

# draft-ietf-dprive-start-tls-for-dns-01

IETF 93, Prague

July 24, 2015

# Changes since -00

- Incorporated a number of suggestions and comments from Daniel Kahn Gillmor, Sara Dickinson, and others.
- Removed a discussion question on utility of the TO in a UDP message. There was no input from the working group on this point.
- When a client receives TO=0 in response to TO=1 query, the client MAY (was SHOULD) use the established connection for unencrypted queries.
- Clarify that when TLS handshake fails, both sides must close the connection.

# Changes since -00

- Rewrote the "established connection" section.
- This document no longer makes specific recommendations on idle timeouts. It defers to other documents.
- Added reference to TLS fast session resumption and mention of TLS false start work-in-progress.
- Added an "implementation status" section.

# Strong TLS Profile

- We will add reference to RFC 7525 (BCP 195), Recommendations for Secure Use of TLS and DTLS.

# Discussion: Upgrade vs. Port

- Authors heard working group desire to eliminate “STARTTLS” upgrade approach from the draft.
- Would simplify implementations.
- We have asked the chairs to request RFC 7120 early allocation of port.

# Implementation Status

- Unbound
  - supports port-based DNS-over-TLS since 1.4.14
  - upgrade-based patch for 1.5.1
- ldns & drill
  - port-based and upgrade-based patch
- digit (USC/ISI tool)
  - supports both port- and upgrade-based
- getdns (client)
  - port-based and upgrade-based
  - new: certificate authentication (hackathon!)

# Hackathon Screenshot

```
count": 4,  
count": 5,  
f": 0,  
f": 21547,  
count": 0,  
code": GETINS_OPCODE_QUERY,  
count": 1,  
f": 1,  
f": 1,  
code": GETINS_RCODE_INTERNAL,  
f": 1,  
f": 0,  
f": 0  
ation":  
  
class": GETINS_RESPONSE_IN,  
name": "data of \"google.com.\">,  
type": GETINS_RTYPE_NS  
  
: GETINS_RESPSTATUS_GOOD  
  
ole was: GOOD. Status was: At least one response was returned  
  
e:"/src/getdns/getdns$ src/test/getdns_query -l L @185,49,141,38"dnsec-nae@  
e.com -s google.com
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
95	43.503352000	31.133.162.154	185.49.141.38	TCP	74	40712-1021 [SYN] Seq=0
96	43.523269000	185.49.141.38	31.133.162.154	TCP	74	1021-40712 [SYN, ACK] S
97	43.523327000	31.133.162.154	185.49.141.38	TCP	66	40712-1021 [ACK] Seq=1
98	43.523650000	31.133.162.154	185.49.141.38	TLSv1.2	415	Client Hello
99	43.542063000	185.49.141.38	31.133.162.154	TLSv1.2	1514	Server Hello
100	43.542128000	31.133.162.154	185.49.141.38	TCP	66	40712-1021 [ACK] Seq=35
101	43.542465000	185.49.141.38	31.133.162.154	TCP	1514	[TCP segment of a reass
102	43.542485000	31.133.162.154	185.49.141.38	TCP	66	40712-1021 [ACK] Seq=35
103	43.542920000	185.49.141.38	31.133.162.154	TLSv1.2	747	Certificate
104	43.542938000	31.133.162.154	185.49.141.38	TCP	66	40712-1021 [ACK] Seq=35
105	43.545554000	31.133.162.154	185.49.141.38	TLSv1.2	640	Client Key Exchange, Ch
106	43.572020000	185.49.141.38	31.133.162.154	TLSv1.2	324	New Session Ticket, Cha

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello  
Content Type: Handshake (22)  
Version: TLS 1.2 (0x0303)  
Length: 58

▼ Handshake Protocol: Server Hello  
Handshake Type: Server Hello (2)  
Length: 54  
Version: TLS 1.2 (0x0303)

- ▶ Random  
Session ID Length: 0  
Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)  
Compression Method: null (0)  
Extensions Length: 14
  - ▶ Extension: renegotiation\_info
  - ▶ Extension: SessionTicket TLS
  - ▶ Extension: Heartbeat

0000	8c a9 82 be b5 aa 08 81 f4 8a a7 f1 08 00 45 00	.....E.
0010	05 dc e1 d2 40 00 35 06 55 d2 b9 31 8d 26 1f 85	...0.5. U..1.&..
0020	a2 9a 03 fd 9f 08 88 33 bb e4 c7 38 5f d1 80 10	.....3 ..8...
0030	04 10 37 5d 00 00 01 01 08 0a 32 dd d6 d5 02 74	...7]... ..2....t
0040	82 2c 16 03 03 00 3a 02 00 00 36 03 03 9b 9b 95	.....: ..5.....

Frame (frame), 1514 bytes Profile: Default

**Q & A**