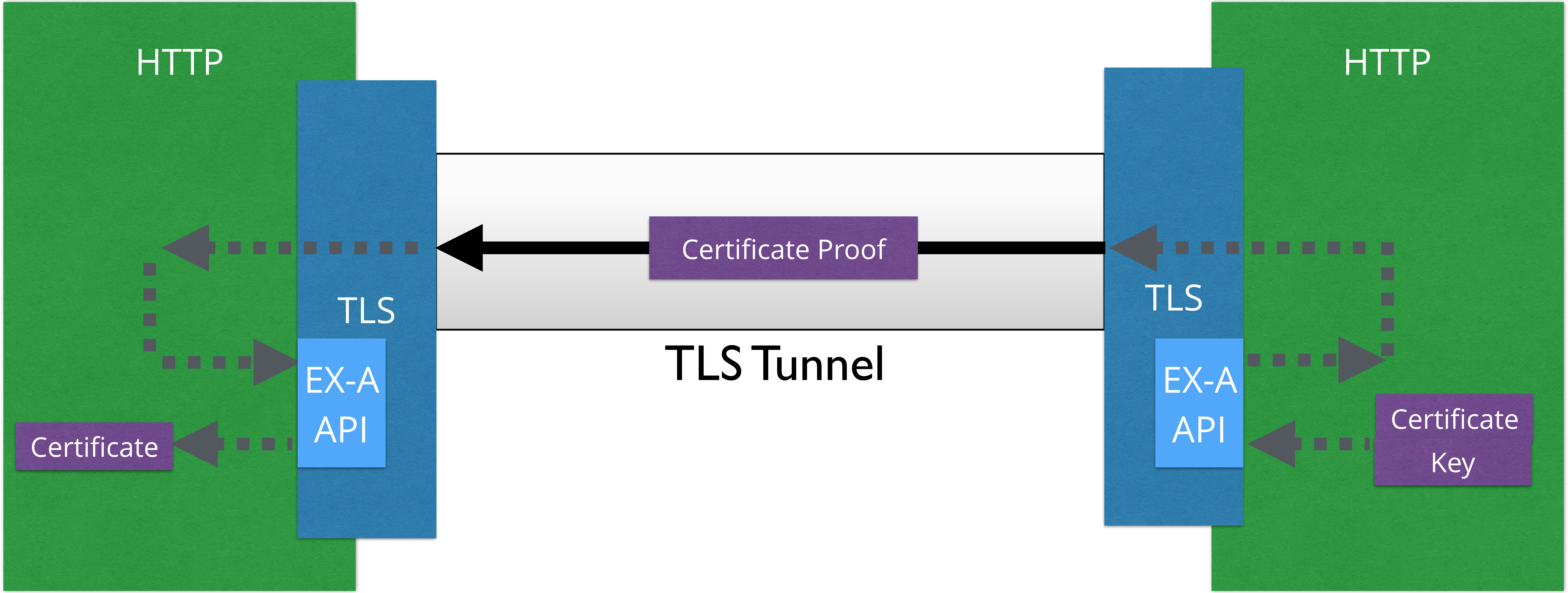
TLS Working Group
Monday, July 17, 2017

Exported Authenticators

Nick Sullivan, Cloudflare


HTTP
TLS
EX-A
API
Certificate
Certificate Proof
TLS Tunnel
HTTP
TLS
EX-A
API
Certificate
Key

Exported Authenticators

- Adopted as a working group document at IETF 98
- Working implementation in fork of Golang crypto/tls by Watson B. Ladd, nginx/BoringSSL implementation underway
- Deployed on ***https://leftshark.tls13.com*** as part of Secondary Certificate Authentication in HTTP/2 (*draft-bishop-httpbis-http2-additional-certs-04*)

Exported Authenticators

- Updates from -00 to -03, from implementation feedback and mailing list:
  - Signature and HMAC is now asymmetric
  - CertificateVerify format updated to match latest TLS 1.3 draft
  - Only support signatures supported by TLS 1.3
  - Text clarifications
- Issues managed on Github
  - https://github.com/tlswg/tls-exported-authenticator

Next Steps?

Move to last call?