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
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: ...
Client-Cert: MIIBqDCCAU6gAwIBAgIBBzAKBggqhkJ0PQDAja6MRswGQYDVQKDBJMXQncyBBdBXBW50aNWhdGUxGzAZBgNVBAMEmxhJELudGVybWVkaWf0ZSBDQkueFw0yMDAxMTQyMjU1MzNaFw0yMTAxMjMyMjU1MzNaMA0x
CzA3BgNVBAMNakJDMFkwEwYHkoZizj0CAQYIKoZizj0DAQcDQgAE8YnXXfaUgnmMtocxU/IncWlRhebrXmckC8vdgj3ip5Be5f/3YCB0thxM4+kiMo6aAEF
CgZk5iNy6J84y7uoz9M6NyMhAcQyDVR0TBATwAdAFBgNVHSMGDAQgBRm3Wlija381beYCU1C8cGdC06J4bML6KeClyY7P0Sn9f185bBwYjN6K1MmRy
DjYkxBQQHuAwIwHQYDVR0RAQH/BMMwEYEPYmRjQGy4W1wBUuY29tMAoGCCqGSM49BAMCA0gAMEUCIBHda/r1vaL6G3VilL4/Di6YK0Q6bMjeSKC3dF
COO8TAiEX/kHSB4urmI0NX5r5XarmP0wmuVdBVoU4hBvZ1yhk=
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