Signed Zone.

Workers

Workers are responsible for executing the tasks on the Task Queue. A Worker will pick the first task on the queue, only if its execution time is at this exact moment or is in the past. A successful executed task is always followed with its succeeding task. For example, after performing the 'Load Sign Configuration' task, a Worker will work on the 'Read Unsigned Zone' task. After writing the signed zone, the zone task is set to 'Sign Zone' at the appropriate time and put back on the Task Queue.

Sign Queue

The 'Sign Zone' task is a though task, consisting of hard, menial work, namely doing signing operations. A Worker will not do these operations by itself, but queue this work on the Sign Queue. If all queued items have been resolved, the Worker will continue its task.

Drudgers

Drudgers are similar to workers, only they are responsible for executing the signing operations listed in the Sign Queue. Such a signing operation consists of taking an RRset from the queue, re-sign it with the appropriate key (if necessary, sometimes its signature can be refreshed or is not required anymore) and increment the number of completed jobs. The Drudger that completes the final queued work for its superior worker, will notify the Worker that the 'Sign Zone' task has been fulfilled.

Zone Adapters

The zone adapters can store the zones as flat files, in a database or any other data structure that is supported by the Signer Engine and is highly dependent on the protocol used for data transfer. Any support for incremental changes (i.e. IXFR or DDNS) most probably requires a data structure that can be processed incrementally and feed the resulting incremental changes through outbound zone adapter.

The Inbound Zone Adapter fetches the unsigned zone using AXFR/IXFR/CP.
The Outbound Zone Adapter delivers the signed zone using AXFR/IXFR/CP.

Command Handler

The command handler can deal with commands given by the operator. See **man ods-signer** for more information.

DNS Handler

The DNS Handler can handle queries, zone transfer requests and NOTIFY messages.

XFR Handler

The XFR Handler will do the actual zone transfer from the master servers and send out NOTIFY messages to the secondaries.