

# External Auditing of Zones

In the 1.4 release of OpenDNSSEC the auditor component has been removed. This component was only lightly used in deployed systems and its removal means that OpenDNSSEC no longer depends on Ruby.

There are a number of third party products available that specialise in generalised zone auditing. It is anticipated that users wishing to audit their zones will use such a product and some recommendations are made below.

## On this Page

- [Workflow](#)
- [Validation Tools](#)
  - [validdns](#)
  - [credns](#)

## Workflow

With no 'in-built' auditing function in OpenDNSSEC one option is to post process the zone. It is possible to do this using the NotifyCommand in conf.xml. An example workflow would be:

- Configure the signer put the signed zone files into an intermediate directory e.g. /signed\_but\_unchecked
- Configure the NotifyCommand in conf.xml to call a script which does the following:
  - Call the validation tool of choice and parse the reply
  - On success: copy the signed zone file into a directory for distribution to a nameserver e.g. /signed\_and\_checked and notify the nameserver
  - On failure: e.g. send an e-mail to prompt further investigation

An alternative solution is that the signed zones from OpenDNSSEC may be transferred to a hidden master and a validation tool may be run before the zones are distributed to the slave servers.

## Validation Tools

### validdns

<http://www.validdns.net/>

### credns

<http://www.nlnetlabs.nl/projects/credns/>