# Secondary Certificates

How and Whether?

# Useful feedback on -06

## Separate Client and Server Opt-In

- **Previous:** Single setting controls use of extension
- **Now:** Separate settings allow each side to opt-in to C2S and S2C certificate exchanges

## Better Error Handling

- **Previous:** Several error codes defined for certificate issues; pushes for non-authoritative origins are connection-fatal
- **Now:** Error codes only for protocol misbehavior, using 4XX errors for unacceptable certificates; pushes for non-authoritative origins are stream errors

## Clarifying the Confused Deputy

- **Previous:** Didn't clearly say that server could not consider client certificates on other requests
- **Now:** Explicitly state that server MUST NOT consider client certificates unless the client indicates their use

# Divergent Currents

## Client Certificates

- Some stakeholders want to discourage use of client certificates
- Some stakeholders have existing uses of client certificates and want to use HTTP/2 (and HTTP/3)

## Server Certificates

- Privacy gain from using an existing connection without DNS or SNI exposure
- Probing for certificates is a potential privacy exposure

# Are we still doing this?

- Little feedback on recent draft versions, PRs
- Everyone interested, but no one implementing?
- New proposals being raised related to client certificates
  - Clearly still in active use