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

Client-Cert HTTP Header
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 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

- Here by way of a conversation in the OAuth WG that begat a draft and moved to SECDISPATCH
A simple proposal that could potentially enable turn-key interoperable integration between independent components

draft-bdc-something-something-certificate-03

HTTP over a client certificate mutually-authenticated TLS connection

Verify certificate on presentation and sanitize headers on each request

pass the leaf client certificate as new header with a defined name and encoding

Client

GET /stuff HTTP/1.1
Host: example.com

Reverse Proxy

GET /stuff HTTP/1.1
Host: ...
Client-Cert: MIIBqcDCAA6gAwIBAgIBBzAKBggqhkJOPQDAjA6MRswGQ
YDVQKDDBMZXQncyBBdXRoZw50aWnddGUxGzA2B9NVBAAMExxbEIiudGVyb
WKawF0ZSBDQTAwFw8yMgA0MTQyMjU1MzNaFw0yMTAxMjMyMjU1MzNaMA0x
CzA3BgNVBAMHAKJDMFkwEwYHkoZizjZAQYIKoZizjZAQcDcEoAEYnXXfa
UgmmMtOwUICwFHRhebrXmcCK8vdg3J1p5Be5F/3YCBthxhM4+kiM6aEAF
CGzk3iNy6J84y7uzo9M6NHyAwCQYDVR0TBAIwADAFBgNVHSMEQDAwBRm3
WjLa381bEYCuicPc62aSEd2DAO8hNVHQDBAfEBA4MBsAwEwYDV0LBpAw
CyIkwYBQHUAxiwYHQDVR0RAQJ/BMMwEYEPYiMrjQGV4Yw1bGVUyY2tMAo
GCCqGSM49BAMCA0gAMEUCIBHda/r1vaL6G3V1lL4/1i6YK8Q6bMjeSKC3dF
COOB8TAiEAX/kHSB4urmiZONX5r5XarmP0wmydBV0U4hBVZ1ykh=
Considerations to Consider

- WG adoption
- Appropriate mechanism to prevent header injection
  - Sanitization vs. something more
  - Scope of applicability
- Sufficiency of just the whole end-entity certificate
- Appropriate error-handling across layers and other layering issues
Gratuitous closing slide featuring the city where we might meet together next* as backdrop for discussion.

- Adoption
- Injection
- EE cert
- Layering & errors

* Maybe Bangkok in the fall