Council of European National Top-Level Domain Registries

CENTR Issue Paper on DNS over HTTPs

Brussels, Belgium
17 June 2019

Introduction

This is an issue paper drafted by the CENTR Secretariat. It aims to inform the CENTR community about DNS over HTTPS (DoH).

Executive Summary

In discussions about DoH, it is important to distinguish the protocol from the way it could be implemented. DoH is a protocol that addresses some structural weaknesses of the Domain Name System[1]. The implementation of DoH will effectively solve those weaknesses but could also lead to a significant shift in the way a crucial part of the internet functions. Browser vendors might get even more power and control and, depending on their choices, other parties that are involved in providing users with a stable and secure internet experience (such as ISPs) might be affected. It might also affect the users by limiting their choice, as well as governments' and the courts' ability to block traffic, and could even have an impact on the universality of the internet. Most of the consequences will rely entirely on the choices made by a handful of companies that dominate the browser market. This paper explores the possible impact of those choices.

We conclude that DoH is a step towards a more secure internet, but the way in which it will be implemented, and the effects of consolidated market power might have far-reaching consequences.

What is DoH (short explanation)

A domain name is an address that is readable by humans (as opposed to machines) and that helps users remember the location of websites and email addresses. However, computers and other devices cannot interpret these domain names as they rely on IP addresses to communicate with each other. Therefore, every time a domain name is used (by the user or by an application), the domain name needs to be translated to an IP address. In a standard configuration, the operating system of a device (like a laptop or mobile) will send the question "What is the IP address for www.example.com?" to a resolver. Today this resolver is typically provided for by the user's internet Service Provider (ISP).

[1] For the purposes of this paper, all references to the Domain Name System are only made to the part of it that is affected by DoH. For the full description of how the DNS works, please refer to https://centr.org/education/the-dns.html

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium

Phone: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org

www.centr.org

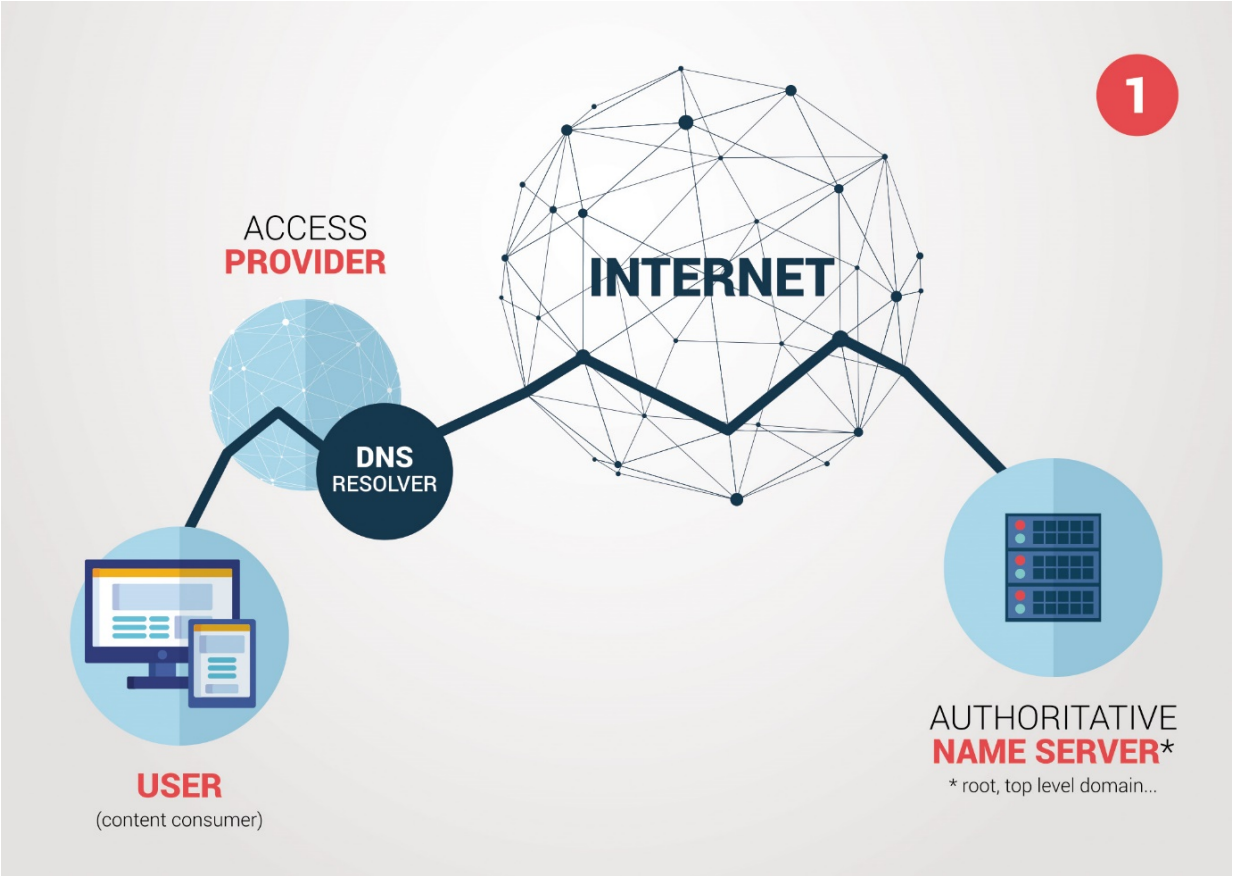


Fig. 1 – The typical setup of DNS resolution traffic without DNS over HTTPS.

The domain name system (DNS) is a very stable and efficient protocol, but it has a few weaknesses that were not identified as issues at the time the DNS was developed. These two main weaknesses are:

1. Questions to resolve a domain name are sent in clear text. This means that anyone who can monitor the traffic (e.g. the provider of the free WIFI at your coffee shop) can see which domains users of that WIFI are looking for.
2. Partly because of that transparency, there is a risk of these questions being intercepted, and of an incorrect answer being sent to the user. In some cases this could lead to users being misguided to fraudulent websites.

In order to address those weaknesses, DNS over HTTPs (DoH) was developed. It is a technical protocol and was adopted by the internet Engineering Task Force (IETF) in October 2018[2].

In essence, DoH is a light-weight and elegant solution that uses existing technology to solve these two issues. It does so by sending these questions over the HTTPS protocol that is a part of a browser. Therefore, rather than relying on the operating system of the device, it uses the browser to ask these questions. The

[2] DNS Queries over HTTPS (DoH), RFC 8484. The status of adoption and the standard itself are available at: https://datatracker.ietf.org/doc/rfc8484/

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

advantages are: 1. Since this is encrypted traffic (the 's' in HTTPS stands for 'secure'), an intermediary (such as the ISP or WIFI provider) can no longer look at the domains a user is visiting. 2. As a result it becomes nigh on impossible to intercept the traffic and misdirect the user (so called man-in-the-middle-attacks).

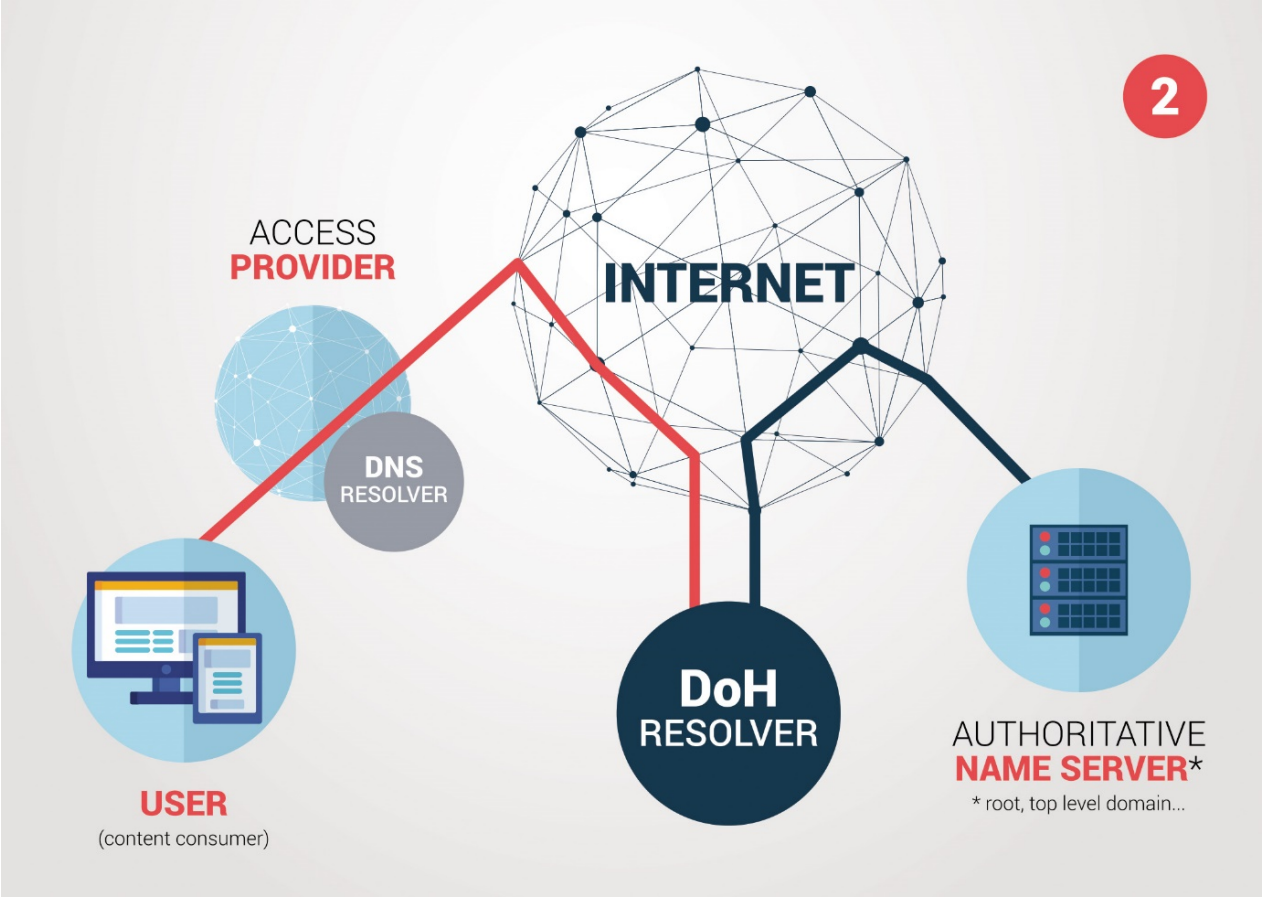


Fig. 2 – Schematic overview of DNS traffic with DNS over HTTPS.

So far so good. DoH is undeniably an improvement as it solves these two important weaknesses.

However, the protocol does not define who answers the questions. It could still be the ISP, but it could also be another resolver. This is where things get interesting.

Following the adoption of the protocol, browser companies identified an opportunity to get more control over the traffic of their users. They get to choose where (i.e. which jurisdiction) they will send those billions of queries per day from users all over the world. There are obvious advantages for browser vendors: they increase their control over the quality of the browsing experience, they get to protect their users better since the weaknesses mentioned above have been addressed and they get to choose who resolves these questions.

However, for the broader internet industry, this also has important consequences, which were not in the scope of the technical specifications of DoH, but which may result from implementation choices made by browsers.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Effects of DoH

The effects of DoH can be split into three categories: effects on users, effects on top-level domain registries and effects on the internet ecosystem.

Effects on the users

Most internet users are blissfully unaware of what goes on in the background of a simple surfing or emailing session. While currently, they can easily change the way their queries are resolved, most would not know why they would do that or where to find those options.

Nevertheless that freedom is important on a user level. It can in some cases allow the user to choose a more secure browsing experience or a more unrestricted or uncensored one. It can allow parental control mechanisms. Most importantly, that freedom allows users to choose the resolver that has the privacy policy that they feel comfortable with. They can choose a European resolver, or one based in the US. It should be noted that all queries from that user will end up with the resolver, and as such do reveal a lot of personally-identifiable and even sensitive information.

Another aspect of relevance to users is what is often referred to as the universality of the internet. This means that whatever software one uses, the query will always yield the same answer (as it is the operating system that will do the lookup). Currently it does not matter which browser one uses; the answer to 'Where do I find www.example.com?' will always be the same on any given machine. Following the deployment of DoH, it is not unrealistic to expect that different resolvers in different jurisdictions than the user could provide different answers. Local legislation might oblige them to restrict access to content which would be perfectly legal in the user's own jurisdiction. This would only affect a limited number of domains but, depending on the choice for a particular browser, the user could see a different internet.

Effects on top-level domain registries

The technical effects on TLD registries are limited. The main effect is probably a marginally-reduced query load on the registries' authoritative name servers.

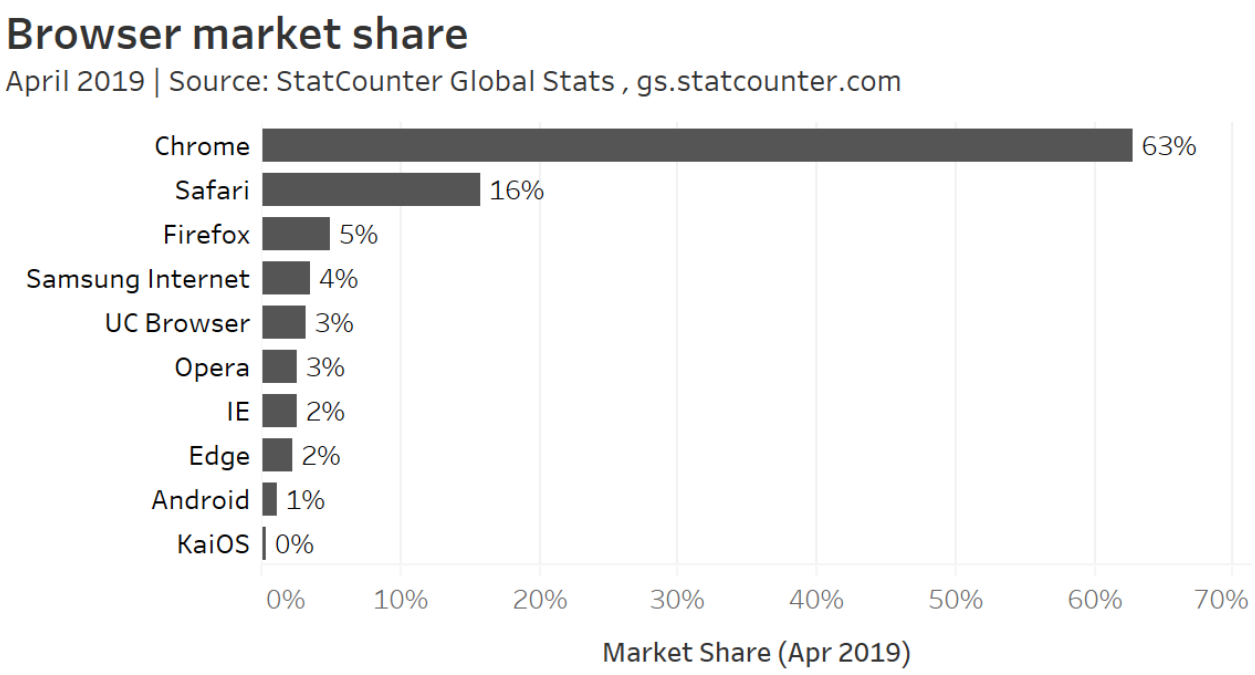
What is much more relevant is the possible impact at policy-level. Currently, TLD registries can enforce a range of policies that tell millions of resolvers from all around the world how to behave when querying their zone. If – after the successful implementation of DoH – a handful of resolvers serve 95% of internet users, it might affect the way in which TLD registries can enforce their policies. Examples include restrictions on queries per second and respect for Time To Live (TTL)[3].

Effects on the internet industry

The key aspect to understand the possible effects of the implementation of DoH on the wider internet industry is the distribution of market share in the browser market. Five browsers currently cover about 90% of the browser market. This significantly limits consumer choice. This effect is reinforced by the compatibility requirements and browser optimisation. Any website will try to limit their development costs by catering for the wishes of the few dominant players (this is illustrated by the welcoming message: "This website is optimised for viewing in browser X.").

[3] These policies are regarded as essential features to safeguard the stability and security of the resolution service.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



This consolidation of power in the hands of a few browsers (and the resolvers they identified) has a couple of consequences.

Firstly, while it might seem far-fetched at this stage, it could have an impact on the way the global DNS system functions and develops. It is worth noting at this point that the respect for the authority of the root zone is voluntary. Currently, every ISP resolver that is looking to resolve a domain name will query the root zone and respect the answer it receives. It respects the root zone because not respecting it would mean that their customers would quickly move to ISPs that do. With a handful of dominant players, it is less certain that this would still be the case. Should they (jointly or individually) decide not to respect the authority of the root zone, they could easily do so without repercussions. This would have far-reaching consequences on the multistakeholder model that currently develops the policy for the root zone under the ICANN umbrella. Theoretically, one or a handful of resolvers could decide to reject queries for a specific top-level domain which it considers to be too loose on abuse, spam or malware.

Secondly, an important “point of control” changes.

At the moment the ISP sees the DNS traffic and can protect its own network from abuse. The most cited example is where ISPs block requests from malware sitting on their customers’ devices. By blocking these requests, ISPs make their network more secure, but also prevent attacks and abuse from spreading to other networks. With DoH, ISPs no longer see this traffic and therefore cannot prevent this abuse any longer.

This also has other consequences. Since ISPs can control traffic, they have been identified by regulators, courts and law enforcement agencies as a party that can help them block access to unwanted or illegal content. In the example of The Pirate Bay, many European countries prevent their citizens from accessing this website. They do so by ordering access providers to stop any DNS query to those domains and redirecting users to a website managed by local Law Enforcement Agencies. This has proven to be a quick

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

(though inefficient[4]) way of preventing access to material hosted in other jurisdictions[5]. With DoH, blocking at ISP-level becomes impossible. The level of control will change to whichever resolver is identified by the browsers to answer the queries. Since these resolvers are currently US-based, it will mean that US jurisdiction applies. One of these resolvers (Cloudflare) has already made public statements on how it intends to resist legislative or jurisdictional pressures, but it remains to be seen how long they would be able to hold off that pressure.

Status of implementation

This overview started with the assumption that each browser would only select one resolver and hard-code that in its software. This would mean that users could not change it even if they wished to. It also assumes that these resolvers are US-based. These assumptions were based on the initial statements from some of the browsers and resolvers.

Since the start of the public discussions, more details are becoming available, and browser vendors and resolvers have made public statements about their intentions. In the case of Mozilla (and the resolver of their choice: Cloudflare), they have indicated that they are leaning more towards allowing restricted choice by the consumers[6]. This would be made possible by offering a list of resolvers that have been approved by Mozilla to users. Google Chrome (and its own 8.8.8.8 resolver) has indicated that it will allow the ISP to continue taking care of the resolving if they can provide their users with a DoH-enabled resolver[7]. Standards to codify the exchange between the browser and the ISP would still need to be agreed upon.

CENTR discussions

In May 2019, European ccTLD managers met in Amsterdam to discuss DoH and its possible impact. They agreed that CENTR should encourage its members to provide open resolvers to increase consumer choice. Some CENTR members already provide that service (such as the operators of .lu and .cz.)

[4] CENTR, "Analysis of blocking and redirection of domain names as tools to restrict access to content", available at: https://centr.org/library/library/policy-document/centr-paper-domainblocking-20120302.html

[5] It should be noted that currently even without DoH, users can opt for alternative open resolvers. This is one of the reasons why blocking is ineffective, but only a small percentage of users currently use that possibility.

[6] Marshall Erwin, "DNS-over-HTTPS Policy Requirements for Resolvers", Mozilla Security Blog, available at: https://blog.mozilla.org/security/2019/04/09/dns-over-https-policy-requirements-for-resolvers/

[7] According to the statement made by Google Chrome on the public IETF mailing list, available at: https://mailarchive.ietf.org/arch/msg/dnsop/dCuB-32Tz5YKCWsrJZ42SXmDs40

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Further reading

- V. Bertola, The DoH dilemma: https://www.icann.org/sites/default/files/packages/ids-2019/07-bertola-the-doh-dilemma-dns-symposium-2019-v2-11may19-en.pdf

- G. Huston APNIC DNS over HTTPS Explained: https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/

- O. Guðmundsson, Cloudflare ppt at DNSOARC: https://indico.dns-oarc.net/event/29/contributions/653/attachments/640/1027/DoT_and_DoH_experience.pdf

- For a status on IETF discussions read the CENTR report from IETF 104: https://centr.org/library/library/external-event/centr-report-on-ietf104.html

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org