DNS + Nameserver

- DNS (Domain Name System)
- Die 3 Server zum Laden einer Webseite
- DNS-Zone
- DNSSEC

DNS (Domain Name System)

Was ist ein DNS?

DNS oder auch "Domain Name System" ist wie das Telefonbuch des Internets. Jedes Gerät, dass mit dem Internet verbunden ist, hat eine eindeutige IP-Adresse. (z. B. 10.12.15.257)

Web-Browser benutzen die IP-Adressen zur Interaktion. Damit man die IP-Adressen nicht jedes mal eingeben muss, um auf eine Website zu gelangen, übersetzt DNS die Domain-Namen um, damit die Ressourcen im Browser geladen werden können.

Wie funktioniert DNS?

Um eine DNS aufzulösen, benötigt man einen Hostnamen (z. B. alexandergreub.ch) damit der Computer die Domain in eine verständliche IP-Adresse umwandeln kann.

Jedes Gerät, dass sich mit dem Internet verbindet, erhält eine IP-Adresse, damit das Gerät gefunden werden kann, wie z. B. eine Postanschrift bei einem Haus.

Es gibt 2 Verschieden Arten von IP-Adressen:

- IPv4 Adressen: Diese Adressen sind die zurzeit gängigsten und bekanntesten IP-Adressen. Sie teilen sich in 4 Dezimalzahlen und haben eine Range von 1 - 255. Leider kommen IPv4 Adressen immer mehr an eine Grenze, da es nur eine begrenzte Anzahl gibt. Bei IPv4 Adressen gibt es nur 4 Milliarden mögliche Kombinationen, deswegen wird immer mehr auf IPv6 umgestellt.
- IPv6 Adressen: Diese Adressen werden in Zukunft immer mehr vorkommen, da sie das Hexadezimal-System verwenden. Das heisst sie bestehen aus Zahlen und Buchstaben. IPv6 werden aber nicht so gern verwendet, da sie sehr lang und kompliziert werden können. (z. B. **2001:0db8:85a3:08d3:1319:8a2e:0370:7344**)

Kürzungsschema für IPv6-Adressen	
Originaladresse	2001:0db8:0000:0000:08d3:8a2e:0070:7344
ohne führende Nullen	2001:db8:0:0:8d3:8a2e:70:7344
ohne Blöcke aus Nullen	2001: db8: : : 8d3:8a2e: 70:7344
Kurzform	2001:db8::8d3:8a2e:70:7344

IP-Adresse nach IPv4

192.168.2.105

- 8 Bit großer Zahlenblock

- Dezimal im Bereich zwischen 0 bis 255

- bestehend aus 4 Zahlenblöcken

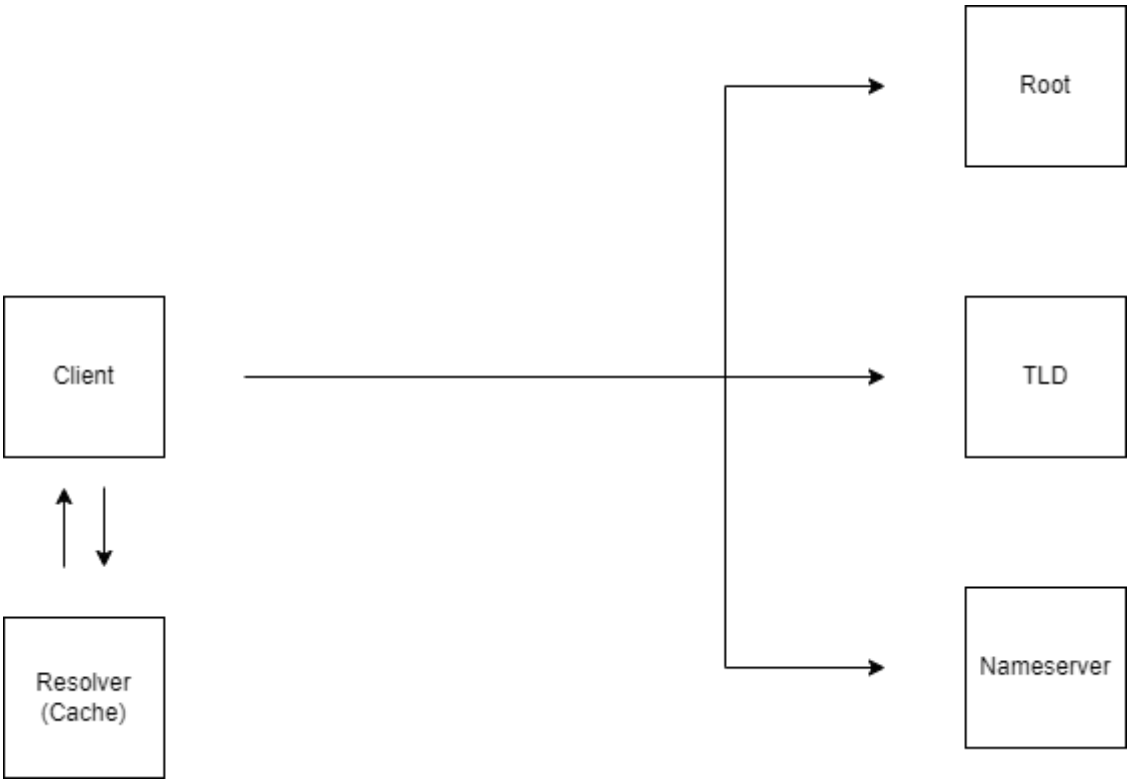
Hilfreiche Ressourcen:

https://www.cloudflare.com/de-de/learning/dns/what-is-dns/

Die 3 Server zum Laden einer Webseite

Damit eine Webseite geladen werden kann, braucht es noch 3 Schritte.

- **Der rekursive DNS Resolver** - Der DNS Resolver ist ein Server, der die Anfragen der Clients, die z. B. eine Domain im Browser eintippen empfängt und sendet die Anfrage weiter an die nächsten zuständigen Sever. Falls eine Webseite schon einmal aufgerufen wurde, wird sie im sogenannten Cache gespeichert, damit die Domain z. B. erscheint, wenn man nur ein paar Buchstaben eintippt.
  Diese Server sind auch beliebte Angriffsziele für Hacker, da der Traffic sehr hoch sein kann.
- **Der DNS Nameserver** - Bei Webland gibt es 4 Nameserver. NS1 und NS2 sind die Hauptnameserver und NS3 sowie NS4 sind Backup Server. Bei den Nameservern sind die Domaininformationen einer Webseite hinterlegt.
- **Der DNS Root Nameserver** - Es gib insgesamt 8 Root-Server. Die Root-Zone beinhaltet die Informationen aller Top-Level-Domains (TLD). Jeder Rechner der mit dem Internet verbunden ist, ist bei einem Root-Server zugewiesen.
- **Der TLD Nameserver** - Diese Server sind Länderspezifisch und werden vom Root-Server angefragt und werden



Ablauf einer DNS-Anfrage

Zur Repetition beschreibe ich kurz die einzelnen Schritte einer DNS-Abfrage für www.alexandergreub.ch, um darauf aufbauen zu können:

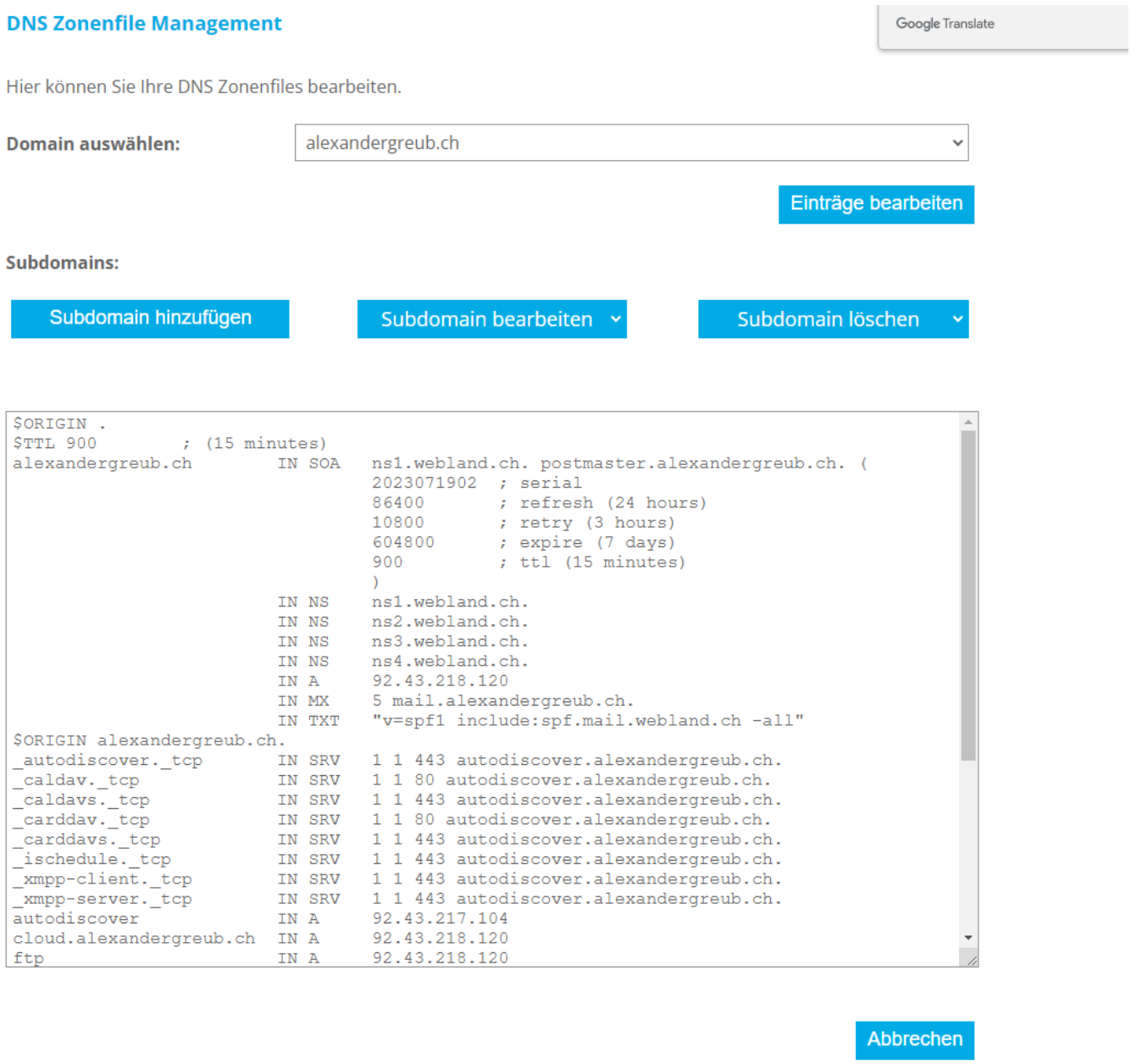
- Der Client durchsucht zuerst seine Host-Datei und anschliessend seinen DNS-Cache, ob dort alexandergreub.ch mit der dazugehörigen IP-Adresse hinterlegt ist.
- Falls nicht, leitet der Client die DNS-Anfrage an seinen DNS-Resolver weiter. Wenn der DNS-Resolver die IP-Adresse zu alexandergreub.ch nicht in seinem Cache hat, kontaktiert er als nächstes einen Root-Nameserver. Der Root-Nameserver sendet die IP-Adressen der «.ch»-Zone-Nameserver an den DNS-Resolver zurück.
- Nun sendet der DNS-Resolver die DNS-Anfrage an einen der «.ch»-Zone-Nameserver (z.B. nic.ch). Dieser wiederum sendet die IP-Adresse der autoritativen Nameserver für tec-bite.ch zurück.
- Als nächster Schritt sendet der DNS-Resolver die DNS-Anfrage an den autoritativen Nameserver von alexandergreub.ch. Dieser antwortet anschliessend mit der IP-Adresse welche für alexandergreub.ch hinterlegt ist.
- Der DNS-Resolver sendet die erhaltene Antwort an den Client.

DNS-Zone

Erklärung der DNS-Zoneneinträge

`A`	IPv4 Adresse
`AAAA`	IPv6 Adresse
`MX`	Mail-Server
`SRV`	Gibt einen Host und einen Port für bestimmte Dienste an (z.B. Instant Messaging, Kalender, VoIP)
`NS`	Autoritative Nameserver
`TXT`	Texteintrag (z. B. zur Unterbindung von Spam)
`CNAME`	Kanonischer Name (z. B. Verweis von einer Domain, wenn ein Alias besteht)

Zonen-File im System Configurator



Zonen-Editor im WLCM

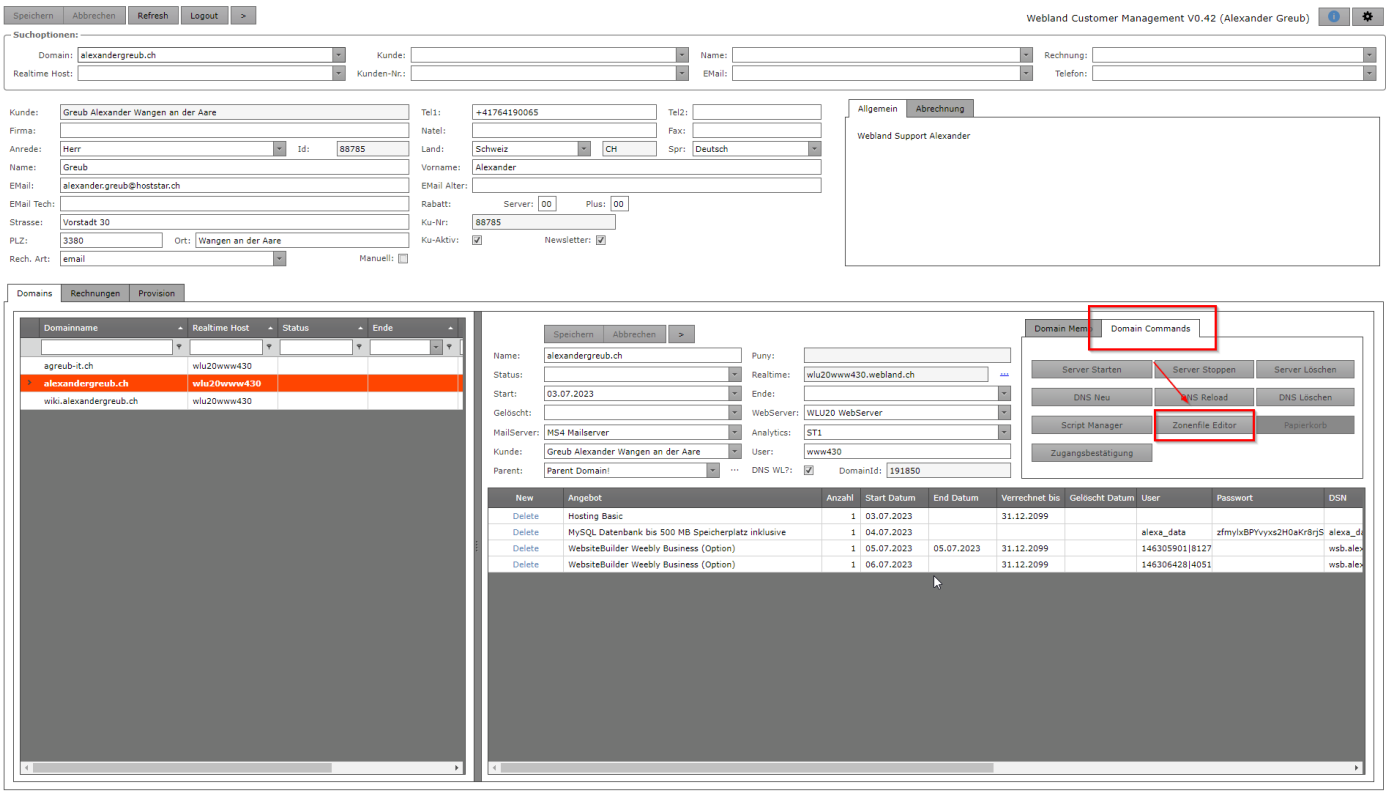
Zone File Editor

Domain: **alexandergreub.ch**

```
$ORIGIN .
$TTL 900        ; (15 minutes)
alexandergreub.ch        IN SOA   ns1.webland.ch. postmaster.alexandergreub.ch. (
                                  2023071902  ; serial
                                  86400       ; refresh (24 hours)
                                  10800       ; retry (3 hours)
                                  604800      ; expire (7 days)
                                  900         ; ttl (15 minutes)
                                  )
                         IN NS    ns1.webland.ch.
                         IN NS    ns2.webland.ch.
                         IN NS    ns3.webland.ch.
                         IN NS    ns4.webland.ch.
                         IN A     92.43.218.120
                         IN MX    5 mail.alexandergreub.ch.
                         IN TXT   "v=spf1 include:spf.mail.webland.ch -all"
$ORIGIN alexandergreub.ch.
_autodiscover._tcp       IN SRV   1 1 443 autodiscover.alexandergreub.ch.
_caldav._tcp             IN SRV   1 1 80 autodiscover.alexandergreub.ch.
_caldavs._tcp            IN SRV   1 1 443 autodiscover.alexandergreub.ch.
_carddav._tcp            IN SRV   1 1 80 autodiscover.alexandergreub.ch.
_carddavs._tcp           IN SRV   1 1 443 autodiscover.alexandergreub.ch.
_ischedule._tcp          IN SRV   1 1 443 autodiscover.alexandergreub.ch.
_xmpp-client._tcp        IN SRV   1 1 443 autodiscover.alexandergreub.ch.
_xmpp-server._tcp        IN SRV   1 1 443 autodiscover.alexandergreub.ch.
autodiscover             IN A     92.43.217.104
cloud.alexandergreub.ch  IN A     92.43.218.120
ftp                      IN A     92.43.218.120
imap                     IN A     92.43.217.104
mail                     IN A     92.43.217.104
pop                      IN A     92.43.217.104
smtp                     IN A     92.43.217.104
wiki                     IN A     92.43.218.120
www.wiki                 IN A     92.43.218.120
wp                       IN A     92.43.218.120
www.wp                   IN A     92.43.218.120
wsb                      IN A     92.43.219.74
www.wsb                  IN A     92.43.219.74
```

☐ Zonen File editieren (Vorsicht!)

Speichern Abbrechen


Speichern
Abbrechen
Refresh
Logout
>
Webland Customer Management V0.42 (Alexander Greub)
Suchoptionen:
Domain: alexandergreub.ch
Realtime Host:
Kunde:
Kunden-Nr.:
Name:
EMail:
Rechnung:
Telefon:
Kunde: Greub Alexander Wangen an der Aare
Firma:
Anrede: Herr
Id: 88785
Name: Greub
EMail: alexander.greub@hoststar.ch
EMail Tech:
Strasse: Vorstadt 30
PLZ: 3380
Ort: Wangen an der Aare
Rech. Art: email
Manuell:
Tel1: +41764190065
Natel:
Land: Schweiz
CH
EMail Alter:
Rabatt:
Server: 00
Plus: 00
Ku-Nr: 88785
Ku-Aktiv:
Tel2:
Fax:
Spr: Deutsch
Vorname: Alexander
Newsletter:
Allgemein
Abrechnung
Webland Support Alexander
Domains
Rechnungen
Provision
Domainname
Realtime Host
Status
Ende
agreub-it.ch
wlu20www430
alexandergreub.ch
wlu20www430
wiki.alexandergreub.ch
wlu20www430
Speichern
Abbrechen
>
Name: alexandergreub.ch
Status:
Start: 03.07.2023
Gelöscht:
MailServer: MS4 Mailserver
Kunde: Greub Alexander Wangen an der Aare
Parent: Parent Domain!
Puny:
Realtime: wlu20www430.webland.ch
Ende:
WebServer: WLU20 WebServer
Analytics: ST1
User: www430
DNS WL?:
DomainId: 191850
Domain Mem
Domain Commands
Server Starten
Server Stoppen
Server Löschen
DNS Neu
DNS Reload
DNS Löschen
Script Manager
Zonenfile Editor
Papierkorb
Zugangsbestätigung
New
Angebot
Anzahl
Start Datum
End Datum
Verrechnet bis
Gelöscht Datum
User
Passwort
DSN
Delete
Hosting Basic
1
03.07.2023
31.12.2099
Delete
MySQL Datenbank bis 500 MB Speicherplatz inklusive
1
04.07.2023
alexa_data
zfmylxBPYvyxs2H0aKr8rjS
alexa_d
Delete
WebsiteBuilder Weebly Business (Option)
1
05.07.2023
05.07.2023
31.12.2099
146305901|8127
wsb.alex
Delete
WebsiteBuilder Weebly Business (Option)
1
06.07.2023
31.12.2099
146306428|4051
wsb.alex

DNSSEC

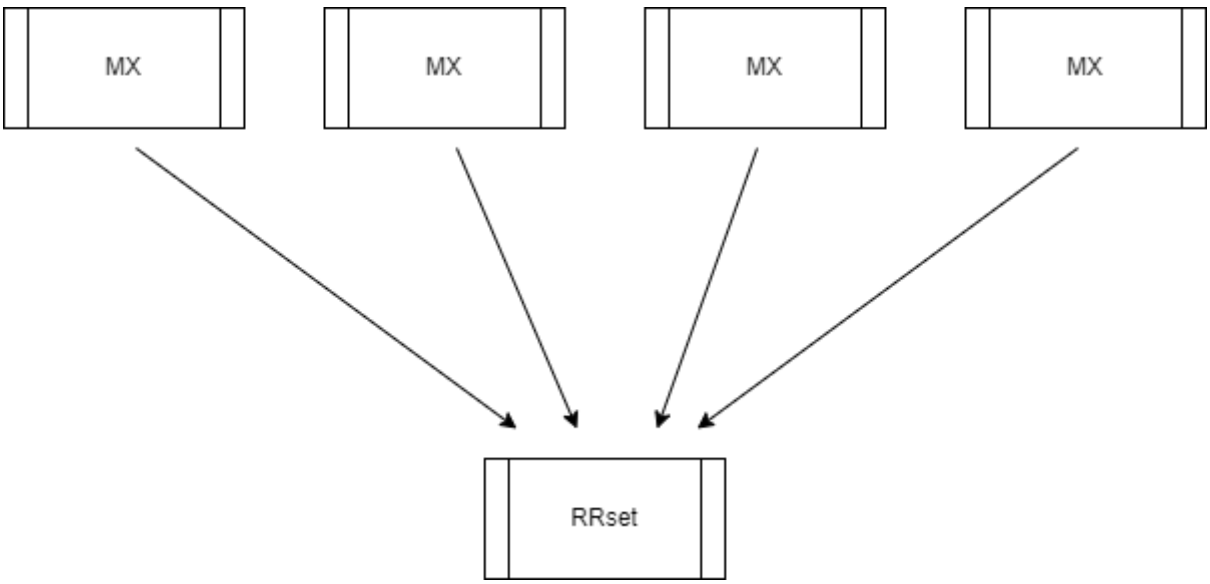
DNSSEC steht für "Domain Name System Security Extension" die das DNS mit verschiedenen Sicherheitsmöglichkeiten erweitert.

Bei der DNS Abfrage wird der ein gesamter Durchlauf durchgeführt, d.h. Der Länder-Nameserver, der Root Server und der Autoritative Nameserver wird angesprochen. Bei allen Server müssen die DNSSEC Daten vorhanden sein, damit die Abfrage erfolgreich ist.

> Auflistung der DNSSEC Abfrage: DNSSEC

Einträge

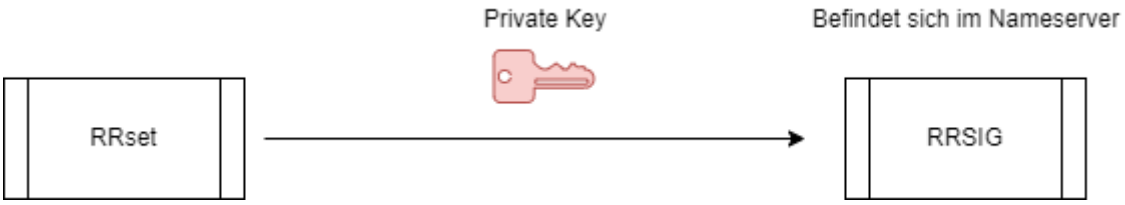
`RRSIG`	Enthält eine kryptographische Signatur
`DNSKEY`	Enthält einen Public Key
`DS`	Enthält den Hash eines DNSKEY Eintrags
`NSEC und NSEC3`	Für die explizite Anerkennung eines Nicht-Existenten DNS Eintrags
`CDNSKEY und CDS`	Für die untergeordnete Zone zur Anfrage von Aktualisierungen eines DNS Eintrags in der Übergeordneten Zone



Definition eines RRset

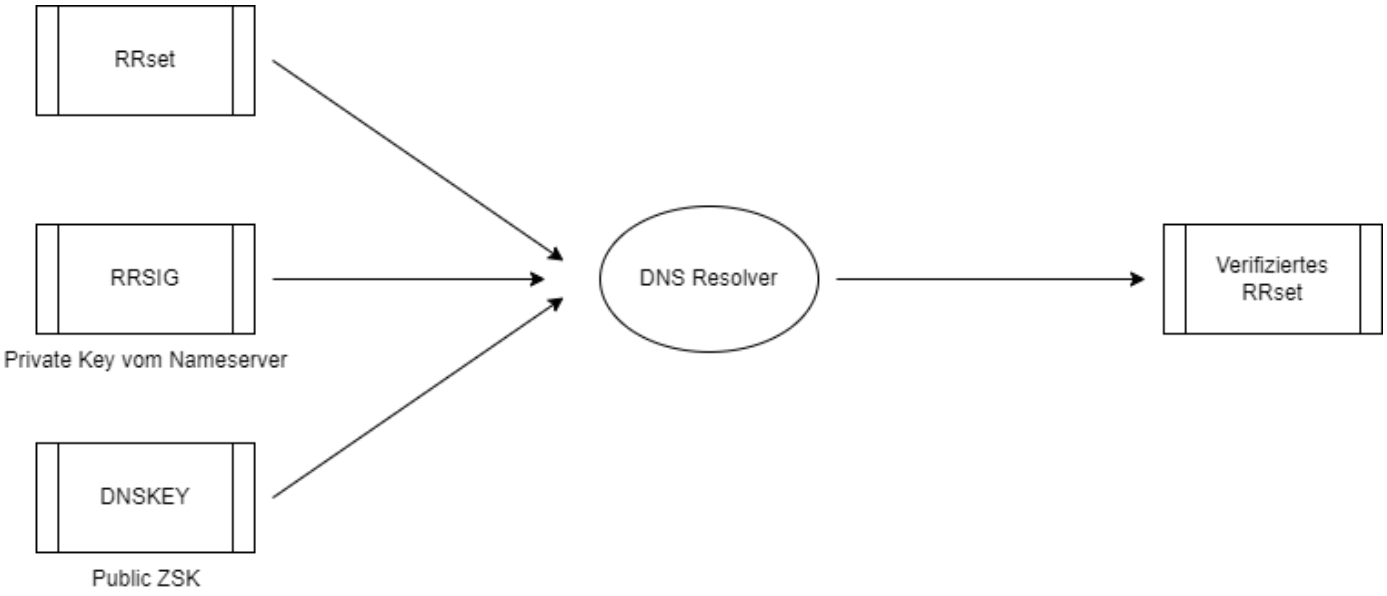
Beim RRset werden Einträge mit dem gleichen Namen und Typ gebündelt.

ZSK (Zone Signing Key)



Definition des RRSIG Eintrags

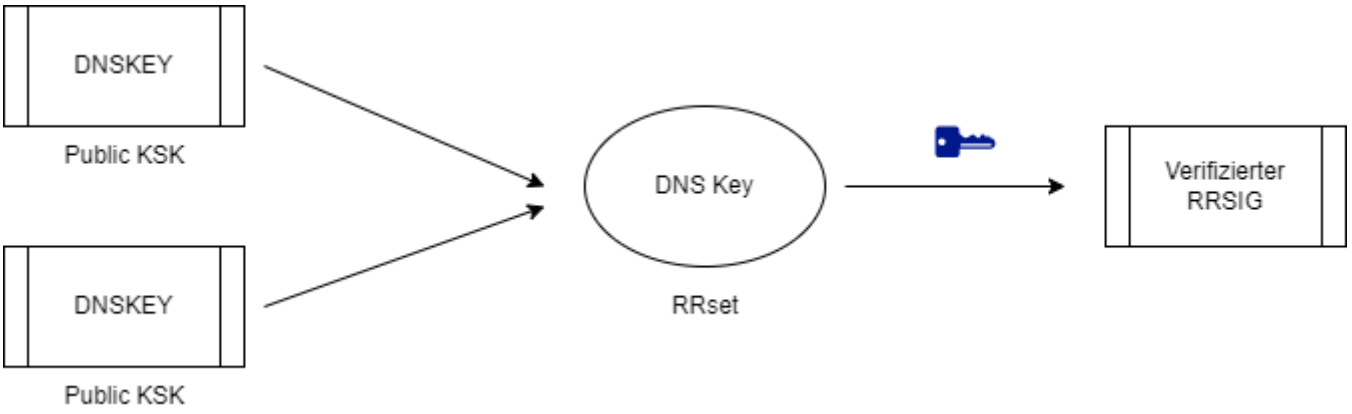
Im RRSIG Eintrag befinden sich die Daten des Private Key und werden beim Zonenbetreiber im Nameserver hinterlegt.



Schema des ZSK

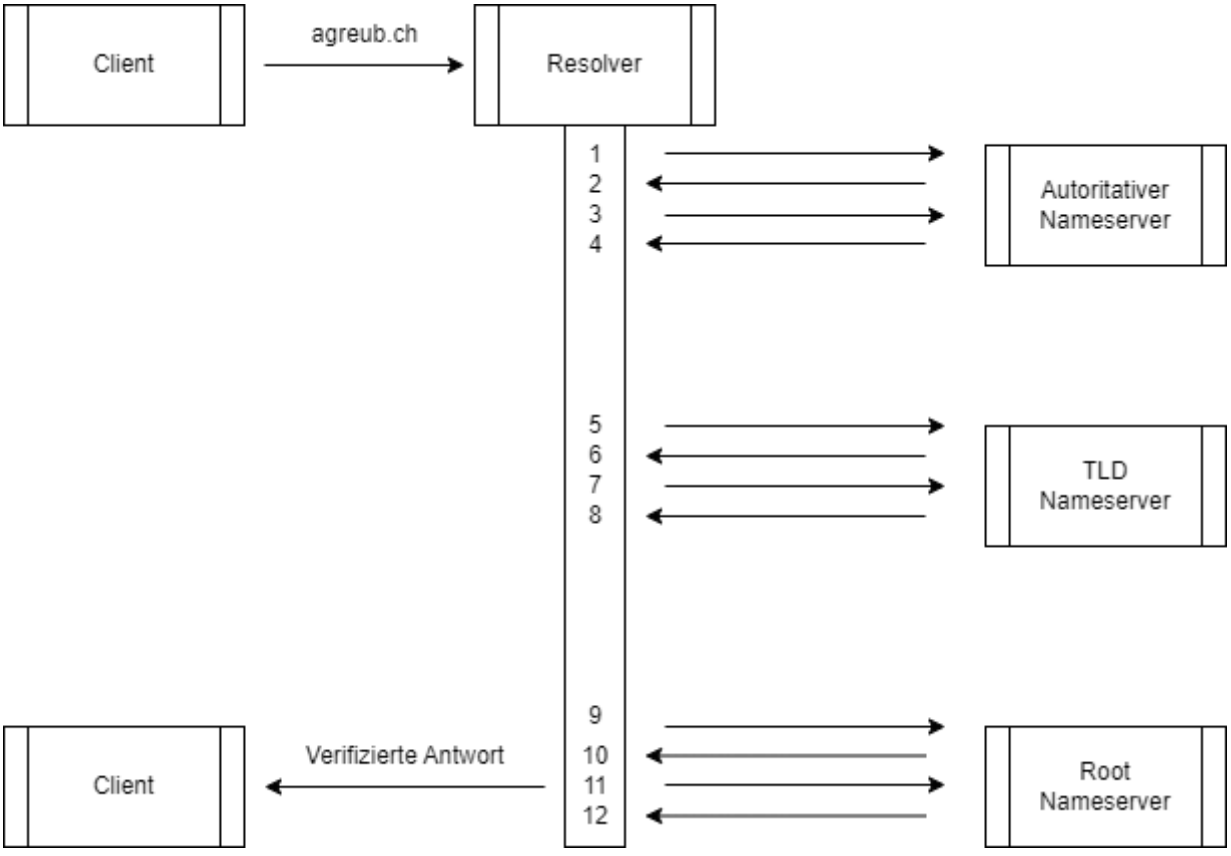
KSK (Key Signing Key)

Der KSK siginert zusätzlich den öffentlichen ZSK, der im DNSKEY Eintrag gespeichert ist und erstellt einen neuen RRSIG für den DNSKEY.



Schema des KSK

Ablauf einer DNSSEC Abfrage



1. Wenn ein Client die www.agreub.ch eintippt, wird die Anfrage zum autoritativen Nameserver geschickt. Wenn der Nameserver nun DNSSEC aktiviert hat, kann die Abfrage weiter erfolgen, ansonsten wird die Abfrage nicht weitergeführt.
2. Der Nameserver hat DNSSEC aktiviert und sendet als Antwort den A-Record und eine verschlüsselte Signatur zurück.

3. Der Resolver benötigt diese kryptographischen Signaturen und holt beim Nameserver den Public und den Private Key.
4. Der Nameserver sendet die Keys und die Signaturen an den Resolver, damit die Verifizierung erfolgreich durchgeführt werden kann.
5. Der Resolver fragt den TLD Nameserver an, ob dort die benötigten Daten hinterlegt sind.
6. Die zu verifizierenden Informationen werden vom TLD Nameserver an den Resolver weitergeleitet.
   Wenn die Informationen übereinstimmen, ist die Domain validiert.
7. Eigentlich wäre der Prozess hier beendet, jedoch ist hier ein Angriff immer noch möglich und deshalb wird der Root-Nameserver von .ch angefragt.
   Der Resolver fragt den TLD Nameserver nach den kryptographischen Keys, um die Informationen zu verifizieren.
8. Der TLD Nameserver erhält die gewünschten Informationen (Keys und Signaturen).
9. Der Resolver fragt den Root-Server für die zu verifizierenden Informationen, die beim TLD Nameserver hinterlegt sind.
10. Der Root-Server sendet die zu verifizierenden Informationen zurück und der Resolver verifiziert die Informationen des TLD Nameservers.
11. Der Resolver fragt den Root-Server nach den Kryptographischen Keys um die Informationen vom Resolver zu verifizieren.
12. Der Root-Server sendet die Keys, damit die Informationen vom TLD Nameserver verifiziert werden können.

Die Kette des Vertrauens

Wie kann man sicherstellen, das der Root-Nameserver sicher ist? Jeder Verifizierende Resolver hat nur einer Entität zu vertrauen und zwar dem Root-Server.

Der Resolver hat bereits die benötigten Schlüssel des Root-Server im Verzeichnis. Das heisst, nach Punkt 12 wird verglichen ob die Informationen des Resolvers und des Root-Server übereinstimmen. Man kann somit der TLD .ch und der Domain vertrauen.