Configuration

Configuration Files

By default OpenDNSSEC expects its configuration files in /etc/opendnssec. This can be configured compiletime if another location is desired.

The OpenDNSSEC XML configuration files (conf.xml and kasp.xml) offer the user many options to customize the OpenDNSSEC signing system. Not all possible configuration texts are meaningful however. **ods-kaspcheckTODO** is a tool to check that the configuration files are syntactically and semantically sane, and contain no inconsistencies. It is advisable to use this tool to check your configuration before starting to use OpenDNSSEC.

conf.xml

This contains settings that apply to the entire OpenDNSSEC instance such as logging, file locations and HSM information. The conf.xml file is read by both the enforcer and the signer.

kasp.xml

kasp.xml defines one or more policies which describe how zones should be signed. Most notably security parameters (key type and size, etc) and timing parameters such as key life times.

zonelist.xml

zonelist.xml can be used to bulk add or remove zones from OpenDNSSEC. Since OpenDNSSEC 2.0 this file is no longer needed for normal operation and operators are encouraged to use the command line client to add and remove zones instead.

addns.xml

OpenDNSSEC can sign zone files on disk, but can also receive and server zone transfers (both AXFR and IXFR). If you configure a listener in conf.xml, the Signer Engine will kick off a DNS handler that will listen to queries, NOTIFY messages from the master and zone transfer requests from secondaries. In formation in this file details where to fetch zone data from and protection mechanisms to be used.

Zonefile Formatting

OpenDNSSEC can handle various formatting of the zone file, including different directives and Resource Records (RRs).

Formatting

The zone file can be formatted in many ways including multi-lined RR, comments, etc.

Supported Directives

As defined in RFC 1035 the following directives are supported by OpenDNSSEC:

$ORIGIN example.com.	What origin to use.
$TTL 1h3m	The default TTL to use. Treated as seconds, if no suffix is used: s, m, h, d, w, S, M, H, D, W
$INCLUDE <path>	Include a file from a given path

RR types

OpenDNSSEC support all of the RR specified by IANA, with some exceptions:

Not supported	ATMA, APL, EID, NIMLOC, HIP, SINK, NINFO, RKEY, TA
Obsoleted	MD, MF, WKS, GPOS, SIG, KEY, NXT, A6, and NSAP-PTR
Not allowed in master	NULL, OPT, TKEY, TSIG, IXFR, AXFR, MAILB, MAILA, *

Handling of unknown RR types

But OpenDNSSEC does handle unknown RR types in accordance with RFC3597 e.g:

```
example.com.    IN          TYPE1               # 4 0A000001
```