DTLS over SCTP

draft-tuexen-tsvwg-dtls-for-sctp-00.txt

Michael Tüxen (tuexen@fh-muenster.de)
Robin Seggelmann (seggelmann@fh-muenster.de)
Eric Rescorla (ekr@networkresonance.com)
Why not just use basic TLS over SCTP?

• TLS requires a reliable and in-sequence transport service provided by the transport layer.

• TLS needs a TLS connection per bi-directional stream and can not be used in combination with PR-SCTP. See RFC 3436.

• Hard to implement in OpenSSL.
Why not just use basic DTLS over SCTP?

• DTLS assumes an unreliable services provided by the transport layer.
• Provides an unreliable service to the DTLS user.
• It may drop user messages, so it can not be used in combination with SCTP trying to provide a reliable service.
• Even without DTLS dropping messages an attacker could force message drops...
SCTP aware DTLS

• It provides to the DTLS user all services provide by SCTP.
• It makes use of SCTP-AUTH.
• The shared secrets used for SCTP-AUTH are derived from the DTLS layer using key extraction described in draft-rescorla-tls-extractor-01.txt.
• Prototype implementation for OpenSSL (supporting the 1-to-1 style socket API) available.
Questions

• Comments?
• Acceptable as a WG item for TSVWG?