How to manage DNSSEC for domains that are pointed to third party DNS?

Question

What data should I provide to Openprovider to enable DNSSEC management if the zone is hosted on a custom nameserver?

Answer

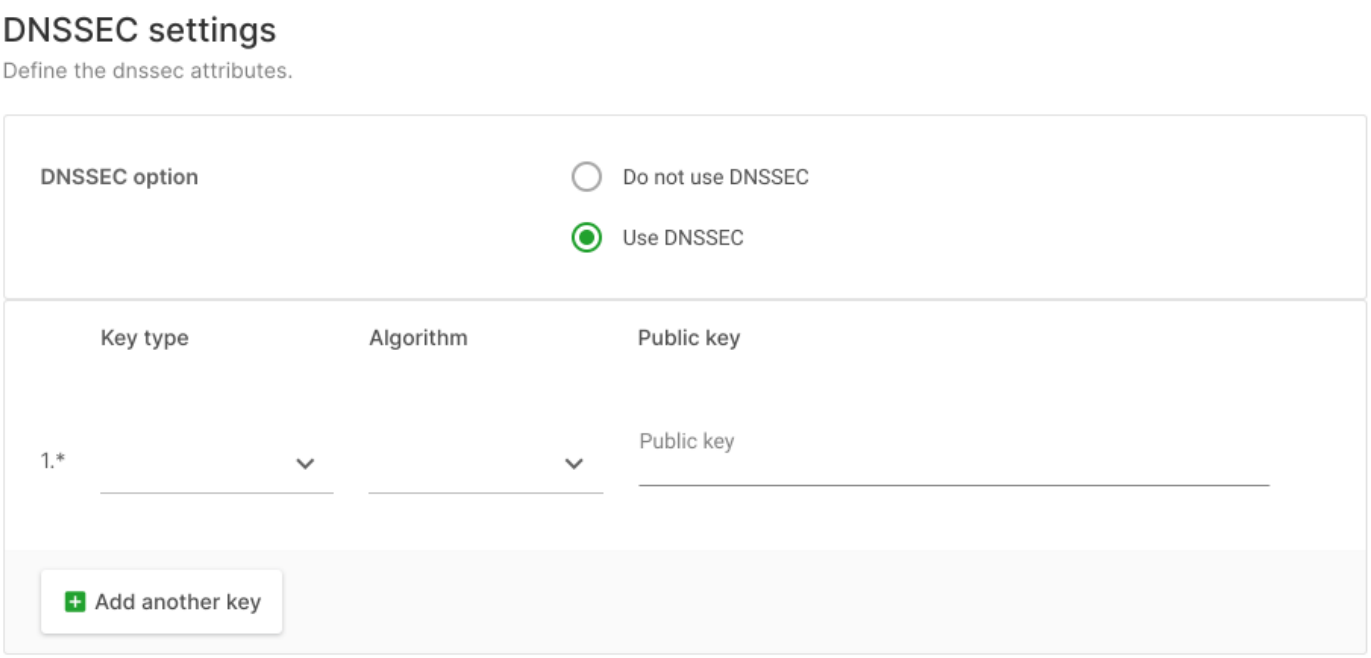
The **DNSSEC** feature for domains pointed to custom nameservers allows to add and manage your DS records.

You can check your configuration here : https://dnsviz.net/

To add a record, one needs to enable DNSSEC first.

Log into your RCP account, select **Domain overview** on the left and click on the **Edit domain data** button for the specified domain.

Once you click **Use DNSSEC** button, the menu to manage your DNSKEY records will appear. To add a new record, fill in the corresponding fields with necessary information:



* **Important**: Not all TLDs/domain extensions allow DNSSEC. The **DNSSEC settings**/**DNSSEC option** will only be shown in RCP (Reseller Control Panel) for TLDs that support DNSSEC.

In RCP each DNSKEY record consists of three fields: Key type, Algorithm and Public key.

There are two types of keys that are used by DNSSEC:

- The zone signing key (**ZSK**) - is used to sign and validate the individual record sets within the zone.
- The key signing key (**KSK**) - is used to sign the DNSKEY records in the zone.

Both of these keys are stored as "DNSKEY" records in the zone file. These values are received from the DNS/hosting provider that hosts your domain zone. If you are not sure where to get the records, please contact your hosting/DNS provider.

Each record consists of three fields: Key type, Algorithm and Public Key.

A DNSKEY record then gets passed to the registry in the following format:

```
secDNS:keyData>
 <secDNS:flags>257</secDNS:flags>
 <secDNS:protocol>3</secDNS:protocol>
 <secDNS:alg>8</secDNS:alg>
 <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
</secDNS:keyData>
```

where the *<secDNS:keyData>* element contains the following child elements:

- **Key type** - a *<secDNS:flags>* element that contains a flags field value as described in Section 2.1.1 of RFC 4034.

- Protocol - a *<secDNS:protocol>* element that contains a protocol field value as described in Section 2.1.2 of RFC 4034. Submitted automatically.
- **Algorithm** - a *<secDNS:alg>* element that contains an algorithm number field value as described in Section 2.1.3 of RFC 4034. Must be set according to the used algorithm.
- **Public key** - a *<secDNS:pubKey>* element that contains an encoded public key field value as described in Section 2.1.4 of RFC 4034.
  The Public key element is represented as a base64Binary with a minimum length of 1.

Once the needed records are added, click on **Save changes** at the bottom of the page.

What to do when the DNSSEC key which your nameserver provider provided does not match this format?

The Openprovider system will only accept the original DNSkey and not a "digests" version / DSDATA of the key.

The reason we have chosen this (for DNSKEY instead of digests / DSDATA) is that registries deal with this in varying ways: some need one format, others the other format. You can make a DSDATA from DNSKEY, but not the other way around. For that reason, the DNSKEY is required as input in Openprovider. We then arrange in the background that the correct format is sent to the registry. Your nameserver provider can provide you with the original DNSkey.

Revision #2
Created 2026-08-07 14:35:50 UTC by Sarath
Updated 2026-08-07 15:51:03 UTC by Sarath