DTLS over SCTP

draft-ietf-tsvwg-dtls-over-sctp-bis-03

Magnus Westerlund
Claudio Porfiri
John Preuß Mattsson

2022-03-21

Status

- This work is done to address the user message limit of DTLS/SCTP per RFC 6083
  - 3GPP has a real need to solve this as several RAN protocol uses SCTP
- Received review feedback from Li Yan
- Ericsson has contracted an implementation of this specification
  - The first set of feedback has already been implemented in this specification
  - Work will continue
- IPR Declarations:
  - https://datatracker.ietf.org/ipr/5195/
  - https://datatracker.ietf.org/ipr/5218/

Updates in -03

- Clarify Message length limitations
  - No theoretical limits, but supporting over 2^64-1 bytes are optional
  - SCTP API may limit a sender further
- Stream Usage Update:
  - Allowing other than stream 0 for DTLS messages (Handshake, Alerts etc.)
  - Interleave DTLS messages with DTLS Records with protected messages
    - DTLS/SCTP can anyway not be separate they types when using DTLS 1.3
- Defined Shutdown procedure
- SCTP API Considerations
  - Requirements for full functionality on API
- Clarified Fragmentation description
- Clarified that PPID=0 is used for DTLS messages not carrying protected user message
- Clarified DTSL resumption usage
- Clarify RFC 6083 fallback
- Security Consideration expanded

Features Addressed

- Message Length: at least 2^64-1 instead of 16384 bytes
  - Sender API might limit
- SCTP association handshake negotiate support of DTLS/SCTP
- Minimized impact on ULP protocol
  - Not requiring Stream 0 to be in-order reliable
  - Does not require SCTP User message draining for DTLS/SCTP rekeying
- Addresses shutdown also from peer perspective

- RFC 6083 Dependency Weakness addressed
  - RFC 8996 forced DTLS upgrade to 1.2
    - Lacks DTLS 1.2 specific recommendations
  - Support long lived SCTP association:
    - DTLS 1.2 Renegotiation Security issues
      - Limited to 65534 renegotiations
    - DTLS 1.3
      - No renegotiation with mutual authentication
      - Key update lacks forward secrecy
      - Does not rekey SCTP-AUTH
  - Allows SHA-1 in SCTP-AUTH

Way Forward

The authors believe there are two realistic ways forward

A. Obsoleting RFC 6083 when publishing this draft as RFC
B. Publishing as an alternative RFC to RFC6083 without obsoleting

RFC 6083 has limited applicability and security issues

So, is the IPR declaration blocking obsoleting RFC 6083?

Issues: DTLS 1.2 vs 1.3 Close_Notify

- We have realized that DTLS 1.2 and 1.3 have different behavior with Close_Notify alert message
  - DTLS 1.2: Receiving a Close_Notify immediately close the connection from sending also
  - DTLS 1.3: Receiving a Close_Notify just tells you no more will be received, can still send
- This affects shutdown and closing the old DTLS connection during rekeying process for DTLS 1.2
  - Work around for rekeying: Intercept Close Notify based on content type in DTLS/SCTP layer until ready to close.
  - For Shutdown not ensuring that the alert message is close_notify could case premature shutdown of SCTP association.
- Thinking about how to address this one
- https://github.com/gloinul/draft-westerlund-tsvwg-dtls-over-sctp-bis/issues/103

Issue: Ensuring right SCTP-AUTH and DTLS Record key relationship

- Michael Tüxen proposed a SCTP Socket API extension to detect when all packets with a particular SCTP-AUTH key has been non-renegable acked
  - Useful to determine when old DTLS connection can be closed
- For this to work all DTLS records with old key MUST use be sent in SCTP Data chunks protected by old key.
- Means tweaking the rules for how keys are used in the transition phase between two DTLS Connections.
  - Needs to written up
- https://github.com/gloinul/draft-westerlund-tsvwg-dtls-over-sctp-bis/issues/100

Next Steps

- Address the remaining issues
- Await more feedback from implementation work
- Socket API extension for determining when SCTP-AUTH key is drained

Goal to have a draft without known issues before summer IETF meeting