# Troubleshooting tips



## Something is wrong with www.example.com, what to do?

```
$ ls -al /var/lib/opendnssec/unsigned/example.com
-rw-r--r-- 1 opendnssec opendnssec 1236207 Dec 17 09:17 /var/lib/opendnssec/unsigned/uvt.nl


$ grep ^www /var/lib/opendnssec/unsigned/example.com
www             IN      A       12.34.56.78
```

The file should exist and contain normal DNS records.

Is the unsigned zonefile correct?

```
$ named-checkzone uvt.nl /var/lib/opendnssec/unsigned/example.com
zone example.com/IN: loaded serial 2012121700
OK
```

named-checkzone is part of Bind, any other DNS validator should work

Is the signed zonefile in the right place?

```
$ ls -al /var/lib/opendnssec/signed/example.com
-rw-r--r-- 1 opendnssec opendnssec 26783556 Dec 17 13:17 /var/lib/opendnssec/signed/uvt.nl


$ grep ^www /var/lib/opendnssec/signed/example.com
www.example.com.     3600    IN      A       12.34.56.78
www.example.com.     3600    IN      RRSIG   A 8 3 3600 20121226140702 20121212062213 60069 uvt.nl.
dt4JWUe9IWhkk5pMI0M<ABBREVIATED>Im1quqhd1PH0KdLA1jTUhWB04YkRQZov/xsF0us=
```

If there is no file in that location either 'zonelist.xml' is wrong or the signer is not running. If there are no RRSIGs in the file you are probably looking at the *unsigned* file.

Is the DNS-server working?

```
$ dig +short www.example.com @mydnsserver
12.34.56.78
```

If this fails check if the nameserver is running at all.

### Does the zone served match the zone on disk?

```
$ dig +short -tSOA example.com @mydnsserver
mydnsserver.example.com. hostmaster.example.com. 2012121706 28800 14400 604800 3600


$ head -n1 /var/lib/opendnssec/signed/example.com
example.com. 3600    IN      SOA     mydnsserver.example.com. hostmaster.example.com. 2012121706 28800 14400
604800 3600
```

The SOA should be the same, if there is a difference, use the higher value

Does the DNSKEY served by DNS match the key stored in the HSM?

```
$ dig +short -tDNSKEY example.com @mydnsserver|grep ^257
257 3 8 AwEAAew<ABBREVIATED>jzvVb7LeI+thgsQAgi+EeyN8=


$ grep 'DNSKEY.*257' /var/lib/opendnssec/signed/example.com
example.com. 3600    IN      DNSKEY  257 3 8 AwEAAew<ABBREVIATED>jzvVb7LeI+thgsQAgi+EeyN8= ;{id = 39269 (ksk),
size = 2048b}


$ ods-ksmutil key export --keytype KSK --keystate ACTIVE --zone example.com
;active KSK DNSKEY record:
example.com. 3600    IN      DNSKEY  257 3 8 AwEAAew<ABBREVIATED>jzvVb7LeI+thgsQAgi+EeyN8= ;{id = 39269 (ksk),
size = 2048b}
```

There should be one active KSK.

### Have the signatures on the zone expired?

```
$ grep 'RRSIG.*SOA ' /var/lib/opendnssec/signed/example.com
example.com. 3600    IN      RRSIG   SOA 8 2 3600 20121231023929 20121217120754 60069 example.com.
jeYlzkygV1HJ4PQ9TN1YQ8a9ZjLslsj1H5Z
/MJyGVKWB5JEM9jxqp7foD7qZZ9jQI3+2AB8FRv7BUCb7pfBParRx9XsHEGHhHMf0aIktgxjD41TEGaHufjZj3LToD957qM6BUSOtu9HK0hl7zmf
pz0iCJnd5FzT0bcPvkAf/k2k=
```

Look at the numbers 20121231023929 and 20121217120754 . These are timestamps, the key is only valid in this interval. (carefull, the first value is the expiration date!).

Preventing this situation is one of the primary purposes of OpenDNSSEC.  If this happens you should check that the OpenDNNSEC signer and validator are running. If they are running you should inspect the logs for problems.

### There is not enough information in the logs

Temporarily increase the loglevel by using the ods-signer command:

```
$ ods-signer verbosity 6
```

### OpenDNSSEC doesn't seem to recogninze a zone while other zones work fine.  / Split-DNS doens't work.

OpenDNSSEC requires every zone to have a unique name and a unique outputfile (the inputfile can be shared among several zones). These requirements are more strict than those of the commonly used DNS-servers. Some tricks (like split-horizon DNS) are not yet possible with OpenDNSSEC.