DTLS for SCTP

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

draft-westerlund-tsvwg-sctp-dtls-chunk-02
draft-westerlund-tsvwg-sctp-dtls-handshake-02

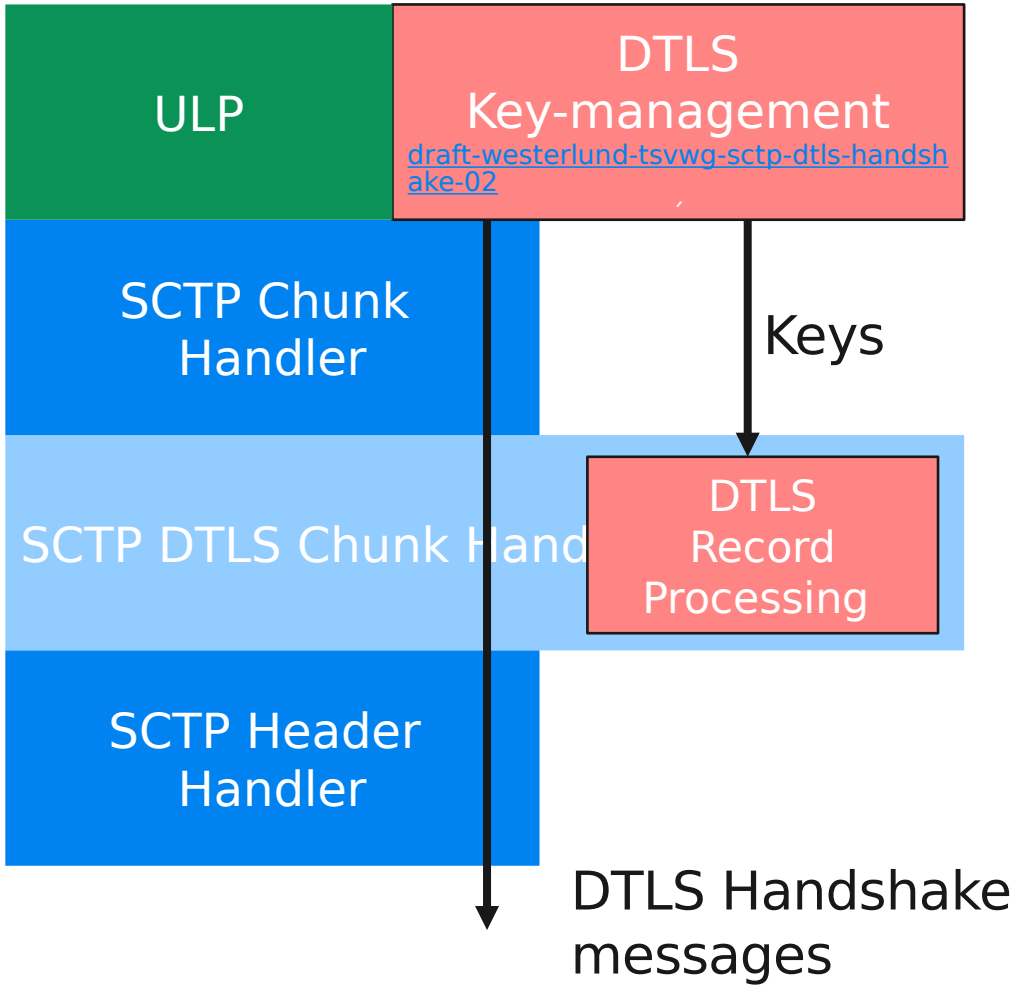
Magnus Westerlund
John Preuß Mattsson
Claudio Porfiri

IPR Declarations

- draft-ietf-tsvwg-dtls-over-sctp-bis
  - https://datatracker.ietf.org/ipr/5195/
  - https://datatracker.ietf.org/ipr/6218/
- draft-westerlund-tsvwg-sctp-dtls-chunk-02
  - https://datatracker.ietf.org/ipr/6219/
- draft-westerlund-tsvwg-sctp-dtls-handshake-02
  - https://datatracker.ietf.org/ipr/6220/

DTLS Chunk and Handshake Overview

- DTLS in SCTP
  - draft-westerlund-tsvwg-sctp-dtls-chunk-02
  - draft-westerlund-tsvwg-sctp-dtls-handshake-02
- DTLS Chunk is a new SCTP Chunk
  - Encapsulates all other chunks on a per SCTP packet basis in a DTLS record
- DTLS handshake is run over SCTP as messages
  - DTLS handshake messages sent as SCTP messages using a specific PPID
  - After DTLS keys are established all future SCTP packet's contents are protected
  - At rekeying perform handshake for a new DTLS connection
- User Message Fragmentation done by SCTP's normal message fragmentation mechanism



Update on DTLS Chunk

- https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-dtls-chunk/
- Draft Updated
  - Clarified the need to include Heart Beat messages over different paths in Replay Window Size
  - Resolved unclarity about PVALID solution indicator field, now an array that can be one or multiple 32-bit words if ever needed.
  - PVALID retransmission specified to be done on RTO interval if no response have been received until T-Valid timer timeout
  - Clarified how Error During Handshake message can be used by Handshake
  - Clarified that if SCTP chunks are bundled with DTLS chunk ignore all other chunks
  - PVALID Protection Solution Indicator IANA registry updated
  - Mandate DTLS Replay Protection being used

Update on DTLS Chunk Handshake

- https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-dtls-handshake/
- Document updates
  - State that `draft-mattsson-tls-super-jumbo-record-limit` could be used to allow extending IP MTU support from 16k to 64k
  - Clarified considerations for DPLMTUD on when DTLS handshake may impact the DTLS Record overhead due to cipher changes.
  - Editorial improvements

Implementation Work

- We are currently implementing DTLS Chunk and handshake
- Will verify that this solution works as intended integrated into mobile system
- Expect to be able to report on learnings by next IETF meeting

Open Issues

These are new issues found during the resolving the previous issues and review before submission

- DTLS Chunk:
  - Are there benefits to encrypt PPID 4242 when possible
  - Does the API need a: Set Q limit call?
  - Clarify privacy properties impact

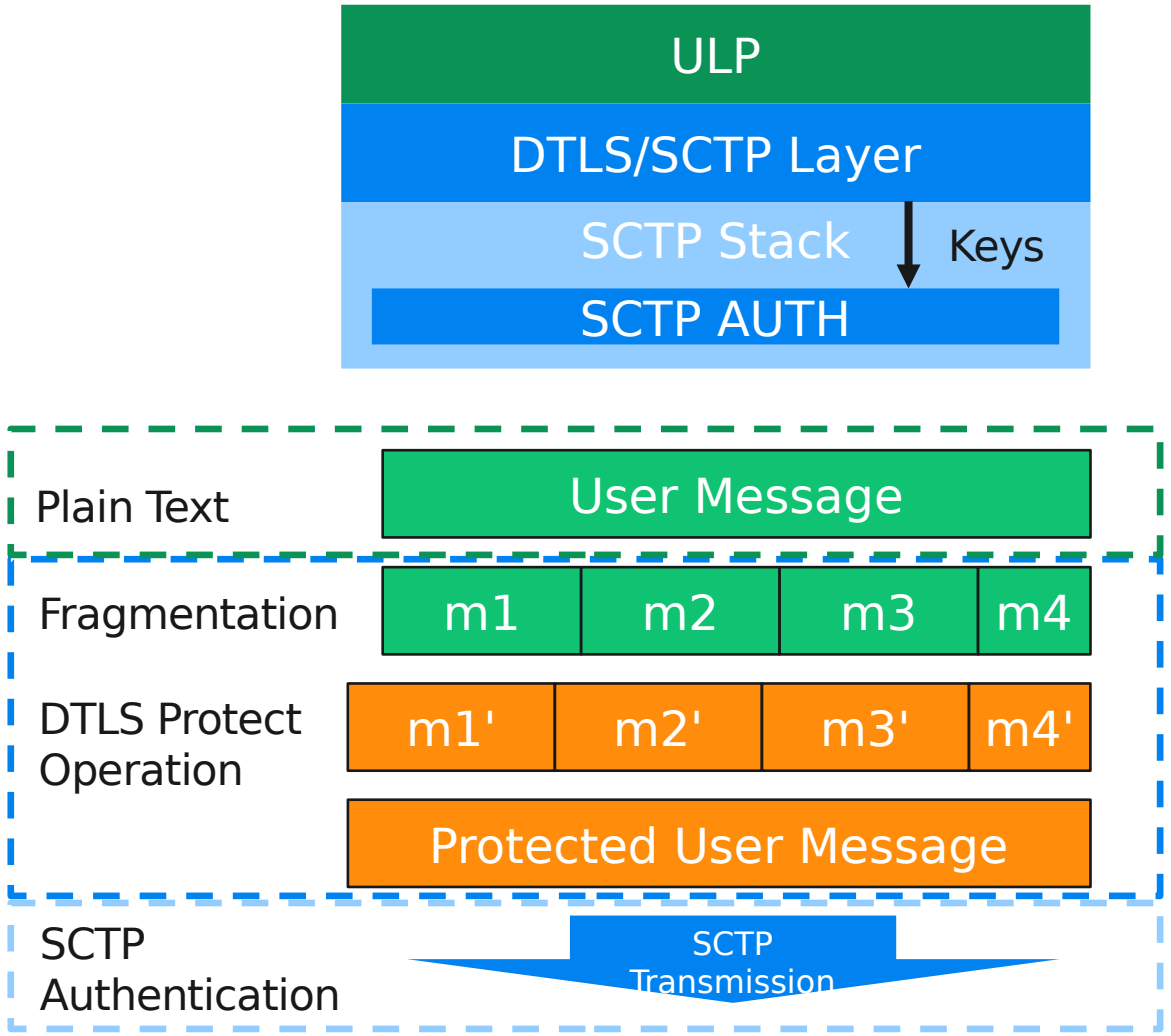
- DTLS Handshake
  - Editorial improvement of handshake usage description.
  - Clarify why restart DCI can go immediately to Protected
  - Clarify in which states one can perform DTLS close.

Should we encrypt the DTLS handshake messages?

- Currently all PPID=4242 messages, i.e. all DTLS message's Data Chunks are bypassing DTLS chunk protection and send as unencrypted Data Chunks in their own SCTP Packets
- When one have keys for the DTLS Chunk possible to also encrypt these DATA chunks
- Should we recommend that they are encrypted?
- Pro:
  - Hides the DTLS handshake from direct targeting
  - Allows them bundled with other chunks
- Con:
  - In case of DTLS record processing failure or key-expiry new DTLS handshakes the sender will not learn that they failed to be delivered until loss report or timeout
    - Could at that point fallback but makes the key-exchange less robust and potentially slower

DTLS over SCTP

- DTLS over SCTP (SCTP/DTLS)
  - draft-ietf-tsvwg-dtls-over-sctp-bis-08
  - draft-ietf-tsvwg-rfc4895-bis-03
  - An Adaptation layer between Upper Layer Protocol (ULP)
  - Fragments user messages into multiple fragments
  - Each fragment protected by a DTLS record
- Relies on SCTP-AUTH to ensure record order
  - DTLS keys the SCTP-AUTH
- Uses parallel DTLS connection for rekeying
  - Use DTLS Connection IDs for identification



DTLS over SCTP

- https://datatracker.ietf.org/doc/draft-ietf-tsvwg-dtls-over-sctp-bis/
  - Was updated to keep it alive without any changes
- Open Issues (10)
  - https://github.com/gloinul/draft-westerlund-tsvwg-dtls-over-sctp-bis/issues
  - No works since last meeting awaiting WG direction decision