Secondary Certificate Authentication of HTTP servers

draft-egorbaty-httpbis-secondary-server-certs

Eric Gorbaty, Mike Bishop
HTTPBIS
IETF 118, November 2023, Prague
Recap

• TLS Exported Authenticators (RFC 9261) allow the ability to send and receive X.509 certificates at the application layer

• Define support for HTTP/2 and HTTP/3 servers to send *unprompted* secondary certificates to clients, and make themselves authoritative for different origins

• New frame type on HTTP/2 stream 0 and HTTP/3 server->client control stream to carry the exported authenticators

• Based on an older draft that the WG has previously discussed
  • draft-ietf-httpbis-http2-secondary-certs-06
Draft Revisions since 117

• Clearly Indicate usage of the spontaneous server authentication flow in section 3 of RFC 9261
  • Certificate request context is chosen arbitrarily by the server. This draft does not (yet?) define a specific usage. Maybe it should.
• More clearly suggest usage of ORIGIN in absence of a DNS check
• Scrubbed remaining references to client certs
• HTTP/2 framing unchanged for now, current focus is clarifying the purpose and uses for the draft
What is different this time?

• Intentionally reduced scope
  • No client certs
  • Spontaneous server authentication flow only
• Demonstrated interest in multiple use-cases
  • More granular certificate management for servers instead of large “cruise-liner” certificates
  • “Hybrid proxy” - Make an HTTP forward proxy (MASQUE) be able to act as a reverse-proxy for particular origins
Closing remarks

• Multiple potential use-cases enabled by this scoped-down version of the mechanism
• Change to enable currently identified use cases > change to enable new use cases
• Does not block future expansions on this concept
• Seeking adoption (In HTTPBIS)
Questions?