Allgemein

Domain Name Security Extensions (DNSSEC) sind eine Erweiterung des DNS (Domain Name System), die darauf abzielt, Sicherheitslücken im Internet - wie Cache-Poisoning, DNS-Umleitungen und DNS-Spoofing - zu schließen.

Begriffe

- **Key Signing Key** (KSK) – Unterschreibt Zone Signing Key (ZSK)
- **Zone Signing Key** (ZSK) – Unterschreibt einzelne Einträge des Zonefiles
- **Registrar** – hier hast Du Deine Domain registriert / gekauft.

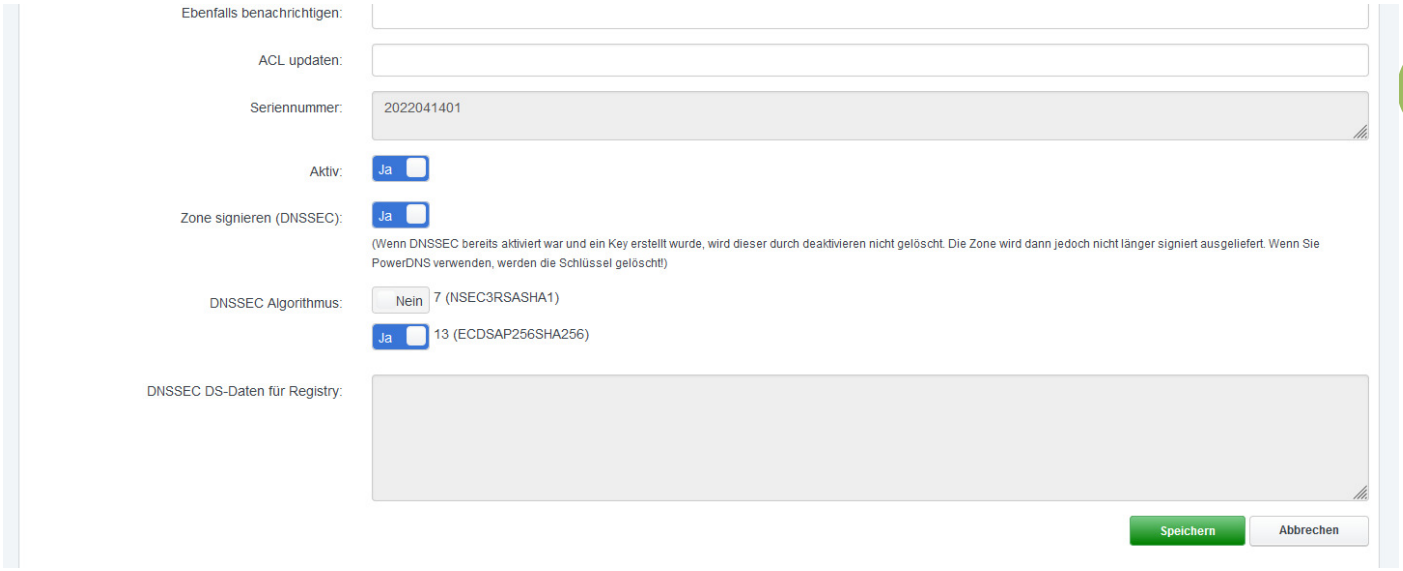
Der Public-Anteil der beiden Keys steht als DNSKEY als Record in der Zone selbst.

- **DNSKEY** – Record Typ für KSK und ZSK. Es können (und müssen) gleichzeitig mehrere ZSK und KSK hinterlegt sein.
- **RRSIG** – Signatur eines Records
- **DS** – Delegation Signer Record - Enthält den Digest des KSK Public Keys

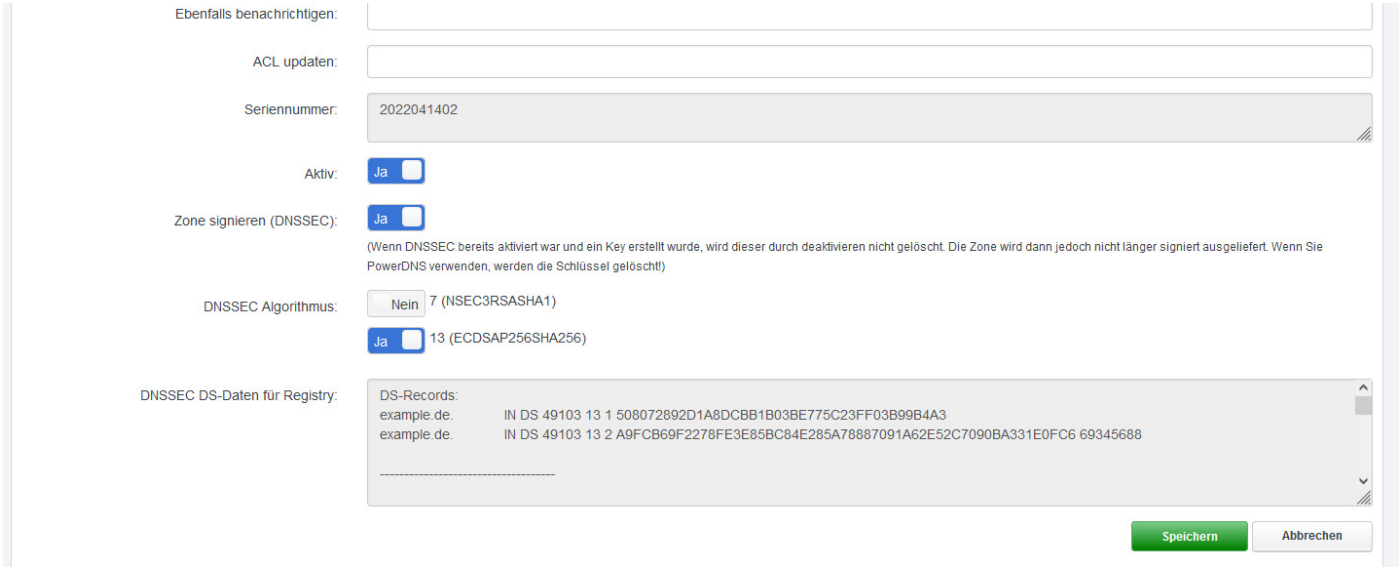
DNSSEC verwalten

DNSSEC aktivieren

Um DNSSEC zu aktivieren, öffnest Du in ISPConfig die entsprechende Zone und wählst den Reiter **Zonen Einstellungen**. Im unteren Teil der Maske aktivierst Du dann „Zone signieren (DNSSEC)“ und den DNSSEC Algorithmus 13. Der „DNSSEC Algorithmus 7“ existiert nur für eine bestehende Signierung und sollte nicht mehr verwendet werden.



Sobald Du die Einstellungen gespeichert hast, wird die DNS-Zone signiert. Dies kann bis zu einer Minute dauern, danach bekommst Du dann im Feld „DNSSEC DS-Daten für Registry“ weitere Informationen angezeigt:



DNSSEC deaktivieren

Wenn Du DNSSEC abschalten willst, musst Du nur „Zone signieren (DNSSEC)“ abschalten. Du kannst DNSSEC später wieder aktivieren und das gleiche Schlüsselpaar verwenden.

DNSSEC Algorithmus wechseln

Um vom veralteten Algorithmus 7 auf den aktuellen Algorithmus 13 zu wechseln, aktivierst Du den Algorithmus 13 und **deaktivierst nicht** den alten Algorithmus. Nachdem die Schlüssel neu generiert wurden, werden Dir weitere Informationen im Feld „DNSSEC DS-Daten für Registry“ angezeigt. Du siehst dann den Key für den alten und den neuen Algorithmus.

; This is a zone-signing key, keyid **6417**, for example.de.
; 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.de. IN DNSKEY **257** 3 **13** DBOqv9nfRRmR7WoDH6WVSWra2gHkFF9gdvsVyDoyfv2D3oV3pGa2TAqw JMyLIrrB/LqyEnhowR3r9pWNISpbpw==

Hier ist die ID des Keys **6417**, der Key Signing Key ist **257** und der Algorithmus **13**.

Die neuen Daten kannst Du jetzt an den Registrar übertragen. Sobald das neue Schlüsselpaar verfügbar ist (das kann zwischen 4 und 24 Stunden dauern), kannst Du den alten Algorithmus deaktivieren.

Daten für den Registrar

Wenn Du das Feld „DNSSEC DS-Daten für Registry“ vergrößerst, werden Dir alle erforderlichen Daten angezeigt, um beim Registrar die Signierung zu aktivieren.

```
DS-Records:
example.de.        IN DS 49103 13 1 508072892D1A8DCBB1B03BE775C23FF03B99B4A3
example.de.        IN DS 49103 13 2 A9FCB69F2278FE3E85BC84E285A78887091A62E52C7090BA331E0FC6 69345688

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

DNSKEY-Records:
; This is a zone-signing key, keyid 4078, for example.de.
; Created: 20220414054748 (Thu Apr 14 07:47:48 2022)
; Publish: 20220414054748 (Thu Apr 14 07:47:48 2022)
; Activate: 20220414054748 (Thu Apr 14 07:47:48 2022)
example.de. IN DNSKEY 256 3 13 yheULHp6iKqWWXpl+6gstjXVO+BPGBqHS9ZJOTIdal4NA83Lbe8tTEQH eBpYs9TcpCEgbfMW0+qUuNKKWEy0LA==


; This is a key-signing key, keyid 49103, for example.de.
; Created: 20220414054748 (Thu Apr 14 07:47:48 2022)
; Publish: 20220414054748 (Thu Apr 14 07:47:48 2022)
; Activate: 20220414054748 (Thu Apr 14 07:47:48 2022)
example.de. IN DNSKEY 257 3 13 XFLpL0kVSC4dVRa4vMBeE6DAqzGFoAVtSCn5aXmlK97uL4Rhu+sxRsw8 ajXX9da8qZ//ZU8ZAg+HH+WG619BBA==
```

Es hängt leider vom jeweiligen Registrar ab, wie Du die Daten übermitteln musst. Einige bieten dazu einen passenden Bereich in der Verwaltung, bei anderen geht dies nur manuell.

In jedem Fall musst Du DS-Records und die DNSKEY-Records übertragen.

DNSSEC - Domain Name System Security Extensions

Was ist DNSSEC?

Die Domain Name Security Extensions (DNSSEC) sind eine Erweiterung des DNS (Domain Name System), um Sicherheitslücken im Internet (z.B. DNS-Umleitungen oder DNS-Spoofing) zu verhindern.

Bei klassischen DNS-Anfragen wird davon ausgegangen, dass die Antwort zutreffend ist und von der richtigen Quelle stammt. In der Vergangenheit hat es vereinzelt Fälle gegeben, bei denen gezielt Fehlinformationen in DNS-Caches eingebracht wurde (sog. Cache-Poisoning).

Das potenzielle Risiko wurde bereits in den neunziger Jahren des letzten Jahrhunderts erkannt. Die Internet Engineering Task Force (IETF) hat auf diese – zunächst theoretische – Bedrohung reagiert und im März 2005 die drei RFCs RFC 4033, RFC 4034 und RFC 4035 veröffentlicht und damit den Weg für DNSSEC frei gemacht.

Welchen Schutz bietet DNSSEC?

Für den Nutzer ist es elementar, dass z. B. die angezeigte Webseite auch tatsächlich derjenigen entspricht, die er aufrufen wollte.

Mittels DNSSEC wird der Weg von der Anfrage (Eingabe der Domain) bis zur Antwort (Anzeige der Webseite) abgesichert. Dabei wird die Abfrage zwischen DNS-Servern und validierenden DNS-Anwendungen abgesichert. Anhand der verwendeten Signatur lässt sich die Echtheit prüfen, d.h. ob die Daten aus der autoritativen Zone stammen. Gleichzeitig wird verhindert, dass die DNS-Daten auf dem Transportweg verfälscht werden können.

Ob die ursprünglichen Daten einer Webseite richtig oder harmlos sind oder ob die aufgerufene Webseite eine Fälschung ist, kann mit DNSSEC nicht erkannt werden. Auch Domain-Hijacking oder Eingriffe in Registrierungsprozesse lassen sich damit nicht feststellen.

Wie funktioniert DNSSEC?

Durch DNSSEC wird eine Abfrage mittels kryptografisch gesicherter Signaturen verifiziert.

Die Prüfung der Daten erfolgt im Client oder in dem davor liegenden Resolver gegenüber den zur jeweiligen Zone passenden öffentlichen Schlüsseln. Diese Schlüssel können DNS-Server hinterlegt und abgerufen werden. Dabei ist kein Bruch des Sicherheitsmechanismus möglich, da auch der Transfer der Schlüssel mit Hilfe von DNSSEC abgesichert erfolgt. Lediglich der für den Beginn der Kette notwendige Schlüssel (der Key der Root-Zone) wird im Client fest hinterlegt oder per Konfiguration festgelegt.

DNSSEC überprüfen

Um die Nutzung von DNSSEC einer DNS-Zone zu überprüfen oder diese insgesamt zu testen, bietet sich die Webseite https://dnsviz.net/ an.