Encrypted Client Hello

draft-ietf-tls-esni

IETF 111 - TLS WG - Online
Document is complete enough to implement
No known security issues
Needs bake time for analysis and test deployments
Overall proposed approach: defer unnecessary changes
Acceptance Signal (#450, #441)

Two related questions:

1. Should the non-HRR acceptance signal use an extension?
2. Should the acceptance signal extension be GREASEd?

Options:

(Yes, Yes): Consistent with HRR, risks new server-side extension ossification to hedge against HRR extension ossification
(No, No): No changes, risks HRR extension ossification
(Yes, No): Consistent with HRR, risks HRR extension ossification
(No, Yes): ???
Acceptance Signal (#450, #441)

Proposal: No change (No, No).

Rationale: Park and run experiments to determine if HRR is impacted.
Server-Side Padding (#264)

How should we pad server-side flights in ECH?

- New handshake message
- Handshake message extensions
- Pad-to-the-max

Considerations: QUIC integrations, certificate compression relation, state machine impact, RFC8446 restrictions, etc.
Server-Side Padding (#264)

Proposal: Do nothing (maybe spin out handshake message padding to a separate draft).

Rationale: Server-side padding may not be needed for experiments, and may not be needed for privacy benefits given alternatives (default padding, use existing mechanisms, etc).
Extensibility (#427)

Should ECHConfig be extensible?

Proposal: Park (or close and reopen later).

Rationale: We have no new information to make a decision now. Experiments may reveal new insights about whether or not extensions are needed. Plus, it’s no cost to parse now.
Interop Target

Proposal: Move to -12

Fill out results in the matrix
Moving Forward

Resolve (or park) open issues as above
Refactor document for editorial clarity
Start test deployments with -12
Revisit in IETF 112