Client-Cert HTTP Header Field

draft-ietf-httpbis-client-cert-field
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...
Draft’s Approach

Verify certificate on presentation
+ sanitize headers on each request

end-entity client certificate passed as value of the `client-cert` header field (and maybe `client-cert-chain`)

HTTP over a mutually-authenticated TLS connection

GET /stuff HTTP/1.1
Host: example.com

GET /stuff HTTP/1.1
Host: ...
Client-Cert: :MIIBqDCCAU6g [...]XarmPk0wmuuydBVoU4hBVZ1yhk=: Client-Cert-Chain: :MIIB5 [...]KGMy==, :MIICBj [...]QPWDC:
Recentish Happenings

-02 submitted 5/25
- Add a note about cert retention on TLS session resumption
- In the case of multiple post-handshake client cert authentications, say to use only the last one
Openish Stuff

IETF 114 will be in Philadelphia