Exported Authenticators

Nick Sullivan
Problem

• Application layer protocols may want authentication for multiple certificates on the same connection

• Intended first use case is HTTP/2 Additional Certificates

• Client authentication for HTTP/2 on a per-stream basis

• Additional server certificates (spontaneous or requested)
Solution: Exported Authenticators

• Allow TLS library to export a blob that proves possession of a certificate and bound to an existing connection

• Closely resembles a series of TLS 1.3 messages: Certificate, CertificateVerify, Finished
History

- Originally proposed at IETF 96
- Adopted at IETF 98
- Implemented and tested in Golang
- Exported Authenticators draft-04: only cosmetic changes
Formal Analysis

- Cas Cremers and Jonathan Hoyland (Oxford) have preliminary Tamarin model
- Promising results
Duplicated Logic

- Requires the application layer to select certificates
- No binding between requests and responses
- This logic exists already in TLS: CertificateRequest
Proposed Change

• Add an “Exported Request” API

• Exported Authenticator hash covers Exported Request if present
Exported Authenticators

Nick Sullivan