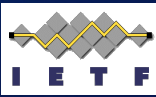


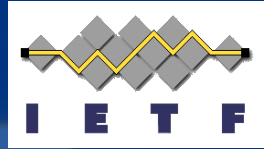
HTTPBIS WG
Virtual Interim
February 3, 2022



Client-Cert HTTP Header Field

draft-ietf-httpbis-client-cert-field

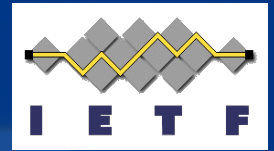
Brian Campbell
Mike Bishop



Context and Motivation

- HTTPS application deployments often have TLS ‘terminated’ by a reverse proxy somewhere in front of the actual HTTP(S) application
 - 'Old fashioned' n-tier reverse proxy and origin server
 - CDN-as-a-service type offerings or application load balancing services
 - Ingress controllers
- TLS client certificate authentication is *sometimes* used
 - In which case the actual application often needs to know something about the client certificate
 - But the original TLS connection terminated upstream so that info isn't available
- In the absence of a standardized method of conveying the client certificate information, different implementations have done it differently (or not at all)

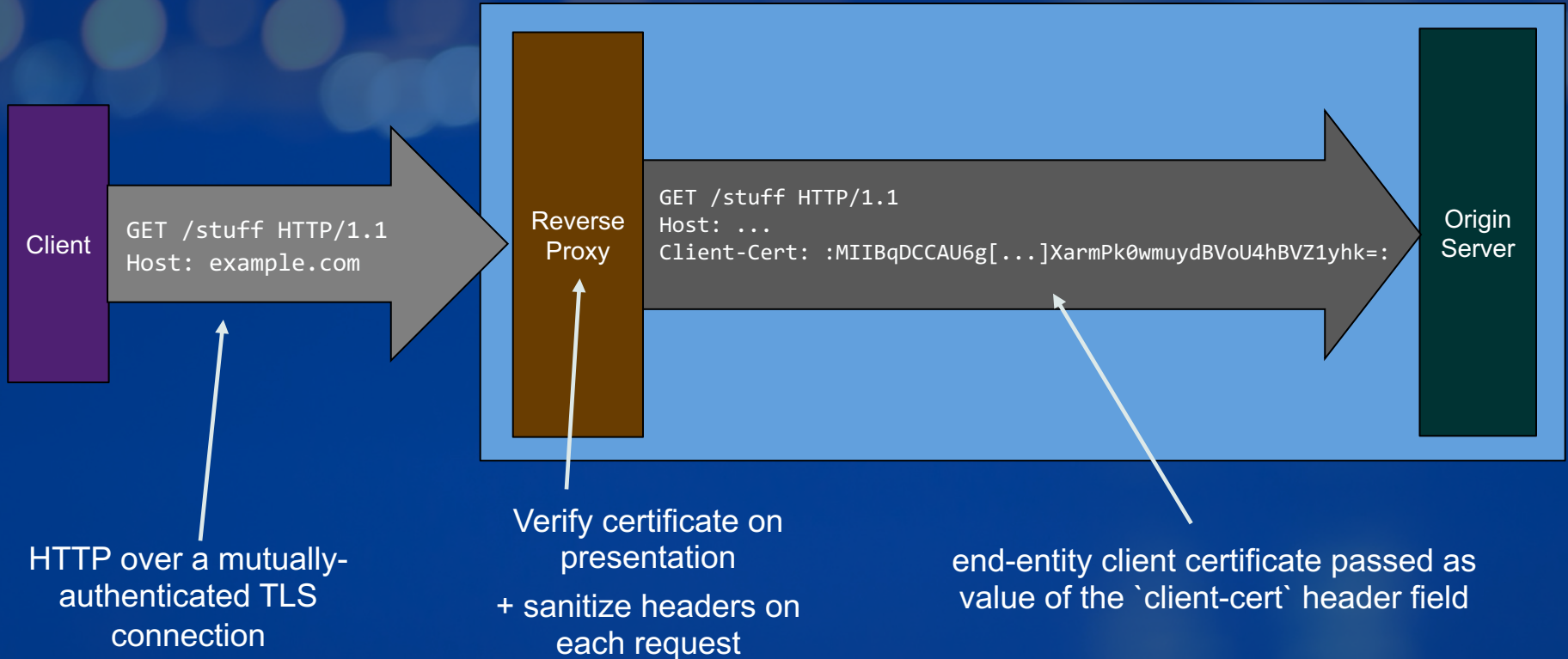
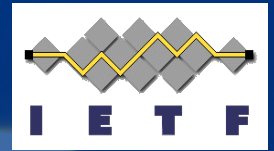
Goal



- Informational RFC that documents existing practice while codifying specific details sufficient to facilitate improved and lower-touch interoperability going forward
- Participate...

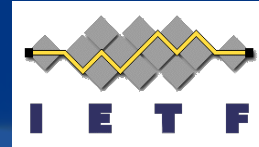
A screenshot of the IETF website. The top navigation bar includes the IETF logo, 'News & blog', 'Support us', 'Get started', 'Contact', 'Links', and a search icon. Below the navigation bar, there are dropdown menus for 'ABOUT', 'TOPICS OF INTEREST', 'PARTICIPATE', and 'INTERNET STANDARDS'. The main content area features a background image of a city skyline at night. The text on the page reads: '↑ > Participate > Meetings and events', 'IETF 106 Singapore', '16 Nov 2019 - 22 Nov 2019', and 'IETF 106 started Saturday 16 November and ran through Friday afternoon, 22 November 2019 in Singapore.'

The `Client-Cert` header field *solution* offered by the draft



Recent Updates

draft-ietf-httpbis-client-cert-field-01



- Now uses Structured Fields aka RFC 8941
- Introduced a separate `client_cert_chain` header that can convey the certificate chain
 - Two fields is a bit awkward...
- Considerations added about header compression and size
- Described potential interaction with caching
- Discussed renegotiation / post-handshake auth
- Filled out IANA Considerations with HTTP field name registrations

