Encrypted Client Hello
draft-ietf-tls-esni

Rescorla, Oku, Sullivan, Wood — IETF 112 Online— TLS
Recap

Status update

draft-ietf-tls-esni-13 is the current interop and deployment target

Open issues parked:

• Handshake padding
• Revisiting acceptance/rejection signal and HRR GREASE
• ECHConfig extensibility

Plan: Seek resolution once we gain deployment experience
Interop
Status update

Known implementations tracked in the wiki

• BoringSSL: -13
• OpenSSL fork: -13
• NSS: -13 (nearly complete)
• Go fork: -13
• rustls: -10 (-13 underway)

Request: add your implementation to the wiki
Implementation Red Flags

Status update

Several sharp edges

- DNS dependency and plumbing can be non-trivial (who parses ECHConfig?)
- ECHConfig.public_name IP address parsing is non-trivial (WHATWG? Something else?)
- ECH split-mode and HRR is challenging on the server side
- ... what else?

Request: start compiling sharp edges in the wiki
Encrypted Client Hello

draft-ietf-tls-esni