DNS Privacy Implementation Status

DNS-over-TLS Implementation Status

This table lists the best understanding of the current status of DNS-over-TLS related features in the latest stable releases of **a selection of standalone open source DNS software**.

> Also see DNS Privacy Clients for a full list of OS, mobile apps, routers and browsers that support DoT.

If there are errors or glaring omission please email sara@sinodun.com

> **Also see** guides on how to use NGINX and other proxies to provide DNS-over-TLS, also see here.

This works with a couple of provisos:

- Be aware that a client will think it is talking to a DNS-over-TLS server and so may keep connections open when idle even when not using EDNS0 Keepalive (as allowed by RFC7858). The nameserver will see only TCP connections which were historically used just for one-shot TCP and may not be robust to many long-lived connections.
- Therefore this **will work much better** if the nameserver has robust TCP capabilities (as described in Sections 6.2.2 and 10 of RFC7766), and would be required for production level service. Any server that fully implements EDNS0 Keepalive (RFC7828) should meet this criteria.

See the DNS Privacy Reference Material page for more details on the individual features.

Clients/Forwarders

Mode		Stub						Caching forwarder/proxy			
Software		ldns (drill)	digit	getdns (Stubby)	BIND (dig)	Go DNS	Knot (kdig)	Unbound	BIND	Knot Res	dndist
General	Send ECS with SOURCE PREFIX-LENGTH value of 0			✓	✓		✓				
TCP/TLS Features	TCP fast open[b]		✓	✓				✓			✓
	Connection reuse (Q/R, Q/R, Q/R)		✓	✓	✓	✓	✓		✓	✓	✓
	Pipelining of queries(Q,Q,Q,R,R,R)	n/a	✓	✓	✓	✓	✓		✓	✓	✓
	Process OOOR (Q1,Q2,R2,R1)	n/a	✓	✓	✓				✓	✓	✓
	EDNS0 Keepalive[c]			✓	✓				(f)		
TLS Features	TLS encryption (Port 853)		✓	✓		✓	✓	✓		✓	
	TLS authentication			✓			✓	✓		✓	
	EDNS0 Padding		✓	✓	✓		✓		✓		
	TLS DNSSEC Chain Extension[h]										

Servers

Mode	Load Balancer	Recursive	Auth

Software		dnsdist	Unbound	BIND	Knot Res	CoreDNS[e]	Tenta[e]	NSD	BIND	Knot Auth
General	**QNAME minimisation**	n/a	✅	✅	✅					
TCP/TLS Features	**TCP fast open[b]**	✅	✅	✅	✅				✅	✅
	Process Pipelined queries	✅	✅	✅	✅			✅	✅	✅
	Provide OOOR	(g)	✅	✅	✅			n/a	n/a	n/a
	EDNS0 Keepalive[c]		✅	✅	✅				✅	
TLS Features	**TLS encryption (Port 853)**	✅	✅	(d)	✅	✅	✅			
	Provide TLS auth credentials	✅	✅	(d)	✅	✅	✅			
	EDNS0 Padding (basic)			✅	✅				✅	
	TLS DNSSEC Chain Extension[h]									

KEY:

- Green square ✅ - indicates latest release already supports this functionality
- Blue square - indicates that a patch is available in our git repo. See here for details: DNS-over-TLS patches
- Yellow square - indicates work in progress, or availabe in next release
- P - Requires building against a patched version of libunbound

(a) getdns uses libunbound in recursive mode
(b) not yet available on Windows
(c) Implies robust TCP connection management (see RFC7828 and RFC7766)
(d) See this article for how to use stunnel with BIND to provide DNS-over-TLS - thanks Francis Dupont!
(e) Full list of supported features to be confirmed
(f) Can be added to queries but the response is currently ignored.
(g) Supports OOOR but could be limited by the nameserver or configuration used for recursion.
(h) This is no longer an active draft in the TLS working group.

Note pipelining and OOOP are not applicable for synchronous applications.

Other implementation work

- There is also a RUST implementation of a DNS client/server in development that supports DNS-over-TLS.
- Also see the Technitium DNS Server project project (supports DoT and DoT), source code is on Github).

DOH Implementation status

The picture for DOH implementation is move very rapidly. Some work to date

> ⓘ See the list of implementations maintained on the curl github site:
>
> - Browsers and Clients
> - Tools including various proxies (client and server) e.g dnscrypt-proxy, Facebooks experimental DoH proxy

- For work done at the IETF 101 Hackathon see the DOH Hackathon presentation
- We also maintain a list of some DOH clients (includes web browsers)
- And below is the state of DoH implementation is well know open-source DNS recursive resolvers/load-balancers

Mode	**Load Balancer**	**Recursive**		
Software	**dnsdist**	**Unbound**	**BIND**	**Knot Res**
DoH support	WIP			Experimental Implementation released in 4.0.0