HTTPBIS WG
~~IETF 107, Vancouver~~
Virtual Interim
May 2020

Client-Cert HTTP Header

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

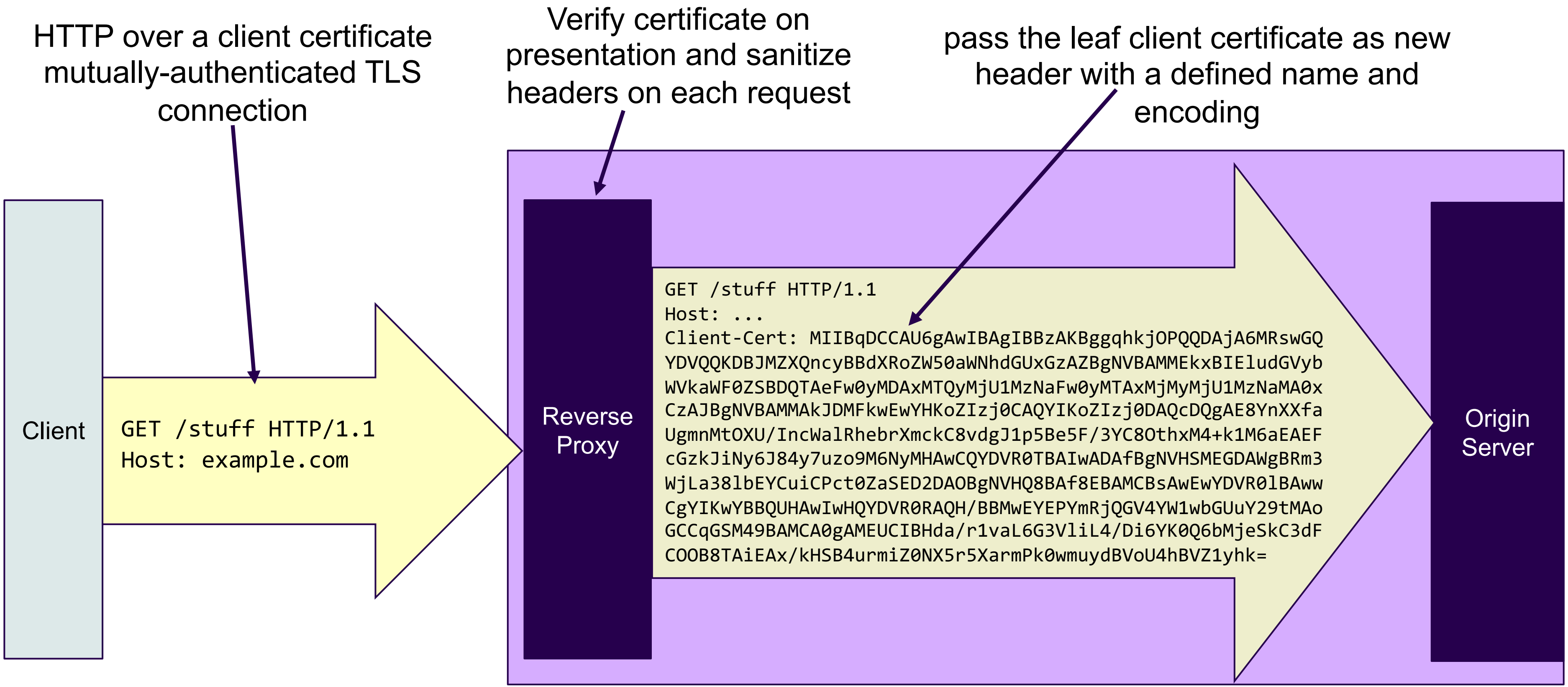
Brian Campbell
draft-bdc-something-something-certificate

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

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

```
GET /stuff HTTP/1.1
Host: ...
Client-Cert: MIIBqDCCAU6gAwIBAgIBBzAKBggqhkjOPQQDAjA6MRswGQ
YDVQQKDBJMZXQncyBBdXRoZW50aWNhdGUxGzAZBgNVBAMMEkxBIEludGVyb
WVkaWF0ZSBDQTAeFw0yMDAxMTQyMjU1MzNaFw0yMTAxMjMyMjU1MzNaMA0x
CzAJBgNVBAMMAkJDMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE8YnXXfa
UgmnMtOXU/IncWalRhebrXmckC8vdgJ1p5Be5F/3YC8OthxM4+k1M6aEAEF
cGzkJiNy6J84y7uzo9M6NyMHAwCQYDVR0TBAIwADAfBgNVHSMEGDAWgBRm3
WjLa38lbEYCuiCPct0ZaSED2DAOBgNVHQ8BAf8EBAMCBsAwEwYDVR0lBAww
CgYIKwYBBQUHAwIwHQYDVR0RAQH/BBMwEYEPYmRjQGV4YW1wbGUuY29tMAo
GCCqGSM49BAMCA0gAMEUCIBHda/r1vaL6G3VliL4/Di6YK0Q6bMjeSkC3dF
COOB8TAiEAx/kHSB4urmiZ0NX5r5XarmPk0wmuydBVoU4hBVZ1yhk=
```

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