# Secondary Certificate Authentication of HTTP servers

*draft-ietf-httpbis-secondary-server-certs*

Eric Gorbaty, Mike Bishop

HTTPBIS

IETF 120, July 2024, Vancouver

# Current Status

- Recently adopted by the WG
- Non-editorial issues:
  - #2840 - Request and secondary certificate correlation
  - #2841 - Support sending Exported Authenticators in multiple frames over HTTP/2
  - #2842 - Rename CERTIFICATE to SERVER_CERTIFICATE
- Editorial improvements

# #2840 - Request and secondary certificate correlation

- If servers need to know which cert was “used” for a given request, there’s currently no mechanism provided to do that
- A field like CERT ID could be reintroduced
  - The server provides it in the frame or certificate request context
  - The client can then indicate the selected cert in a request header
- Is this worth adding to the draft? Are there any actual interested implementors that may care about this?
- Any alternative solutions if we do care?

# #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
  - Need to provide a way to send them over multiple frames
- No CONTINUATION frames due to certs being on the control stream
- We could add a TO_BE_CONTINUED flag for the frame type
  - If it's set, the next frame is a continuation of the current one
- Any other solutions?

# #2842 - Rename CERTIFICATE to SERVER_CERTIFICATE

- Seems to make more sense from the standpoint of possible client certs in the future
- OK with this name or are there any other suggestions?