Frequently Asked Questions

On this Page

I manually updated my zone file but the signer is still signing the old zone?

You need to also manually tell the signer to use the new file with the following command:

```
ods-signer sign <zonefile>
```

I have updated the conf/kasp/zonelist.xml file but the new parameters have not been picked up?

For changes to the enforcer section of conf.xml, any change to kasp.xml and any changes to zonelist.xml you must run:

```
ods-ksmutil update all
```

For other changes you may need to restart OpenDNSSEC for the changes to be recognized.

The Signer Engine creates files in the tmp-directory, but nothing is written to the signed-directory. What went wrong?

Is auditing enabled for this zone and is there a finalized file in the tmp-directory?

If yes, then the Auditor does not allow to distribute this zone. Could be that unsupported RR were used, Signer Engine and the Auditor disagree on how to parse the information, or that OpenDNSSEC is not following the policy. Check the log to see what it complained about, or run:

```
ods-auditor -s <path to the "zone".finalized file> -z "zone"
```

If no, then something went wrong in the signing process. Please check the logs and report to the OpenDNSSEC team.

I get this message when doing a manual rollover: “WARNING: key rollover not completed as there are no keys in the ‘ready’ state; ods-enforcerd will try again when it runs next”

OpenDNSSEC makes sure that the zone is secure during the rollover process. This message comes when there is no key that has been published long enough. You probably have no standby keys in your policy. When you initiate the rollover, then OpenDNSSEC first needs to publish the key and after a moment make it active. So do not worry, the rollover process will be finished in a moment.

The message "failed to increment serial" is logged

In the following scenarios the content of the currently signed may be updated by OpenDNSSEC:
1. a key rollover is happening
2. the signer configuration has changed in an other way (the enforcer will issue an ods-signer update <zone> command)
3. the signatures are too old and need to be refreshed, the signer will resign the current zone.

Normally the signer would increment the serial in the signed zone in these cases. However for the specific case where the configuration specifies the "keep" option for the <Serial> value and the serial in the unsigned zone has not been incremented then the signer is blocked from updating the serial and these log messages will be generated.

I am using a Sun Crypto Accelerator (SCA) 6000 under Linux and all HSM operations fail with CKR_HOST_MEMORY

You need to make sure the user running OpenDNSSEC is a member of the opencryptoki group (usually “pkcs11?), or it cannot access the shared memory region used by openCryptoki.

How does OpenDNSSEC provide the DS record to the parent zone?

Currently, manual intervention is required for a KSK rollover. This intervention is a three-stage process that is described in the Uploading a Trust Anchor section of the Running OpenDNSSEC page.

For future versions, we are automating this process as much as possible, including integration points for interfacing with a parent registry.

How can I load the signed zone into my name server?

The configuration file conf.xml holds a specific Signer configuration section. In there, you can configure*NotifyCommand* to be called by the signer after the zone has been successfully signed. You can put %zone and %zonefile in here, which will expand to the name of the zone that was signed and the filename of the signed zone.

For example:

```
<NotifyCommand>nsdc reload<\NotifyCommand>
```

or

```
<NotifyCommand>rndc reload %zone<\NotifyCommand>
```

SoftHSM doesn't work with OpenSC on MacOSX 10.6

If you're building SoftHSM in 64-bit mode (which is the default on 10.6), you need a 64-bit version of OpenSC as well – e.g. the latest OpenSC SCA snapshot.

Note: pkcs11-tool from OpenSC is typically used for low-level PKCS#11 debugging and is not required by OpenDNSSEC.

How can I validation the zones produced by OpenDNSSEC?

In version 1.3 and earlier the auditor function in OpenDNSSEC can be used. In 1.4 the auditor has been removed and suggestions for how to use an external tool to validation the zones are given on the Zone Auditing page.