# RFC 6083bis: DTLS 1.3 over SCTP

draft-tuexen-tsvwg-rfc6083-bis-02

Michael Tüxen (tuexen@fh-muenster.de)

Hannes Tschofenig (hannes.tschofenig@gmx.net )

# Dependencies of RFC 6083

- SCTP AUTH (draft-tuexen-tsvwg-rfc4895-bis-06)
  - Changes needed
    - Use of direction specific keys
    - Add more algorithms
    - Deprecate usage of SHA-1 for HMAC
    - Improve API for better observability
  - All changes are not specific to RFC6083bis and have to be done anyway.

# Regressions from RFC 6083

- Handling of key updates unspecified in RFC 6083.
  - Key updates did not exist in DTLS 1.0 and therefore their handling is not described in RFC 6083.
  - Updating SCTP AUTH keys is suggested.
- Arbitrary long communications
  - Limited to $2^{16}$-1 epochs in DTLS 1.2 and $2^{64}$-1 in DTLS 1.3. DTLS 1.3 is good enough.
- Forward secrecy for each epoch of the DTLS connection
  - Improved key update procedure. Not specific to RFC 6083bis, addresses a generic issue for long living DTLS connections.

# Relaxing Limitations of RFC 6083

- Draining during epoch update (re-negotiaton)
  - Can be mitigated by keeping the SCTP AUTH keys from the last epoch active for receiving.
- User message size of 16KB
  - Can be bumped to about 64KB using the Record Size Limit Extension (RFC 8449) in combination with a Flags Extension (draft-ietf-tls-tlsflags-12).
  - Keeps the mapping of a user message to a DTLS record.

# Summary

- We think it would a good to have a way of securing SCTP traffic which is implementable in open source.
- Dependencies
  - Required
    - Generic improvements on SCTP AUTH (generic)
    - Key update procedure for (D)TLS (generic)
  - Optional
    - Bumping the message size limit (RFC6083bis specific)