

A photograph of the Golden Gate Bridge at night, illuminated with warm yellow lights. The bridge spans across a body of water, with its reflection visible. The sky is a deep blue, and the bridge's towers and suspension cables are clearly visible.

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)

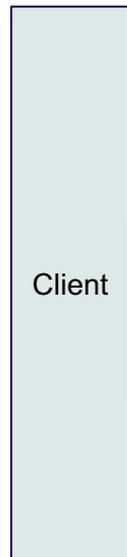
# The `Client-Cert` header field *solution* offered by the draft



HTTP over a client certificate mutually-authenticated TLS connection

Verify certificate on presentation  
+ sanitize headers on each request

end-entity client certificate (base64-encoded DER) passed as value of the `client-cert` header field



```
GET /stuff HTTP/1.1
Host: example.com
```

Reverse Proxy

```
GET /stuff HTTP/1.1
Host: ...
Client-Cert: MIIBqDCCAUGAwIBAgIBBzAKBggqhkJOPQQDAjA6MRswGQ
YDVQQKDBJMZXQncyBBdXRozW50aWNhdGUxGzAZBgNVBAMMEkxBIEludGVyb
WVkaWF0ZSBDQTAeFw0yMDAxMTQyMTU1MzNaFw0yMTAxMjU1MzNaMA0x
CzAJBgNVBAMMAkZDMFkwEwYHKOZIZj0CAQYIKoZIZj0DAQcDQgAE8YnXXfa
UgmnMtOXU/IncWalRhebrXmckC8vdgJ1p5Be5F/3YC80thxM4+k1M6aEAEF
cGzkJiNy6J84y7uzo9M6NyMHAwCQYDVR0TBAlwADAfBgNVHSMGDAAWgBRm3
WjLa381bEYCuiCPct0ZaSEd2DAOBgNVHQ8BAf8EBAMCBsAwEwYDVR01BAww
CgYIKwYBBQUHAWIwHQYDVR0RAQH/BBMwEYEPYmRjQGV4Yw1wbGUuY29tMAo
GCCqGSM49BAMCA0gAMEUCIBHda/r1vaL6G3V1iL4/Di6YK0Q6bMjeSkC3dF
COOB8TAiEAX/kHSB4urmiZ0NX5r5XarmPk0wmuydBVoU4hBVZ1yhk=
```

Origin Server

# 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

A screenshot of a GitHub issues page for the 'client-cert-header' project. The page shows a list of four open issues, all created 17 days ago by MikeBishop. The issues are: 'Support for Raw Public Keys', 'Certificate chain data', 'IANA registration', and 'Renegotiation and Client-Cert'. Each issue has a yellow label 'client-cert-header' and a comment icon with the number '1'. The page header shows '4 Open' and '0 Closed' issues, along with filters for Author, Label, Projects, Milestones, Assignee, and Sort.