QUIC-TLS

...

20170330 - QUIC WG @ IETF 98

Editors: Martin Thomson
Sean Turner

Editors' GH Copy: draft-ietf-quic-tls-latest
WG's version: draft-ietf-quic-tls-01

Short(er) list of changes

The entire handshake is now unencrypted (#262, #337)

The QUIC header is included as AEAD Associated Data (#226, #243, #302)

Rules on use of TLS alerts, simpler QUIC-layer error handling

Require at least TLS 1.3 (#138)

Define transport parameters as a TLS extension (#122)