Exported Authenticators in TLS

draft-ietf-tls-exported-authenticators

Sean Turner

TLS@IETF112 — 20211108

Remaining AD Comment from Ben Kaduk

Are there any security issues caused by the fact that the Exported Authenticator is based on the Exporter Secret, which does not incorporate the entire transcript?

Jonathan Hoyland’s email response and proposal (text on next slide).

Proposed Text

In TLS 1.3 the client and server are not guaranteed to agree on the client’s final flight until the first application message. Because EAs can be negotiated out-of-band it is possible to negotiate EAs without agreeing on the entire transcript. Servers SHOULD send application data before sending a CertificateRequest to the client. If there is no application data to send the server MAY send a NewSessionTicket.

Consensus to merge this and move forward?