HTTPBIS WG
~~IETF 111, San Francisco~~
Virtual Interim
June 15, 2021

Client-Cert HTTP Header Field

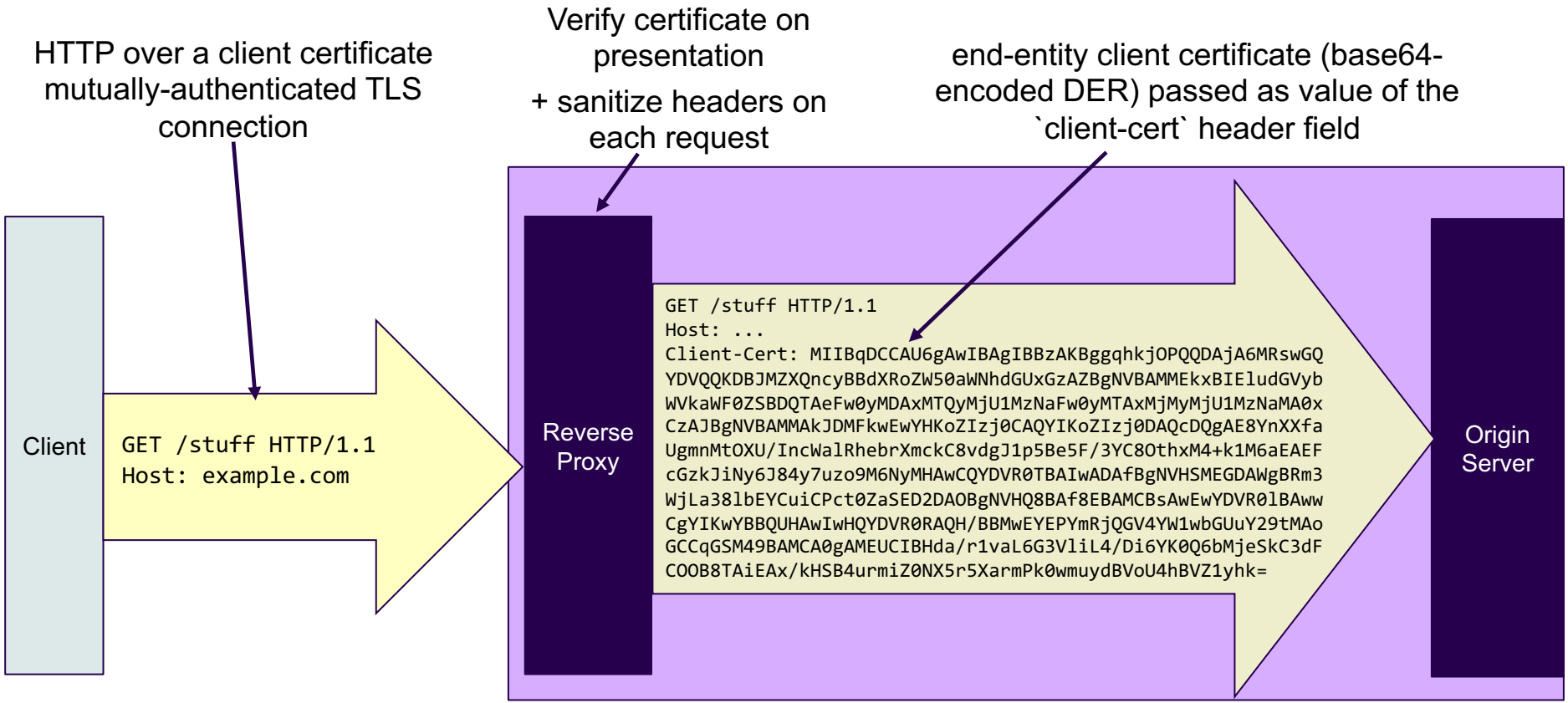
Conveying Client Certificate Information from TLS Terminating Reverse Proxies to Origin Server Applications

Brian Campbell
Mike Bishop
draft-ietf-httpbis-client-cert-field

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
- In the absence of a standardized method of conveying the client certificate information, different implementations have done it differently (or not at all)

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



Goal

- Document existing practice while codifying specific details sufficient to facilitate improved and lower-touch interoperability going forward

Status

- WG adoption after a bit of a hiatus and some fits and starts
- Intended status: Informational
- Mike Bishop joined as an editor
- WG draft -00 published last week (effectively unchanged from the individual draft)
- Editors' draft:
  - header/field terminology update
  - TODOs removed and converted into issues