DTLS over SCTP bis

draft-ietf-tsvwg-dtls-over-sctp-bis-02

Magnus Westerlund
John Preuß Mattsson
Claudio Porfiri

IPR Disclosure

- Ericsson has made two IPR disclosures
  - https://datatracker.ietf.org/ipr/5195/
  - https://datatracker.ietf.org/ipr/5218/

Goals

- Main goal
  - Support DTLS protecting larger than 16384 bytes SCTP messages
  - Done on 3GPP's request: https://datatracker.ietf.org/liaison/1723/
- Derived Requirements
  - Long lived SCTP associations with lifetimes of weeks and months
    - Periodic mutual re-authentication of endpoints
    - Periodic rerunning of Diffie-Hellman key-exchange to provide Perfect Forward Secrecy (PFS) to reduce the impact any key-reveal.
    - SCTP-AUTH rekeying required
  - Support for DTLS 1.2 and DTLS 1.3

Parallel DTLS connections

- Several Issues led here:
  - DTLS 1.3:
    - No mutual re-authentication
    - No PFS rekeying
  - DTLS 1.2
    - Renegotiation unsecure without mutual authentication, thus disabled often
  - Determining when keys DTLS and SCTP-AUTH could be retired
    - Without requiring draining at key updates

- Solution: Use DTLS connections in parallel:
  - When need to rekey or re-authenticate peer
  - Initiate full DTLS handshake
  - Use DTLS Connection IDs in DTLS records to multiplex on (1 byte)
  - When all DTLS records protected by old key has been sent and acked (non-renegable)
    - Each sender is responsible for this determination for their sent data.
    - Send DTLS CloseAlert to indicate to receiver that in this direction keys can be removed.

Benefits

- No dependency on DTLS rekeying or re-authentication features
  - No functionality change between DTLS 1.2 and DTLS 1.3
- No found limitations on number of rekeyings
- Mutual re-authentication
  - Including cert roll over possible
- Full Diffie-Hellman key-exchange
  - Perfect Forward Secrecy
  - Key-reveal limited to single key period
    - Attacker forced to Dynamic Key Extraction

Next Steps

- Need Feedback
  - Are there issues with proposed solution?
  - More eyes reviewing
    - Security
    - Description
- Target
  - WG last call after review and draft update