Exported Authenticators

TLS WG

IETF 102

https://tools.ietf.org/html/draft-ietf-tls-exported-authenticator-07

N. Sullivan

Background

Motivation

Enable a peer in an established TLS connection assert ownership of the private key of an additional certificate. Proof can be sent out of band.

Motivated by HTTP/2 Additional Certificates.

Adopted May 2017

Latest update Draft 07 July 2018

Formal analysis Formal proof of security with Tamarin published by J. Hoyland

Results of first last call

Additional Requirements from draft-ietf-httpbis-http2-secondary-certs

“Empty Authenticator”

> If, given an authenticator request, the endpoint does have an appropriate certificate or does not want to return one, it constructs an authenticated refusal called an empty authenticator. This is an HMAC over the hashed authenticator transcript with a Certificate message containing no CertificateEntries and the CertificateVerify message omitted

Next steps

New last call

Exporte Authenticators

TLS WG

IETF 102

https://tools.ietf.org/html/draft-ietf-tls-exported-authenticator-07

N. Sullivan