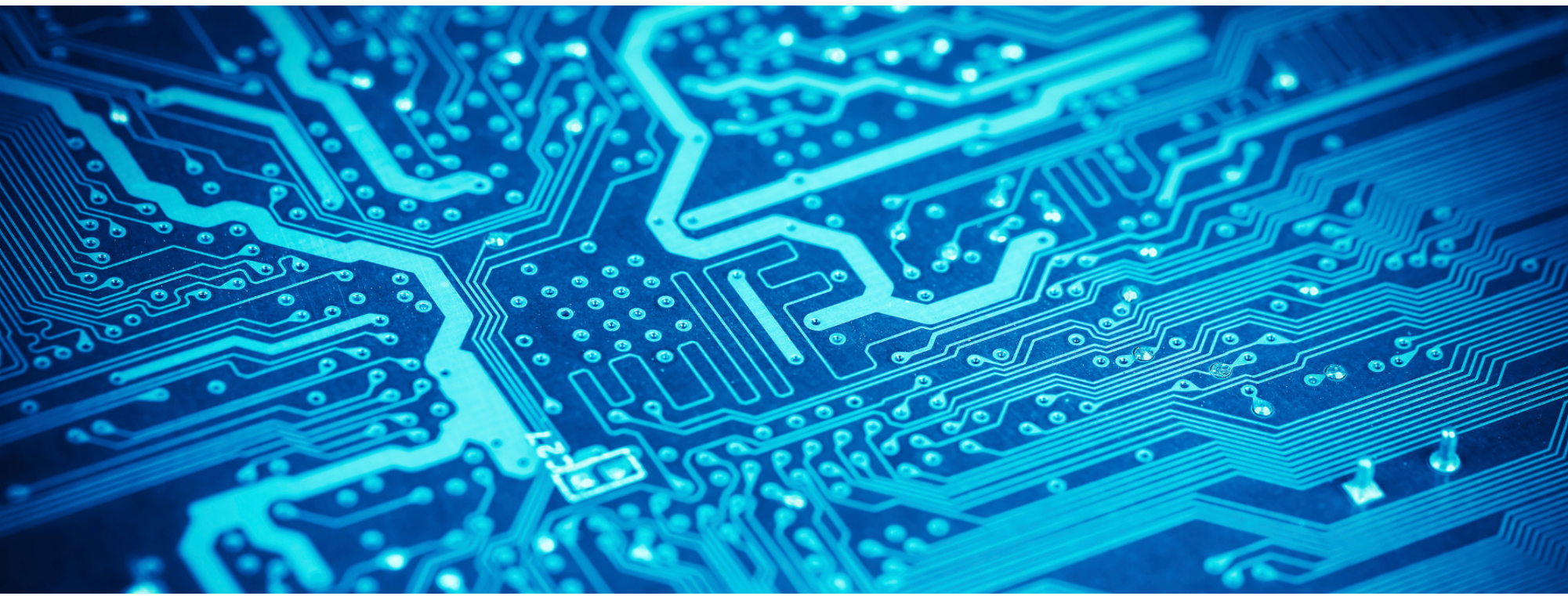
Intern: DNSSec

Secure DNS



Simon Fromme ▪ 25.04.2017

URIs

Definition

```
  foo://example.com:8042/over/there?name=ferret#nose
  \_/   \______________/\_________/ \_________/ \__/
   |           |            |            |        |
scheme     authority       path        query   fragment

authority   = [ userinfo "@" ] host [ ":" port ]
```

- Der Domain-Name kann ein Teil der URI sein (auch z.B. IPv4/IPv6 Adresse möglich):

  `http://`**`de.wikipedia.org`**`/wiki/Karlsruhe`

  $\Rightarrow$ Domain-Name: **`de.wikipedia.org`**

URLs/Domains

- Computer auf dem die Webseite der deutschen Wikipedia liegt, kann nur über die IP-Adresse, nicht aber über den Domain-Namen erreicht werden (gleiches gilt für E-Mail-Postfächer, u.a.)
- Frage: Wie übersetze ich den Domain-Namen in eine IP?

DNS - Geschichte

- Hostname - Adressen Zuordnung in einziger Datei (`HOSTS.TXT`)

  $\Rightarrow$ `BANDBREITE ZUR VERBREITUNG` $\propto$ `(#HOSTS)`^{2}

- Ersetzen der Time-Sharing Hosts des ursprünglichen ARPANET durch Netzwerke einzelner Workstations

  $\Rightarrow$ Lokale Organisationen verwalteten eigene Namen und Adressen, mussten allerdings auf Update der `HOSTS.TXT` durch die NIC[1] warten, um Änderungen dem ganzen Internet verfügbar zu machen.

  $\Rightarrow$ Bedarf nach lokaler Struktur des Namespaces

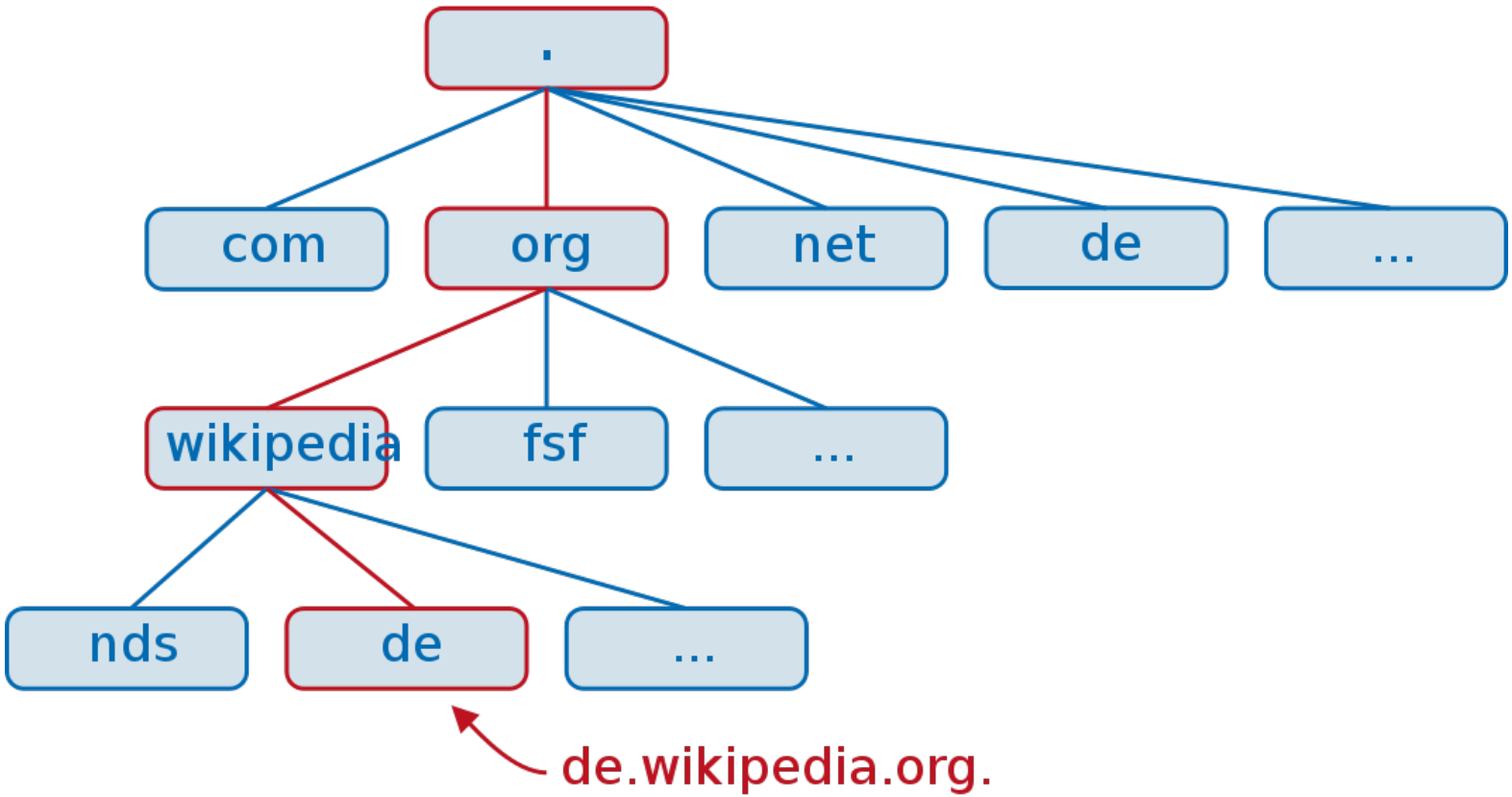
- anspruchsvollere Internetanwendungen machten die Entwicklung eines allgemeinen Nameservices notwendig

- 1983 DNS (Paul Mockapetris, RFC 882, 883)

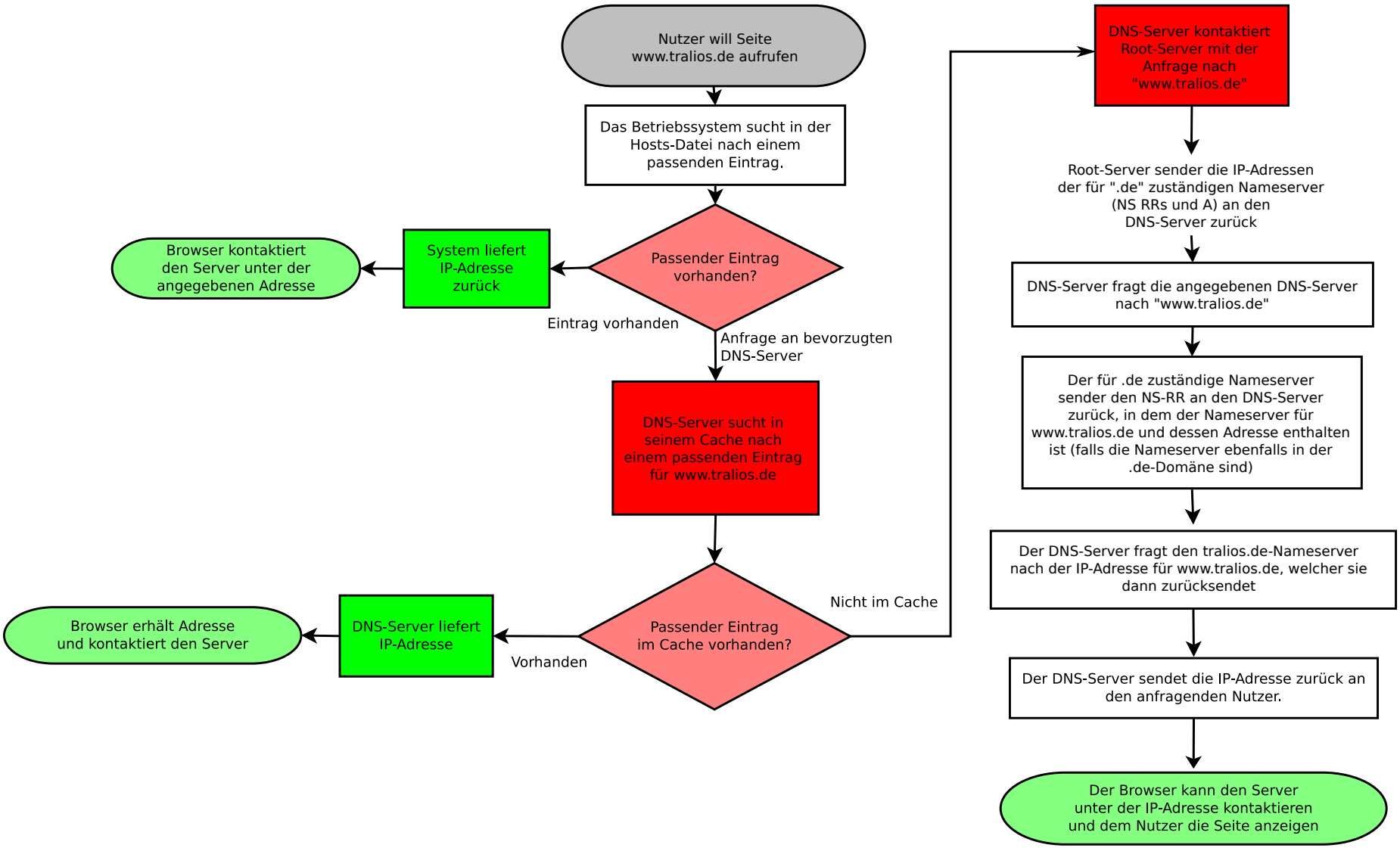
- 1987 DNS-Erweiterung (RFC 1034, 1035)

[1] *Network Information Center*, 1972 - 1991 durch *Stanford Research Institute* betrieben

Lösung: hierarchisches DNS (Dynamic Name System)



Was passiert bei einem DNS-Request?

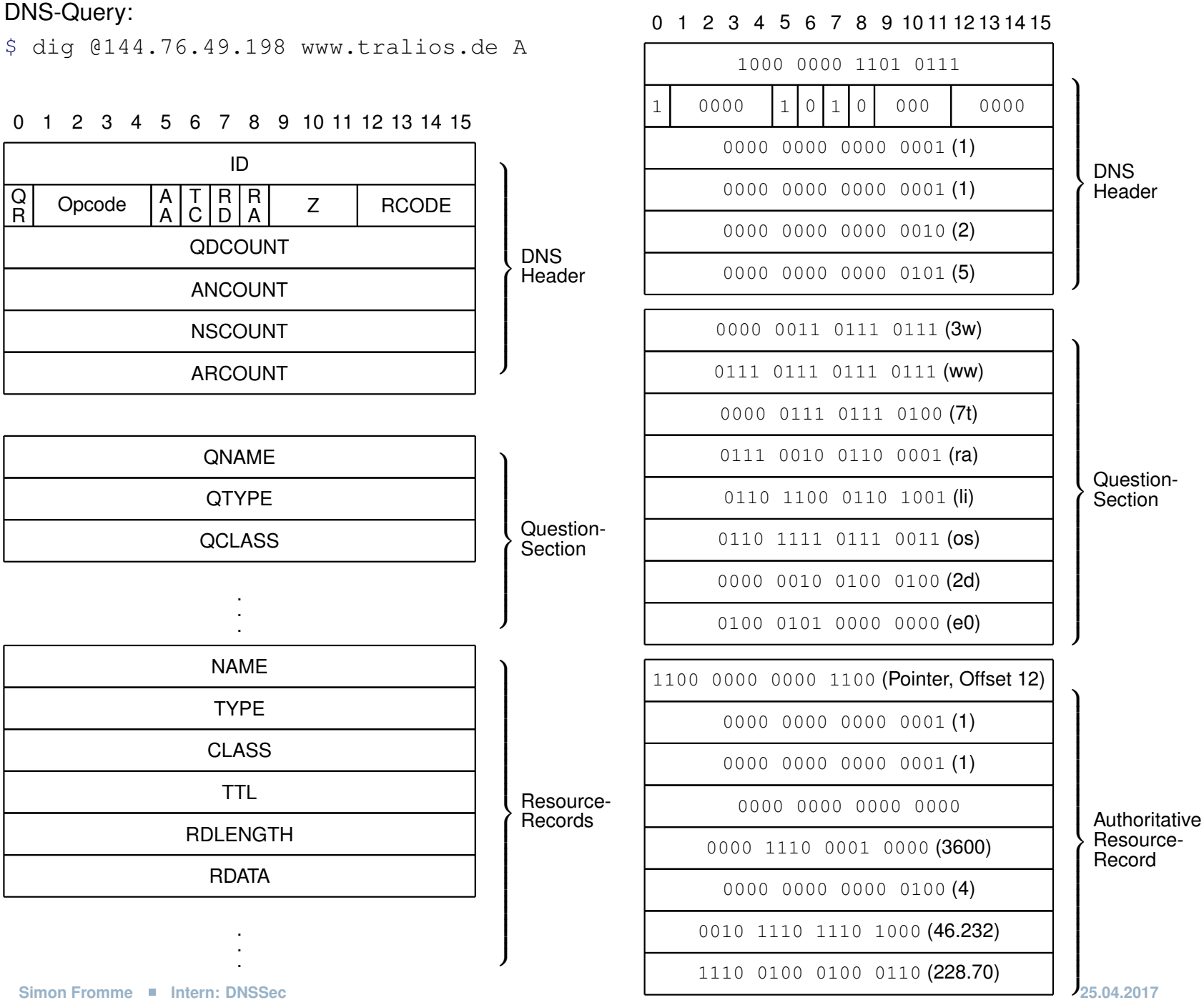


häufig verwendete RR-Typen

- A (IPv4)
- AAAA (IPv6)
- CNAME
- DNAME
- NS (Nameserver)
- MX (Mail eXchange record)
- SOA (Start of Authority)
- TXT (Text)

DNS-Query:

```
$ dig @144.76.49.198 www.tralios.de A
```



Probleme mit DNS

- Wie kann ich sicher sein, dass die Antwort, die ich vom DNS-Resolver bekomme auch wirklich stimmt und nicht unterwegs verändert wurde?
- mögliche Missbrauchsfälle:
  - gefälschte Bankwebseite $\Rightarrow$ Diebstahl von Kontodaten
  - gefälschte Nachrichtenseite (”Fake News...”)
  - u.v.m
- Antwort: **DNSSEC (Domain Name System Security Extensions)**

  $\Rightarrow$ Nachdem Schwachstellen verschiedener Vorgängerversionen behoben wurden, wurde DNSSEC am 5. Mai 2010 auf allen 13 Rootservern eingeführt

  $\Rightarrow$ 1386/1531 TLDs signiert (Stand: 25.04.2017)

  `http://stats.research.icann.org/dns/tld_report/`

DNS/DNSSec - Ein Vergleich

```
$ dig www.tralios.de A
;; ANSWER SECTION:
www.tralios.de. 3142 IN A 46.232.228.70

$ dig +dnssec www.tralios.de A
;; ANSWER SECTION:
www.tralios.de. 2710 IN A 46.232.228.70
www.tralios.de. 2710 IN RRSIG A 8 3 3600 (
                                20170422002145 20170408024920 33480 tralios.de.
                                WrqeY//vgdeV36cwKdJL1SfgF0OuTsu/U5bKmWg8NBMe
                                hpyTi/jWZnBoAFHK49gBB7WNlRDGkBtbXu9ftqgb3zjs
                                AdNvZU1k3w4MadupEdsLeYvFHVQgR7Kup/vNBCKfL+wr
                                s/Iatr6ZBNRAA/Q/8N3tex8GrMcZtXk9ypJLg7U= )
```

DNSSEC - Neue Resource Records

- RRSIG (Resource Record Signatur)
- DNSKEY (DNS Schlüssel)
- DS (Delegation Signer)
- NSEC/NSEC3

RRSIG

- digitale Signatur eines (beliebigen) Record Sets
- Kann mit dem Public ZSK auf Authentizität überprüft werden
- aus Sicherheitsgründen begrenzte Gültigkeitsdauer, vor Ablauf muss jeweils neu signiert werden!

DNSKEY

- Public ZSK (Zone Signing Key)
  - Zur Überprüfung der Authentizität der mit dem **Private ZSK** signierten Resource Records
  - Der dazugehörige RRSIG RR wird als (!) einziger RRSIG RR mit dem **Private KSK** erzeugt
- Public KSK (Key Signing Key)
  - Zur Überprüfung der Authentizität des DNSKEY RRSIG RR (ZSK)
  - Besitzt keinen RRSIG RR, Authentizität kann durch den DS RR der übergeordneten Zone überprüft werden

DS

- dient zur Verkettung von DNSSEC signierten Zonen $\Rightarrow$ “Chain of Trust” bis zum Public ZSK der Root Zone (dem vertraut werden muss)
- Wird als Hash des Public KSK der nachgeordneten Zone berechnet

NSEC/NSEC3

- Beweist kryptografisch, dass eine Domain innerhalb einer Zone nicht existiert
- NSEC RR enthält Vorgänger- und Nachfolge-Domain der nicht existierenden Domain und wird wiederum mit einem RRSIG-Eintrag gesichert

z.B.

```
example.de. NSEC name1
name1       NSEC name2
name2       NSEC name5
name5       NSEC example.de.
```

bzw.

```
name2   NSEC                ; Typ
        name5                ; alphabetischer Nachfolger
        NS DS RRSIG NSEC     ; Liste der Typen des Labels name2
```

DNSSEC Anwendungen

- SSHFP (SSH Fingerprint Resource Record)
- DANE (TLSA Resource Record mit Zertifikat, Fingerprint/Public Key)
  $\Rightarrow$ 3 Arten von Antwort möglich:
  - **Service Certificate Constraints** (“akzeptiere nur ein definiertes Zertifikat, Zertifikat muss Prüfung auf Vertrauenswürdigkeit bestehen”)
  - **Domain-Issued Certificate** (“Vertraue Zertifikat in TLSA Record, keine Prüfung auf Vertrauenswürdigkeit”)
  - **Trust Anchor Assertion** (“Client wird aufgefordert, für die Validierung des Zertifikats nur einen definierten Trust Anchor zu benutzen”)

BIND-Konfiguration

DNS

```
zone "example.com" IN {
    type master;
    file "db/example.com.db";
    allow-transfer { any; };
};
```

DNSSEC

```
zone "example.com" IN {
    type master;
    file "db/example.com.db";

    key-directory "keys/example.com";
    inline-signing yes;
    auto-dnssec maintain;

    allow-transfer { any; };
};
```

- **key-directory** "keys/example.com";

  ⇒ Verzeichnis in dem die Keys liegen

- **inline-signing** yes;

  ⇒ Veränderungen an der unsignierten Zone werden automatisch erkannt

- **auto-dnssec** maintain;

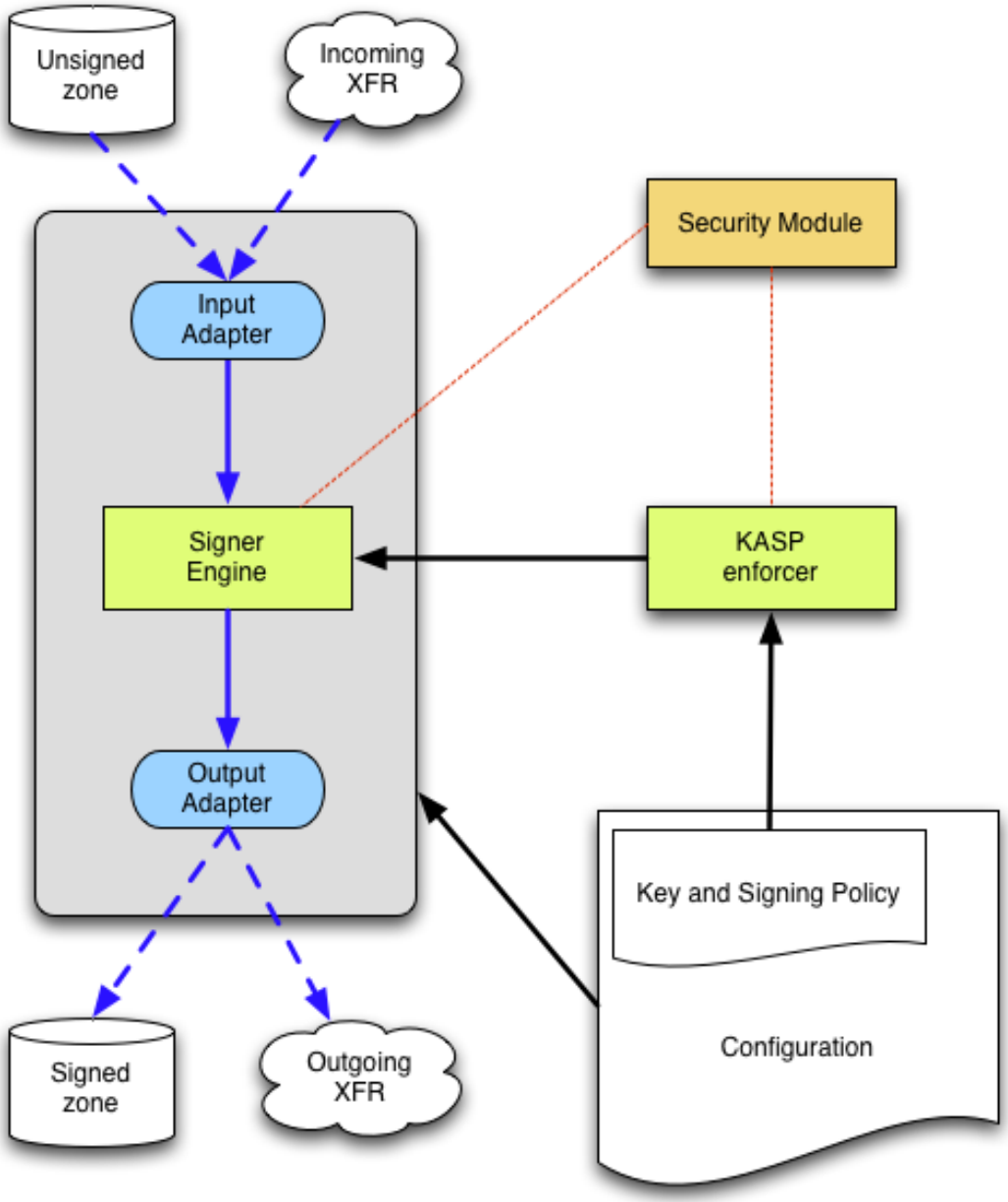
  ⇒ Bind kümmert sich automatisch um das Neu-Signieren u. Key-Management

OpenDNSSEC

- Unterstützt im Gegensatz zu Bind voll-automatisches Key-Management
- Einzige Nutzer-Interaktion: Upload des DS-Records zur übergeordneten Zone
- Signieren von mehren Zonen mit einem einzigen ZSK möglich

Komponenten

- Konfiguration (Kryptografische Parameter, Gültigkeitszeiträume, ...)
- Enforcer (Key Management und Auslösen des Zone-Signing)
- Signer (Signiert Zonen nach Anweisungen des Enforcers)
- (virtuelles) HSM (Key-Management und Speicherung)


Unsigned zone
Incoming XFR
Security Module
Input Adapter
Signer Engine
KASP enforcer
Output Adapter
Key and Signing Policy
Configuration
Signed zone
Outgoing XFR

Bildquellen

- Das DNS-Flussdiagramm auf Seite 6 ist eine modifizierte Version des Bildes https://commons.wikimedia.org/wiki/File:DNS-query-to-wikipedia.svg, welches unter der *CC BY-SA 3.0* Lizenz steht.
- Das OpenDNSSEC Organigram ist der Webseite https://wiki.opendnssec.org/display/DOCS/Overview+of+OpenDNSSEC entnommen. Veränderungen an der Grafik wurden nicht vorgenommen.