RFC 8446-bis

Eric Rescorla
ekr@rtfm.com

2022-11-10

Current Status

- Merged a bunch of stuff
  - Check the changelog
- A few outstanding PRs
  - ... which I hope to mostly resolve now

PR#1275: Unsolicited Extensions

- Clarifies the text around "unsolicited" extensions
- The point is that you can't send "request" extensions in "response" messages (e.g., EE)
- I think this is just a text clarification

PR#1270: KeyUpdate Limits

- Just pulled in the text from 9147
- MT had some comments
- Consistency versus improving this...

PR#1269: Errors for Bogus Tickets

- Plan was to add a new alert
- But it turns out there actually is an "unknown_psk_identity" (new since 8446)
- Propose we just close this

PR#1231: Acknowledge RFC 8773

- I need to review
- Other people's reviews welcome

Issue#1223, #1224: Clarify HRR Behavior

- Yes it is a bit unclear
- But neither DavidBen nor I have managed to improve it much
- This draft is already an improvement over 8446 and no worse in these respects
- Finished is a feature
- Propose to defer these