Secondary Certificate Authentication of HTTP servers

draft-ietf-httpbis-secondary-server-certs

Eric Gorbaty, Mike Bishop
HTTPBIS
IETF 122, March 2025, Bangkok

Current Status

- Non-editorial issues:
  - #2841 - Support sending Exported Authenticators in multiple frames over HTTP/2
- Editorial improvements

#2841 - Support sending Exported Authenticators in multiple frames over HTTP/2

- Exported Authenticators could be large enough (especially with post-quantum certs) to not fit in a single frame for HTTP/2
- A number of possible solutions discussed
  - New stream type over HTTP/2
  - CONTINUATION
  - Specify total size up front prior to sending chunks
  - Possible compression of certs
- So far the preferred solution has been to just ignore SETTINGS_MAX_FRAME_SIZE for SERVER_CERTIFICATE frames
- Objections to just going with this approach for now and revisit if needed?

Implementation interest

- Implementor status
- Interop testing