DTLS 1.3 for SCTP

draft-tuexen-tsvwg-rfc6083-bis-04

Michael Tüxen (tuexen@fh-muenster.de)

Hannes Tschofenig (hannes.tschofenig@gmx.net)

Limitations of RFC 6083

- Relies on DTLS 1.0 and this version is deprecated. Newer versions don’t provide the unlimited number of re-negotiations anymore.
- Limits the user message size to about 16KB.
- Uses draining of user messages before performing a re-negotiation.
- Refers to RFC 4895.

Overcoming the Limitations (1)

- Replacing re-negotiations
  - Since key updates as specified for (D)TLS don’t provide forward secrecy, define extended key updates in draft-tschofenig-tls-extended-key-update-01 to overcome this limitation.
  - The number of key updates is limited to about 2^64, which is acceptable.
  - Use of RFC 9150 for periodic authentication.

Overcoming the Limitations (2)

- Bumping the user message size limit
  - to about 64KB by using a larger record size limit as described in draft-mattsson-tls-super-jumbo-record-limit-02.
  - to unlimited for ordered reliable user messages as described in draft-tuexen-tsvwg-sctp-ppid-frag-00.
- Avoid draining in most cases by using an improved accounting for SCTP AUTH.
- Using RFC 4895bis.