General

Domain Name Security Extensions (DNSSEC) are an extension to the DNS (Domain Name System) that is designed to close Internet security vulnerabilities - such as cache poisoning, DNS redirection, and DNS spoofing.

Terms

- **Key Signing Key** (KSK) – This generates a digital signature for the zone signing key (ZSK).
- **Zone Signing Key** (ZSK) – This generates signatures (or a Resource Record Signature – RRIG) for records in a zone.
- **Registrar** – here you have registered / bought your domain.

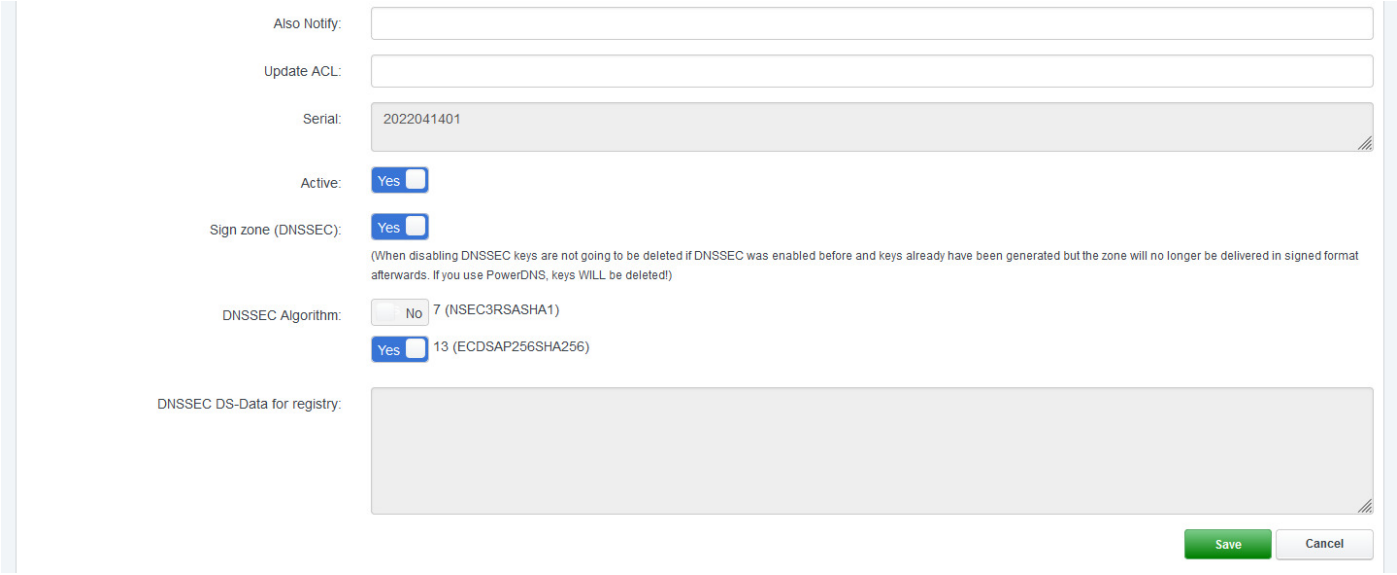
The public part of both keys is stored as a DNSKEY record in the zone itself.

- **DNSKEY** – is the record type for KSK and ZSK. Several ZSK and KSKs can (and must) be stored at the same time.
- **RRSIG** – Signature for a record
- **DS** – Delegation Signer Record – contains the digest for KSK public keys

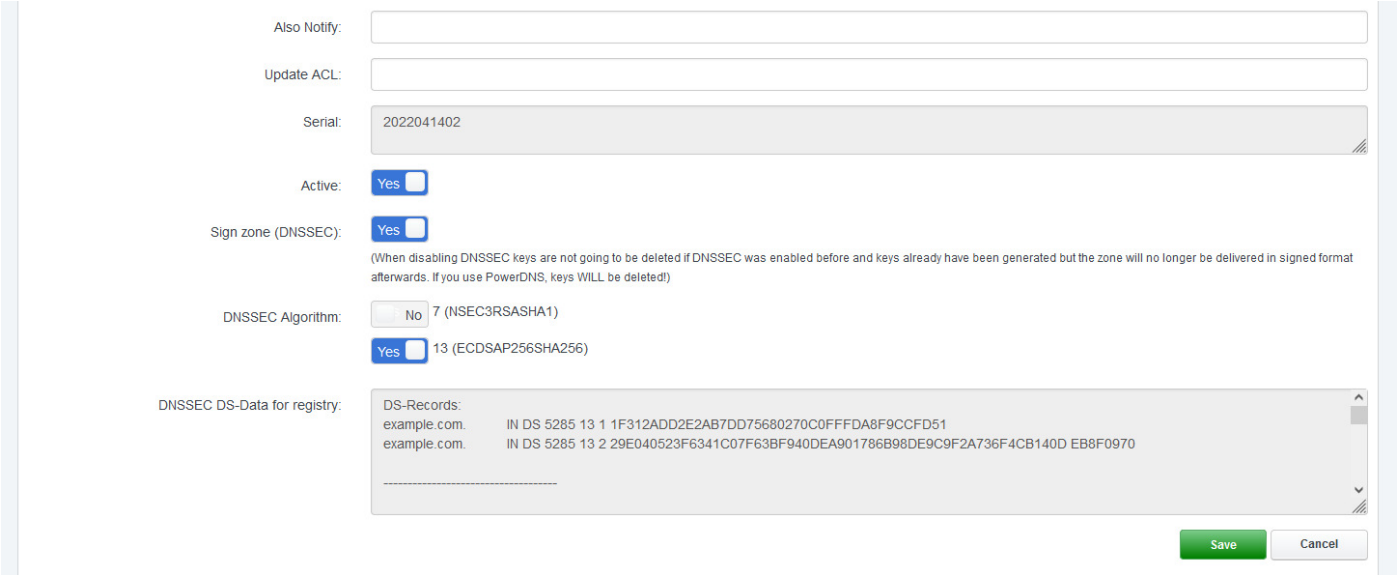
Managed DNSSEC

Enable DNSSEC

To enable DNSSEC, open the corresponding zone in ISPConfig and select the **Zones settings** tab. In the bottom part of the screen you then enable "Sign zone (DNSSEC)" and the DNSSEC algorithm 13. The "DNSSEC algorithm 7" only consists for an existing signing and should not be used anymore.



As soon as you have saved the settings, the DNS zone is signed. This can take up to a minute, after which you will see more information in the "DNSSEC DS-Data for registry" field:



Disable DNSSEC

If you want to disable DNSSEC, you only need to disable "Zone signing (DNSSEC)". You can re-enable DNSSEC later and use the same key pair.

Change DNSSEC algorithm

To switch from the outdated Algorithm 7 to the current Algorithm 13, enable Algorithm 13 and do not disable the old algorithm. After the keys have been regenerated, more information is displayed in the "DNSSEC DS data for registry" field. You will see the key for the old and the new algorithm.

; This is a zone-signing key, keyid **6417**, for example.com.
; Created: 20200812004704 (Wed Aug 12 02:47:04 2020)
; Publish: 20200812004704 (Wed Aug 12 02:47:04 2020)
; Activate: 20200812004704 (Wed Aug 12 02:47:04 2020)
example.com. IN DNSKEY **257** 3 **13** DBOqv9nfRRmR7WoDH6WVSWra2gHkFF9gdvsVyDoyfv2D3oV3pGa2TAqw JMyLIrrB/LqyEnhowR3r9pWNISpbpw==

Here the ID of the key is **6417**, the key signing key is **257** and the algorithm is **13**.

You can now transfer the new data to the registrar. As soon as the new key pair is available (this can take between 4 and 24 hours), you can deactivate the old algorithm.

Data for the registrar

If you zoom in the "DNSSEC DS-Data for registry" field, you will see all the necessary data to enable signing at the registrar.

```
DS-Records:
example.com.        IN DS 5285 13 1 1F312ADD2E2AB7DD75680270C0FFFDA8F9CCFD51
example.com.        IN DS 5285 13 2 29E040523F6341C07F63BF940DEA901786B98DE9C9F2A736F4CB140D EB8F0970

------------------------------------

DNSKEY-Records:
; This is a key-signing key, keyid 5285, for example.com.
; Created: 20220414072825 (Thu Apr 14 09:28:25 2022)
; Publish: 20220414072825 (Thu Apr 14 09:28:25 2022)
; Activate: 20220414072825 (Thu Apr 14 09:28:25 2022)
example.com. IN DNSKEY 257 3 13 64HtBWqU06+M4fPnJw3+BghRSXqZtlc9niMBm4t3TwpT208lIfLZSspV an1oWu0YtRDAO/qwZ/AB23GoVV/NmA==


; This is a zone-signing key, keyid 19850, for example.com.
; Created: 20220414072825 (Thu Apr 14 09:28:25 2022)
; Publish: 20220414072825 (Thu Apr 14 09:28:25 2022)
; Activate: 20220414072825 (Thu Apr 14 09:28:25 2022)
example.com. IN DNSKEY 256 3 13 9JbLeJh7nkgs5M41kYUsBd3JLIMH4hhTBb6hUD+OXIXIkWtAHC7DTzQ+ HIJcAknBVbe5JlzQ+FolKPrgUHsaYA==
```

Unfortunately, it depends on the registrar how you have to submit the data. Some offer a suitable area in the management, while others only allow you to do this manually. In any case you have to transfer DS records and DNSKEY records.

DNSSEC - Domain Name System Security Extensions

What is DNSSEC?

The Domain Name Security Extensions (DNSSEC) are an extension of the DNS (Domain Name System) to prevent security breaches on the Internet (e.g. DNS redirection or DNS spoofing).

With classic DNS queries, it is assumed that the answer is correct and comes from the right source. In the past, there have been isolated cases in which misinformation was deliberately introduced into DNS caches (so-called cache poisoning).

The potential risk was already recognized in the nineties of the last century. The Internet Engineering Task Force (IETF) reacted to this - initially theoretical - threat and published the three RFCs RFC 4033, RFC 4034 and RFC 4035 in March 2005, thus clearing the way for DNSSEC.

Which protection does DNSSEC provide?

For the user, it is elementary that, for example, the website displayed actually corresponds to the one he wanted to access.

DNSSEC is used to secure the path from the request (entry of the domain) to the response (display of the web page). The query between DNS servers and validating DNS applications is secured. The signature used can be used to check authenticity, i.e. whether the data originates from the authoritative zone. At the same time, it prevents the DNS data from being falsified in transit.

Whether the original data of a website is correct or harmless, or whether the accessed website is a fake, cannot be detected with DNSSEC. It also cannot be used to detect domain hijacking or interference in registration processes.

How DNSSEC works

DNSSEC verifies a query by cryptographically secured signatures.

The data is checked in the client or in the resolver in front of it against the public keys matching the respective zone. These keys can be stored and retrieved from DNS servers. No breach of the security mechanism is possible here, since the transfer of the keys is also secured with the help of DNSSEC. Only the key required for the start of the chain (the key of the root zone) is permanently stored in the client or specified by configuration.

Test DNSSEC

To check the use of DNSSEC of a DNS zone or to test it altogether, the website https://dnsviz.net/ is a good place to start.