Huch, mein DNS ist verschwunden ...

Carsten Strotmann, dnsworkshop.de

Agenda

- Grundlagen der (Un-)Sicherheit von DNS im Überblick
- Privacy trotz DNS - wie geht das?
- Zusammenfassung und Ausblick

Wer sprich hier?

Carsten Strotmann

dnsworkshop.de

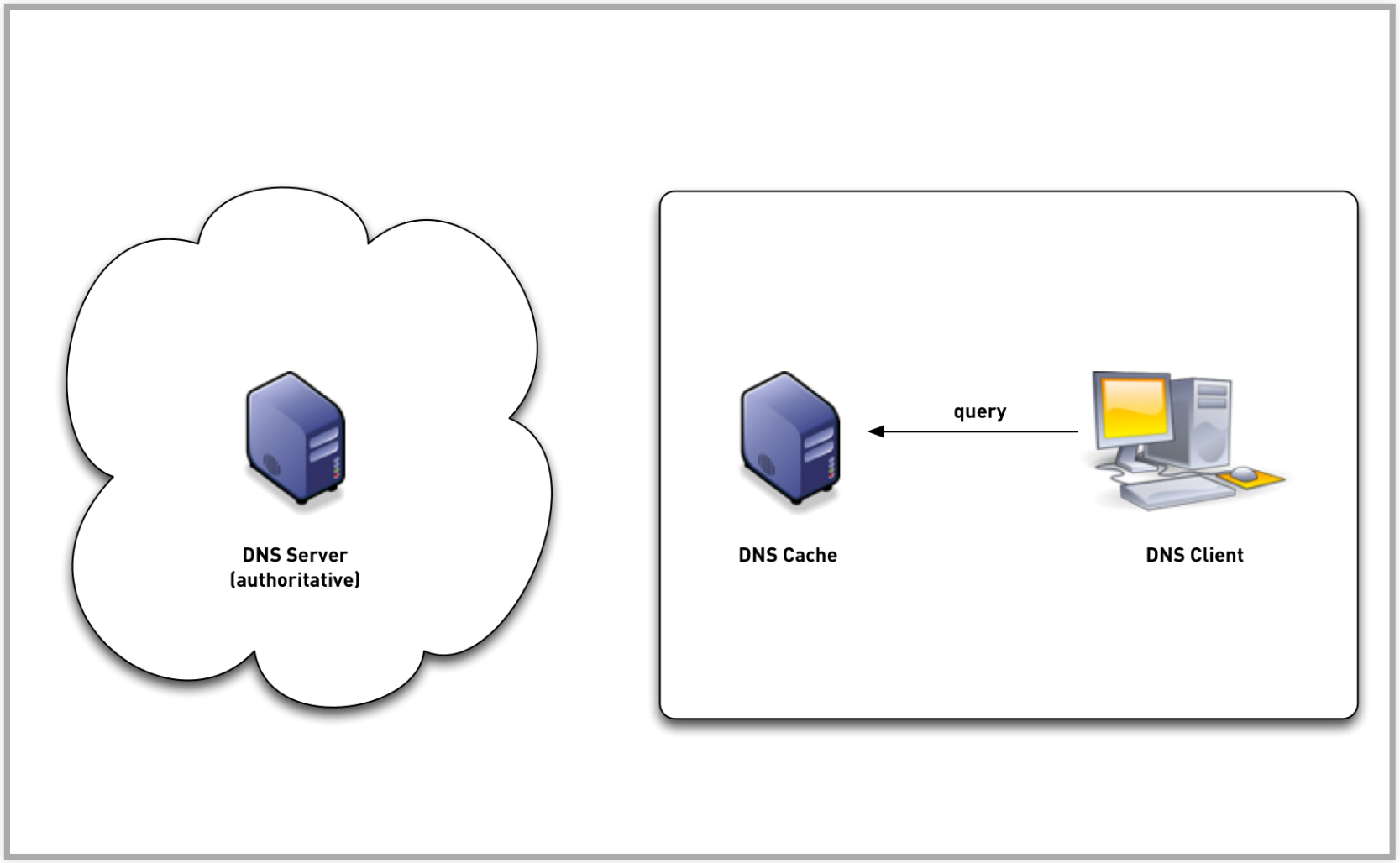
blog.defaultroutes.de

DNS(SEC)/DANE/DHCP/IPv6 Trainer und Helfer

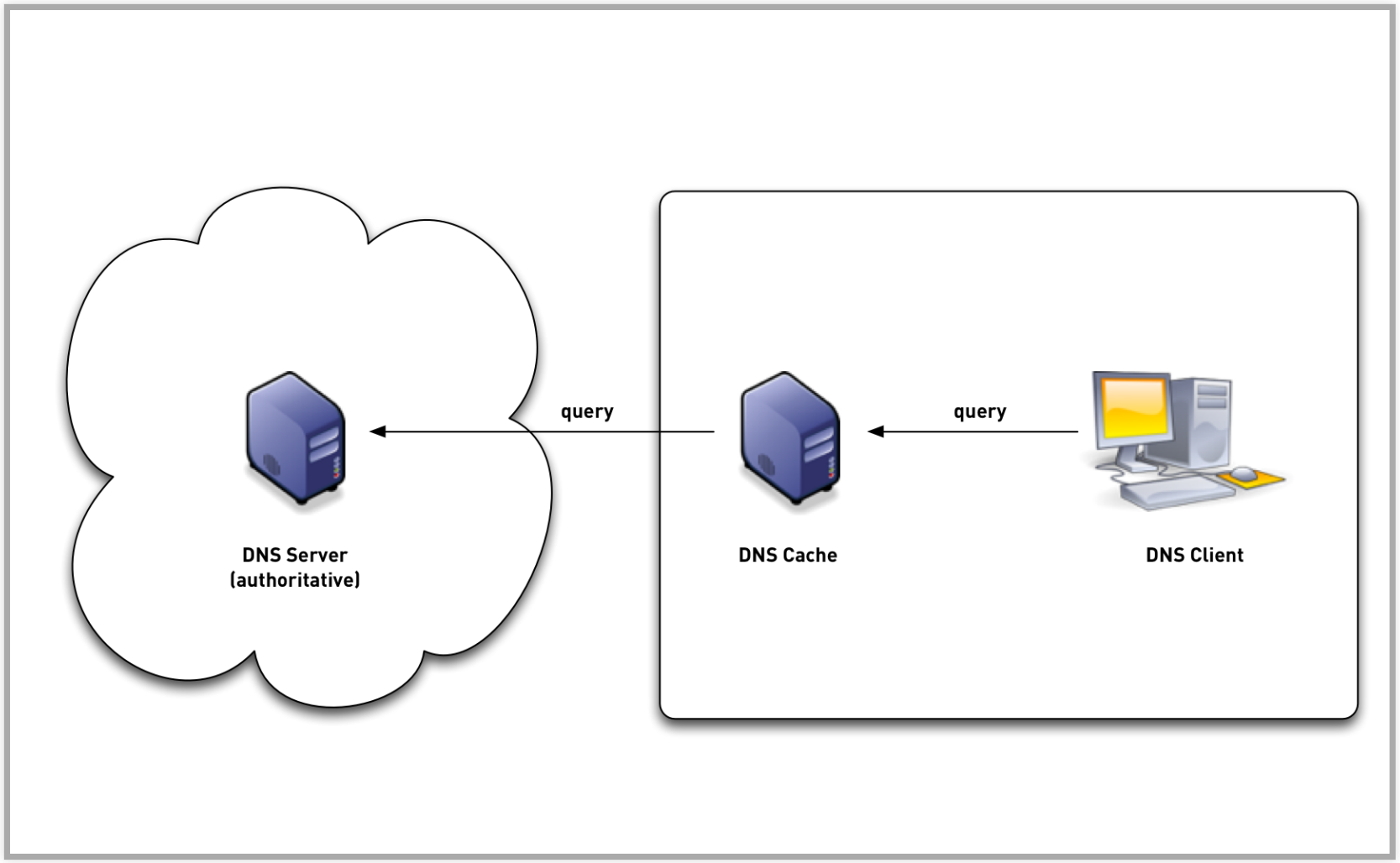
RIPE/IETF

Grundlagen der (Un-)Sicherheit von DNS im Überblick

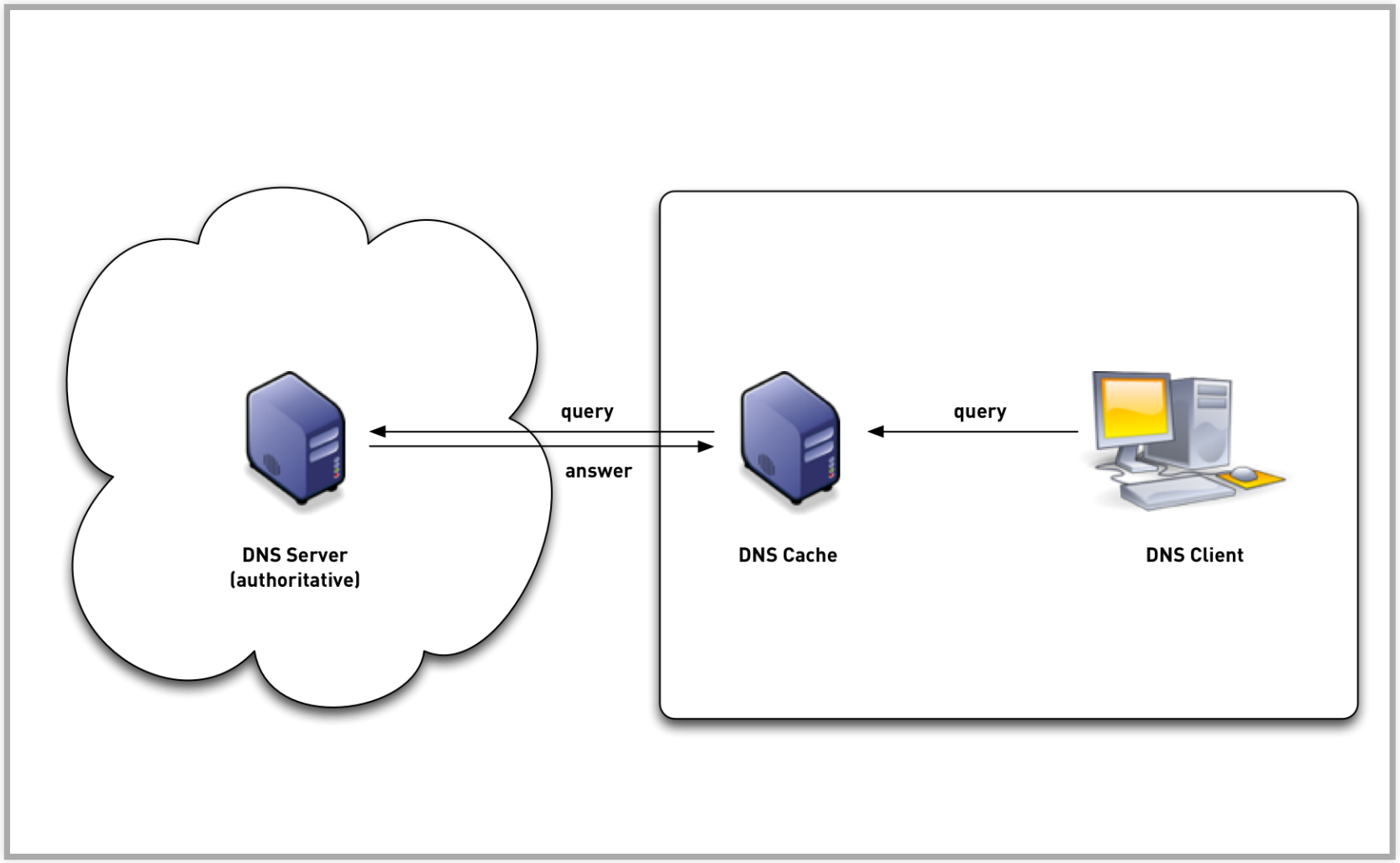
DNS Sicherheit - Grundlagen



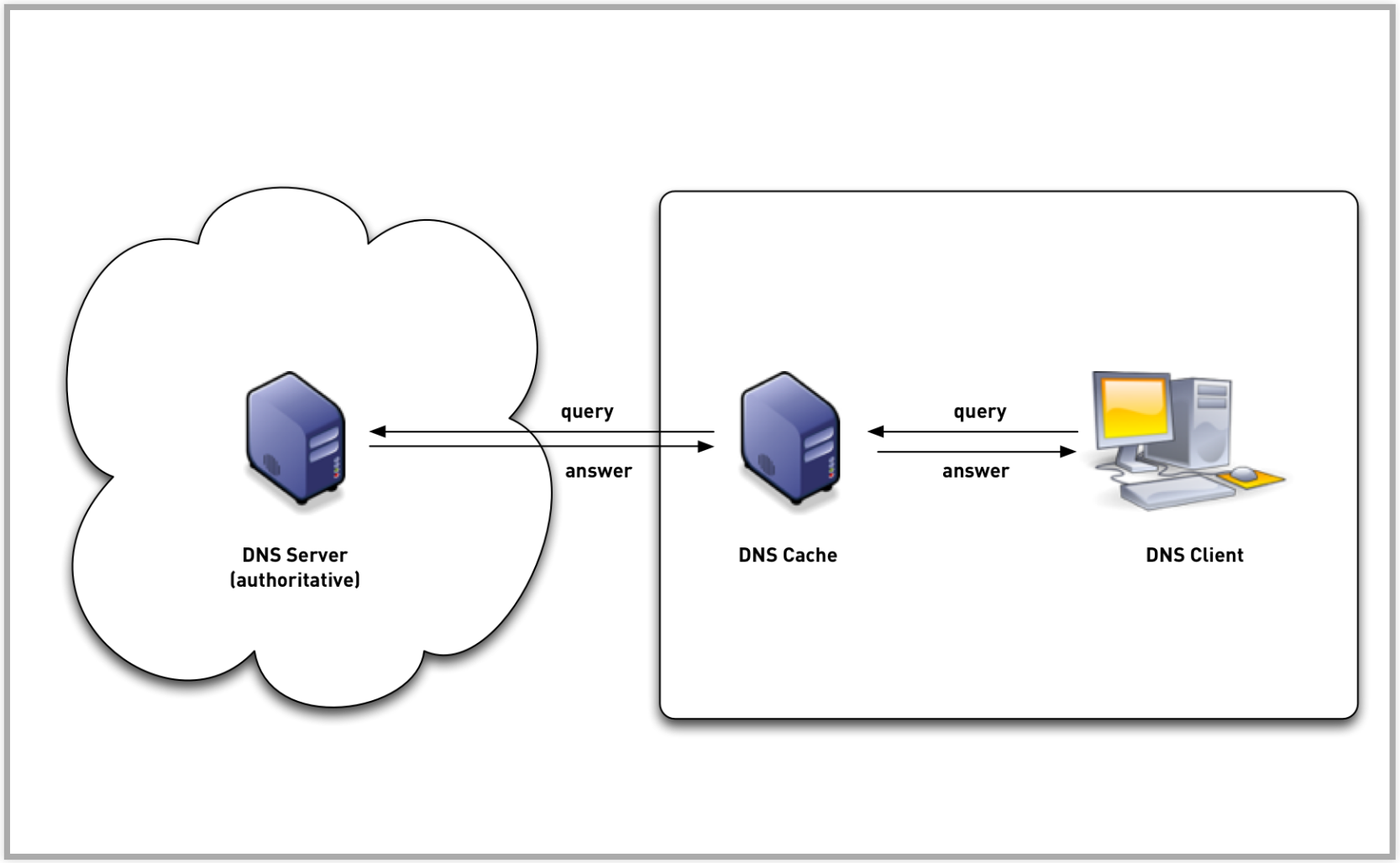
DNS Sicherheit - Grundlagen



DNS Sicherheit - Grundlagen



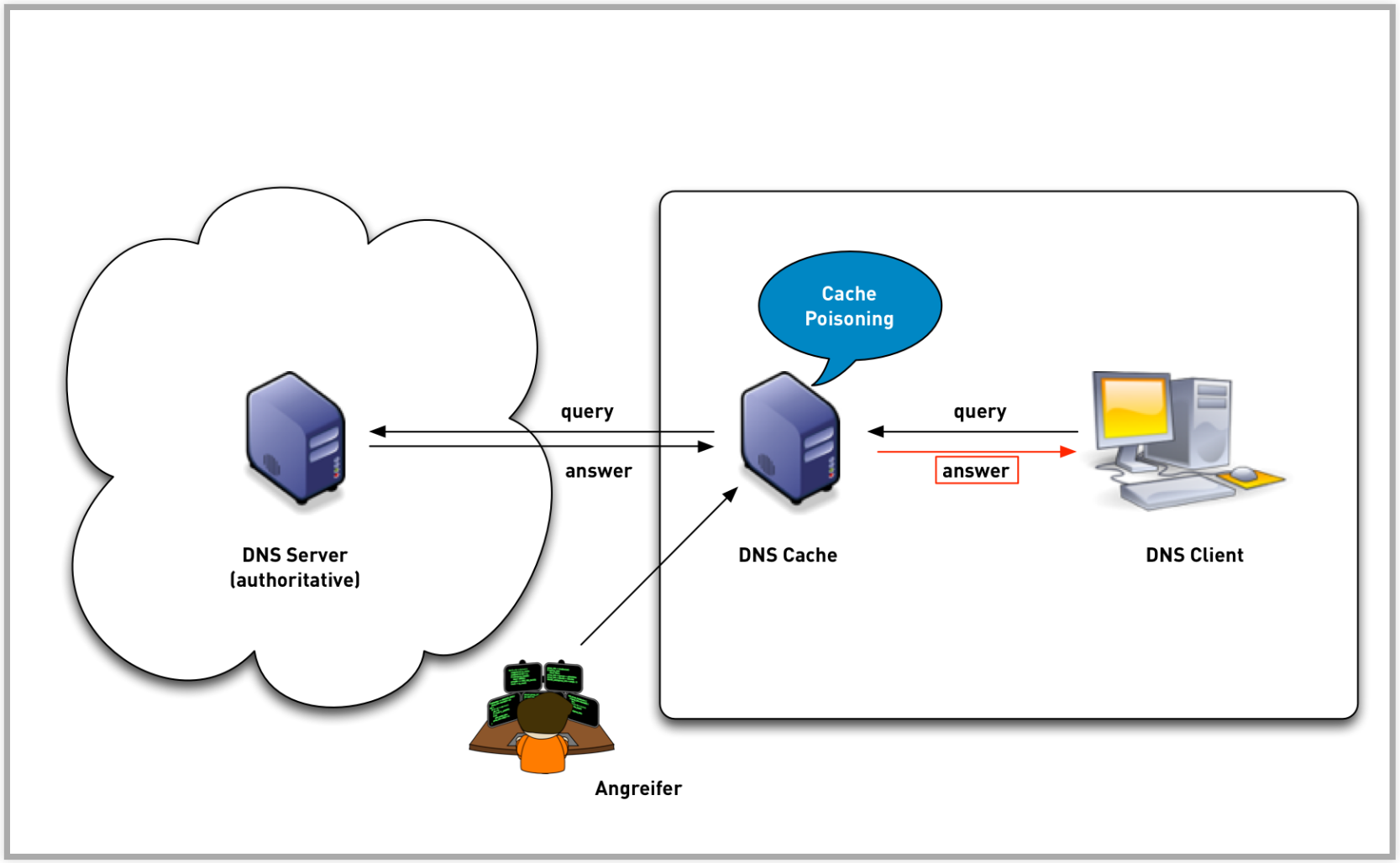
DNS Sicherheit - Grundlagen



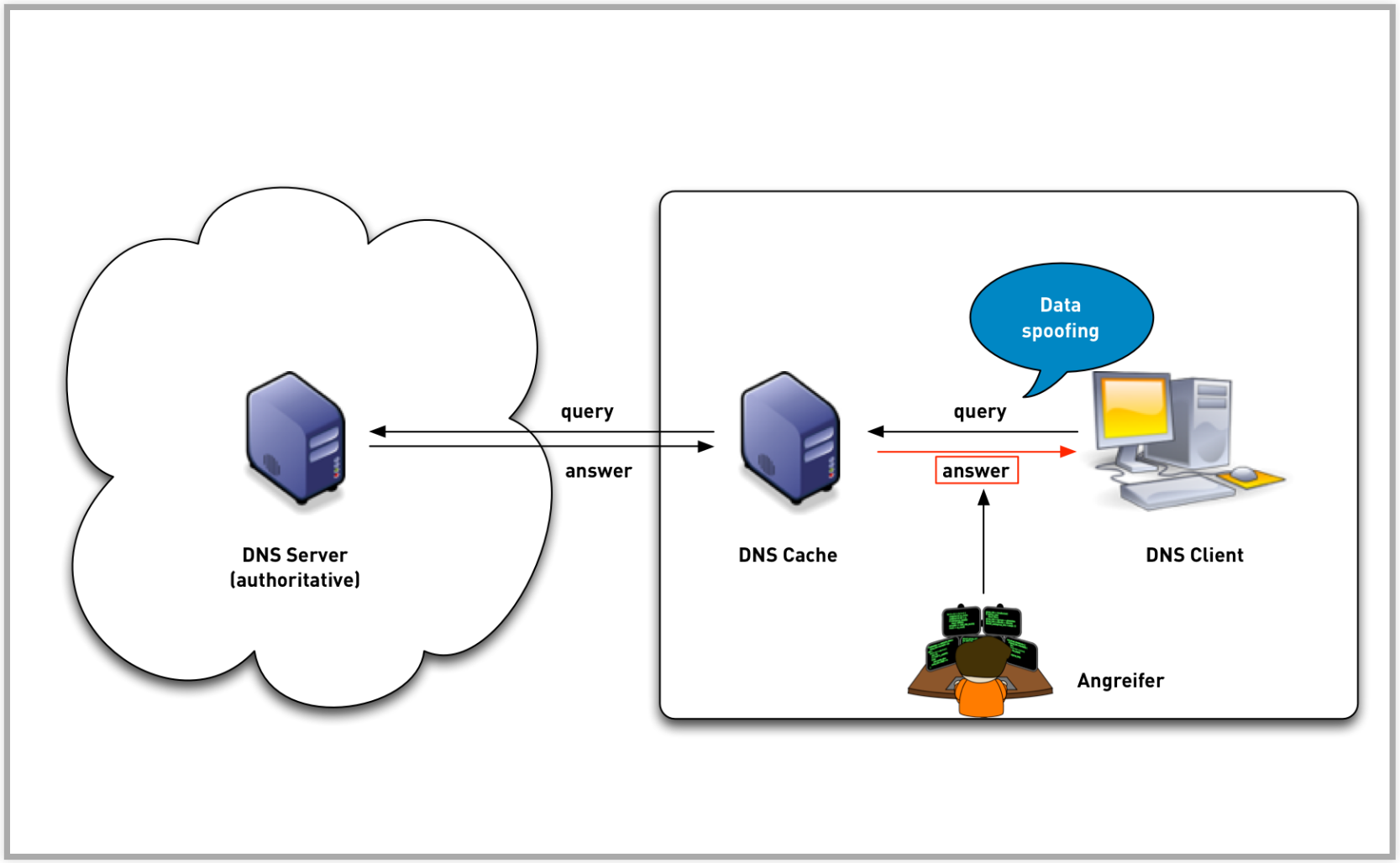
DNS-Sicherheit - Angriffe

- das ursprüngliche DNS Protokoll war nicht für sichere Kommunikation ausgelegt
- es gibt eine Reihe Angriffe auf die DNS-Daten und -Infrastruktur

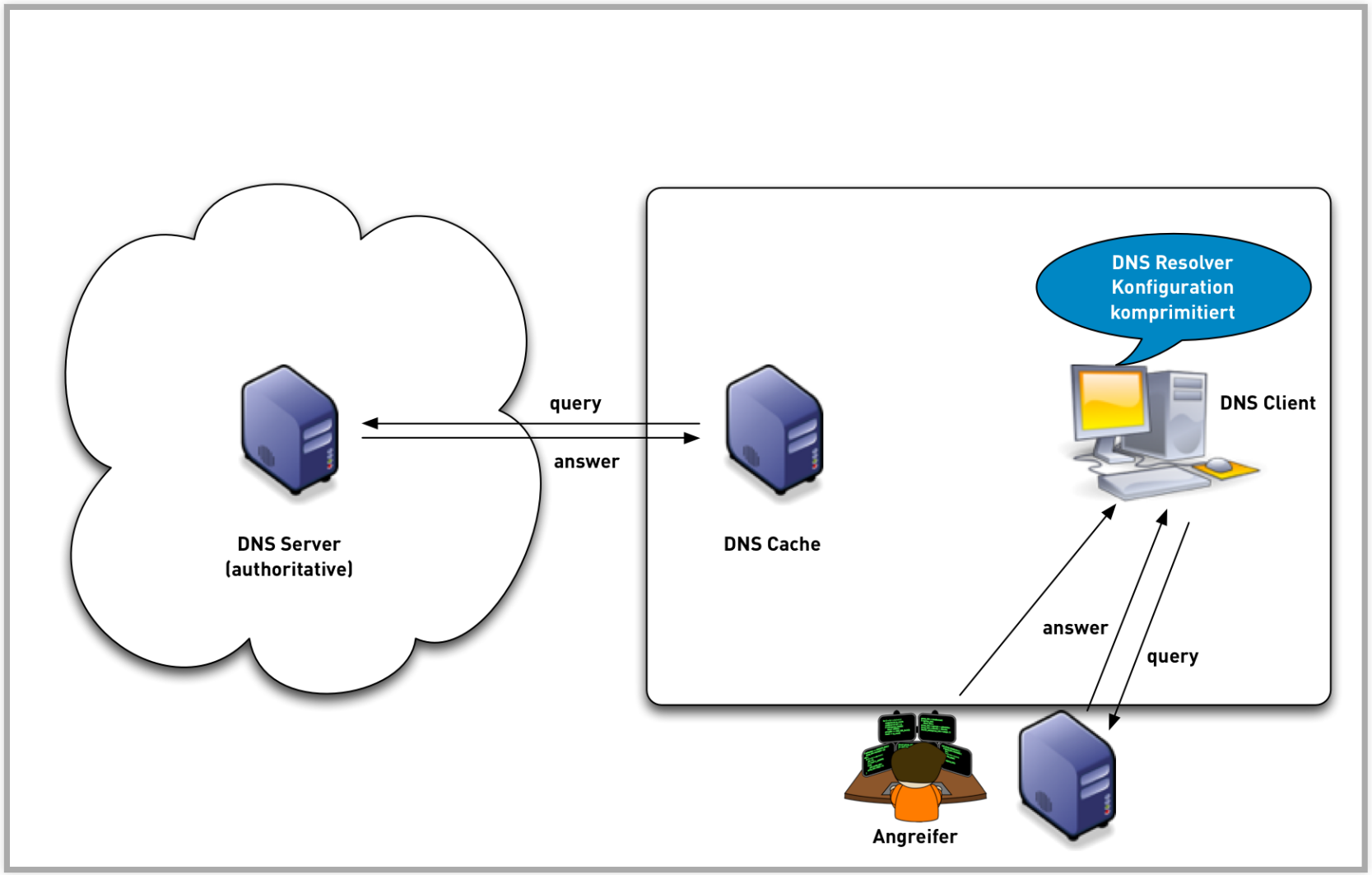
DNS Sicherheit - Angriffe



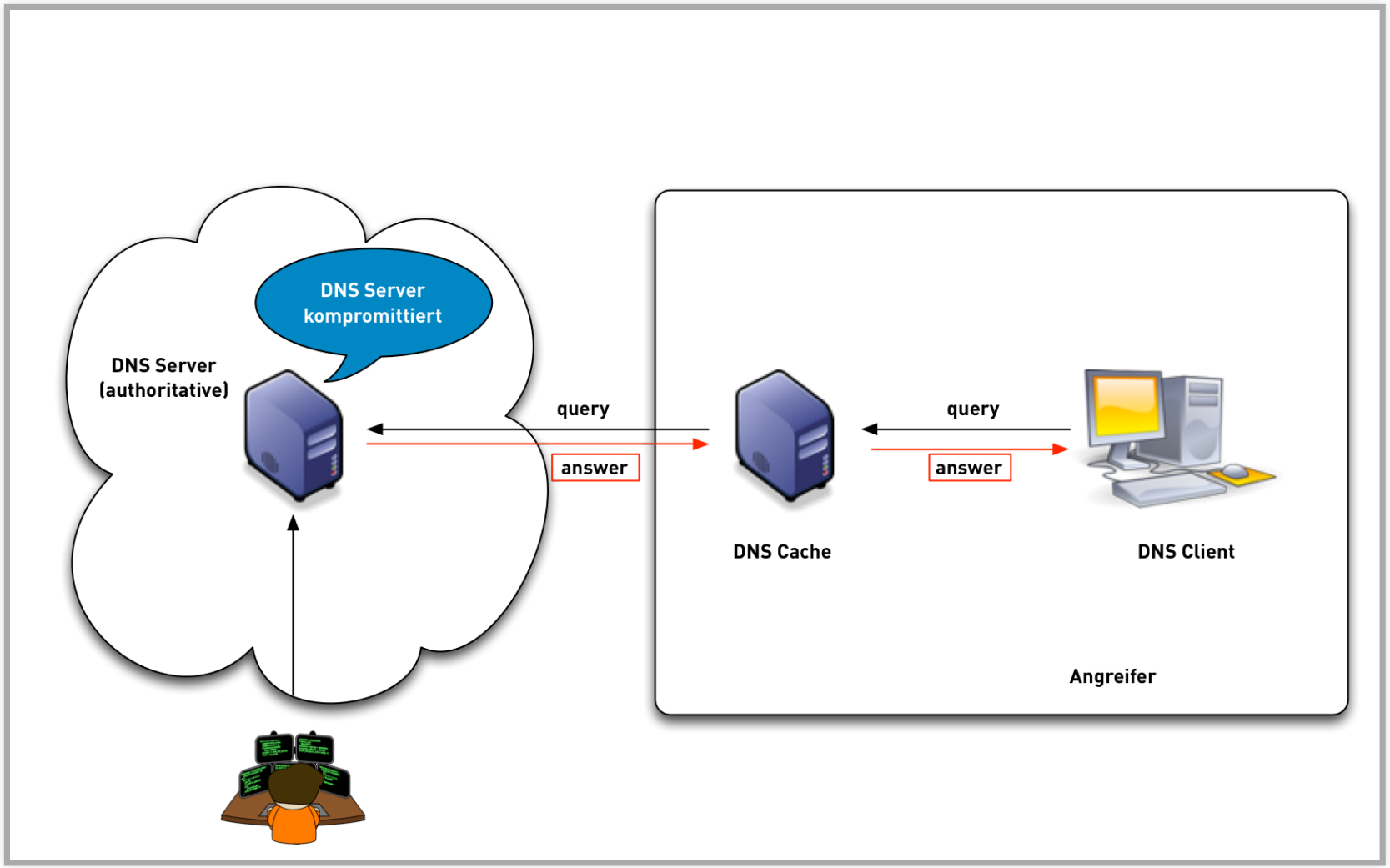
DNS Sicherheit - Angriffe



DNS Sicherheit - Angriffe



DNS Sicherheit - Angriffe



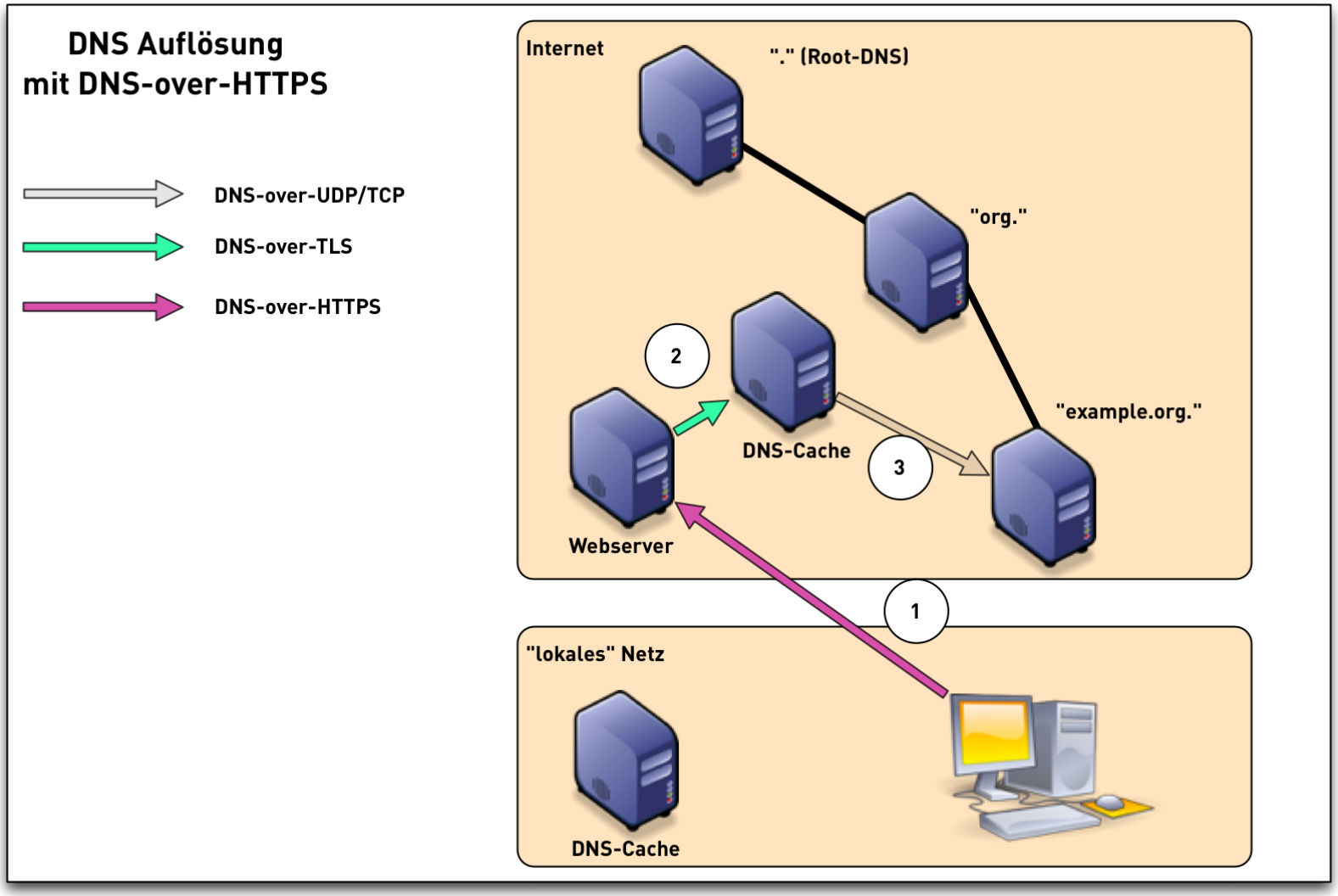
Privacy trotz DNS - wie geht das?

- die IETF hat in den letzten Jahren das DNS-Protokoll um Sicherheitsfunktionen erweitert
  - DNS-over-HTTPS (Verstecken von DNS Anfragen im Web-Kommunikation)
  - DNS-over-TLS (Transportverschlüsselung zwischen Client und DNS-Server)
  - QNAME Minimization (Reduktion von Metadaten)
  - EDNS-Padding (*verstecken* von DNS-Daten in verschlüsselten Verbindungen)
  - NSEC[3] "agressive use" - DDoS Angriffe im DNS per DNSSEC abwehren

DOH - DNS over HTTP(S)

- IETF Internet Draft *DNS Queries over HTTPS* (P. Hoffman, ICANN and P. McManus, Mozilla) https://tools.ietf.org/html/draft-ietf-doh-dns-over-https
- **Status:** *Submitted to IESG for Publication*
- DNS HTTP-Format over HTTPS over TCP, Port 443 (HTTP/2)
- URL (proposed): https://server/.well-known/dns-query
- Verschlüsselung und Authentisierung
- Negative Presse Anfang August 2018 für DoH durch einen Blogpost auf https://ungleich.ch

DNS-over-HTTPS



Vorteile

- HTTPS wird wenig gefiltert (Firewall)
- einfache Benutzbarkeit innerhalb von Web-Anwendungen und Web-Diensten
- HTTPS-APIs in vielen Programmiersprachen verfügbar

Entwicklungen

- IETF 100 - November 2017 - *DNS over HTTP(S)* (DoH) working group established: https://datatracker.ietf.org/wg/doh/about/
- IETF 101 - März 2018 - Arbeit an *DNS Queries over HTTPS* abgeschlossen, Start des *working group last call* (WGLC) im April 2018
- RFC kann jeden Tag erscheinen
- Implementierungen u.a. von Google, Facebook
- Clients im Browser, Debian, Ubuntu ...

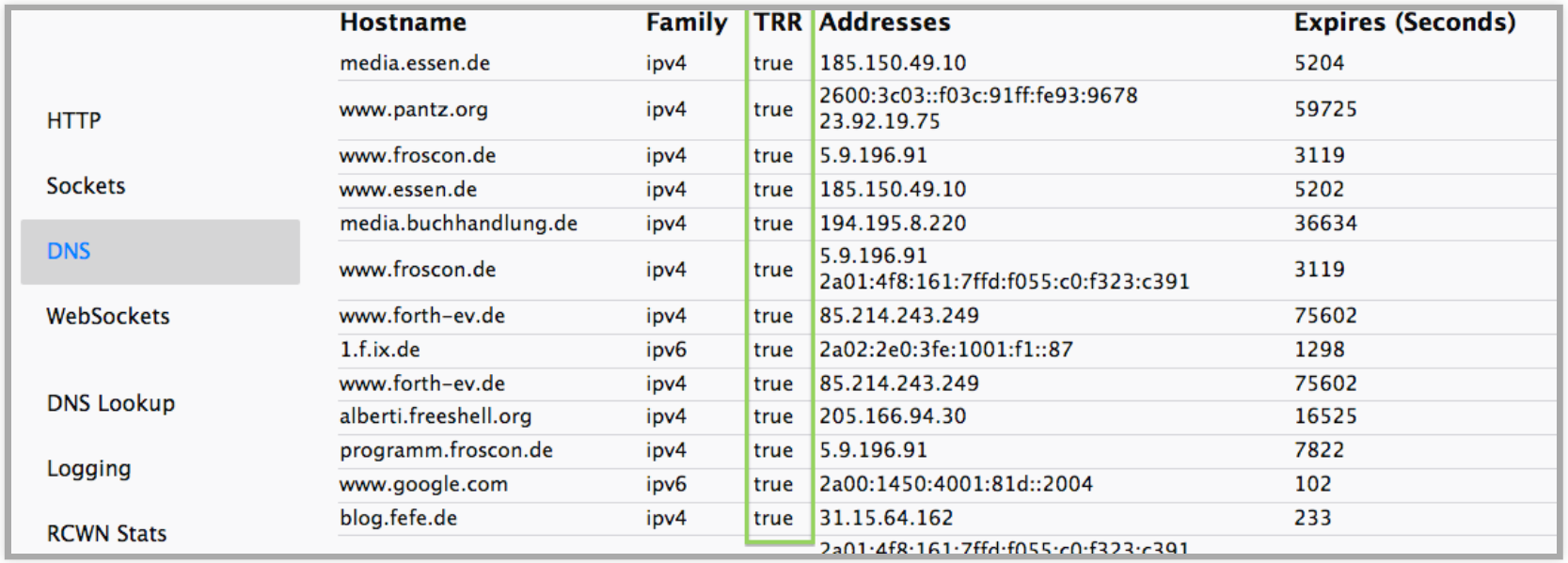
DNS-over-HTTPS und IDS/Netzwerk-Filter

> *1. Operational Considerations*
>
> *[...] Filtering or inspection systems that rely on unsecured transport of DNS will not function in a DNS over HTTPS environment.*

https://www.ietf.org/id/draft-ietf-doh-dns-over-https

DoH Client Implementierungen (1/2)

- Firefox 61+ (manuell anschaltbar)
- Firefox TRR Konfigurations Optionen



Hostname	Family	TRR	Addresses	Expires (Seconds)
media.essen.de	ipv4	true	185.150.49.10	5204
www.pantz.org	ipv4	true	2600:3c03::f03c:91ff:fe93:9678 23.92.19.75	59725
www.froscon.de	ipv4	true	5.9.196.91	3119
www.essen.de	ipv4	true	185.150.49.10	5202
media.buchhandlung.de	ipv4	true	194.195.8.220	36634
www.froscon.de	ipv4	true	5.9.196.91 2a01:4f8:161:7ffd:f055:c0:f323:c391	3119
www.forth-ev.de	ipv4	true	85.214.243.249	75602
1.f.ix.de	ipv6	true	2a02:2e0:3fe:1001:f1::87	1298
www.forth-ev.de	ipv4	true	85.214.243.249	75602
alberti.freeshell.org	ipv4	true	205.166.94.30	16525
programm.froscon.de	ipv4	true	5.9.196.91	7822
www.google.com	ipv6	true	2a00:1450:4001:81d::2004	102
blog.fefe.de	ipv4	true	31.15.64.162	233
			2a01:4f8:161:7ffd:f055:c0:f323:c391	

DoH Client Implementierungen (2/2)

- Bromite Browser *"Bromite is Chromium plus ad blocking and privacy enhancements"*
- `cURL` (Pull Request on Github)

DoH Resolver/Server

- jDNSProxy *Simple fast and lightweight DNS proxy and cache, implementing DNS-over-TLS, DNS-over-HTTPS, and Serve-Stale*
- m13253/DNS-over-HTTPS *High performance DNS over HTTPS client & server*
- rust-doh *A DNS-over-HTTP server proxy*
- doh-proxy *A set of python 3 scripts that supports proxying DNS over HTTPS*
- dnss *a daemon for using DNS over HTTPS (Client + Server)*

DoH Anbieter (Auswahl)

- Cloudflare https://cloudflare-dns.com/dns-query
- Cloudflare/Mozilla https://mozilla.cloudflare-dns.com/dns-query
- Clean Browsing https://doh.cleanbrowsing.org/doh/family-filter/
- PowerDNS https://doh.powerdns.org
- BlahDNS (de) https://doh.de.blahdns.com/dns-query
- SecureDNS https://doh.securedns.eu/dns-query

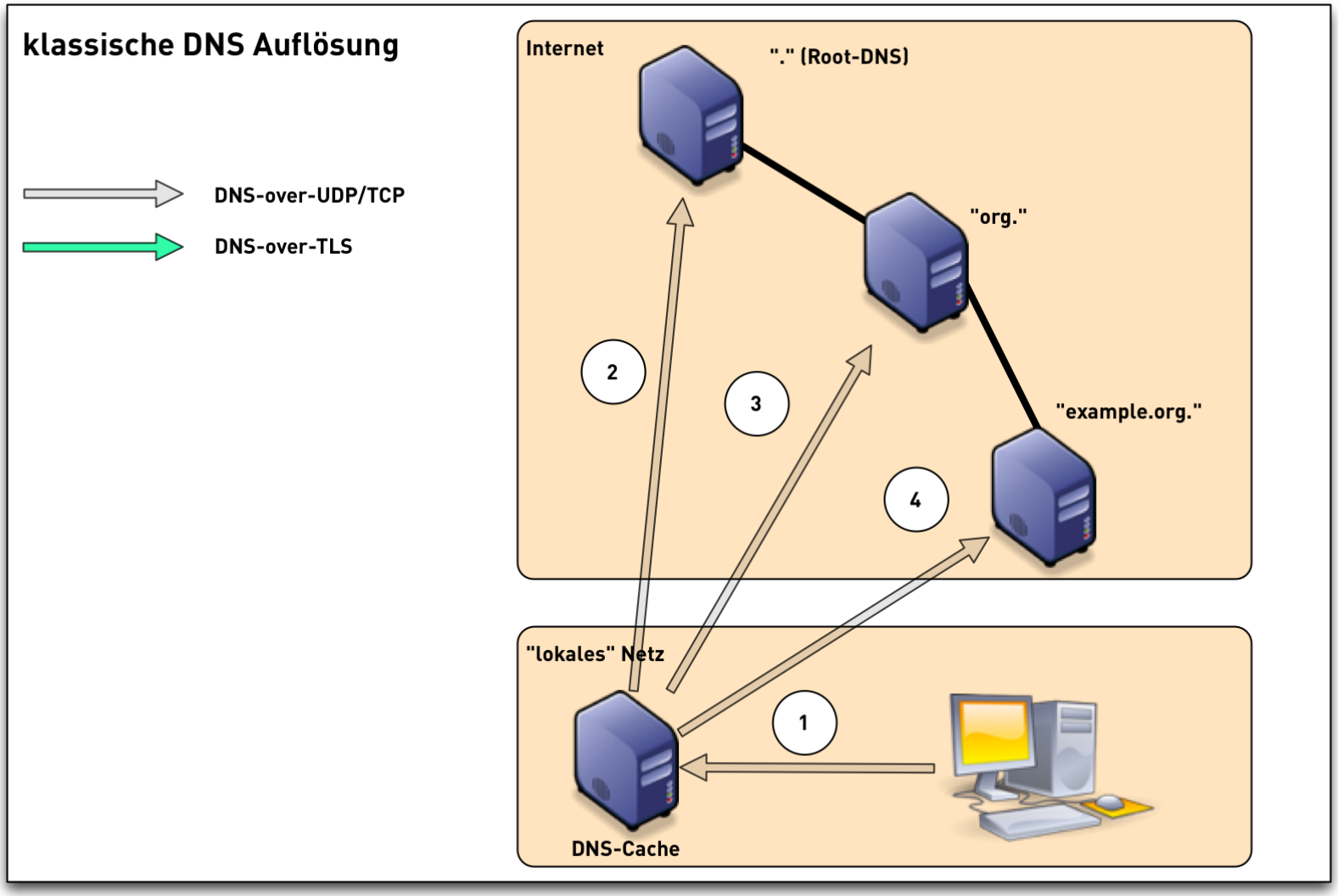
ähnliche Entwicklungen

- DNS over JSON over HTTPS over TCP
  - Google DNS Server-Side https://developers.google.com/speed/public-dns/docs/dns-over-https
  - OpenResolve - OpenDNS Server-Side DNS-over-HTTPS Service https://www.openresolve.com/
  - dingo - ein DNS-Client in Go mit Support für *Google DNS over HTTPS* und *OpenResolve* https://github.com/pforemski/dingo
  - CoreDNS kann als DNS-Resolver-Proxy konfiguriert werden: https://coredns.io/2016/11/26/dns-over-https/

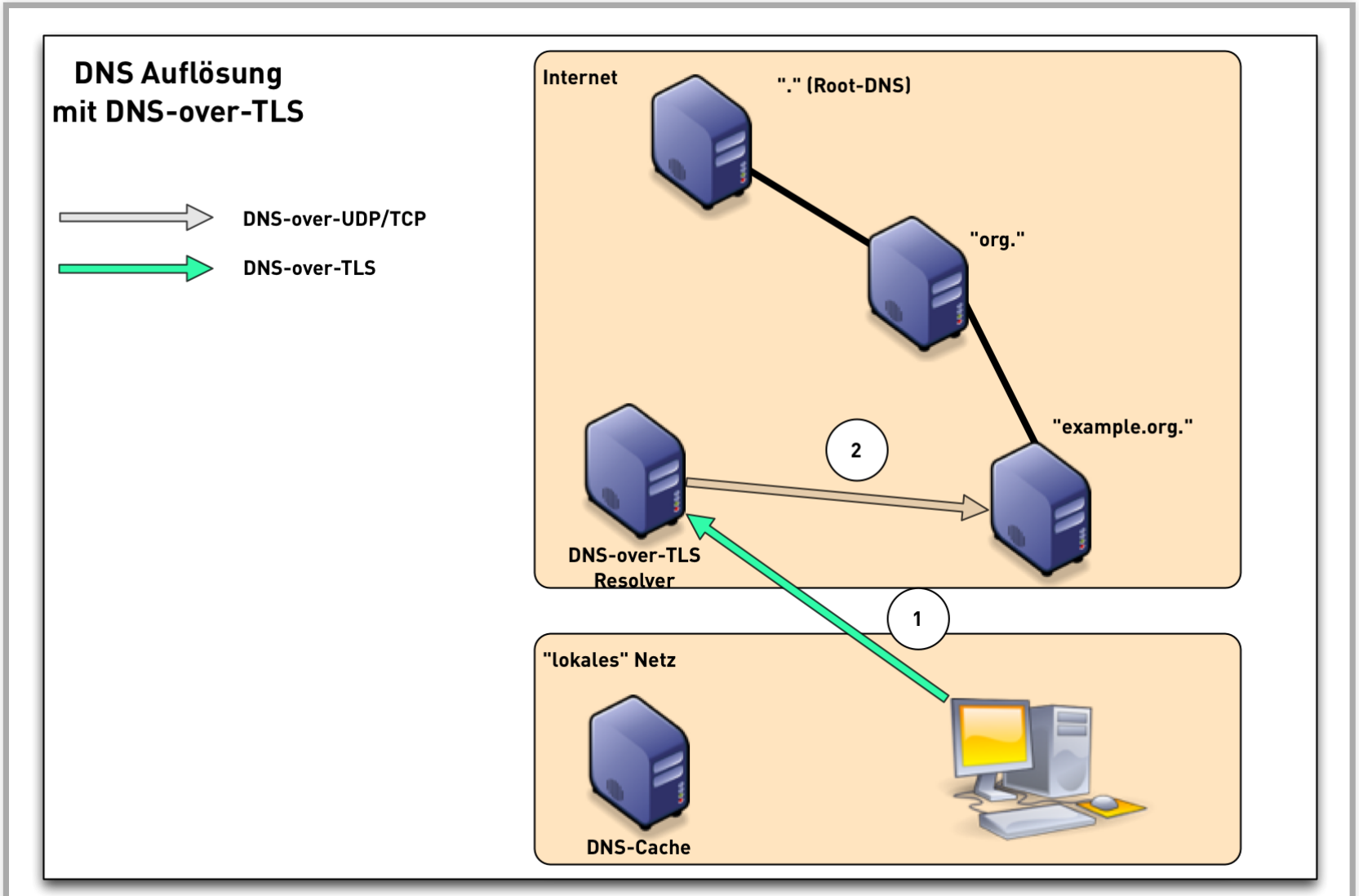
DoT - DNS-over-TLS

- RFC 7858 "Specification for DNS over Transport Layer Security (TLS)"
- DNS wireformat over TLS over TCP
- Port 853 (TCP)
- Bietet Verschlüsselung und Authentisierung (CA-Modell oder per DANE)

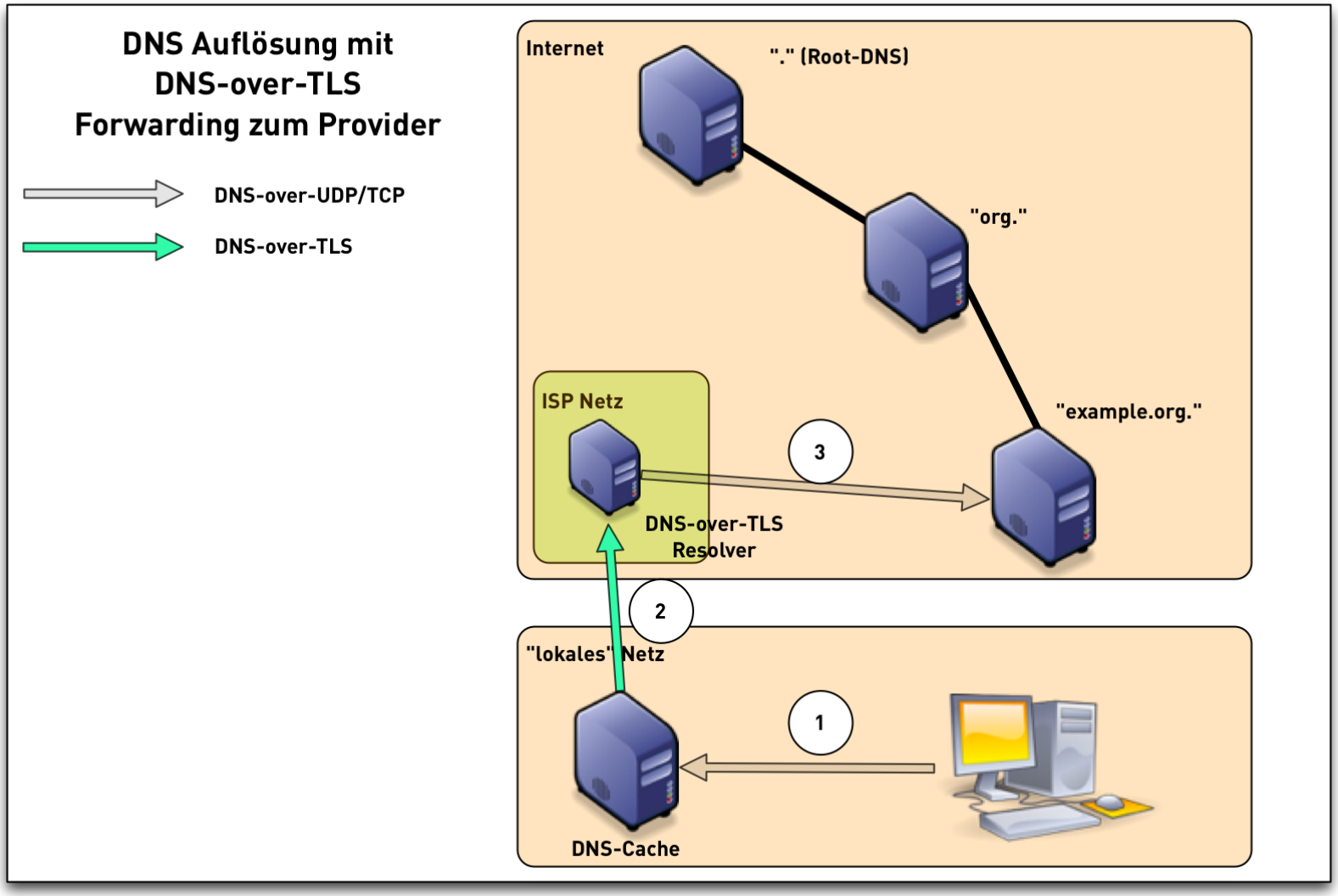
DNS-over-TLS (1/3)



DNS-over-TLS (2/3)



DNS-over-TLS (3/3)



Geschwindigkeit von DNS-over-TLS

- DNS-over-TLS Geschwindigkeit/Latenz bei der Benutzung von TLS 1.3 ist sehr gut
- bei bestehenden TLS-Verbindungen vergleichbare Geschwindigkeit zu DNS-over-UDP
  - Pipelining
  - TCP fast open
  - 0-RTT resume
- derzeit sind die verfügbaren Implementationen noch nicht vollständig optimiert

DNS-over-TLS Betriebsmodi

- DNS-over-TLS kann in zwei Modi betrieben werden
  - **opportunistic** - versuche TLS, benutze den Server auch wenn die TLS-Authentisierung fehlschlägt
  - **strict** - Verbindung wird nur benutzt, wenn es beim TLS-Verbindungsaufbau keine Fehler gab (Authentisierung etc.)

DNS-over-TLS Client Implementierungen

- DoT Client Implementierungen
  - Android "Pi" (9)
  - Linux systemd
  - Knot-DNS / Unbound / PowerDNS dnsdist Load-Balancer
  - DNS Privacy Daemon - Stubby
  - jDNSProxy *Simple fast and lightweight DNS proxy and cache, implementing DNS-over-TLS, DNS-over-HTTPS, and Serve-Stale*

DNS-over-TLS Server Implementierungen

- DoT Server Implementierungen
  - CoreDNS
  - TentaDNS
  - jeder DNS-Server via `stunnel`, `ha-proxy`, `nginx`, `relayd` (OpenBSD)

DNS-over-TLS Anbieter

- Anbieter
  - Cloudflare/APNIC Resolver (1.1.1.1)
  - Quad9 Resolver (9.9.9.9)
  - SurfNET
  - Verisign
  - weitere DoT Server auf der Seite des DNS Privacy Projektes...

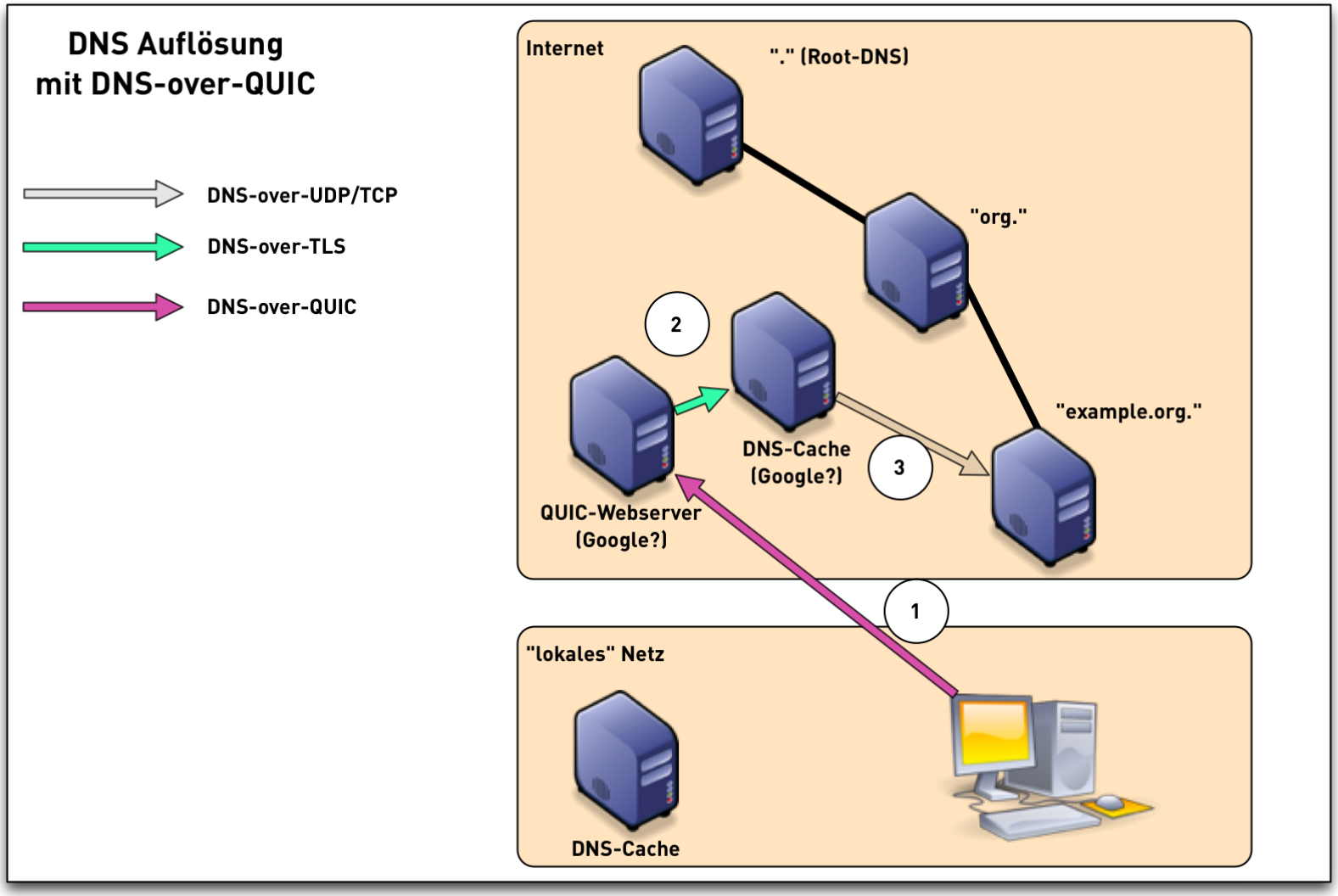
DoQ - DNS over QUIC

- DNS over QUIC over UDP
- *Specification of DNS over Dedicated QUIC Connections* https://tools.ietf.org/html/draft-huitema-quic-dnsoquic

was ist QUIC

- moderner TCP-Ersatz von Google, wird derzeit in der IETF standardisiert
  - benutzt UDP, implementiert TCP Funktionen
  - ist Bestandteil von Anwendungen, nicht im Betriebssystem-Kern
  - beinhaltet TLS 1.3
  - 0-RTT
- Geschwindigkeit vergleichbar mit klassischem DNS-over-UDP
- QUIC Dokumente https://tools.ietf.org/wg/quic/

DNS over QUIC



DNS over QUIC im Vergleich

	UDP	TCP	TLS	DTLS	QUIC
Transport efficiency					
Connection set up time	✓	✗	✗	✗	**0-RTT**
Head of queue blocking	✓	✗	✗	✓	✓
Retransmission efficiency	✗	✓	✓	✗	✓
Long messages (DNSSEC)	✗	✓	✓	✗	✓
Security					
Three ways handshake	✗	✓	✓	✓	✓
Encryption & Authentication	✗	✗	✓	✓	✓

Source: https://datatracker.ietf.org/meeting/99/materials/slides-99-dprive-dns-over-quic

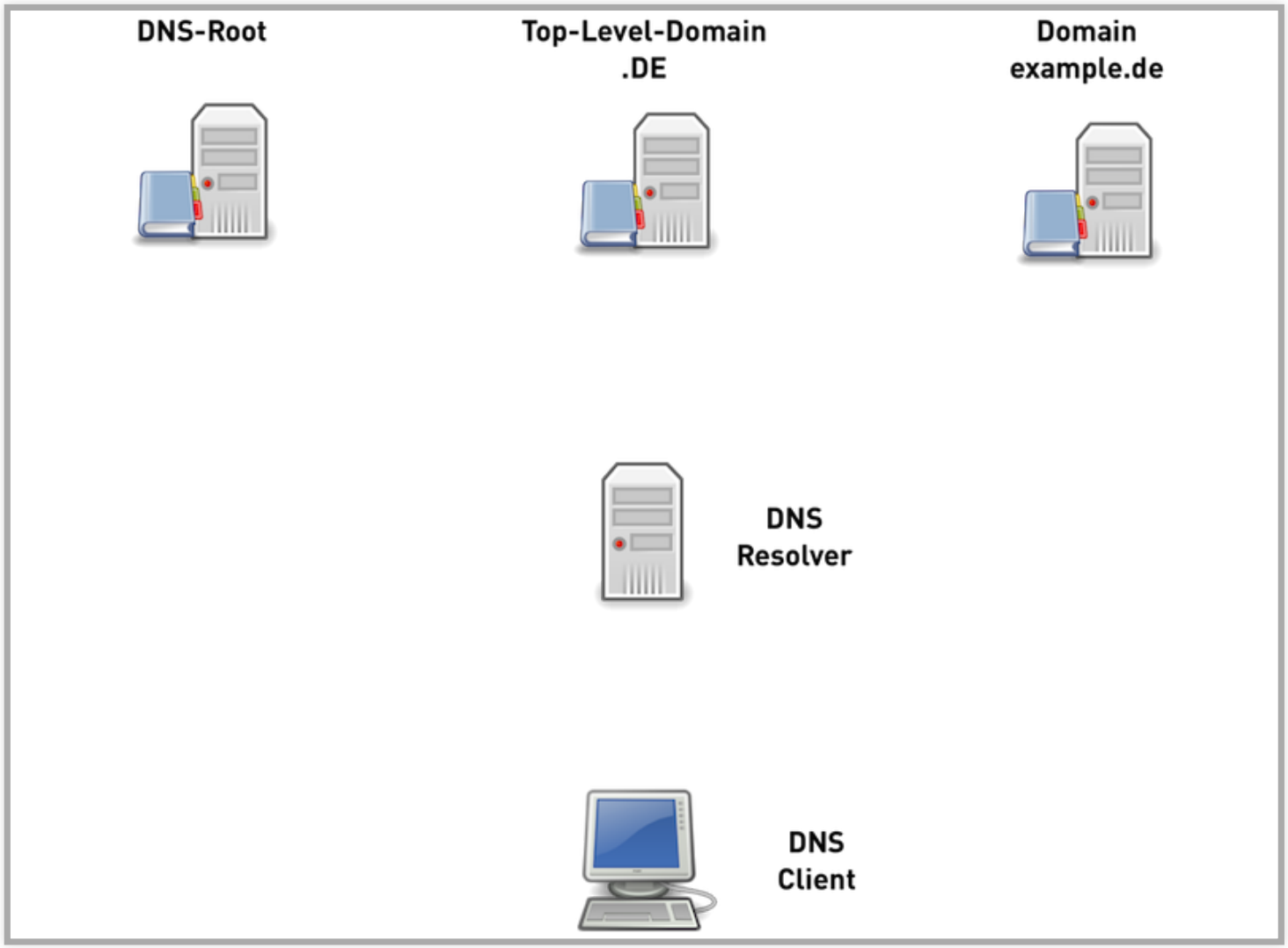
QNAME-Minimization

- klassische Implementierungen sind sehr gesprächig
  - es werden Daten gefragt/geliefert, welche (heute) vom DNS-Protokoll nicht unbedingt benötigt werden

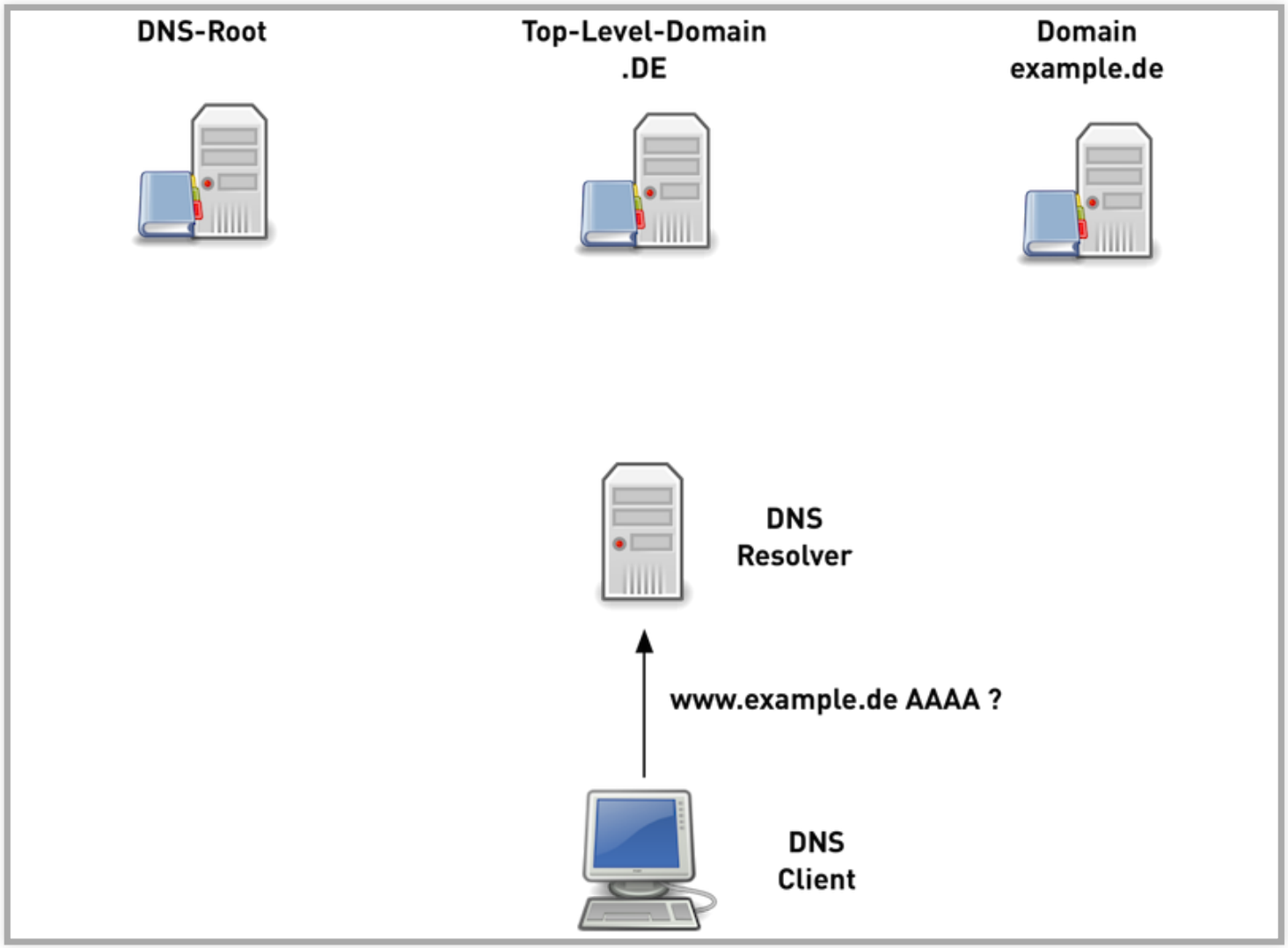
QNAME-Minimization

- RFC 7816 *DNS Query Name Minimisation to Improve Privacy* spezifiziert DNS-Namensauflösung mit minimalen Metadaten
  - nur DNS-Resolver müssen angepasst werden.
  - DNS-Clients, DNS-Authoritative-Server, Firewalls etc. brauchen keine Anpassung
  - QNAME-Minimization ist keine Änderung des DNS-Protokolls, nur eine Implementierungs-Empfehlung!

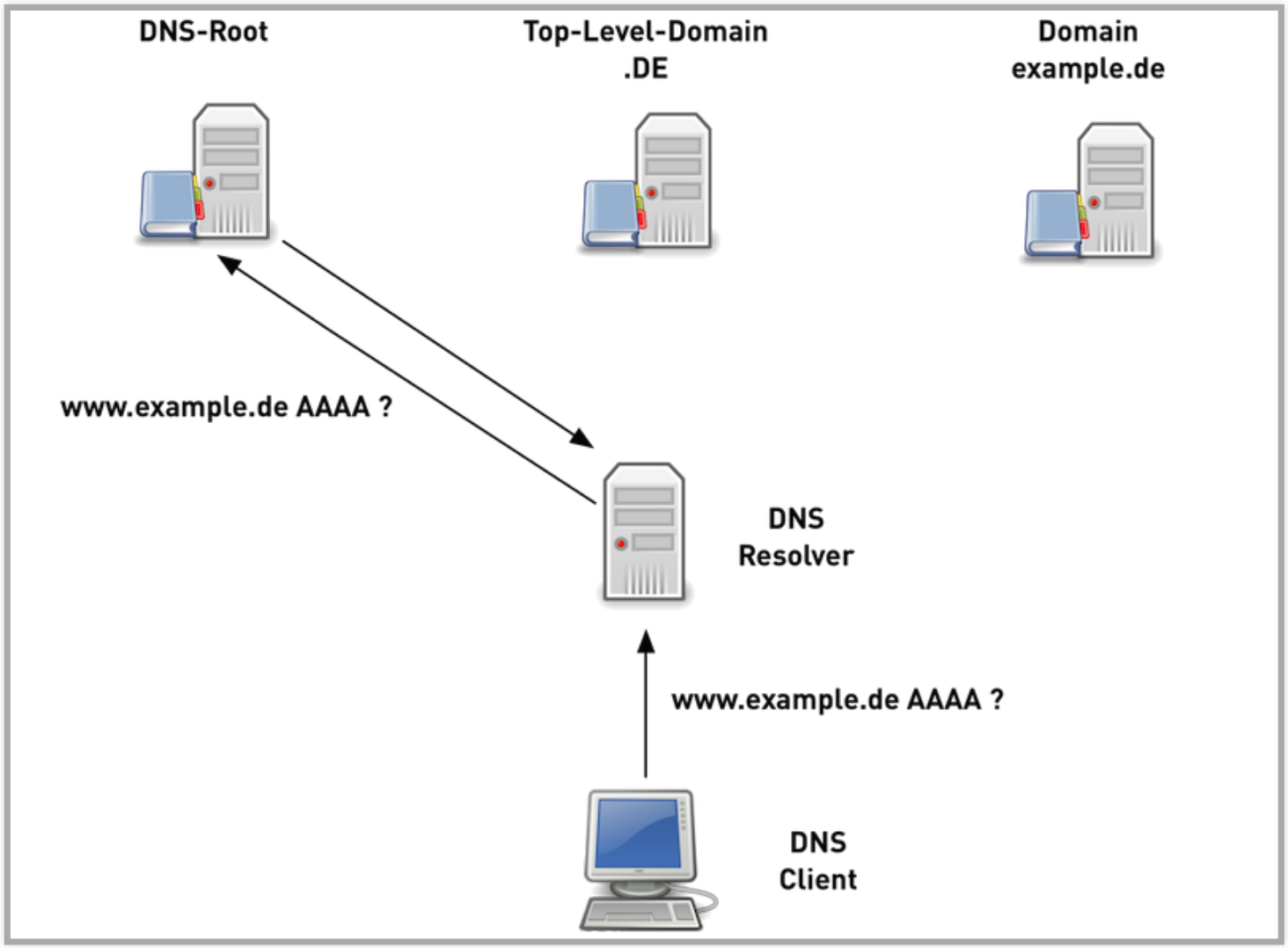
Traditionelle DNS Namensauflösung (1/6)



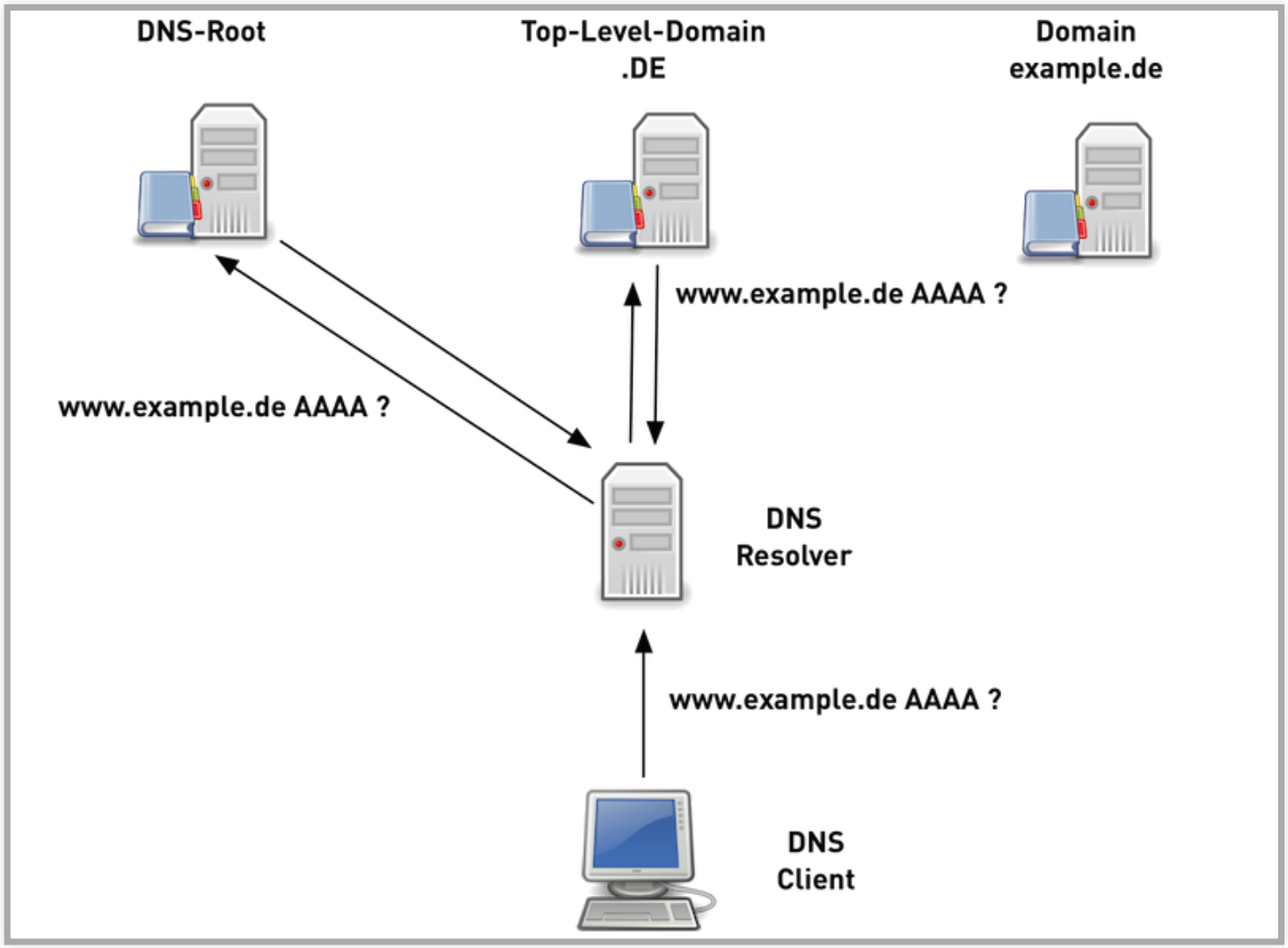
Traditionelle DNS Namensauflösung (2/6)



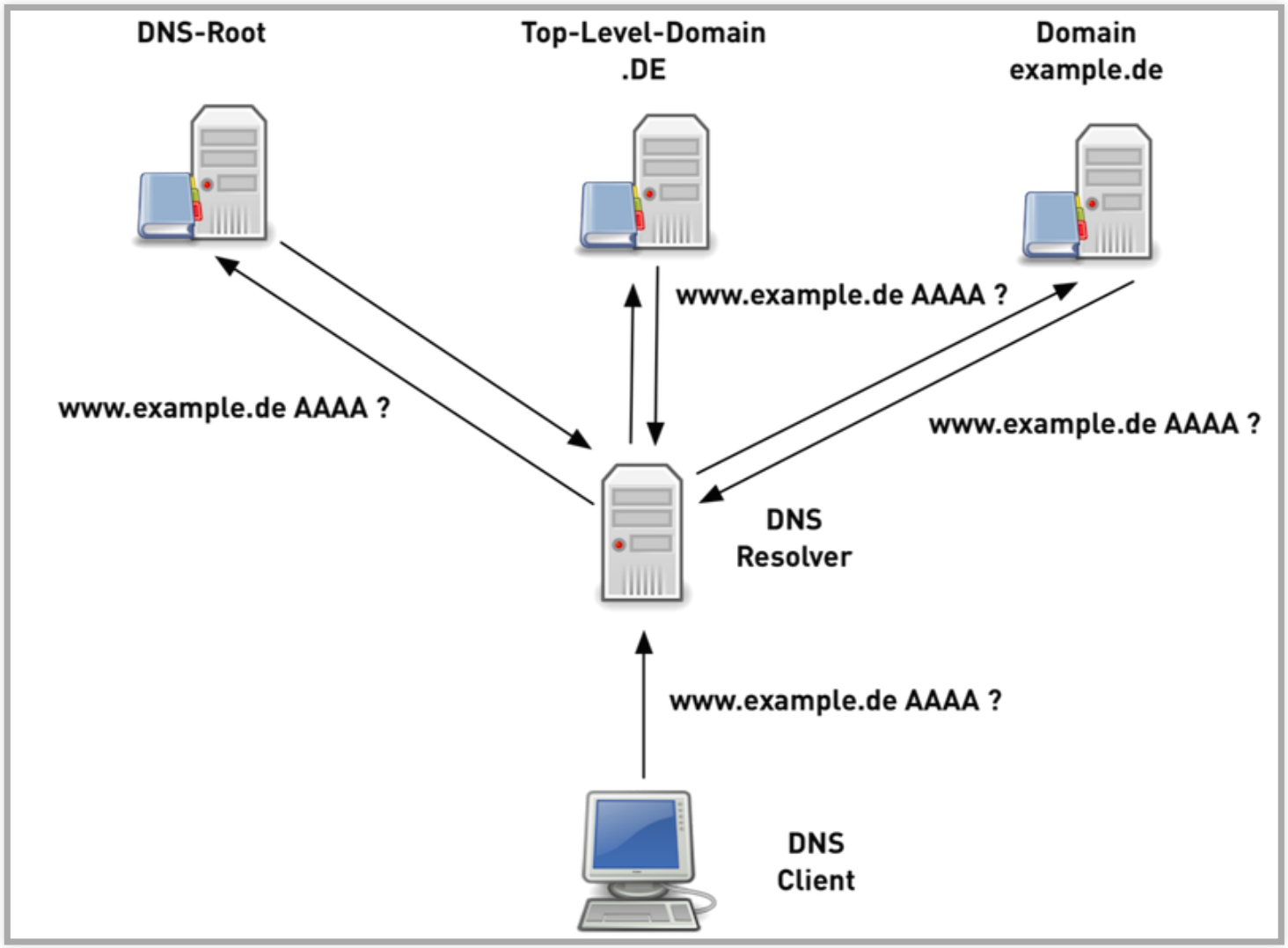
Traditionelle DNS Namensauflösung (3/6)



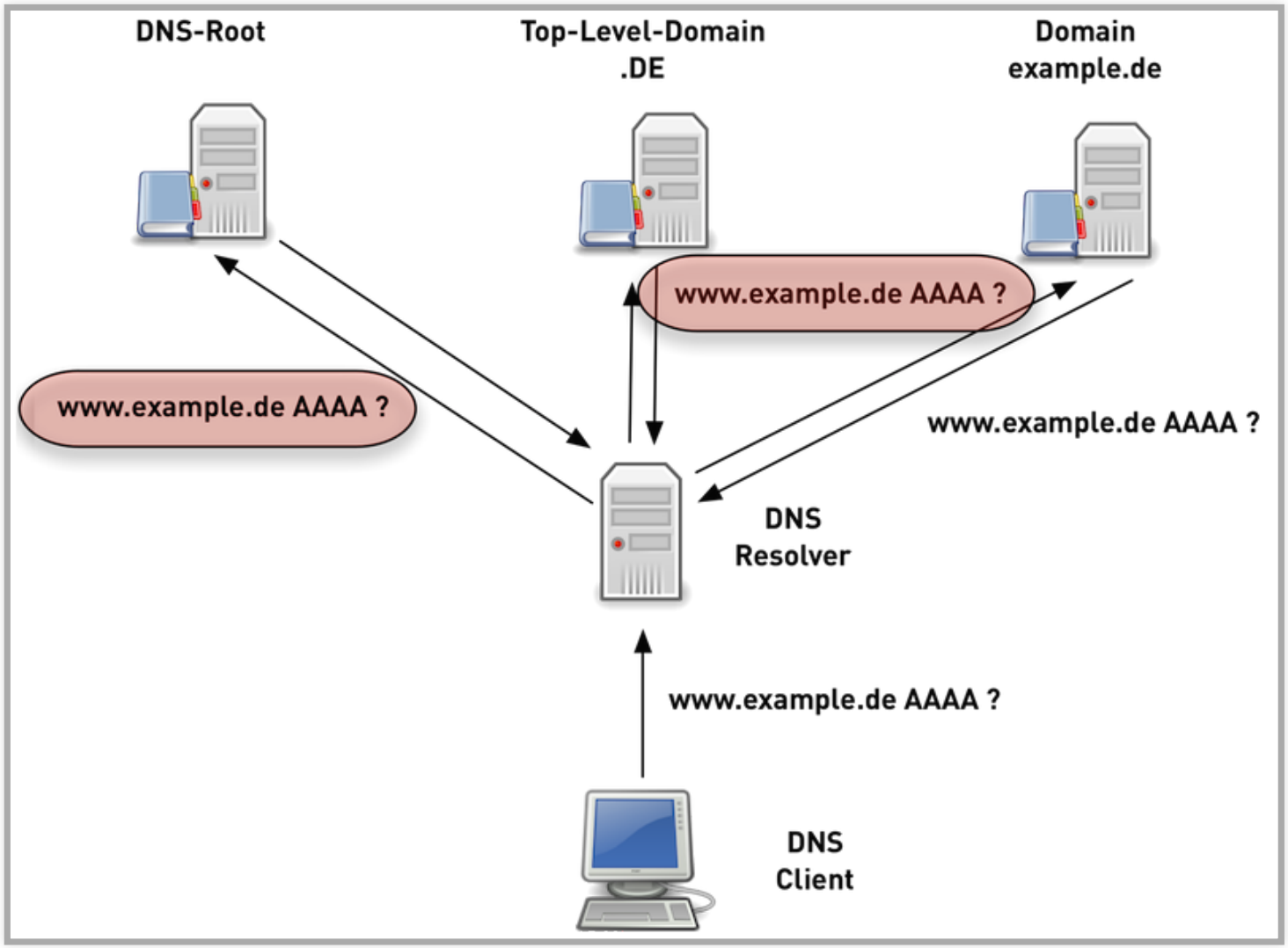
Traditionelle DNS Namensauflösung (4/6)



Traditionelle DNS Namensauflösung (5/6)



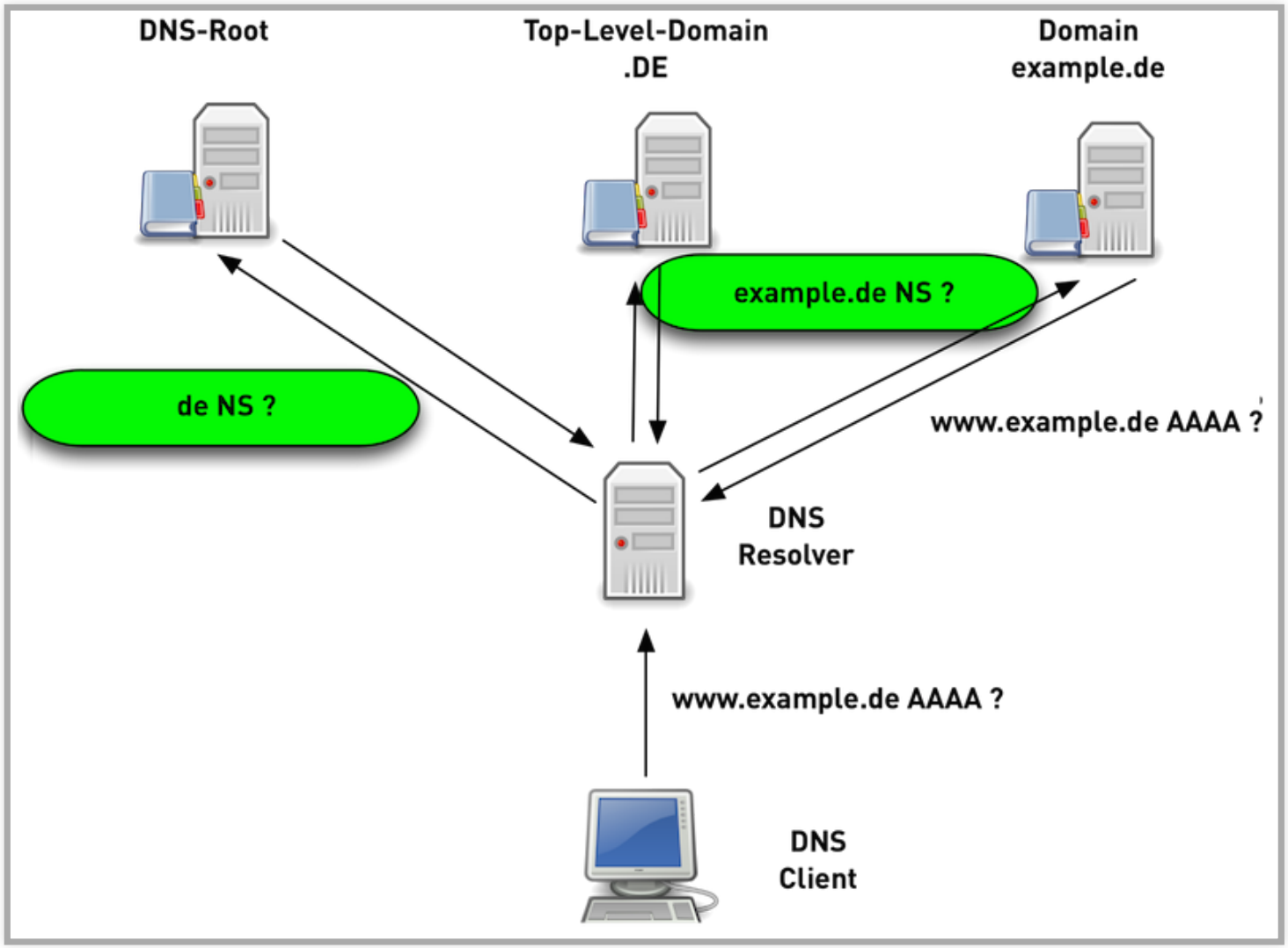
Traditionelle DNS Namensauflösung (6/6)



DNS Namensauflösung mit QNAME Minimization

- bei einem DNS-Resolver mit QNAME Minimization *kennt* der DNS-Server die Struktur des DNS im Internet (Root -> TLD -> SLD ...)
- der DNS-Resolver fragt für jede Ebene nach dem *notwendigen* Domain-Namen (Delegation/Ziel-Name)
- in den meisten Fällen ist DNS-Auflösung mit QNAME-Minimization *gleich schnell* oder sogar *schneller* verglichen mit traditioneller DNS Auflösung

DNS Namensauflösung mit QNAME Minimization



QNAME-Minimization Implementierungen

- Unbound
- Knot-Resolver
- BIND 9.13 (in Entwicklung)

QNAME Minimization Test

Einfacher Test per `dig`, ob der benutzte DNS-Resolver QNAME-Minimization anbietet

```
shell$ dig txt qnamemintest.internet.nl +short
a.b.qnamemin-test.internet.nl.
"HOORAY - QNAME minimisation is enabled on your resolver :)!"
```

Zusammenfassung und Ausblick (1/3)

- das DNS Protokoll entwickelt sich derzeit schnell weiter
  - zu schnell? (siehe “The DNS Camel”, or, the rise in DNS complexity und RFC 8324 *DNS Privacy, ...: Time for Another Look?*)
- Kommunikation zwischen DNS-Client und DNS-Resolver wird in Zukunft verschlüsselt (DNS-over-TLS, DNS-over-HTTPS, DNS-over-QUIC)
- DNS-over-HTTPS/QUIC kann zur Zentralisierung, oder aber auch zur De-Zentralisierung von DNS-Diensten führen

Zusammenfassung und Ausblick (2/3)

- neue DNS-Protokollerweiterungen ...
  - ... schützen die Privatsphähre von DNS-Nutzern
  - ... erhöhen die Sicherheit der DNS-Kommunikation
  - ... verringern die Nutzbarkeit von DNS-IDS/Passive-DNS
- Sicherheitstechniken, basierend auf der Auswerung von DNS-Daten, sind in Zukunft weniger effektiv

Zusammenfassung und Ausblick (3/3)

- was kann heute getan werden?
  - DNSSEC Validierung auf DNS-Resolvern einschalten
  - Absicherung der eigenen Zonen per DNSSEC-Signaturen (DNSSEC-Signing)
  - bei Forwarding zum ISP-Resolver: **DNS-over-TLS** einsetzen (Provider motivieren, DoT anzubieten)
  - Authoritative-DNS-Server und DNS-Resolver Funktionen im Unternehmensnetzwerk trennen
  - QNAME-Minimization einschalten
  - eigene DNS-Resolver überwachen (Monitoring)

Vielen Dank!

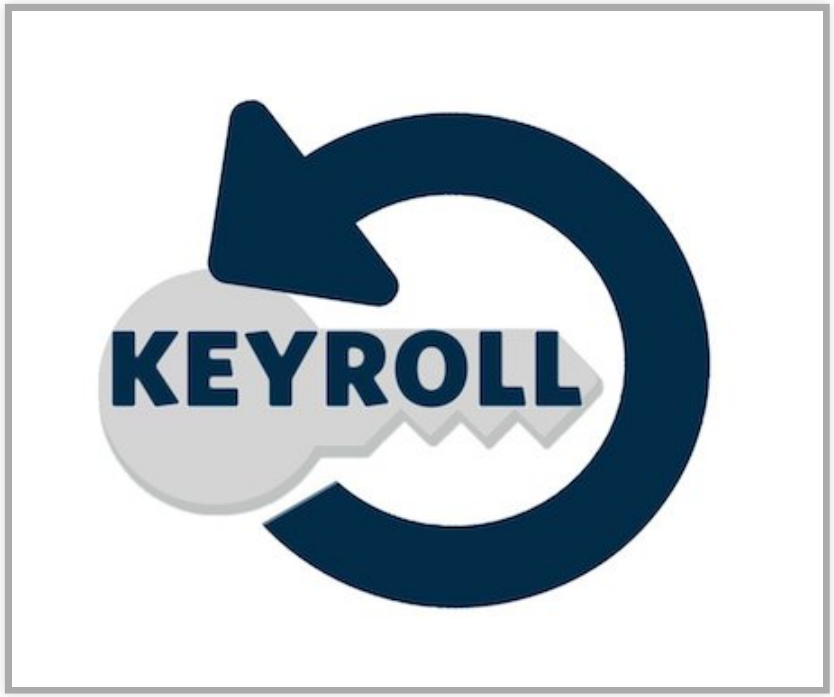
Fragen ?

Kontakt: `cstrotm@dnsworkshop.de`

Dank an sys4 AG, Men & Mice, Heise Verlag und Linuxhotel

Präsentation mit Hilfe von Emacs 26, Org-Mode und Reveal.js

KSK-Roll nicht vergessen



https://twitter.com/hashtag/keyroll