draft-ietf-httpbis-origin-frame-03

“Clients MUST NOT consult DNS to establish the connection's authority for new requests.”

Has not yet reached WG consensus

draft-ietf-httpbis-origin-frame-03

Existing DNS provision of 7540 is viewed as a weak second factor. Disagreement about how valuable it is.

Is the substitution of different (more performance and privacy friendly) second factors into ORIGIN a path forward?

draft-ietf-httpbis-origin-frame-03

One potential proposal coalesced from list suggestions addresses the increased vulnerability for a certificate mis issuance (2) or key compromise (3).

1. The usual certificate checks from 7540 9.1.1
2. Plus certificate meets client CT-Policy (e.g. one or more SCTs)
3. Plus certificate meets client revocation policy.