Mozilla TRR



Lars Eggert & Valentin Gosu

FAQ

- Why do we want more DoH?
 - Because we want more ECH (TLS Encrypted Client Hello)
- Why do we need DoH for ECH?
 - Because we need to acquire the keys for ECH over a trusted & encrypted DNS transport
- But I don't like DoH
 - So disable it (easy, e.g., canary domain)
 - But accept you'll be bleeding cleartext SNIs all over the net

We want to do DoH with you

- Mozilla Trusted Recursive Resolver Program for DoH
- Trusted partners that we use for DoH in a region or network
 - Currently contracts
 - US → Cloudflare (Unless on Comcast network, then → Comcast)
 - Canada → CIRA (Unless on Shaw network, then → Shaw)
 - Russia, Ukraine → Cloudflare
- System resolver used everywhere else
- Goal: Find TRR partners for other regions

What other regions?

DT (DE) Orange (FR) Vodafone (DE) Jio (IN) Free (FR) Airtel (IN) SFR (FR) China Telecom (CN) Telkomsel (ID) PT Telkom (ID) Bouygues (FR)

1&1 (DE) 02 (DE) Mobile CC (IR) MTN (IR) China Mobile (CN) Telmex (MX) Vivo (BR) Telefonica (ES) Claro NET (BR)

Play (PL) BT (GB) Telecom Egypt (EG) BSNL (IN) China Unicom (CN) Virgin Media (GB) Orange (PL) TIM (IT) NTT (JP) Wind Tre (IT)

Mozilla Trusted Recursive Resolver Program for DNS-over-HTTPS (DoH)

A Performance

~Do53

Min. idle time

Dual-stack

Transparency

Privacy notice

Transparency report

Privacy

24h storage for ops reasons Aggregation must strip PII No selling/sharing of data

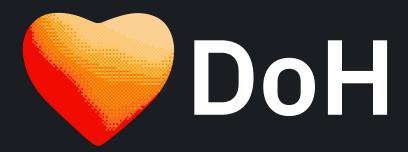
Blocking

Only filter as required by law Public blocklist (or reporting)



https://wiki.mozilla.org/Security/DOH-resolver-policy |≤

Thank you



Lars Eggert, leggert@mozilla.com

lars@social.secret-wg.org

Valentin Gosu, vgosu@mozilla.com

valenting@fosstodon.org