Authentication and (D)TLS Profile for DNS-over-(D)TLS

draft-ietf-dprive-dtls-and-tls-profiles-07

S. Dickinson  Sinodun
D. Gillmor  ACLU
T. Reddy  Cisco
Current Status

- 2 week WGLC started on 6th Oct (on -03 version)
- WGLC extended due to lack of review
- More review since
- -07 version published with moderate re-structure
Remaining issues

• Opportunistic - specifics of behaviour
  • Auth & Enc
  • Enc
  • Clear text
  • Hard fail

“Clients using Opportunistic Privacy SHOULD try for the best case but MAY fallback…”

Change this to MUST to maximise privacy but potentially increasing latency?
Remaining issues

- Opportunistic - specifics of behaviour
- Auth & Enc
- Enc
- Clear text
- Hard fail

RFC7354 allows this - but should we remove this so clients ALWAYS use clear text for improved usability?

Or is there a small set of cases where this may be desirable?
Implementations

- **stubby** - a DNS Privacy enabling stub resolver
- getdns running as a daemon, pointed at DNS Privacy test servers (work in progress)

From this draft:

- Strict and Opportunistic
- Name and SPKI authentication
Lets make DNS great again!

• Really need to move the draft forward
• Last big piece in the stub to recursive story

Please review!

Volunteers?