DTLS over SCTP

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

Michael Tüxen (tuexen@fh-muenster.de)
Robin Seggelmann (seggelmann@fh-muenster.de)
Eric Rescorla (ekr@networkresonance.com)
Features of 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-ietf-tls-extractor-03.txt.
• Implementable in OpenSSL.
Status

• DTLS connection setup and transfer of Application data is clear and also implemented.
• Renegotiation is the only technical work item remaining:
  – A couple of issues were not clear in RFC 4347.
  – DTLS implementation in OpenSSL had some bugs/features.
  – Making sure it works with the SocketAPI.
  – Is hopefully implemented this week...
To Do

• Clarify Renegotiation behavior in draft-ietf-tls-rfc4347-bis-01.txt.
• Make sure it is implementable in OpenSSL und the SCTP socket API defined in draft-ietf-tsvwg-sctpsocket-18.
• Write the ‘Security Considerations’ section.
• Ready for WG Last call by the next IETF.
Questions

• Any comments?