RFC 8446-bis

Eric Rescorla
ekr@rtfm.com

Next steps

- Close these issues and the other editorial stuff
- Call for other remaining issues
- New draft
- WGLC

Issue 1214: Recommended vs. Not Recommended

- Concerns
  - “Not Recommended” covers a lot of ground
  - Categorizations can be use-case specific
- Proposal:
  - Recommended: The WG thinks this is good for general use. (E.g., TLS_AES_128_GCM_SHA256). Requires a standards track RFC.

  - Conditionally Recommended: The WG thinks this is good for limited scope, as with IoT (must come with some description of that scope) (e.g., TLS_AES_128_CCM_8_SHA256). Requires a standards track RFC.

  - Not recommended: The WG expresses no opinion on this (e.g., TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC)

  - Discouraged: Known not to provide the rated TLS 1.3 security guarantees (e.g., TLS_SHA256_SHA256)

Issue 1212: “general alert”

- Should we allow a non-specific “something went wrong” alert
- To be used instead of specific alerts
- Proposal: define something at MAY level and say SHOULD send more specific if you can

Issue 1208: user_cancelled

- Current text is confusing
- We know people *send* user_cancelled
- Options:
    - ignore it
    - treat it as an alias for close_notify

Issue 1221: unsolicited extensions

- kaduk: “Apparently Johnathan Hoyland thinks that the current text allows for unsolicited non-request-response extensions unless specifically forbidden (e.g., for HRR), but Ekr and I think they are forbidden. Perhaps this should be clarified.”
- S 4.2 seems clear: “Implementations MUST NOT send extension responses if the remote endpoint did not send the corresponding extension requests, with the exception of the "cookie" extension in the HelloRetryRequest.”
- Hoyland?

Not much left

- Some editorial PRs and issues (pending)
- A few substantive PRs (below)