DNSSEC in Openprovider

DNSSEC is an extension to the DNS protocol to increase security across the internet. The following article introduces the concepts of DNSSEC and its implementation in Openprovider.

Background information

The DNS protocol translates a human-readable address like *openprovider.com* into a machine-readable number, known as the IP address. At the moment a domain name is typed into the browser or any other application, your computer will search for the corresponding IP address.

The DNS protocol is not secured: your computer will use the found IP address without the ability to check if it's valid. There is a risk, however small, that the returned IP address is wrong. This can be accidentally, and you'll notice it immediately because the website you expect is not loaded. But it can also be part of a phishing attempt: somebody able to fake the bankofamerica.com website might try to pollute the DNS results. In that case, you expect the website of your bank, you see the website of your bank, but in fact you enter your private data on a fraudulent website.

DNSSEC is an extension to the DNS protocol, and includes digital signatures for each record. This signature can be validated by your computer, and tells two things: the record is created by the source you expect it to be, and the information in it is not altered. That way, you can fully trust the result you get, and be sure you are on the website you want to be.

We have published a separate article dedicated to the DNSSEC validation process and the chain of trust.

An easier start is the interesting introduction into DNSSEC as created by the Dutch registry SIDN, which can be found at dnsseccourse.nl. If you rather view a 2-minute introductory video (created by .no registry Norid), click the link below:

Current state of DNSSEC

After a slow start until around 2010, DNSSEC is now supported by the majority of registries. The Internet Society publishes nice graphs of the current state of adoption within ccTLDs. At the moment of writing (June 2018), the big exceptions are Italy, Argentina and most African countries. For gTLDs DNSSEC is required by ICANN, so the gTLD adoption is 100%.

Note that DNSSEC can only be used as designed if the complete resolving chain, from your computer to the root servers, support DNSSEC. Openprovider supports DNSSEC for most extensions, so if you use the Openprovider nameservers, you can benefit from its advantages without having to maintain a DNSSEC nameserver yourself.

Adoption at the end of the chain (your ISP) becomes more and more common. Google is a good incubator because the Google nameservers, used by many, many internet users, already validate DNSSEC information. If your ISP does not support it yet, know that there are work-arounds in the form of plugins. The number of DNSSEC-secured domains rapidly increases, so the pressure on ISPs to support it grows as well.

DNSSEC vs SSL certificates

Although DNSSEC and SSL certificates both use the same principle for securing data, they should not be mixed up, as they serve a different purpose. DNSSEC *authenticates* the data: the received data is from the source that was expected and is not tampered with. An SSL certificate *encrypts* the transmitted data: no third party can read the data except the server you are sending it to.

DNSSEC does not encrypt any data: a website running on DNSSEC will thus still require an SSL certificate for secure data transmission. This is the perfect combination for your website's security!

However the DANE technology is a combination of both: it stores a domain validated certificates (encryption without authentication) in a DNSSEC secured DNS zone. Because the DNS record is DNSSEC secured, the included certificate can be fully trusted. With this certificate, the traffic can be secured.

DNSSEC on Openprovider nameservers

If you use the nameservers of Openprovider, there's no need to do anything: Openprovider will take care of signing the zones and publishing the corresponding keys in the registry's zone files. Of course, if ever you want a zone to be unsigned, you can easily do so!

DNSSEC on Premium Global Anycast DNS Service

If you use the nameservers of Sectigo (Premium DNS), there's no need to do anything: system will take care of signing the zones and publishing the corresponding keys in the registry's zone files. Of course, if ever you want a zone to be unsigned, you can easily do so!

DNSSEC on third-party nameservers

If you use your own nameservers for your domains or use your own nameservers combined with the Openprovider slave nameserver, you will need to enable DNSSEC in your nameservers first. Check your nameserver's manual for the exact procedures.

Once your zone(s) have been signed, you can provide the corresponding keys (up to a maximum of 4 keys) to the registry, using the API or control panel of Openprovider. Once the key has been published in the registry's zone file, your domain will be secured by DNSSEC.

Note: You only need to select the **Key type** (KSK or ZSK), **Algorithm** (8, 10, 12, 13, 14, 15, or 16), and enter the **Public key** using the API or control panel of Openprovider and don't need to specify **Key Tag.**

DNSSEC, the tricky part: updates

The tricky part of DNSSEC involves nameserver updates on domains which is secured by DNSSEC. These can be regular nameserver updates, but also a domain transfer to or from Openprovider. With good preparation, the update will proceed smoothly and the domain will be secured without interruption.

The key to successful DNSSEC domain updates is timing and the use of multiple keys that are active at the same time. Openprovider supports up to four keys for each domain. We have listed all available kinds of updates in our Knowledge Base.

If there's no opportunity to do the update secured (for example if the current DNS provider cannot or does not want to cooperate), a simple alternative is temporarily disabling DNSSEC for the domain until the update has been fully processed, and then enabling DNSSEC again. Of course, this temporarily reduces the security of the domain.

Check your DNSSEC secured domain

There are a number of useful tools available online to check the configuration of your DNSSEC-secured domain name. Some of them that we especially recommend are:

- VeriSign Labs DNSSEC debugger, clean and quick
- DNSViz, very complete, graphical results
- ZoneMaster, for general DNS checks containing a lot of detailed feedback

For any check, please keep in mind the registry's zonefile update frequency: if you update a .nl domain for example, it will take up to 45 minutes before the registry publishes the new keys in the zonefile. Any checks will have to wait until that moment.

Revision #2
Created 2026-08-07 14:27:35 UTC by Sarath
Updated 2026-08-07 15:45:09 UTC by Sarath