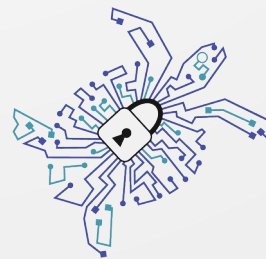


# DNS-over-HTTPS Intro für ISPs

**ATNOG Juli 2019**



Foundation for  
Applied Privacy

# Foundation for Applied Privacy

- Non-profit Privacy Infrastruktur Provider
- Privacy Enhancing Technology Dienste für die Öffentlichkeit
- 2018 gegründet
- Top 3 Tor Relay Operator (weltweit)
- DoH und DoT Resolver Betreiber
- ISPA Member



# Ziele dieses Vortrags

- Welche Probleme löst DoH?
- Wie sieht DoH technisch aus?
- Browser Deployment Strategien
- Potentielle neuen Herausforderungen für ISPs
- DNS Zentralisierung: Risiko + Mitigation



# Warum DNS Traffic schützen?



Foundation for  
Applied Privacy



User/Browser

de.wikipedia.org  
Webserver

DNS  
Resolver



Foundation for  
Applied Privacy

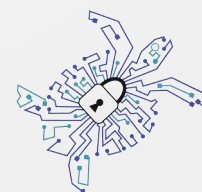
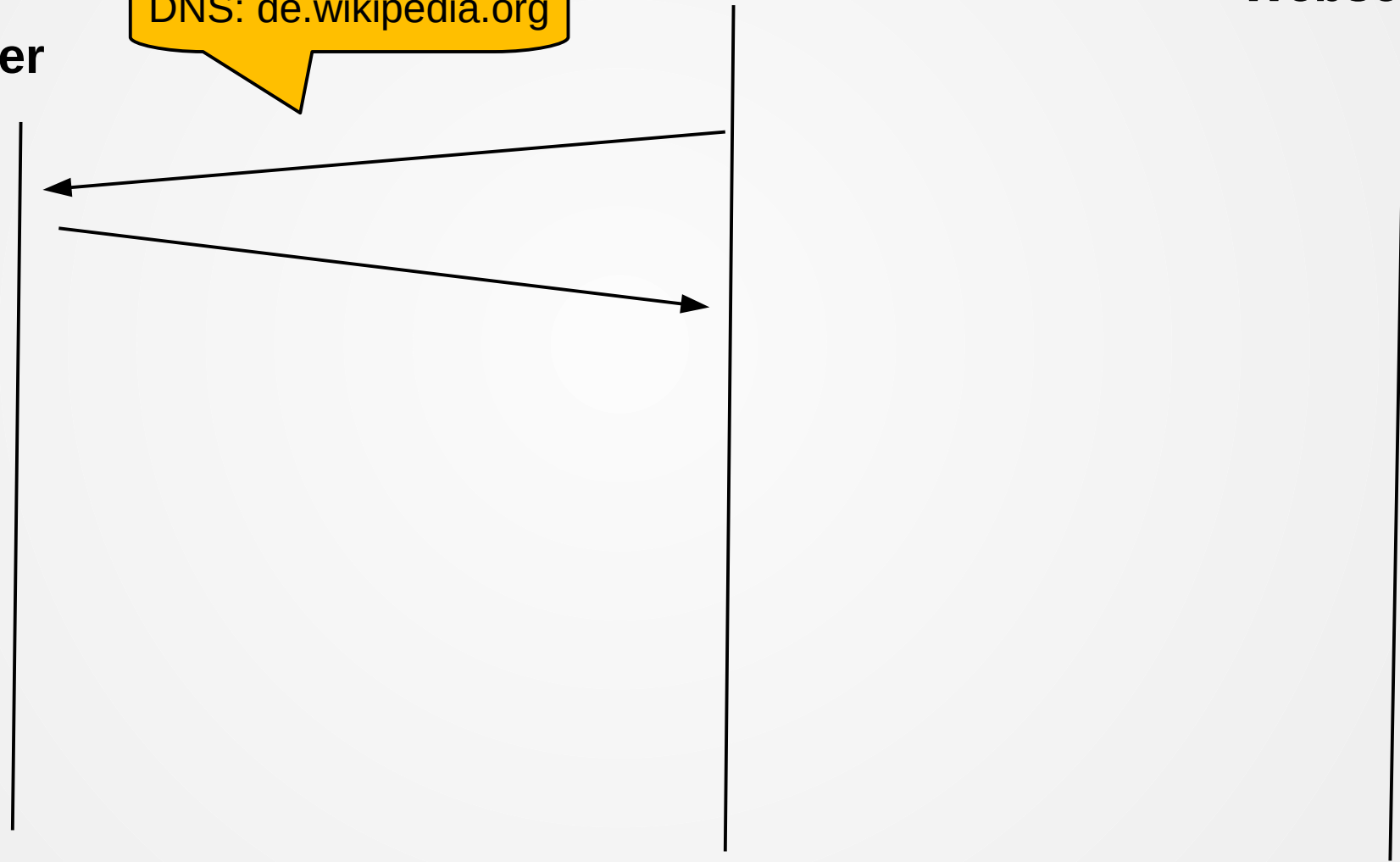


User/Browser

de.wikipedia.org  
Webserver

DNS  
Resolver

DNS: de.wikipedia.org



Foundation for  
Applied Privacy



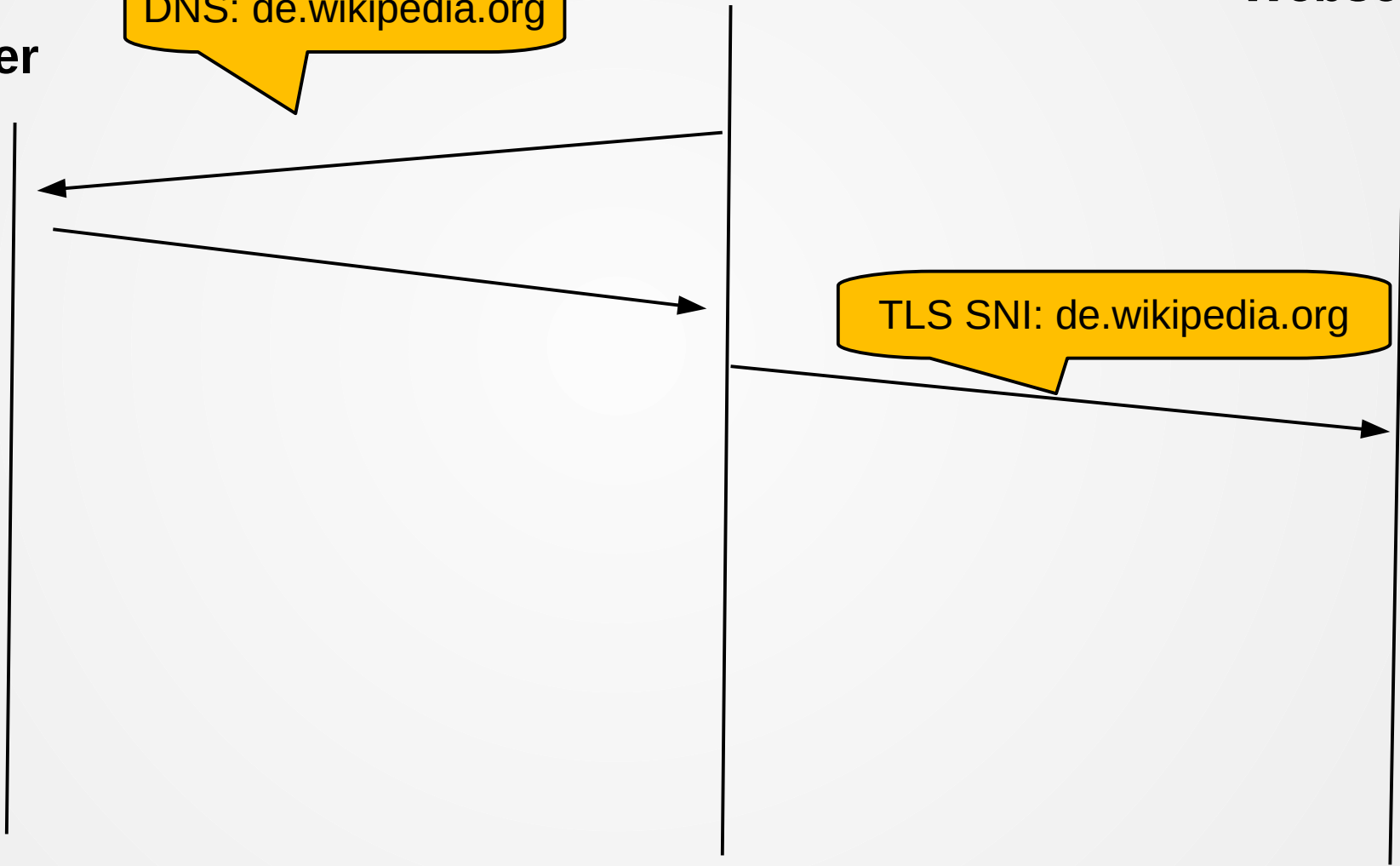
User/Browser

de.wikipedia.org  
Webserver

DNS  
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org



Foundation for  
Applied Privacy

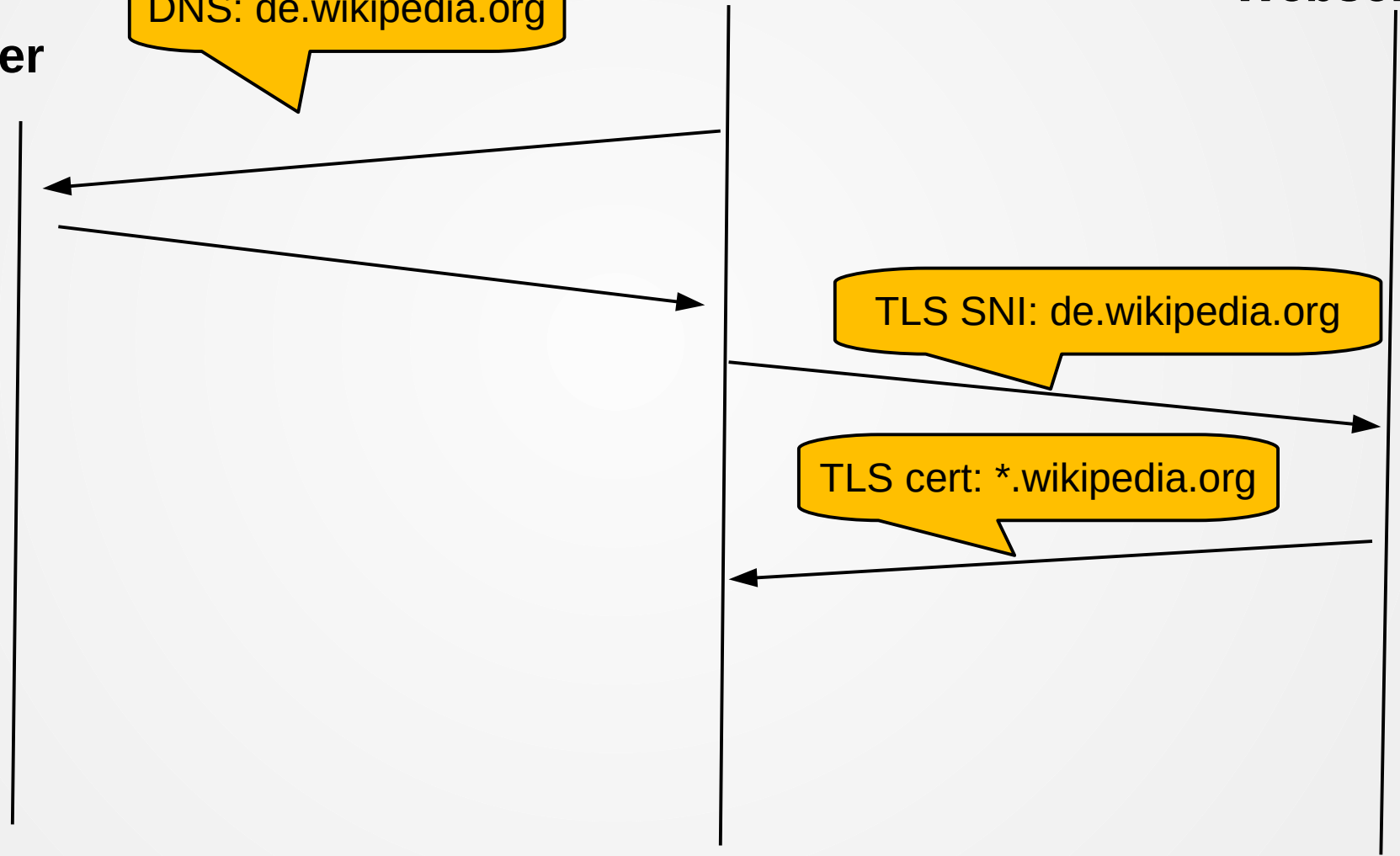


User/Browser

de.wikipedia.org  
Webserver

DNS  
Resolver

DNS: de.wikipedia.org



Foundation for  
Applied Privacy



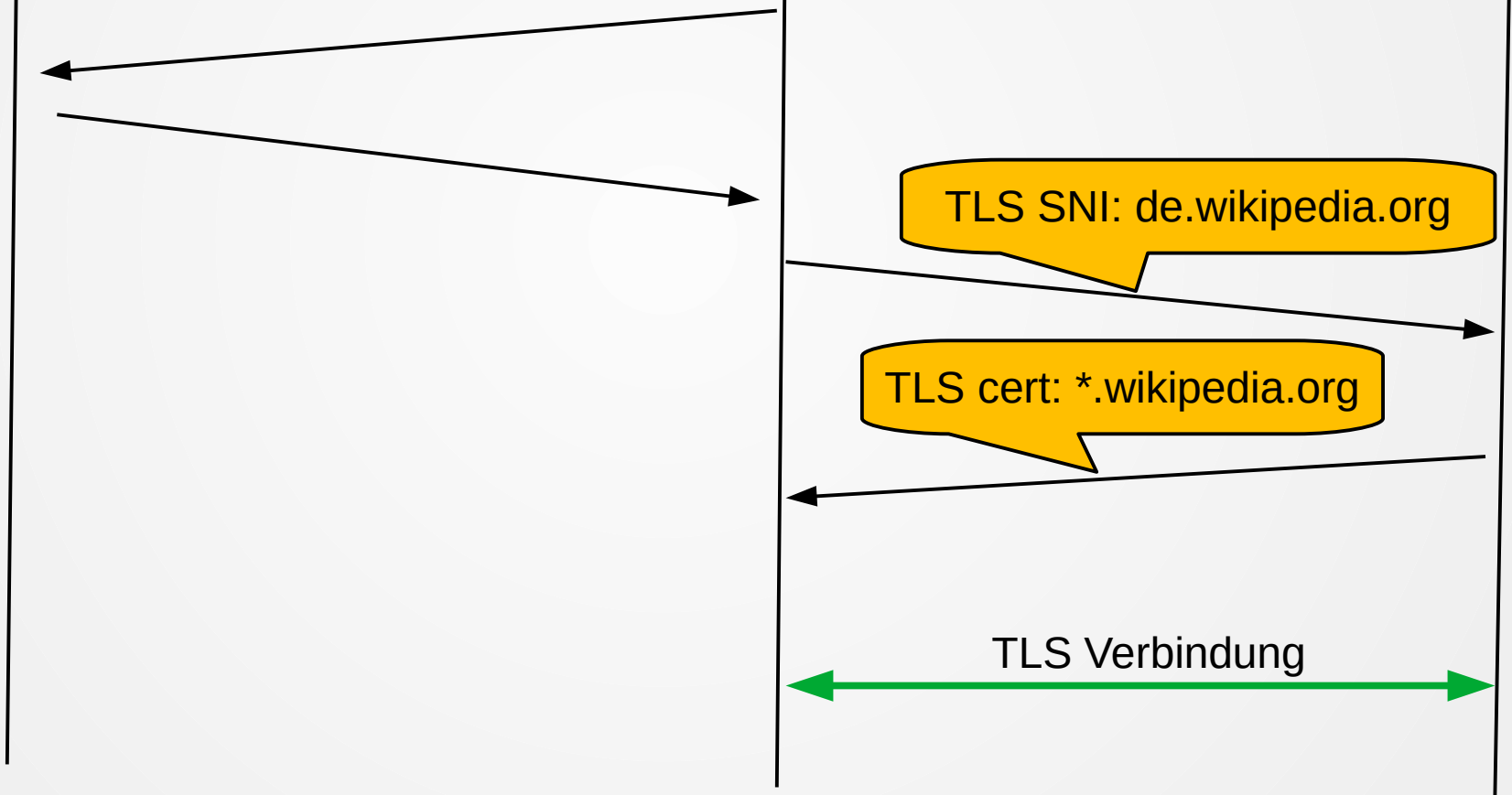


User/Browser

de.wikipedia.org  
Webserver

DNS  
Resolver

DNS: de.wikipedia.org



TLS SNI: de.wikipedia.org

TLS cert: \*.wikipedia.org

TLS Verbindung



Foundation for  
Applied Privacy



User/Browser

de.wikipedia.org  
Webserver

DNS  
Resolver

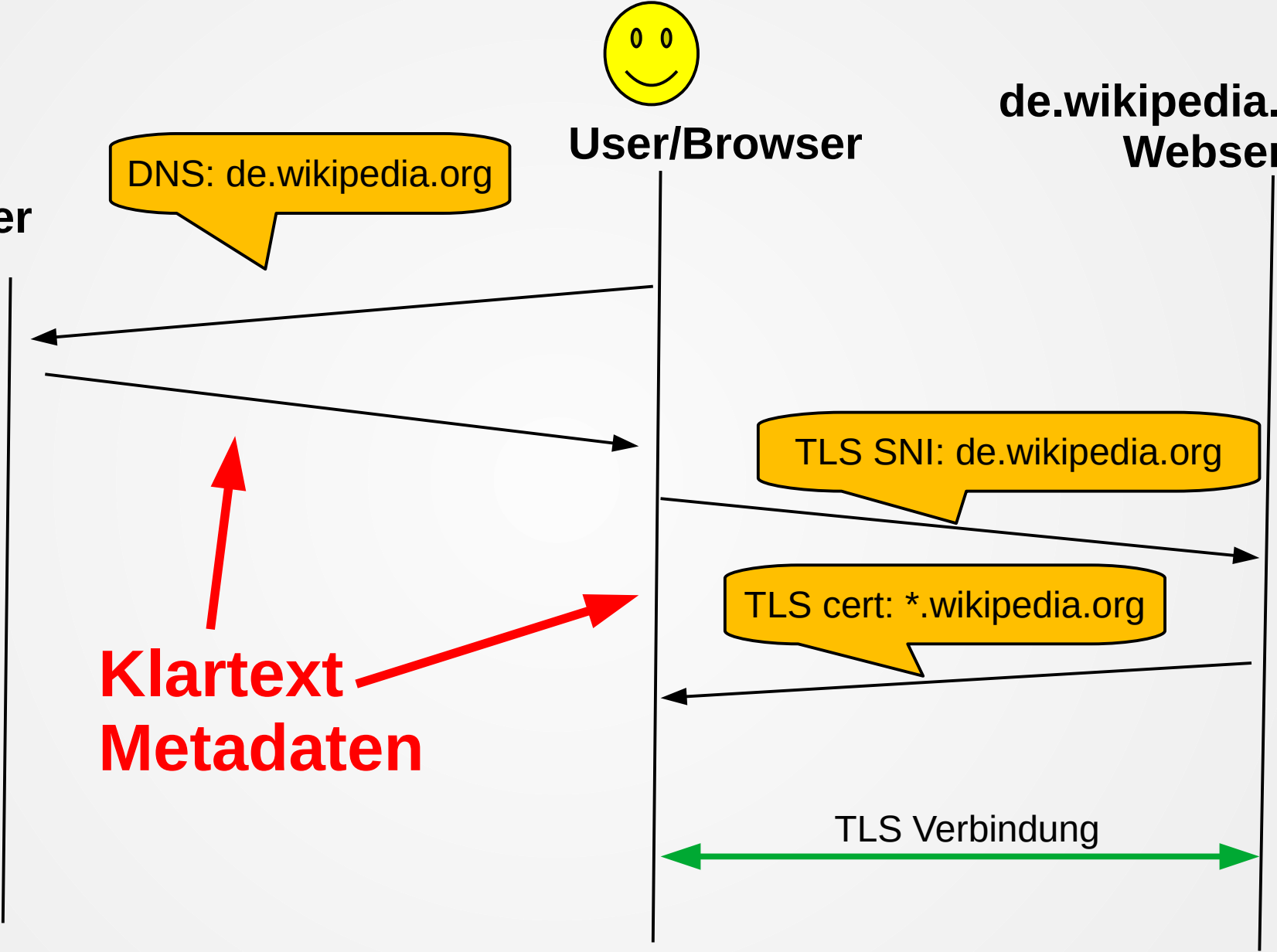
DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: \*.wikipedia.org

**Klartext  
Metadaten**

TLS Verbindung



Foundation for  
Applied Privacy

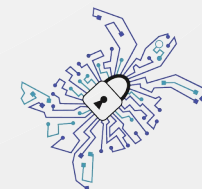
Internet Engineering Task Force (IETF)  
Request for Comments: 7258  
BCP: 188  
Category: Best Current Practice  
ISSN: 2070-1721

S. Farrell  
Trinity College Dublin  
H. Tschofenig  
ARM Ltd.  
May 2014

## **Pervasive Monitoring Is an Attack**

### Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.



# Ziel

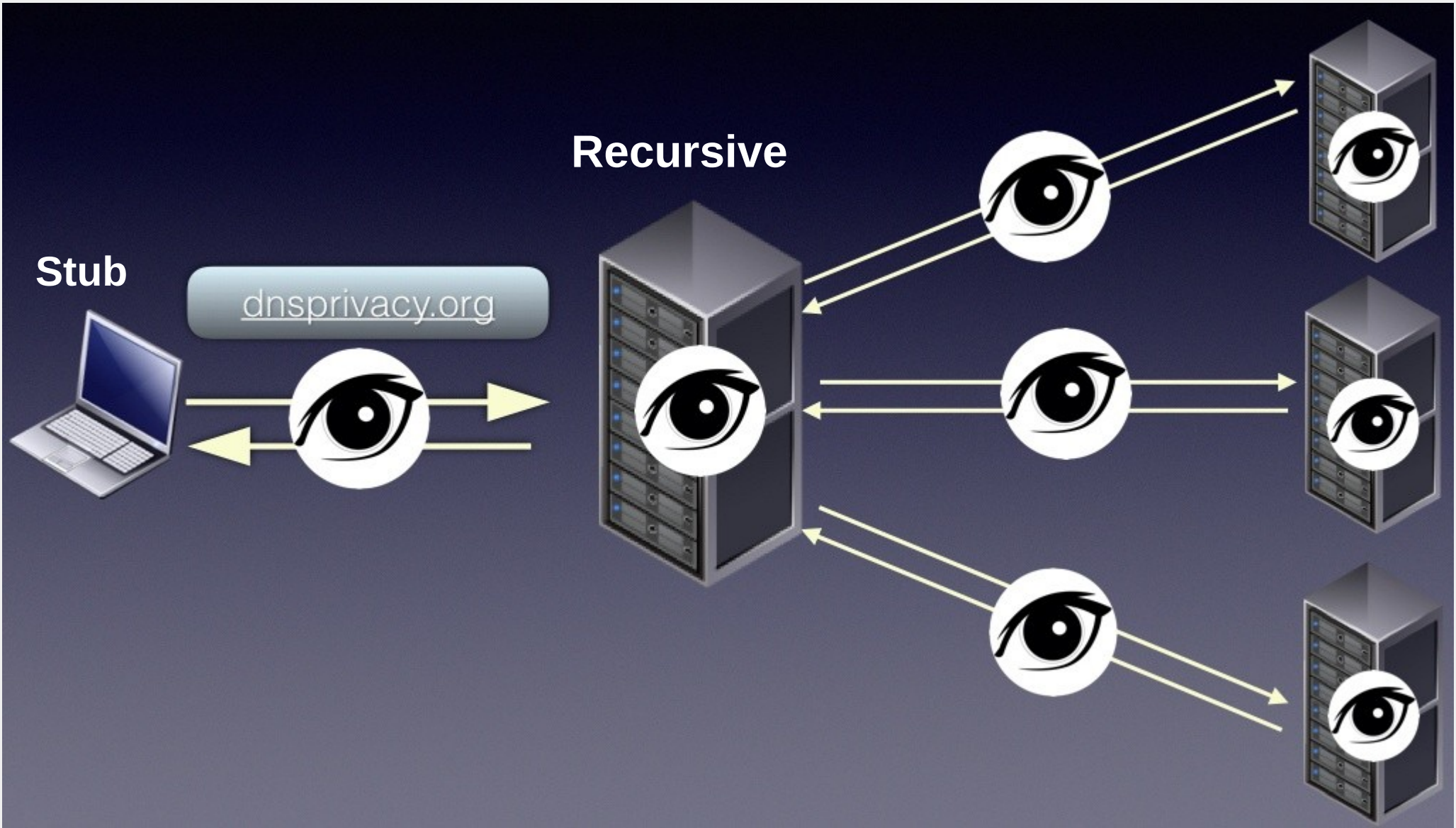
## **Schutz von Metadaten (Hostnamen)**



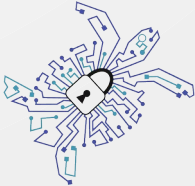
# DNS



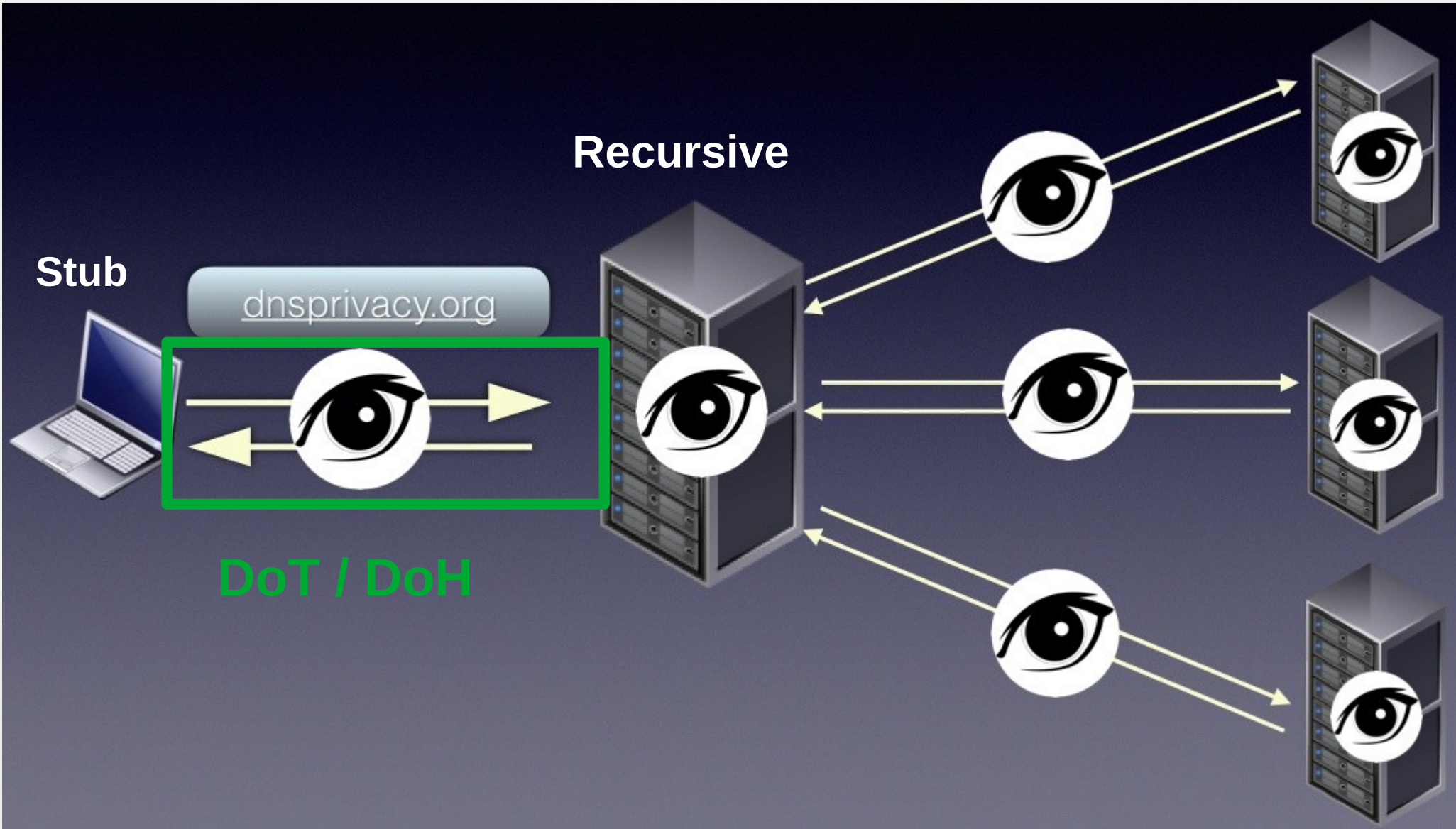
Foundation for  
Applied Privacy



Quelle: [dnsprivacy.org](https://dnsprivacy.org)



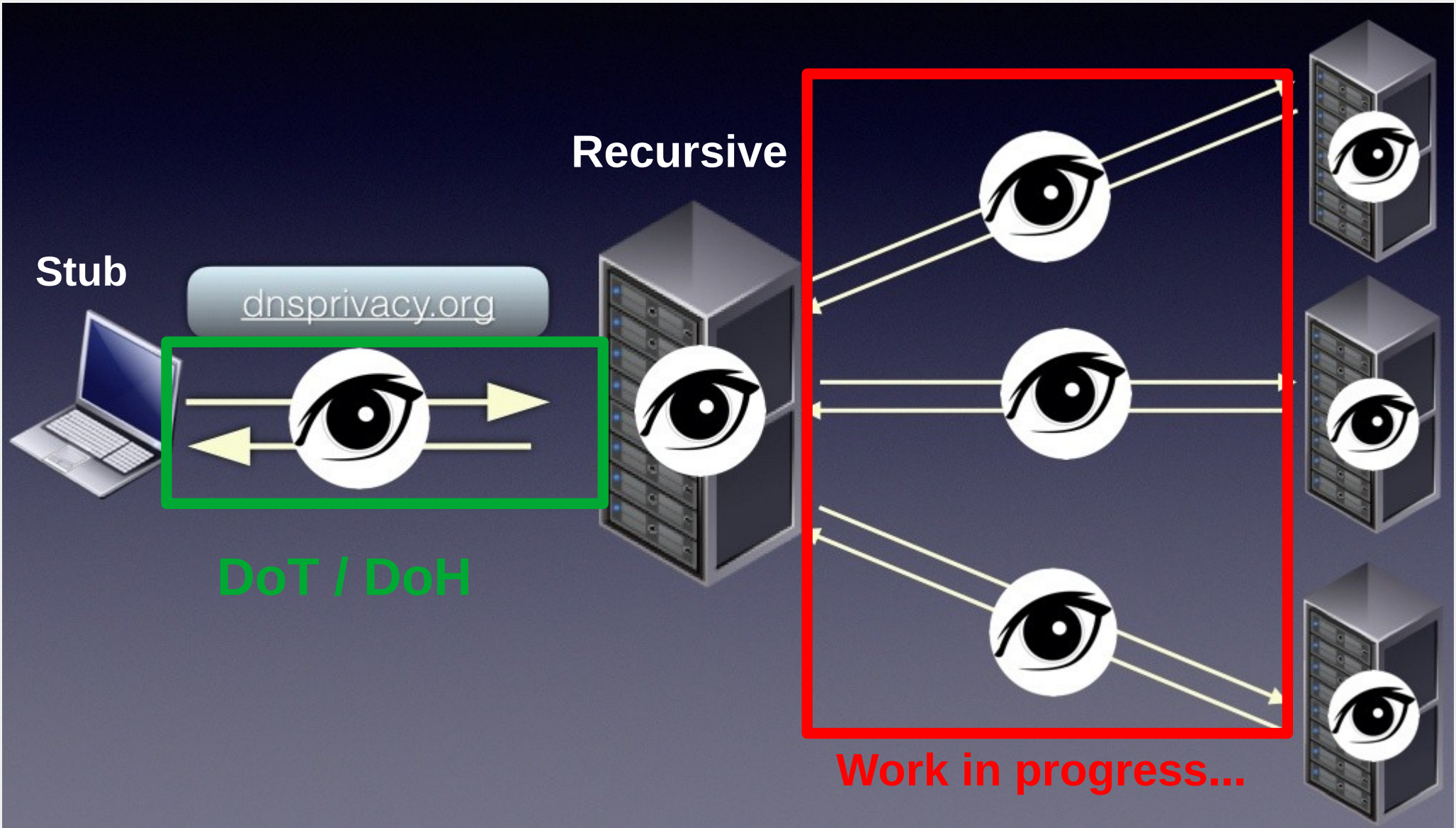
Foundation for Applied Privacy



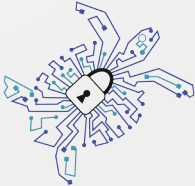
Quelle: dnsprivacy.org



Foundation for  
Applied Privacy



Quelle: dnsprivacy.org



Foundation for Applied Privacy



# DNS-over-HTTPS (DoH)

RFC 8484 (Okt 2018)



Foundation for  
Applied Privacy

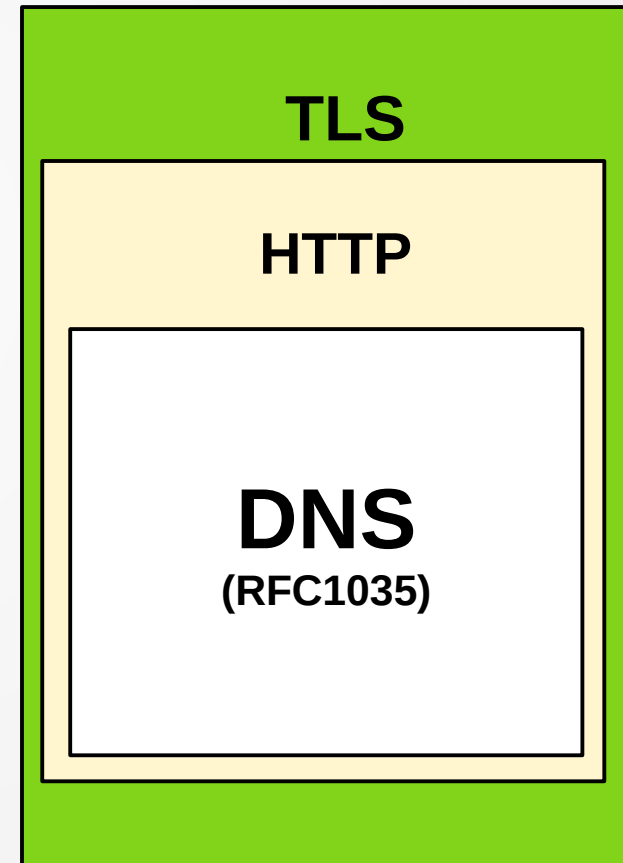
# DoH - Motivation

- DNS Traffic vertraulich übertragen
- DNS Traffic vor Manipulation schützen
- soll auch in restriktiven Netzen funktionieren (in denen zB. nur 53/80/443 erlaubt ist)
- vor allem von Browsern getrieben






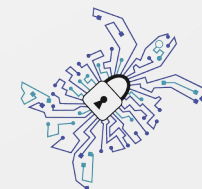
# DoH

- HTTPS (TCP/443)
- **POST**
- oder GET (base64url)
- HTTP/2 (empfohlen)
- Content Type:  
application/dns-message



# DoH Anfrage (entschlüsseltes Beispiel)

- ▼ Transport Layer Security  **TLS**
  - ▶ TLSv1.3 Record Layer: Application Data Protocol: http2
- ▼ HyperText Transfer Protocol 2  **HTTP/2**
  - ▶ Stream: DATA, Stream ID: 71, Length 54
- ▼ Domain Name System (query)  **DNS**  
RFC1035
  - Transaction ID: 0x0000
  - ▶ Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 1
- ▼ Queries
  - ▶ www.wikipedia.org: type AAAA, class IN
  - ▶ Additional records

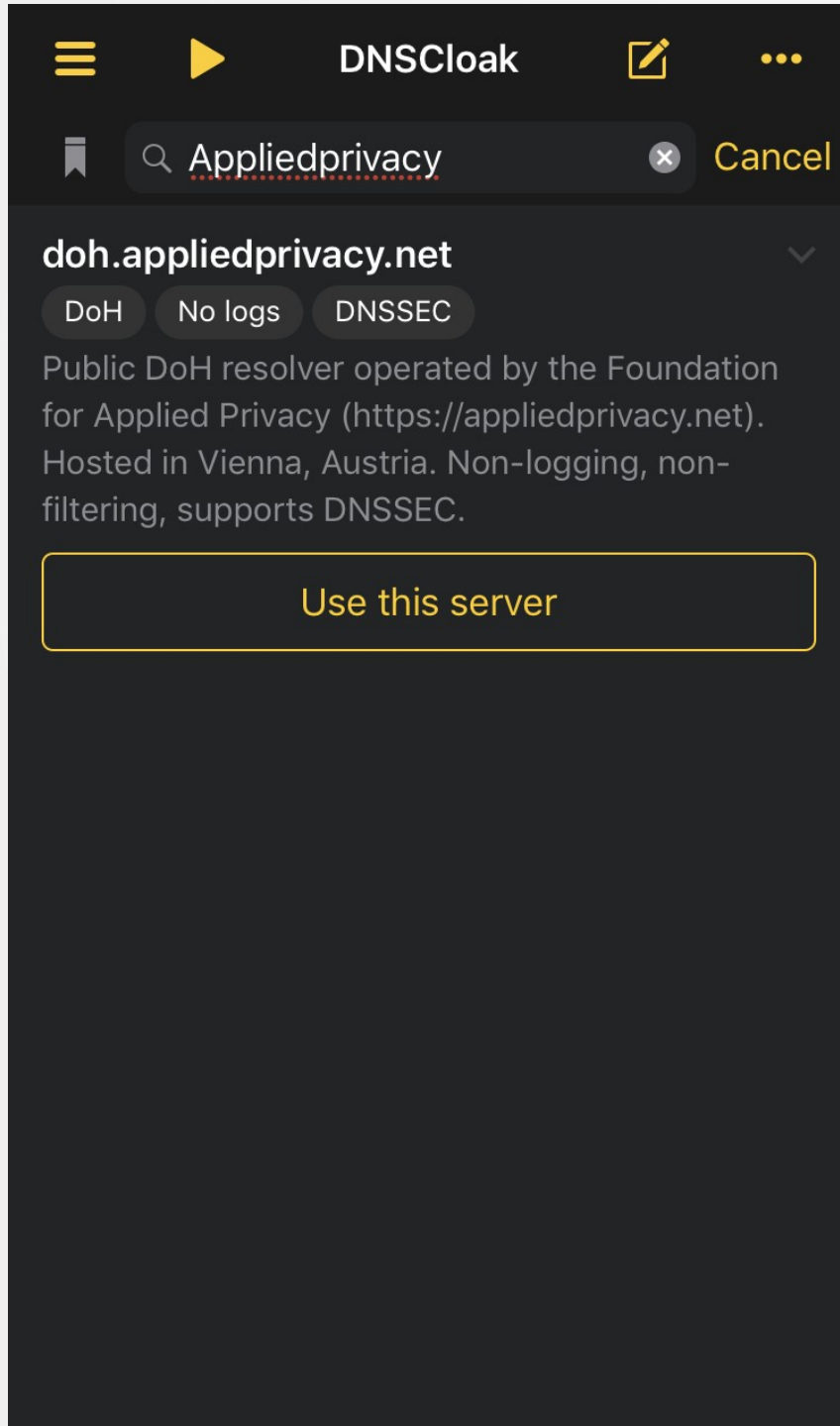


# DoH Client Software

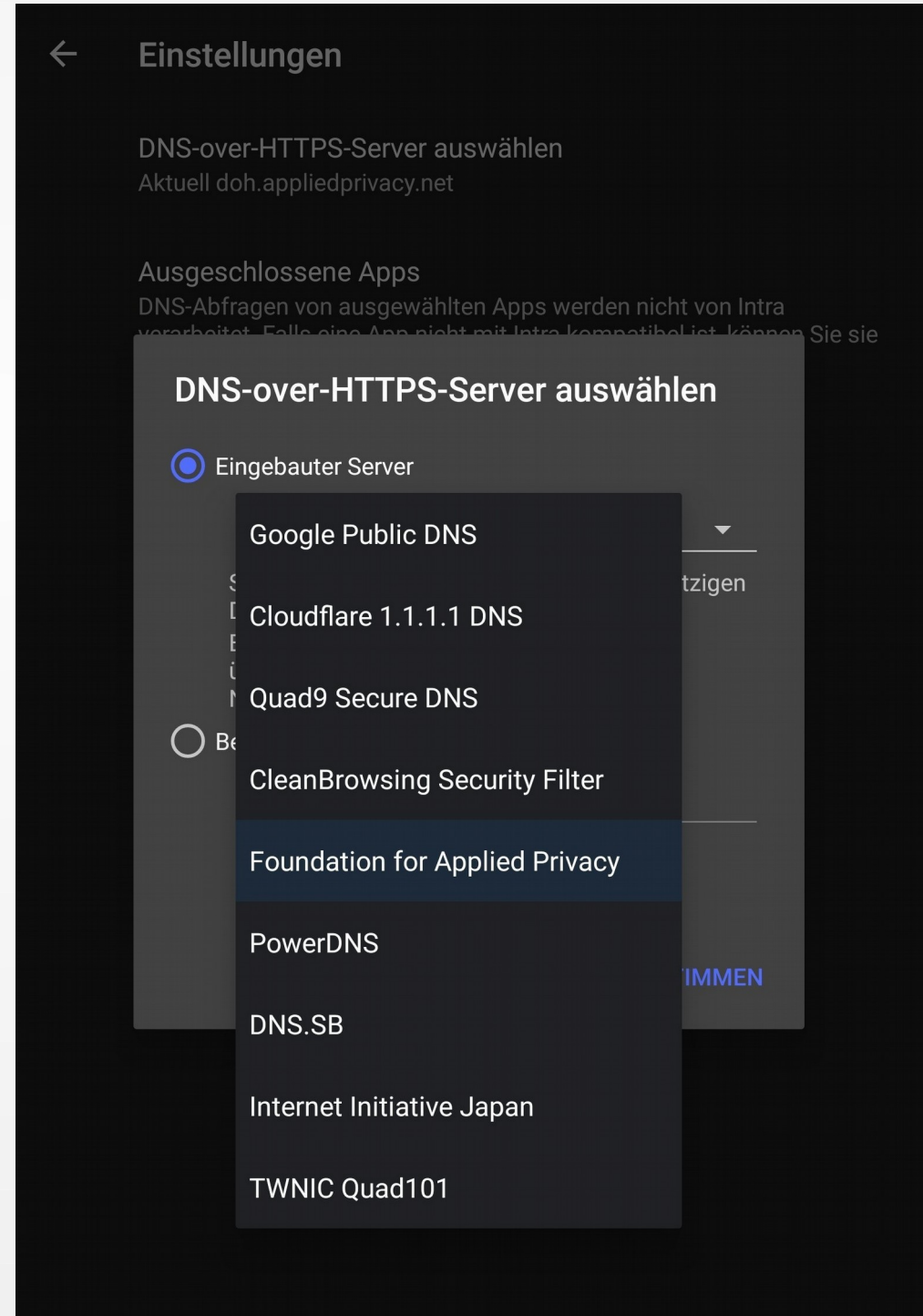
- Firefox
- Chrome (angekündigt)
- Jigsaw Intra (Android)
- dnscrypt-proxy (hat auch DoH Support)
  - DNSCloak (iOS)
  - Simple DNSCrypt (Windows)
- curl, ...



# DNSSCloak (iOS)



# Jigsaw Intra (Android)



# DoH Deployment Strategien von Firefox/Chrome

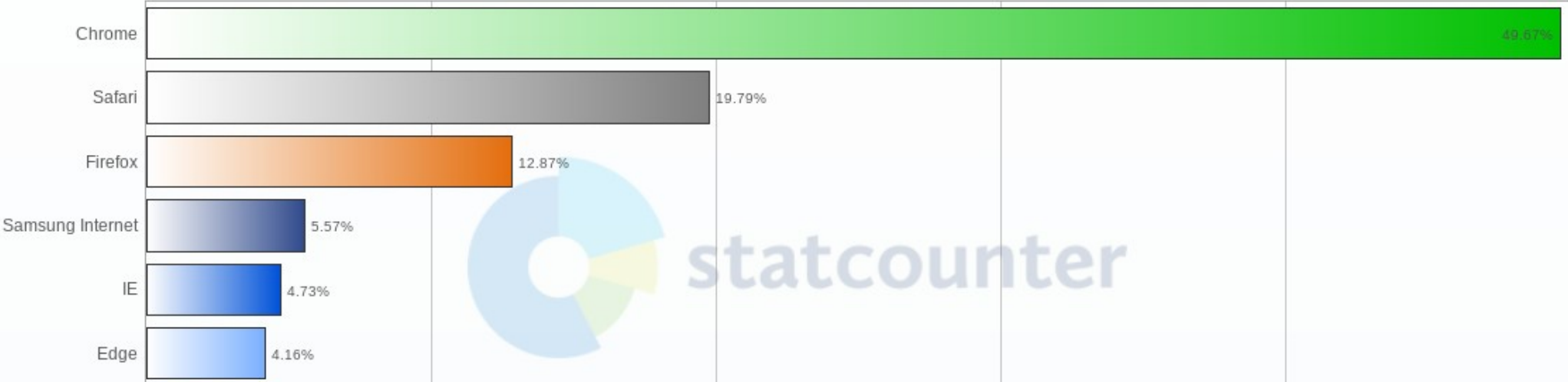


Foundation for  
Applied Privacy

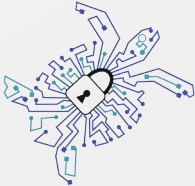
# Browser Market Share Austria

June 2019

Edit Chart Data



<http://gs.statcounter.com/browser-market-share/all/austria/#monthly-201906-201906-bar>

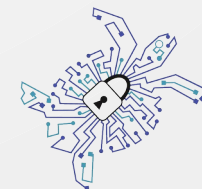


Foundation for Applied Privacy



# Googles Pläne für Chrome (angekündigt)

- DoH wird nicht global per default aktiviert
- Automatisches Upgrade zu DoH sofern vom bereits verwendeten Resolver unterstützt
- Statische Liste im Browser (Resolver IP -> DoH URI)



# Mozillas DoH Pläne für Firefox (angekündigt)

- Mozilla will DoH per default aktiviert
- Eine (kurze) Liste an default DoH Server (TRR) soll mit Firefox ausgeliefert werden
- Zeitplan noch nicht bekannt



# Mozilla / Cloudflare Kritik



## **Mozilla's new DNS resolution is dangerous**

All your DNS traffic will be sent to Cloudflare

*Posted on Aug. 4, 2018*

Quelle: <https://ungleich.ch>



Foundation for  
Applied Privacy

# Mozilla / Cloudflare Kritik

## Mozilla Security Blog



DNS-over-HTTPS Policy  
Requirements for Resolvers



Marshall Erwin



Foundation for  
Applied Privacy

# Mozillas Trusted Recursive Resolver Anforderungen (Auszug)


- kein Datenweitergabe an Dritte
- Speicherlimit nicht-aggregierter Daten: 24h
- QNAME Minimization (RFC 7816)
- kein EDNS Client Subnet (RFC 7871) sofern keine verschlüsselte Verbindung mit autoritativen NS



# Mozillas Trusted Recursive Resolver Anforderungen (Auszug)

- keine Filter die nicht rechtlich vorgeschrieben oder vom Benutzer bestellt sind
- Filterlisten müssen öffentlich sein
- Kein NXDOMAIN Hijacking
- jährliche Transparenzberichte



 MUST READ: [Amazon Prime Day 2019: How and when to find the best deals](#)

# UK ISP group names Mozilla 'Internet Villain' for supporting 'DNS-over-HTTPS'

UK government and local ISPs are putting the pressure on browsers to drop plans to support DoH protocol.



By [Catalin Cimpanu](#) for [Zero Day](#) | July 4, 2019 -- 22:55 GMT (23:55 BST) | Topic: [Security](#)



Foundation for  
Applied Privacy

**MUST READ:** [Amazon Prime Day 2019: How and when to find the best deals](#)

# UK ISP group names Mozilla 'Internet Villain' for supporting 'DNS-over-HTTPS'

UK  
drop



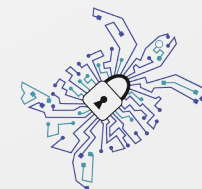
E

[About](#)[Join](#)[Members](#)[Consumers](#)[News](#)[Events](#)[Policy](#)[Contact](#)[Member Area](#)[Partners](#)

## ISPA withdraws Mozilla Internet Villain Nomination and Category

Posted on 9th July 2019

Last week ISPA included Mozilla in our list of Internet Villain nominees for our upcoming annual awards.



Foundation for  
Applied Privacy



# Potentielle neue Herausforderungen für ISPs



# End-User Support

Wen werden Endbenutzer anrufen wenn das “Internet nicht geht” (weil der DoH Provider down ist)?

**502 Bad Gateway**

cloudflare



Foundation for  
Applied Privacy

# Content Caches

- DNS spielt eine wesentliche Rolle bei der Traffic Steuerung zu “lokalen” Caches
- Authoritative Nameserver verwenden dazu die Client-IP Adresse/Subnet, bzw. die Resolver IP Adresse
- Mozilla Firefox: Tests mit/ohne ECS



# Risiko: DNS Zentralisierung

DoH birgt das Risiko einer Zentralisierung der globalen DNS Resolver Infrastruktur.

**502 Bad Gateway**

cloudflare



Foundation for  
Applied Privacy

# Risiko: DNS Zentralisierung

- Empfehlung: DNS Resolver Infrastruktur auf DoH/DoT upgraden
- DoH/DoT Discovery Protokoll auf die Roadmap setzen.

IETF Work in Progress:

<https://datatracker.ietf.org/doc/draft-sah-resolver-information/>



Foundation for  
Applied Privacy

# DoH Server Software

- dnsmist

**POWERDNS** 

- Knot Resolver

**CZ.nIC**

- siehe Slides vom DNSheads Vienna Meetup (Juni 2019)



Foundation for  
Applied Privacy

# Fazit

- DoH schützt DNS Traffic und hat das Potential die DNS Welt nachhaltig zu verändern
- pot. schnelle Verbreitung durch Firefox
- primär wird die Verwendung von zentralisierten Providern kritisiert – nicht das Protokoll selbst
- Empfehlung: DoH und DoT Upgrade der bestehenden DNS Resolver Infrastruktur auf die Roadmap setzen



# Fragen?

[contact@appliedprivacy.net](mailto:contact@appliedprivacy.net)

[https://twitter.com/applied\\_privacy](https://twitter.com/applied_privacy)

<https://appliedprivacy.net>



Foundation for  
Applied Privacy



# Calling ISPs!

Help protect the Internet core.

**JOIN MANRS**

[www.manrs.org](http://www.manrs.org)



**MANRS**

## Deploy RPKI

Why it's time to deploy RPKI (RIPE NCC)

<https://www.youtube.com/watch?v=Y9vbbxr-Gbl> (2min)

<https://rpki.readthedocs.io/en/latest/>

# Bonus Slides Unlocked



Foundation for  
Applied Privacy

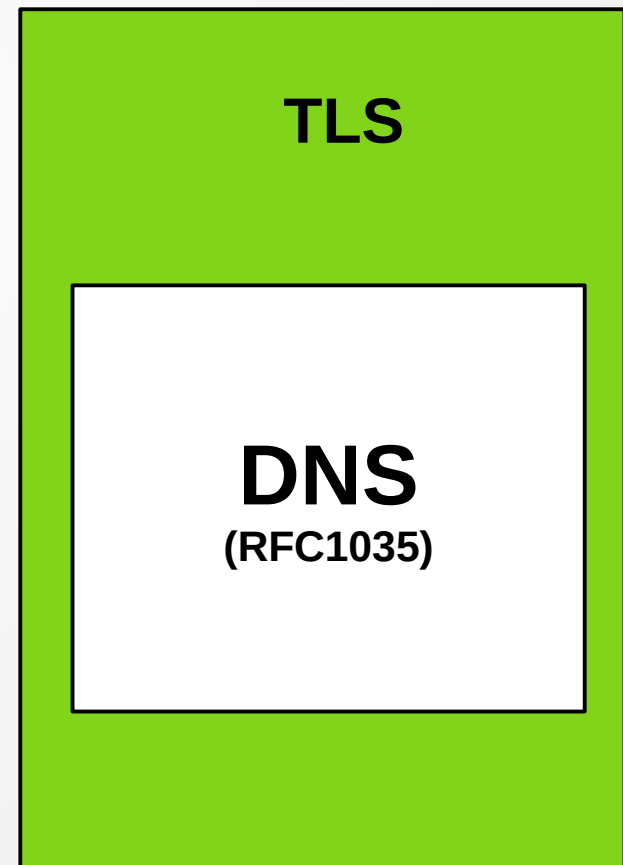
# DoH / DoT – DNSSEC?

- Löst unterschiedliche Probleme
- Am besten in Kombination eingesetzt
- Browser haben jedoch aktuell kein DNSSEC Support

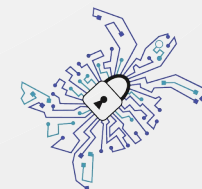


# DoT

- $\geq$ TLS 1.2
- TCP Port 853
- inoffiziell auch beliebt:  
Port 443



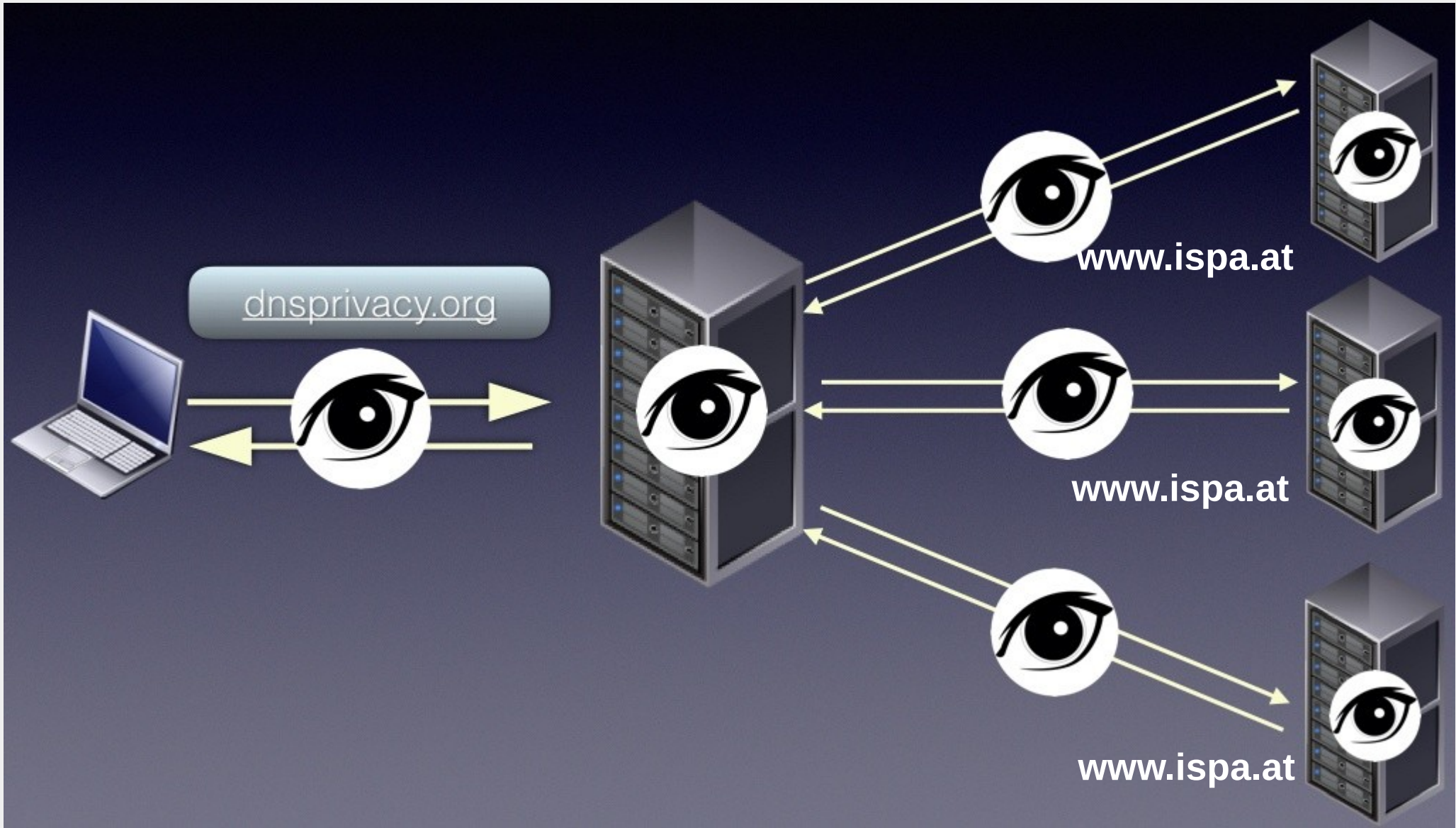
<b>Information Leak</b>	<b>Lösung</b>
IP Adresse	CDN/vHosts
TLS SNI	Work in Progress: Encrypted SNI (ESNI)
TLS Zertifikat	Verschlüsselt ab TLS 1.3
OCSP	OCSP Stapling
<b>DNS</b>	<b>DoH/DoT/...</b>

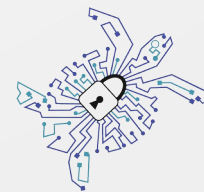
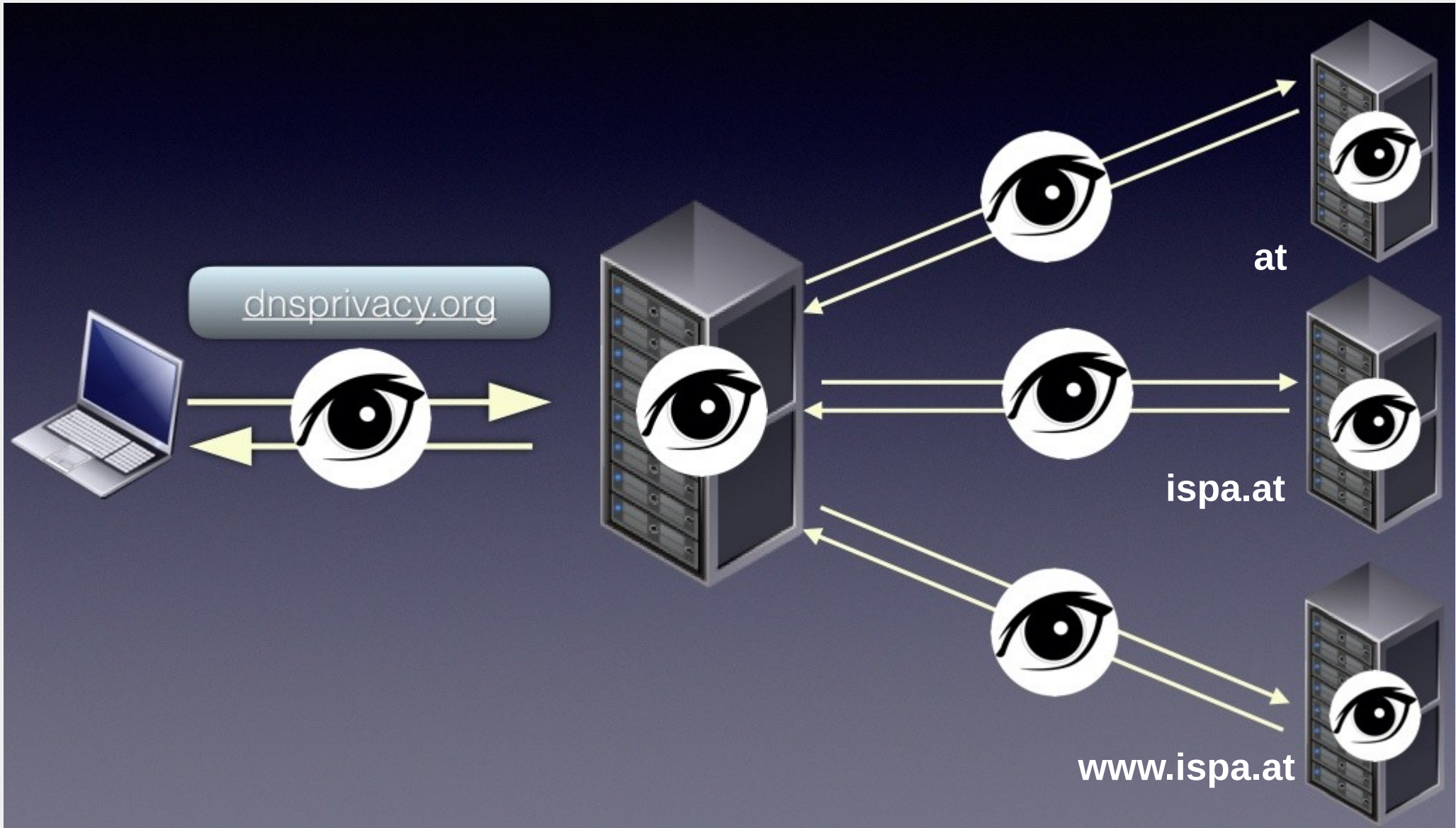


# QNAME Minimization



Foundation for  
Applied Privacy







# DoH mit Firefox nutzen

Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Enable DNS over HTTPS

Use default (https://mozilla.cloudflare-dns.com/dns-query)

Custom

Help Cancel OK



# DoH in Firefox

atnog - AT Network Operatic x About Networking x +

about:networking#dns

## DNS

HTTP

Sockets

**DNS**

WebSockets

DNS Lookup

Logging

RCWN Stats

Hostname	Family	TRR	Addresses
ocsp.digicert.com	ipv4	true	93.184.220.29
detectportal.firefox.com	ipv4	true	2a02:26f0:10e::6860:5af0 2a02:26f0:10e::6860:5ad1 104.96.90.209 104.96.90.240
ocsp.digicert.com	ipv4	true	93.184.220.29
			2a01:468:1000:9::150 2a01:468:1000:9::4 2a01:468:1000:9::149 2a01:468:1000:9::3 194.232.104.149 194.232.104.142 194.232.104.4 194.232.104.141 194.232.104.150 194.232.104.3 194.232.104.139 194.232.104.140
safebrowsing.googleapis.com	ipv4	true	172.217.168.234 2a00:1450:400e:808::200a
atnog.at	ipv4	true	81.16.150.238



# DNS Privacy - Zukunft

- DoH/DoT Server Discovery Protokolle
- Verschlüsselung zu authoritative Server
- DNS over QUIC



**I E T F**®



Foundation for  
Applied Privacy



# Root Zone on Loopback



# EDNS Client Subnet



Foundation for  
Applied Privacy