

DNS Privacy Reference Material

- [Relevant Internet Drafts and RFCs](#)
- [Selection of Presentations](#)
- [Technical reports](#)

Relevant Internet Drafts and RFCs

DPRIVE - [see the DPRIVE document website](#)

draft-ietf-dprive-bcp-op-00	Recommendations for DNS Privacy Service Operators	Describes Best Current Practices for operators of DoT and DoH servers in terms of protocol, service and privacy policy considerations.
RFC7626	DNS Privacy Considerations	This document describes the privacy issues associated with the use of the DNS by Internet users. It is intended to be an analysis of the present situation and does not prescribe solutions.
RFC7858	Specification for DNS over TLS	This document describes the use of TLS to provide privacy for DNS.
RFC7830	The EDNS(0) Padding Option	his document specifies the EDNS(0) 'Padding' option, which allows DNS clients and servers to pad request and response messages by a variable number of octets.
RFC8467	Padding Policy for EDNS(0)	Specifies the preferred algorithm for padding with the option defined in RFC7830
RFC8310	Usage Profiles for DNS over TLS and DNS over DTLS	This document describes how a DNS client can use a domain name to authenticate a DNS server that uses Transport Layer Security (TLS) and Datagram TLS (DTLS). Additionally, it defines (D)TLS profiles for DNS clients and servers implementing DNS-over-TLS and DNS-over- DTLS
RFC8094	Specification for DNS over Datagram Transport Layer Security (DTLS)	
draft-ietf-dprive-eval	Evaluation of Privacy for DNS Private Exchange (expired)	This document describes methods for measuring the performance of DNS privacy mechanisms, particularly it provides methods for measuring effectiveness in the face of pervasive monitoring as defined in RFC7258.

DNSOP

RFC7766	DNS Transport over TCP - Implementation Requirements	This document specifies the requirement for support of TCP as a transport protocol for DNS implementations and provides guidelines towards DNS-over-TCP performance on par with that of DNS-over-UDP.
RFC7816	DNS Query Name Minimisation to Improve Privacy	
RFC7828	The edns-tcp-keepalive EDNS0 Option	This document defines an EDNS0 option ("edns-tcp-keepalive") that allows DNS clients and servers to signal their respective readiness to conduct multiple DNS transactions over individual TCP sessions.

DOH

RFC8484	DNS Queries over HTTPS (DoH)	Document describing the protocol aspects of running DNS over HTTPS.

Other

RFC5246	The Transport Layer Security (TLS) Protocol
RFC7525	Recommendations for Secure Use of TLS and DTLS
RFC7413	TCP Fastopen

Selection of Presentations

Also see the [DNS Privacy Workshop pages!](#)

- **OARC 29**
 - Where will encrypted DNS transports push DNS operators?- [Slides](#), [Video](#)
- **RIPE 77**
 - It's DNS Jim, But Not as We Know It - [Slides](#), [Video](#)
 - DNS Privacy measurements (Benchmarking DoT) - [Slides](#), [Video](#)
- **ICANN DNS Symposium 2018**
 - 'Where's my DNS?' ([video](#))
- **RIPE 76**
 - [Measurements on DNS Privacy](#) (DNS-over-TCP and TLS benchmarking)
 - [BCOP WG - DNS Privacy PCP](#)
 - [Dude, where's my DNS?](#) (subtitle 'DNS-over-HTTPS is coming!')
- **FOSDEM 2018**
 - [Willem Toorop on Stub resolvers](#)
- **OARC 27**
 - [DNS Privacy clients. You tube video.](#)
- **JCSA 2017**
 - [Hands on with getdns](#)
- **IETF 99 EDU Privacy Tutorial**
 - [DNS Privacy Tutorial](#) (Sara Dickinson, Daniel Kahn Gillmor)
- **RIPE 72**
 - [DNS Privacy Public Resolver discussion](#) (Sara Dickinson)
- **IETF 94:**
 - [DNS-over-TLS draft update](#) (D. Wessels, S. Dickinson)
- **IETF 93:**
 - [Update on 5966bis and EDNS0 keepalive](#) (Sara Dickinson)
- **DNS-OARC Fall workshop 2015:**
 - [Using TLS for DNS Privacy in practice](#) (Sara Dickinson)
- **IETF 91:**
 - [DNS over TCP and TLS - draft-hzhwm-dprive-start-tls-for-dns-00](#) (John Heidemann, Sara Dickinson)
 - A short video is demonstrating TCP connection re-use, pipelining, TCP Fast Open and DNS-over-TLS: [DNS-over-TLS demo video](#)
- **IETF 89:**
 - [T-DNS: Connection-Oriented DNS to Improve Privacy and Security](#) (Duane Wessels)
- **DNS-OARC Spring workshop 2014:**
 - [T-DNS: Connection-Oriented DNS to Improve Privacy and Security](#) (John Heidemann)
 - [getdns-api implementation](#) (Willen Toorop)

Technical reports

- **T-DNS: Connection-Oriented DNS to Improve Privacy and Security** (<http://www.isi.edu/publications/trpublic/files/tr-693.pdf>)
- <http://googlecode.blogspot.co.uk/2012/01/lets-make-tcp-faster.html>