RFC 8446-bis

Eric Rescorla
ekr@rtfm.com

2022-03-23

Current Status

- Close to done, hopefully
- Still a few substantive issues

Issue#1253: ECDHE Rekey Recommendations

- KeyUpdate offers PFS
  - Assuming you delete the old keys
- But not PCS
  - For that you need a new ECDHE exchange
- This issue proposes recommending a new exchange every hour/100GB. Seems ad hoc
- Proposal: close with no change

PR#1247: Errors for PSK

- TLS has a rich set of errors for certificate problems
- ... but not much for PSKs
- What about external PSKs that can expire, etc.
- PR#1251 suggests repurposing `certificate_revoked`, `certificate_expired`, and `certificate_unknown`.
  - This seems confusing
  - These granular messages seem not that helpful
- Proposal: `ticket_invalid`

Issue#1227: Which hash?

- PSK binder needs to be computed using PSK-associated hash
  - Obvious for CH1, CH2 for consistency
- Which hash is used for the `message_hash` reinjection?
  - PSK or negotiated?
  - Text is a bit confusing, but DavidBen and EKR agree it should be negotiated
- Proposal: modify the document to make the above clear

Issue#1223, #1224: HRR Confusion

- General model is kind of confusing
  - Mostly use CH1 or...
  - Mostly use CH2
- In any case, sometimes you make decisions in CH1 which impact validity of CH2 (e.g., resumption)
- ...
- What's the minimum thing we can do here to reduce ambiguity?

Last call on some issues

- 1206: More cookie guidance (Kaduk)
  - I don't think we need to say anything
- 1214: Expand Recommended/Not Recommended (EKR)
  - This will be in 8447-bis
- 1250: More guidance on multiple identities for post-handshake auth (Mattsson)
  - Seems like an application issue

Next steps

- New draft
- WGLC?