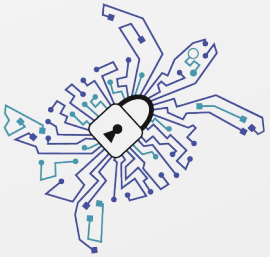
DNS-over-HTTPS Intro für ISPs

ATNOG Juli 2019



Foundation for Applied Privacy

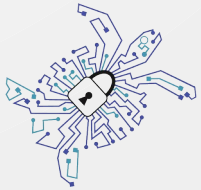
Foundation for Applied Privacy

- 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

Foundation for Applied Privacy

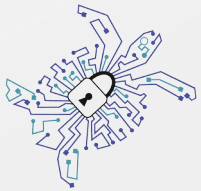
Ziele dieses Vortrags

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



Foundation for
Applied Privacy

Warum DNS Traffic schützen?



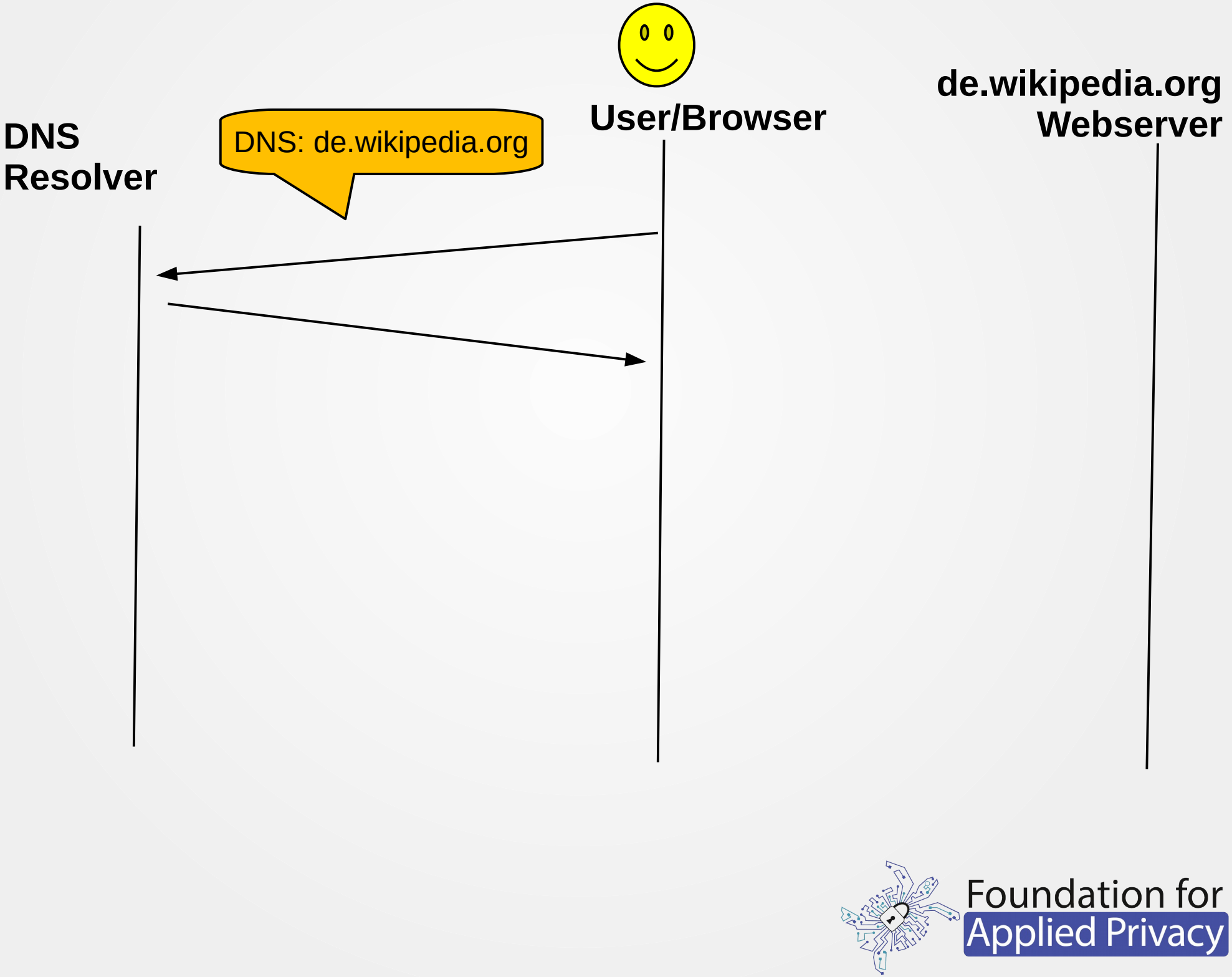
Foundation for Applied Privacy

User/Browser

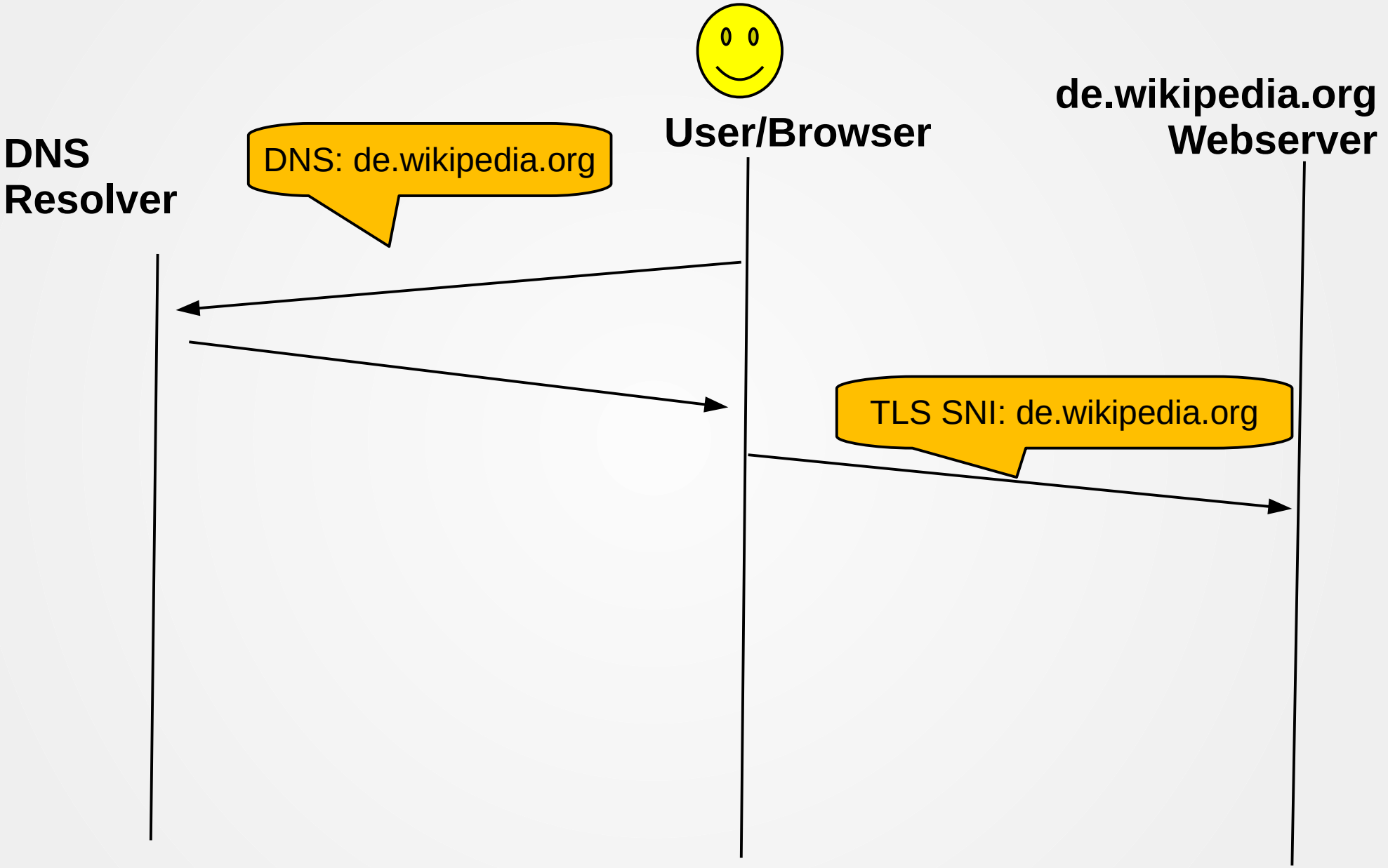
DNS Resolver

de.wikipedia.org Webserver

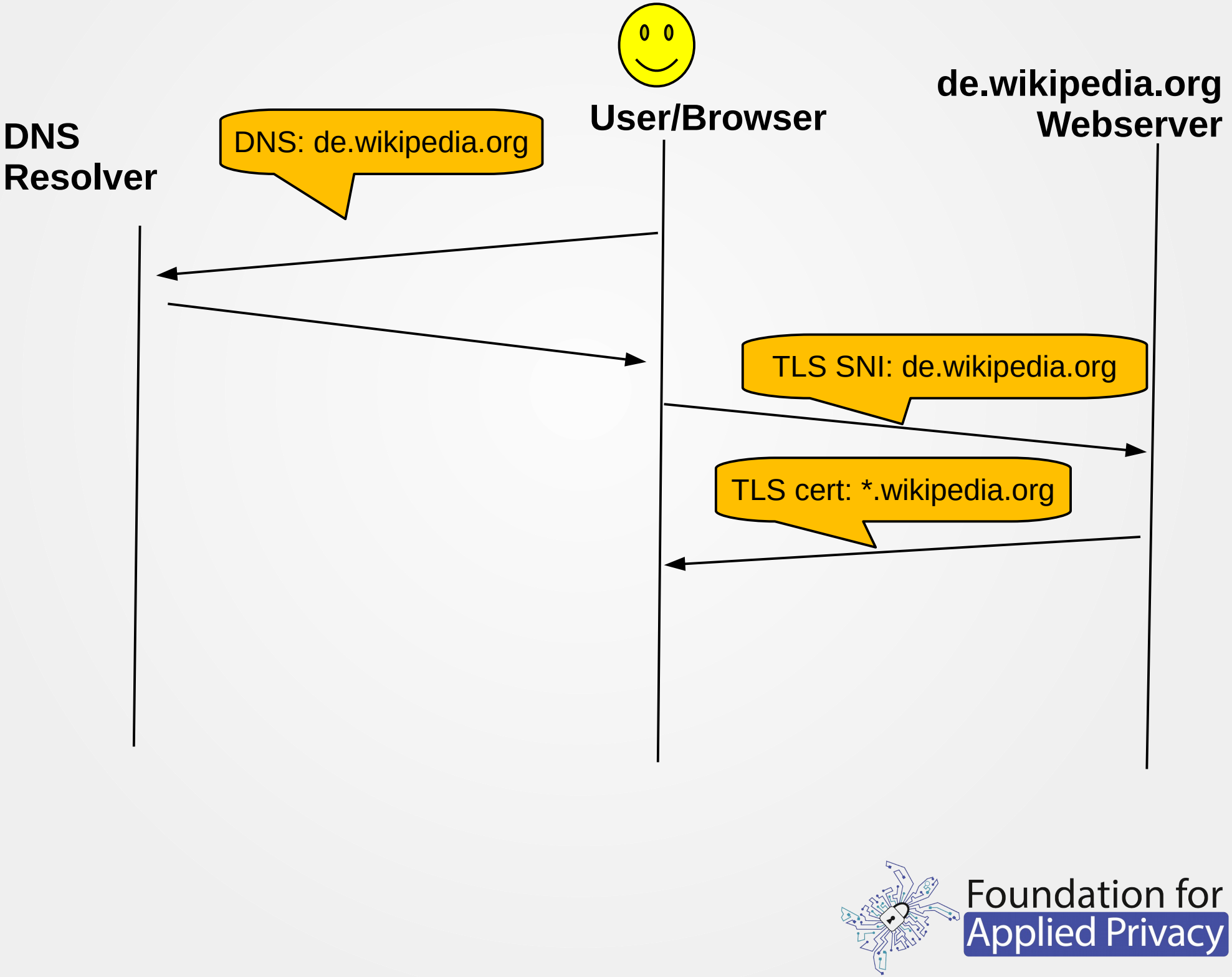
Foundation for Applied Privacy



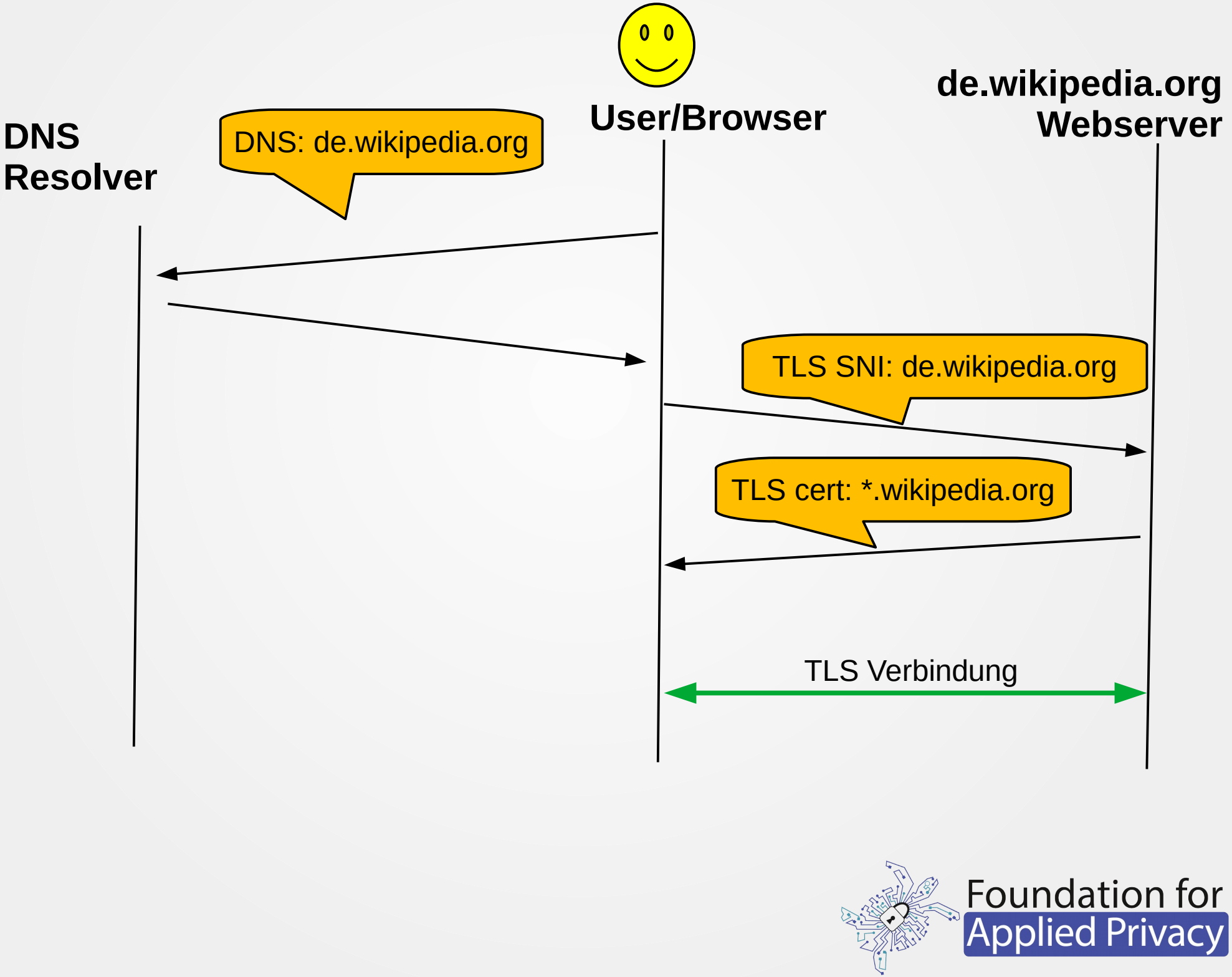
Foundation for Applied Privacy



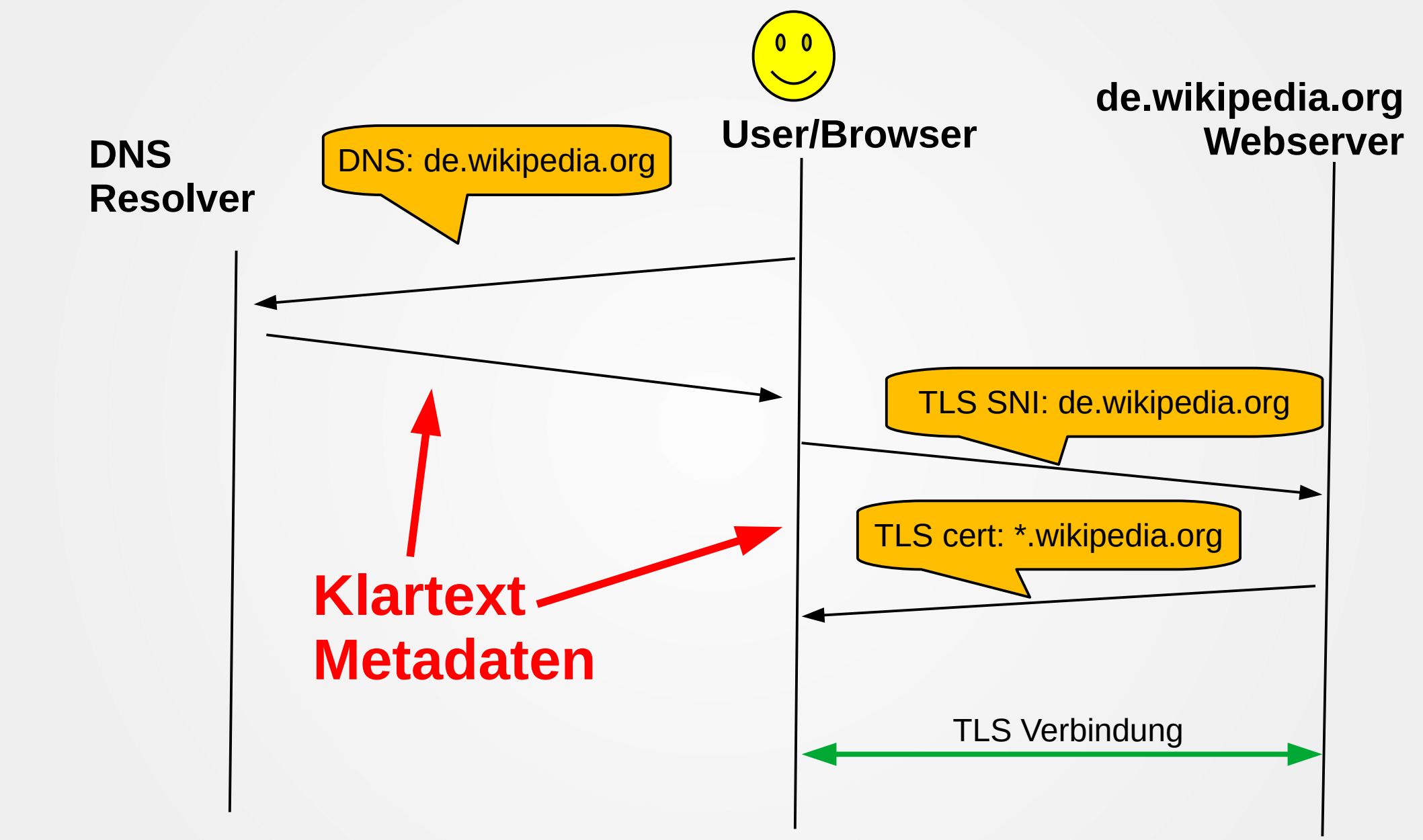
Foundation for Applied Privacy



Foundation for Applied Privacy



Foundation for Applied Privacy



Foundation for Applied Privacy

BEST CURRENT PRACTICE

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

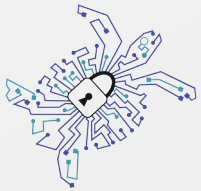
Pervasive Monitoring Is an Attack

Abstract

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

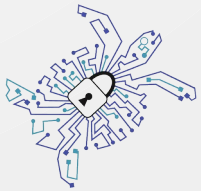
Ziel

Schutz von Metadaten (Hostnamen)

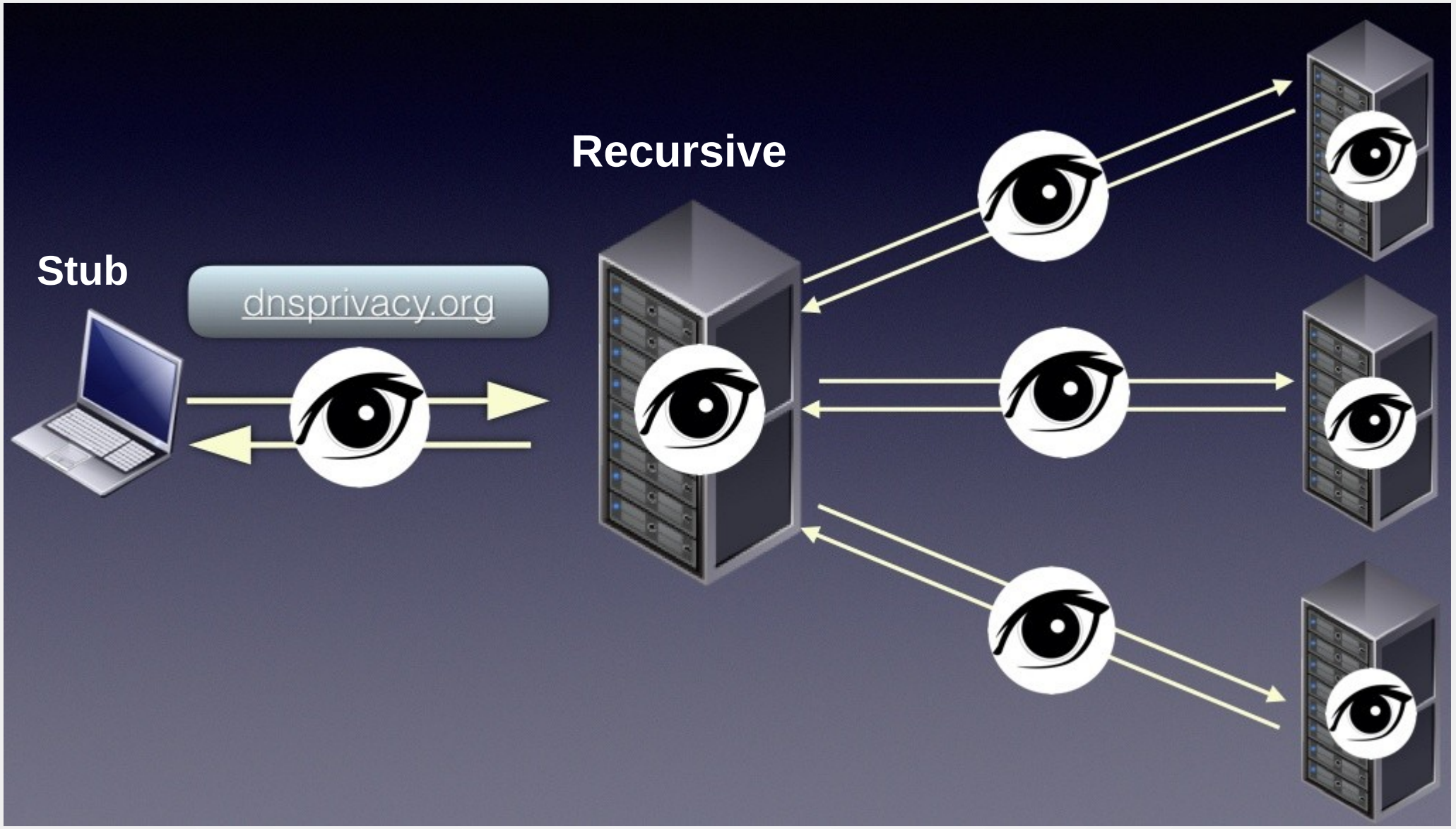


Foundation for Applied Privacy

DNS

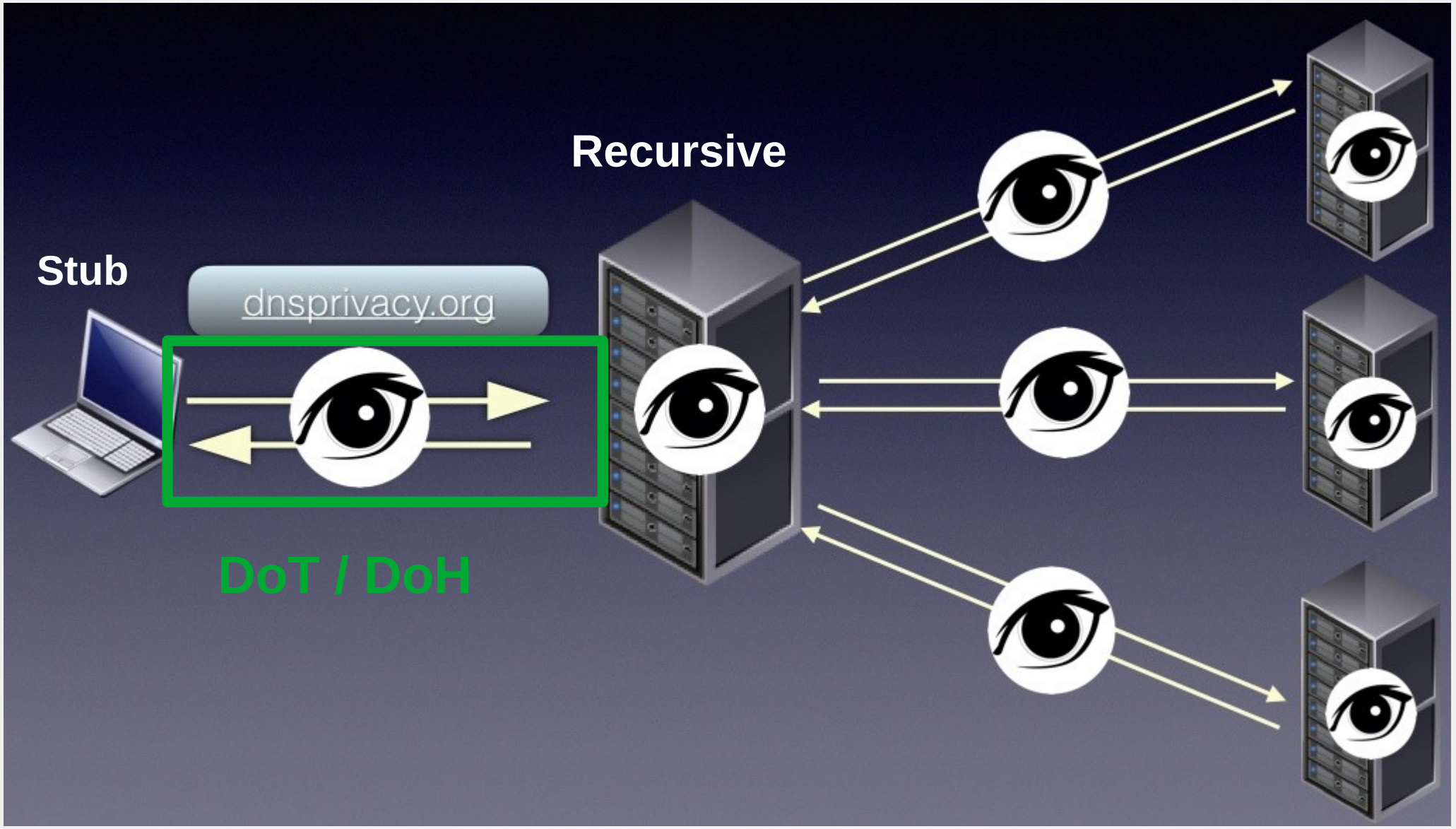


Foundation for
Applied Privacy



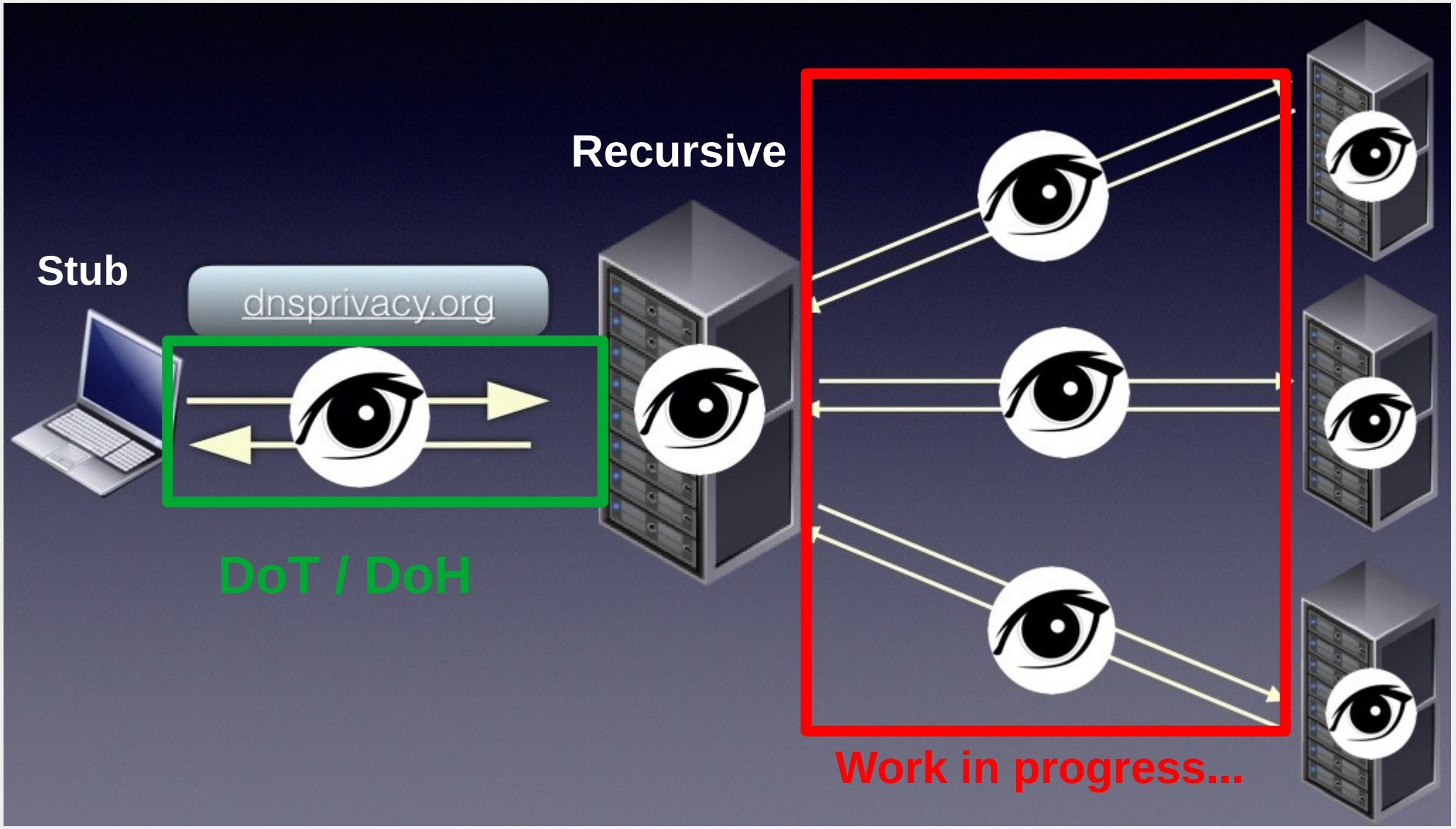
Quelle: dnsprivacy.org

Foundation for Applied Privacy



Quelle: dnsprivacy.org

Foundation for Applied Privacy

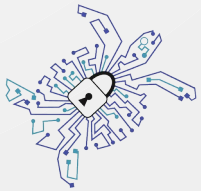


Quelle: dnsprivacy.org

Foundation for Applied Privacy

DNS-over-HTTPS (DoH)

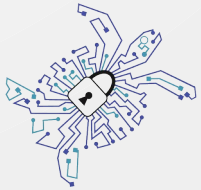
RFC 8484 (Okt 2018)



Foundation for
Applied Privacy

DoH - Motivation

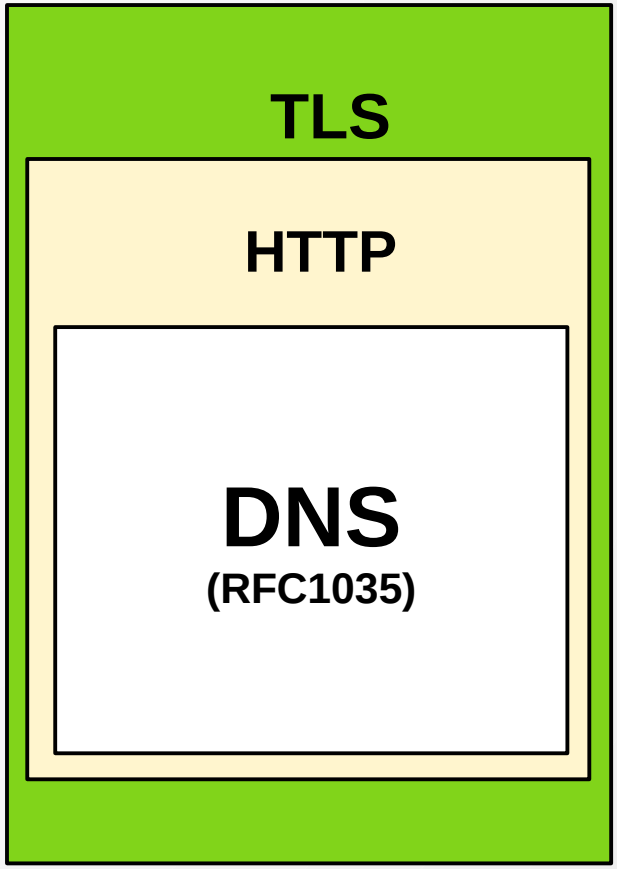
- DNS Traffic vertraulich übertragen
- DNS Traffic vor Manipulation schützen
- soll auch in restriktiven Netzen funktionieren (in denen zB. nur 53/80/443 erlaubt ist)
- vor allem von Browsern getrieben



Foundation for Applied Privacy

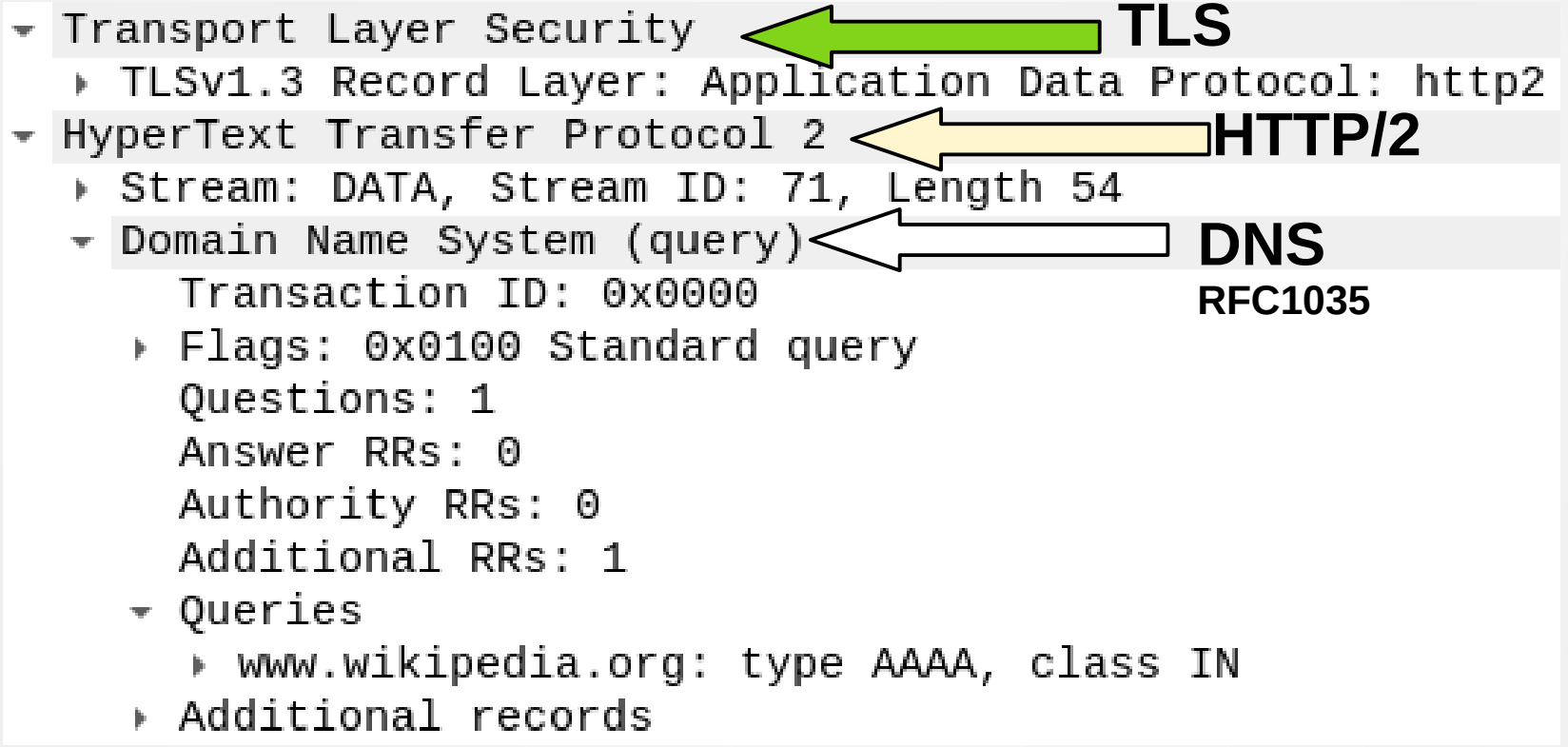
DoH

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



Foundation for Applied Privacy

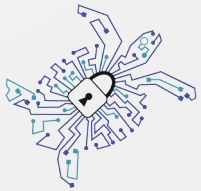
DoH Anfrage (**entschlüsseltes** Beispiel)



Foundation for Applied Privacy

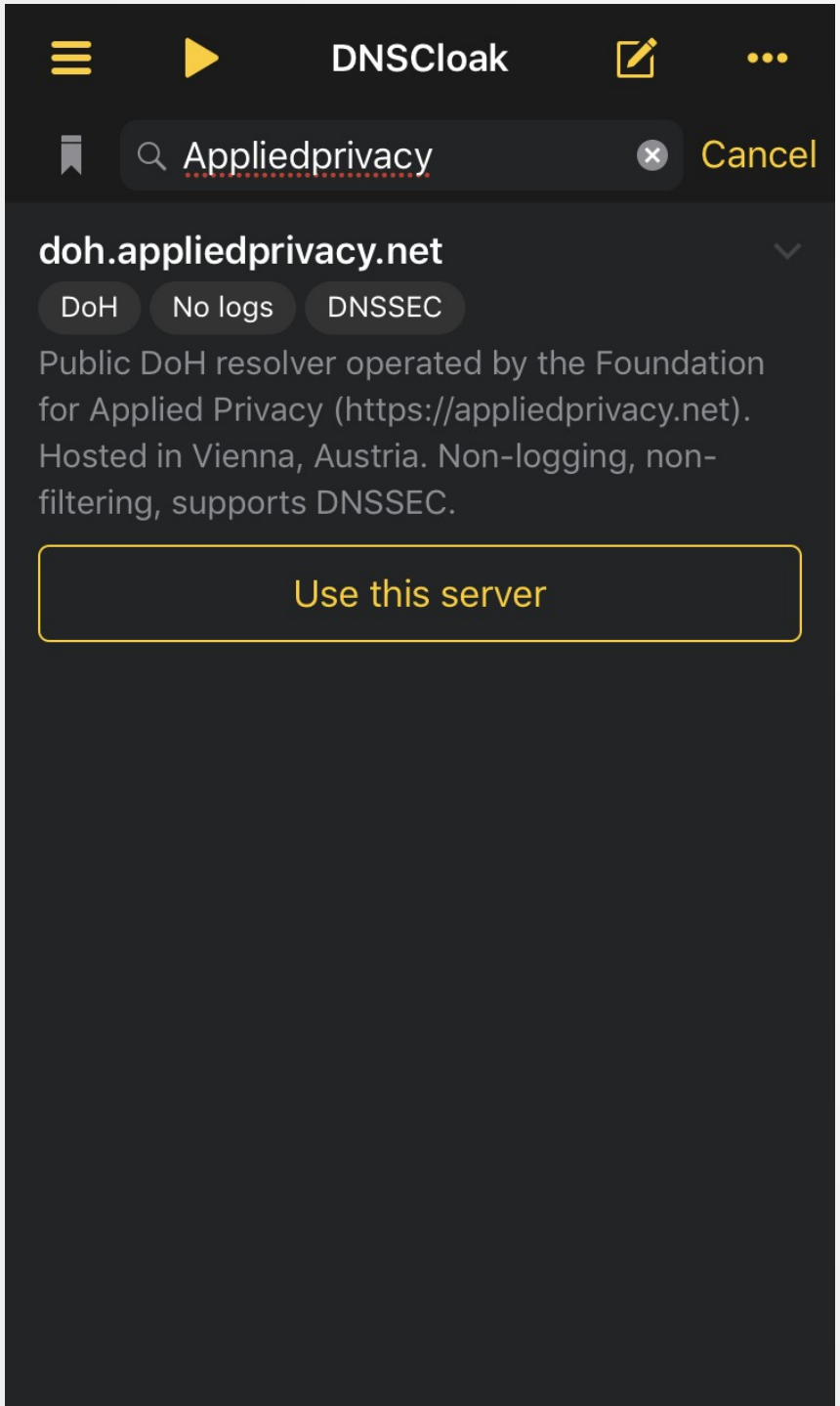
DoH Client Software

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

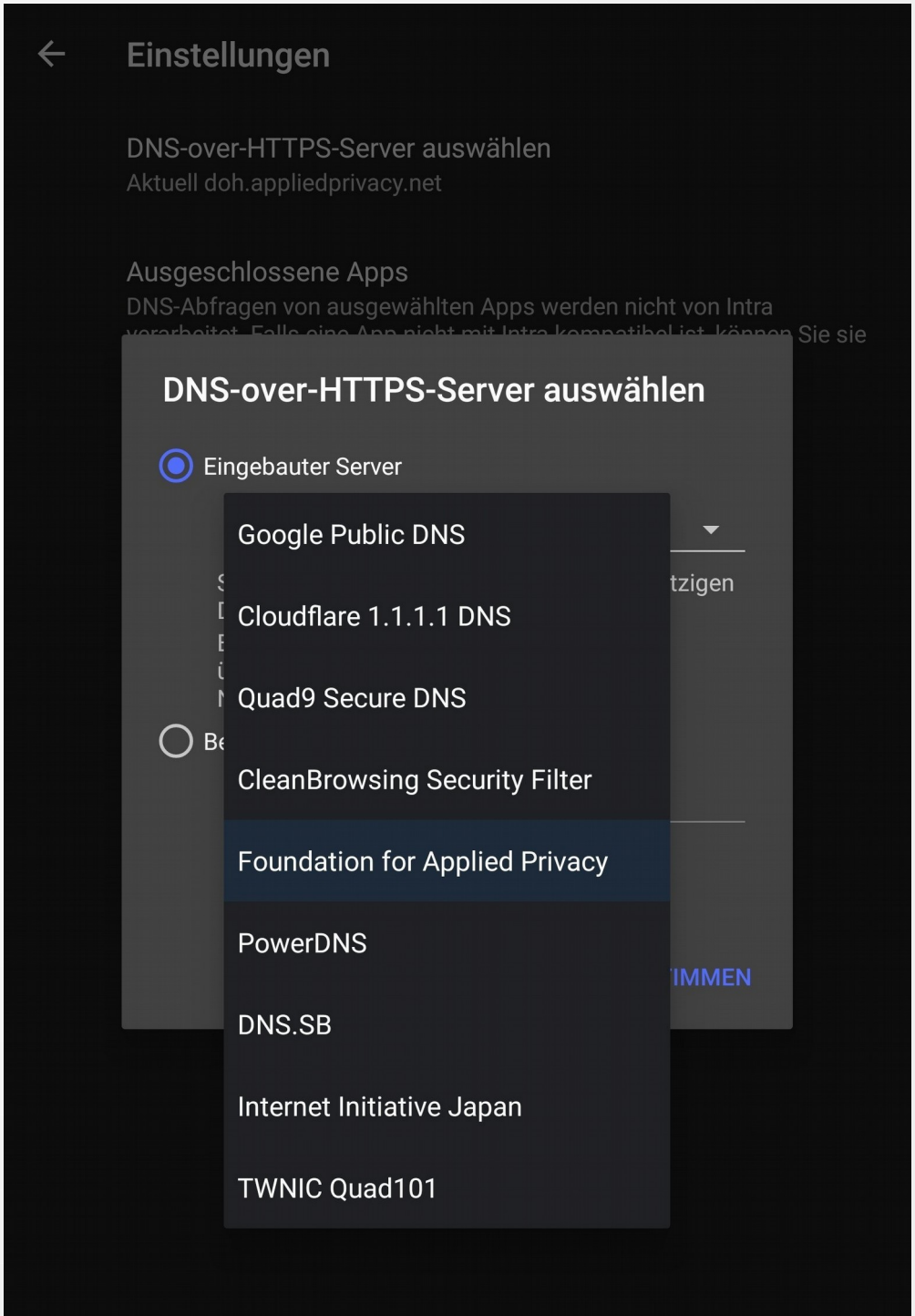


Foundation for Applied Privacy

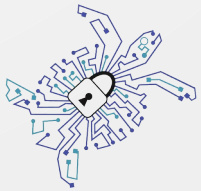
DNSCloak (iOS)



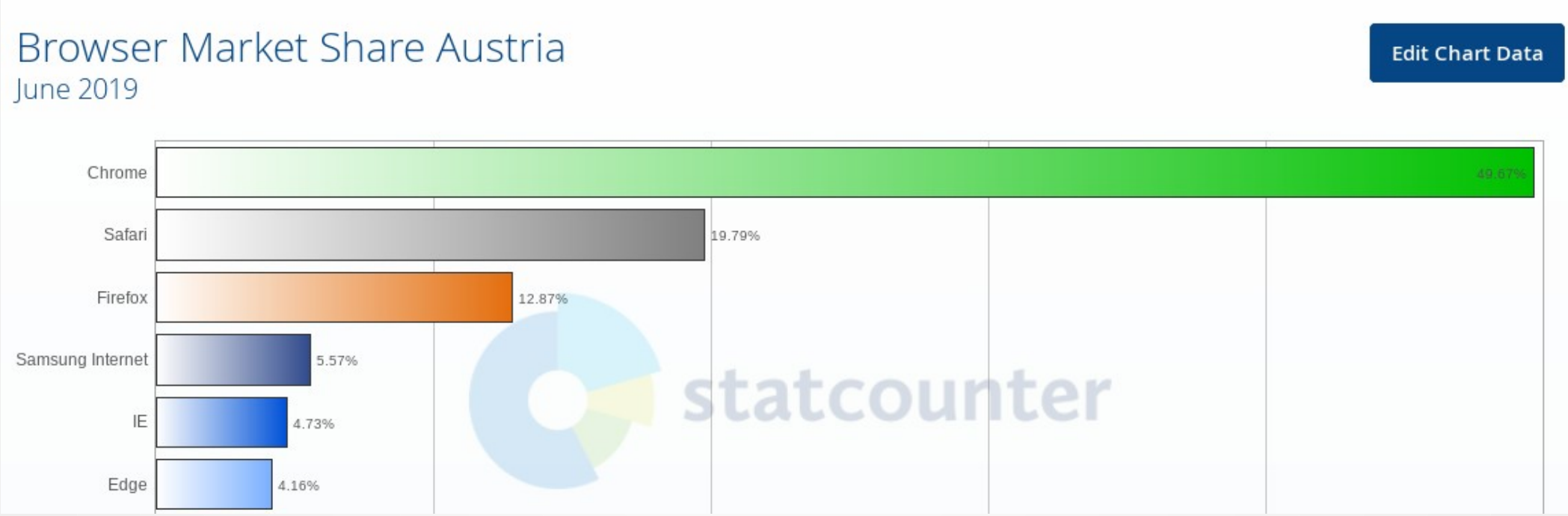
Jigsaw Intra (Android)



DoH Deployment Strategien von Firefox/Chrome



Foundation for Applied Privacy



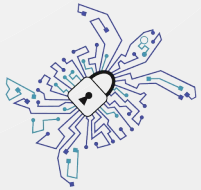
http://gs.statcounter.com/browser-market-share/all/austria/#monthly-201906-201906-bar

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)

https://mailarchive.ietf.org/arch/msg/dns-privacy/kpt6ZYMN5H3DsXPVi_QldmbAdJw

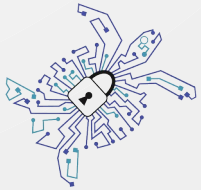


Foundation for Applied Privacy

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

https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw



Foundation for Applied Privacy

Mozilla / Cloudflare Kritik

Quelle: https://ungleich.ch

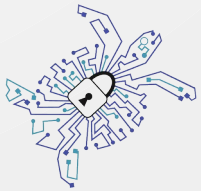
Foundation for Applied Privacy

Mozilla / Cloudflare Kritik

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 authoritativen NS



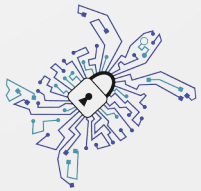
Foundation for Applied Privacy

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



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 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

ZDNet

AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

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 g
drop

E

ISPAUK
THE VOICE OF THE UK INTERNET INDUSTRY

About Join Members Consumers News Events Policy Contact Member Area Partners

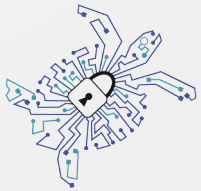
ISPA withdraws Mozilla Internet Villain Nomination and Category

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

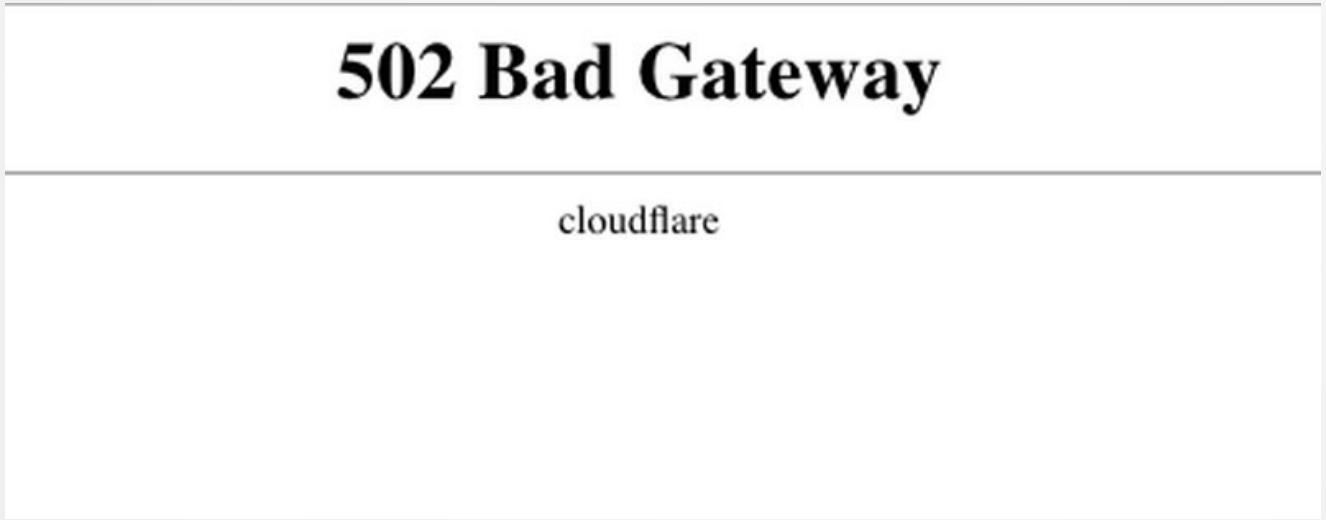
Potentielle neue Herausforderungen für ISPs



Foundation for Applied Privacy

End-User Support

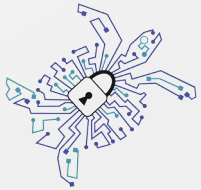
Wen werden Endbenutzer anrufen wenn das “Internet nicht geht” (weil der DoH Provider down ist)?



Foundation for Applied Privacy

Content Caches

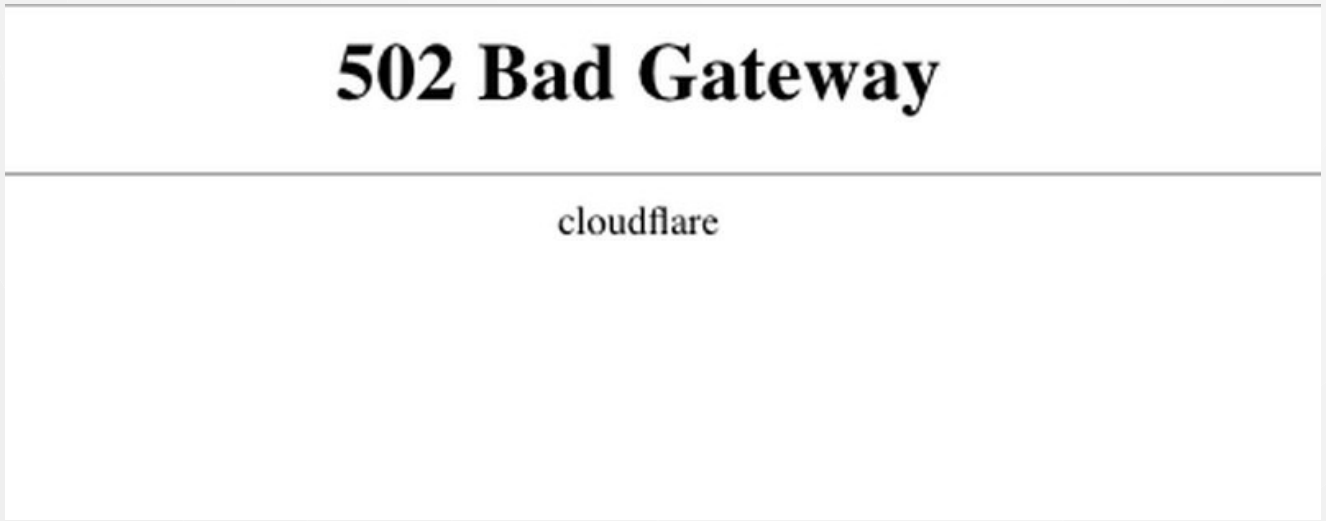
- DNS spielt eine wesentliche Rolle bei der Traffic Steuerung zu “lokalen” Caches
- Authoritative Nameserver verwenden dazu die Client-IP Adresse/Subnet, bzw. die Resolver IP Adresse
- Mozilla Firefox: Tests mit/ohne ECS



Foundation for Applied Privacy

Risiko: DNS Zentralisierung

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



Foundation for Applied Privacy

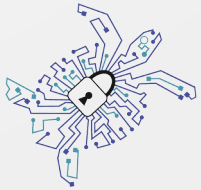
Risiko: DNS Zentralisierung

- 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/

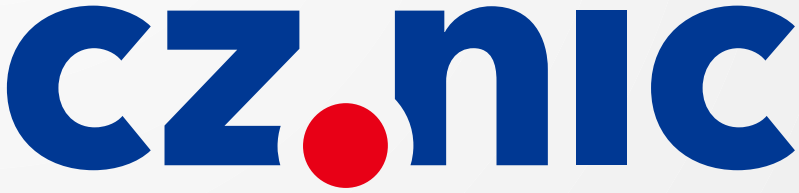


Foundation for Applied Privacy

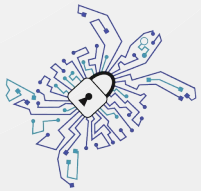
DoH Server Software

- dnsdist

- Knot Resolver



- siehe Slides vom DNSheads Vienna Meetup (Juni 2019)



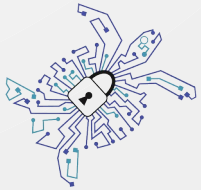
Foundation for Applied Privacy

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



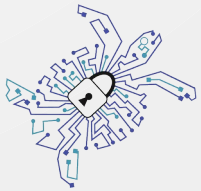
Foundation for Applied Privacy

Fragen?

contact@appliedprivacy.net

https://twitter.com/applied_privacy

https://appliedprivacy.net

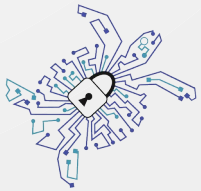


Foundation for
Applied Privacy

Deploy RPKI

Why it's time to deploy RPKI (RIPE NCC)
https://www.youtube.com/watch?v=Y9vbbxr-GbI (2min)
https://rpki.readthedocs.io/en/latest/

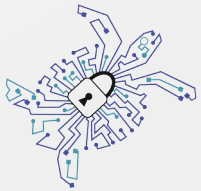
Bonus Slides Unlocked



Foundation for
Applied Privacy

DoH / DoT – DNSSEC?

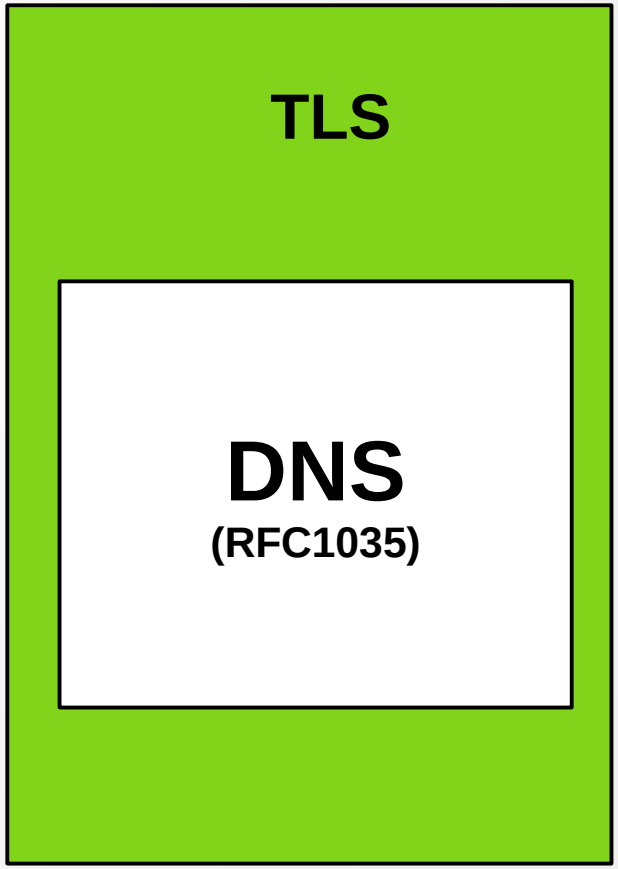
- Löst unterschiedliche Probleme
- Am besten in Kombination eingesetzt
- Browser haben jedoch aktuell kein DNSSEC Support



Foundation for Applied Privacy

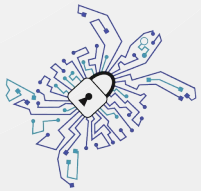
DoT

- >=TLS 1.2
- TCP Port 853
- inoffiziell auch beliebt: Port 443



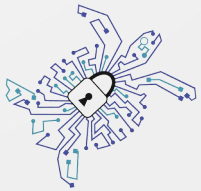
Foundation for Applied Privacy

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

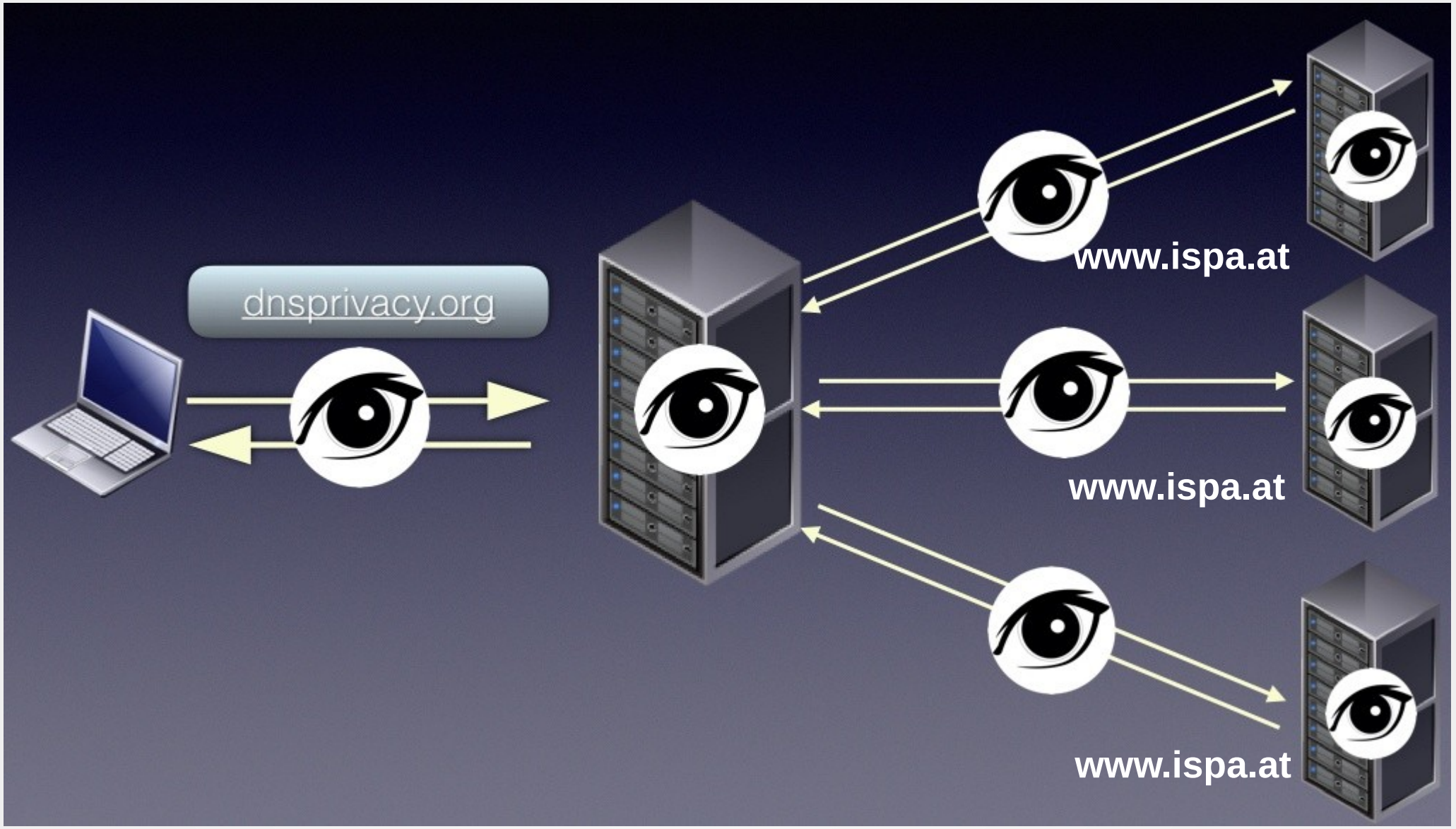


Foundation for Applied Privacy

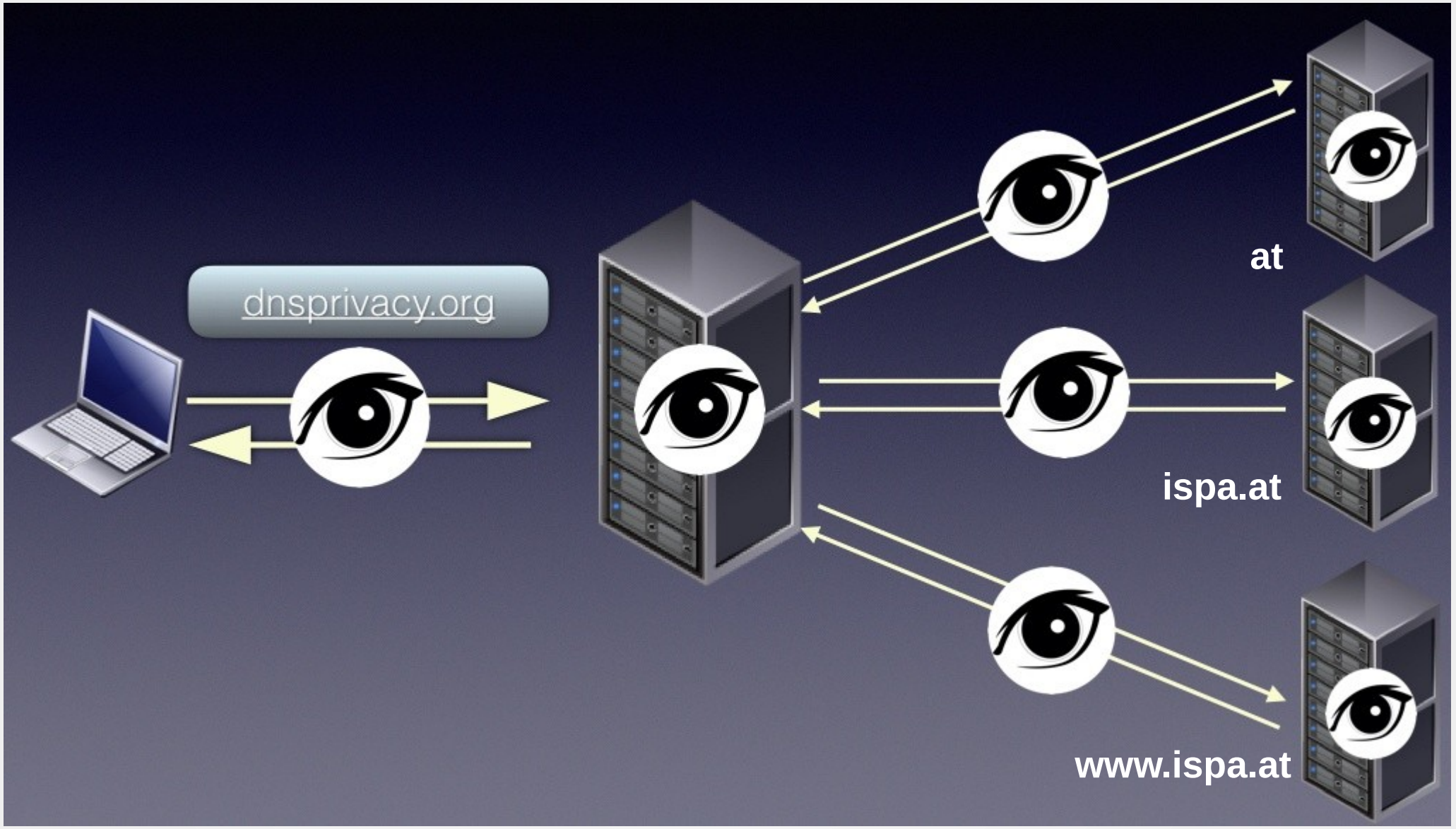
QNAME Minimization



Foundation for
Applied Privacy

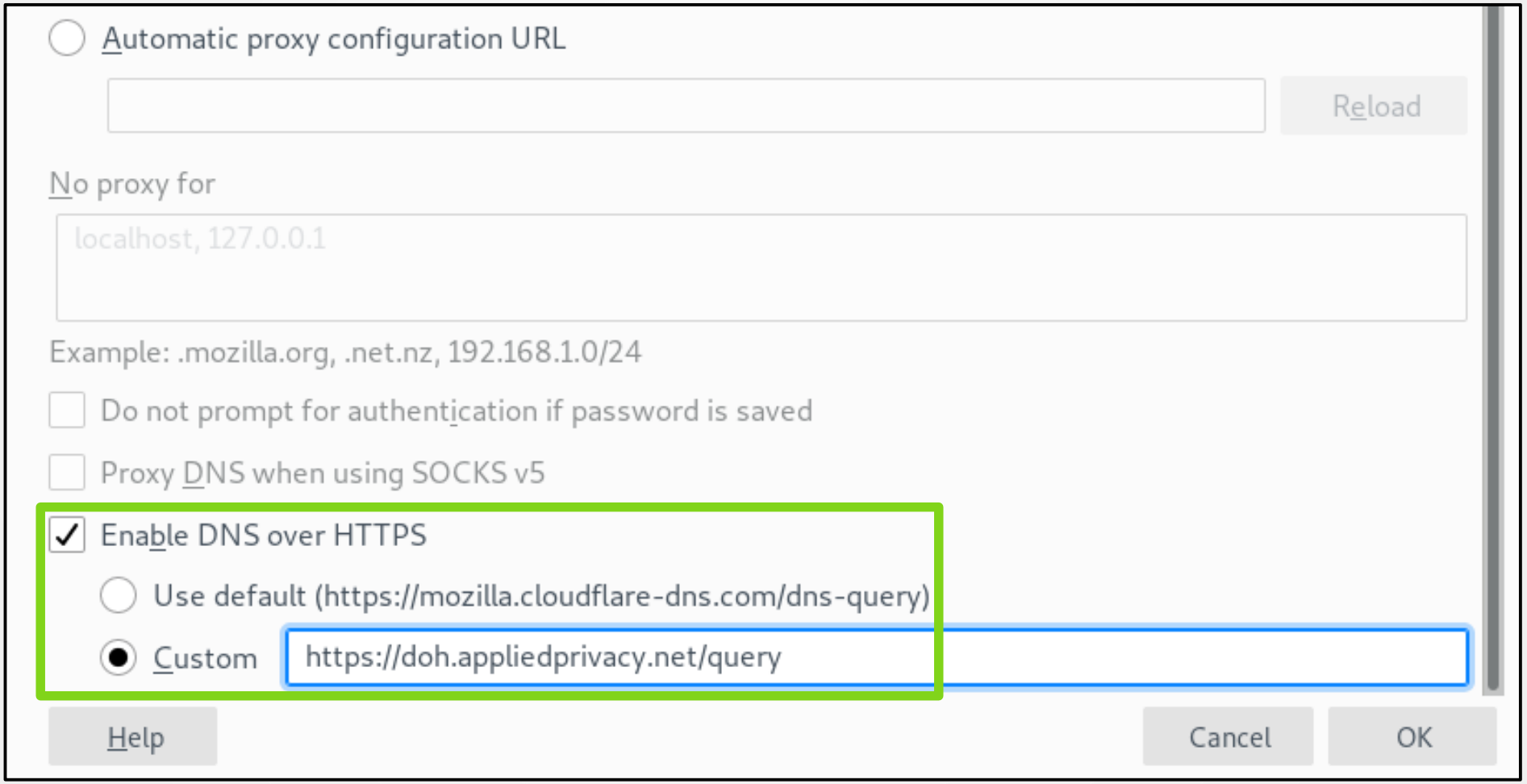


Foundation for Applied Privacy



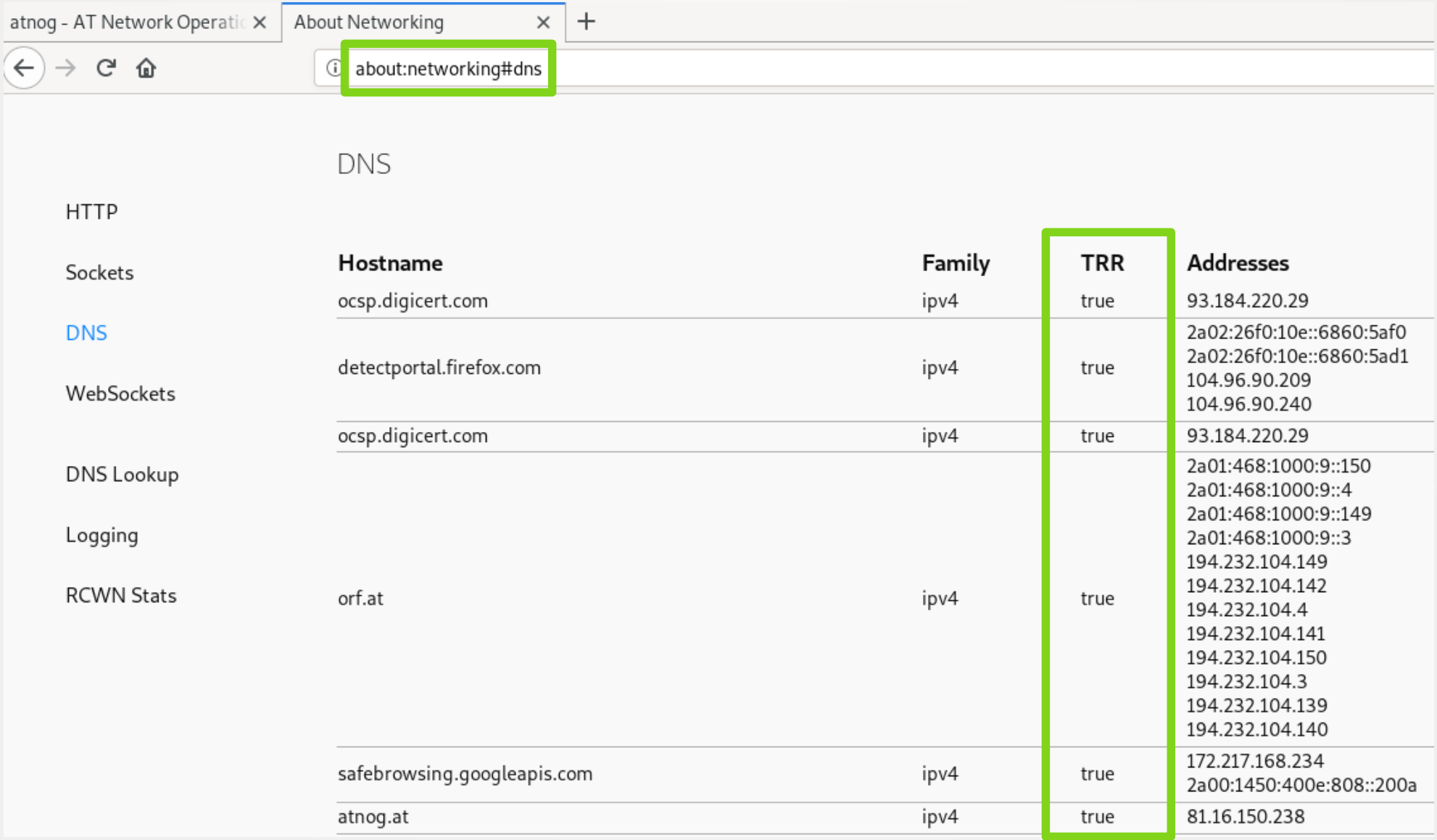
Foundation for Applied Privacy

DoH mit Firefox nutzen



Foundation for Applied Privacy

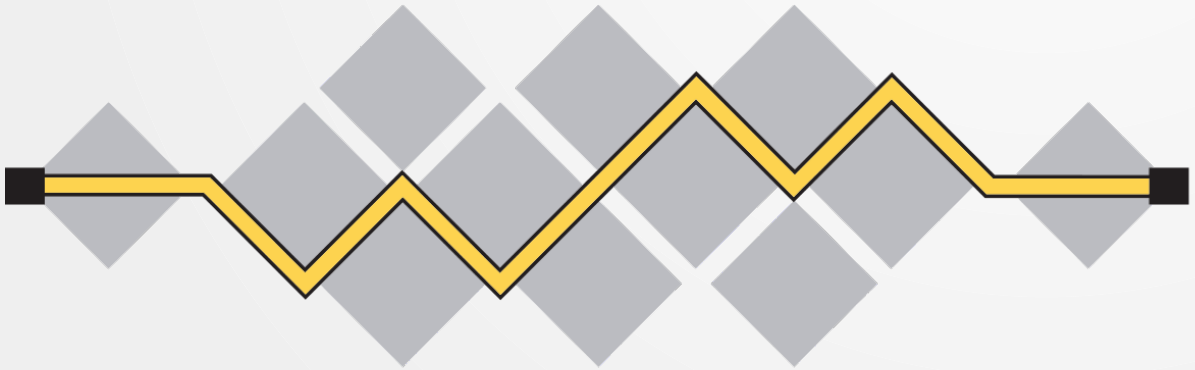
DoH in Firefox



Foundation for Applied Privacy

DNS Privacy - Zukunft

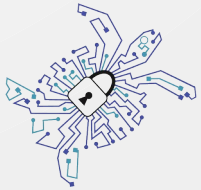
- DoH/DoT Server Discovery Protokolle
- Verschlüsselung zu authoritative Server
- DNS over QUIC



I E T F®

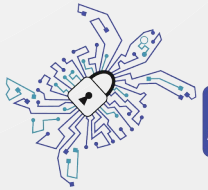
Foundation for Applied Privacy

Root Zone on Loopback



Foundation for
Applied Privacy

EDNS Client Subnet



Foundation for
Applied Privacy