

OpenDNSSEC and SoftHSM Cheat Sheet

By Kgwedi

Most of this was copied from: <http://www.opendnssec.org/documentation/using-opendnssec/>

Dependencies: ldns, libxml2, libxml2-dev, libxml2-utils, ruby, rubygems, dnsruby, libopenssl-ruby, java, sqlite3, libsqlite3, libsqlite3-dev, mysql-client, libmysqlclient15, libmysqlclient15-dev

Time Durations: "P3Y6M4DT12H30M5S" represents a duration of "three years, six months, four days, twelve hours, thirty minutes, and five seconds".

Config Files: In /etc/opendnssec/

conf.xml - - - - The overall configuration of OpenDNSSEC (logging, repositories, privileges, and the databases).

kasp.xml - - - - (Key And Signing Policies) Defines policies used to sign zones.

zonelist.xml - - First setting up the system, but also used by the *ods-signerd* when signing zones.

zonefetch.xml - Sign zones received from transfer (AXFR).

ods commands:

ods-ksmutil setup – initial setup for OpenDNSSEC

ods-control start – Starts enforcer and signing engine

ods-control stop - Stops enforcer and signing engine

ods-ksmutil zone add --zone example.com [--policy <policy> --signerconf <signerconf.xml> --input <input> --output <output>]

ods-ksmutil zone delete --zone example.com

ods-ksmutil update zonelist

This will now show in logs:

ods-enforcerd: Zone example.com found.

ods-enforcerd: Policy for example.com set to default.

ods-enforcerd: Config will be output to /var/opendnssec/signconf/example.com.xml.

ods-ksmutil backup prepare --repository <repository> or just ods-ksmutil backup prepare for all repositories

ods-ksmutil backup commit --repository <repository> or just ods-ksmutil backup commit for all repositories

ods-ksmutil key list –verbose

For manual key rollover, or add commands to a cron job

ods-ksmutil key rollover --zone example.com --keytype KSK (ZSK)

The KSK rollover also requires the adding of the new DSKEY record to the Zone, and submission of the DS record to the parent.

When the new DS record is in the parent...

ods-ksmutil key ds-seen -z example.com -x 22499

or

ods-ksmutil key ds-seen -z example.com -k 9621ca39306ce050e8dd94c5ab837001

To extract the trust anchors:

ods-ksmutil key export --zone example.com For DNSKEY in Bind Format:

ods-ksmutil key export --zone example.com --ds For DS in Bind Format:

If you change a policy:

ods-ksmutil update kasp

If you update an unsigned zone:

ods-signer sign example.com

ods-control ksm|hsm|signer|start|stop

The first three options pipe commands to *ods-ksmutil*, *ods-hsmutil*, and *ods-signer*.

The last two options start and stop the two daemons of OpenDNSSEC, *ods-enforcerd* and *ods-signerd*.

Ods-ksmutil interfaces with the KASP enforcer

To add a zone:

ods-ksmutil zone add -z example.com -p default -i /var/example.com -o /var/example.com.si

ods-signer Interface to the ods-signerd

cmd> help

Commands:

zones show the currently known zones

sign <zone> read zone and schedule zone for immediate (re-)signing

sign --all read all zones and schedule all for immediate (re-)signing.

clear <zone> delete the internal storage of this zone.

queue	show the current task queue.
flush	execute all scheduled tasks immediately.
update <zone>	update this zone signer configurations.
update [--all]	update zone list and all signer configurations.
start	start the engine.
reload	reload the engine.
stop	stop the engine.
verbosity <nr>	set verbosity.

ods-auditor does an audit of the zones in the system to see if the signer complies to what the policy mandates.
ods-auditor -z <zone>

ods-signerd -h
Usage: ods-signerd [OPTIONS]
Supported options:

ods-enforcerd
The Enforcer daemon creates keys if needed (and configured to); it also maintains the states of the keys according to the appropriate policy. As the states of keys change, it communicates these changes to the signer via the configuration files that the signer uses when signing the zones

ods-kaspccheck -h
Usage: ods-kaspccheck [options]
Specific options:
-c, --conf [PATH_TO_CONF_FILE] Path to OpenDNSSEC configuration file
(defaults to the default conf.xml file)
-k, --kasp [PATH_TO_KASP_FILE] Path to KASP policy file

ods-ksmutil key import --cka id <CKA ID> --repository <repository> --zone <zone> --bits