DNSSEC

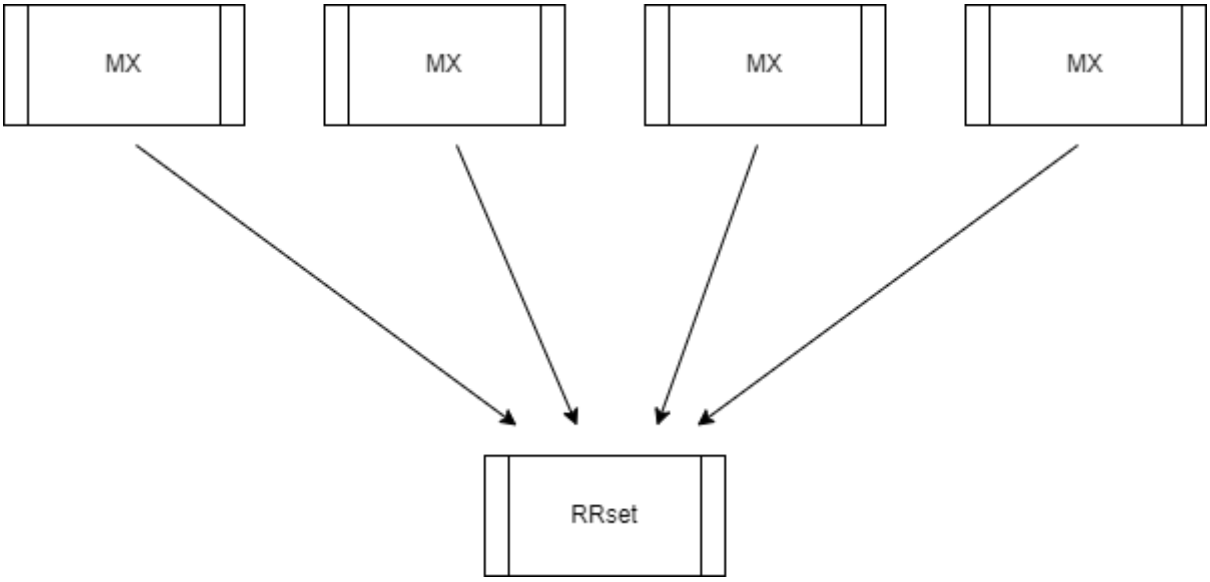
DNSSEC steht für "Domain Name System Security Extension" die das DNS mit verschiedenen Sicherheitsmöglichkeiten erweitert.

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

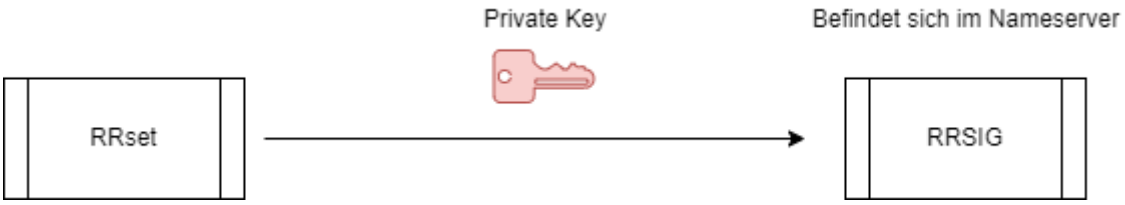
`RRSIG`	Enthält eine kryptographische Signatur
`DNSKEY`	Enthält einen Public Key
`DS`	Enthält den Hash eines DNSKEY Eintrags
`NSEC und NSEC3`	Für die explizite Anerkennung eines Nicht-Existenten DNS Eintrags
`CDNSKEY und CDS`	Für die untergeordnete Zone zur Anfrage von Aktualisierungen eines DNS Eintrags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



Definition eines RRset

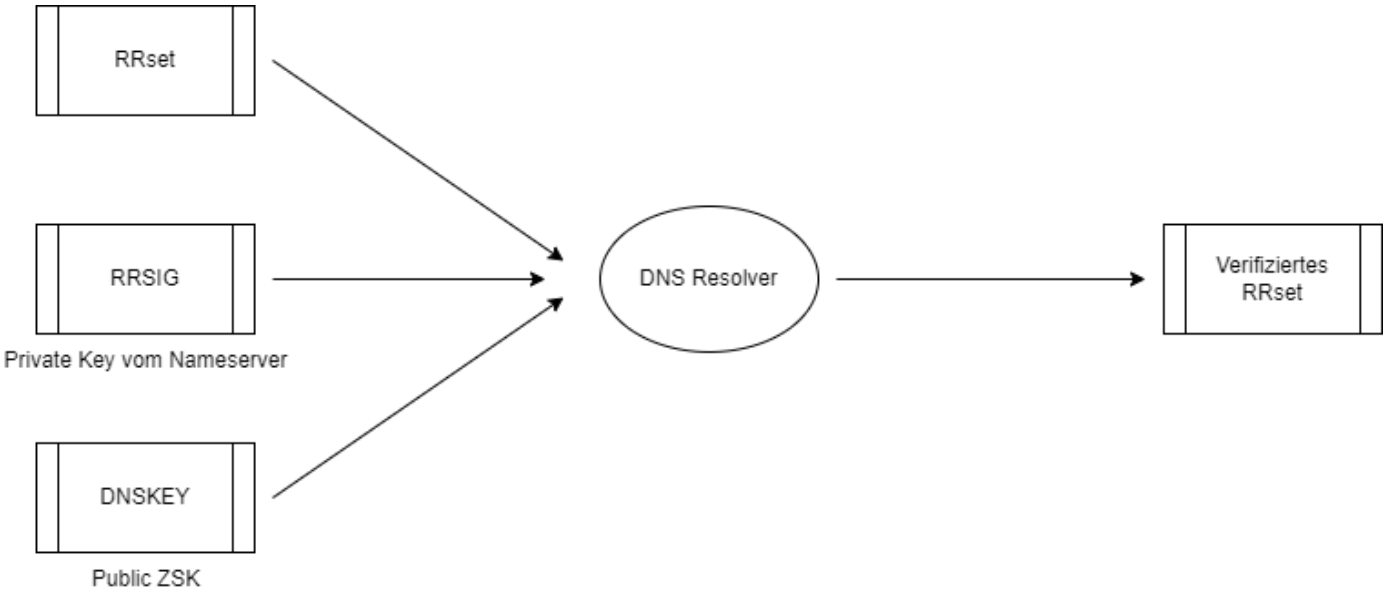
Beim RRset werden Einträge mit dem gleichen Namen und Typ gebündelt.

ZSK (Zone Signing Key)



Definition des RRSIG Eintrags

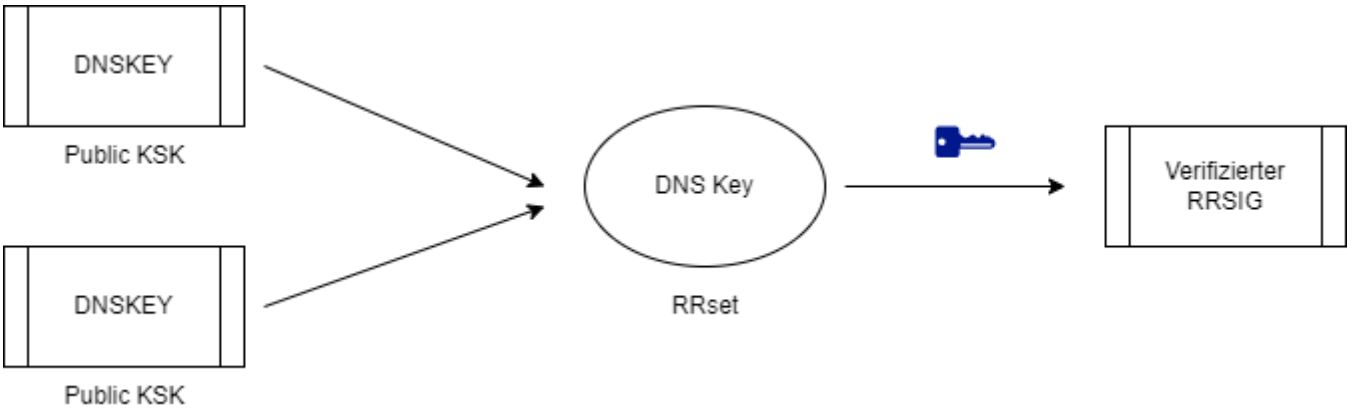
Im RRSIG Eintrag befinden sich die Daten des Private Key und werden beim Zonenbetreiber im Nameserver hinterlegt.



Schema des ZSK

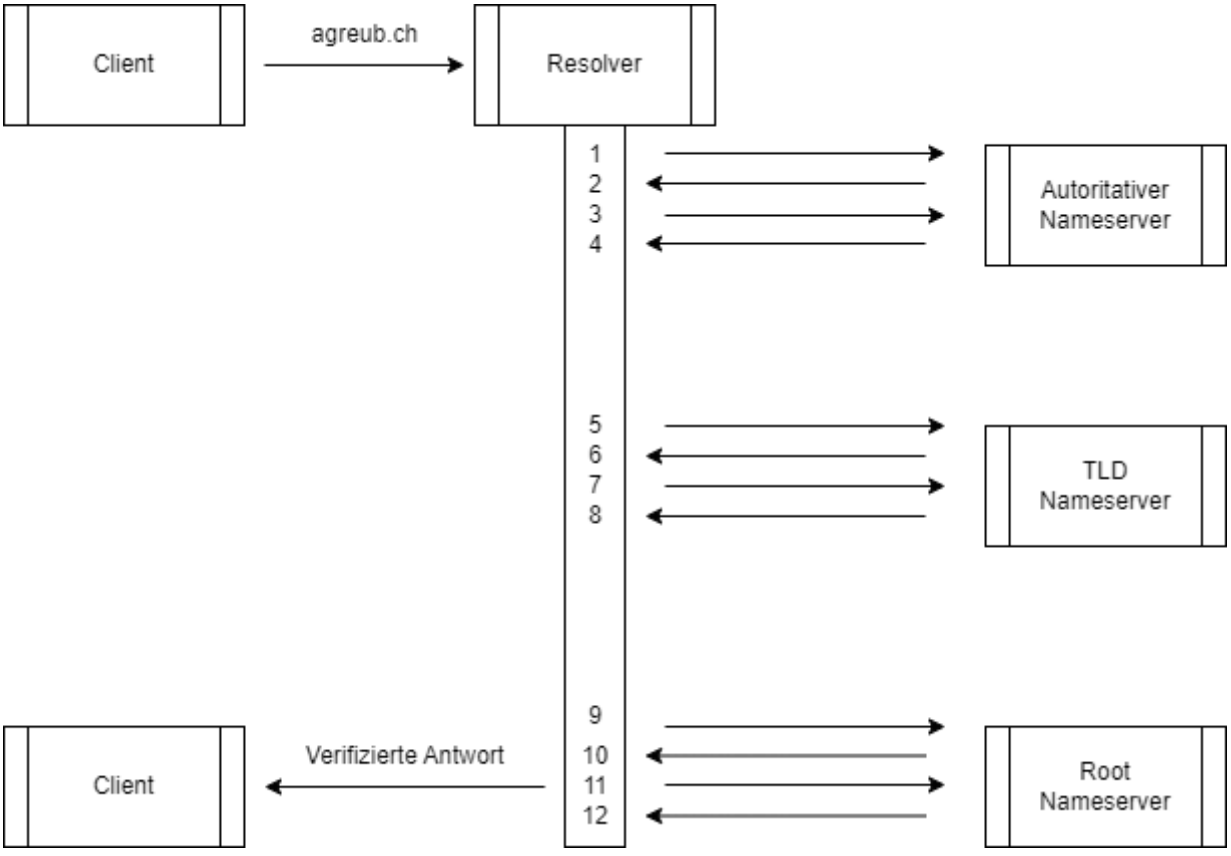
KSK (Key Signing Key)

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.

Revision #8
Created 8 August 2023 13:23:50 by Alexander Greub
Updated 14 August 2023 11:24:07 by Alexander Greub