Requirements for Securing SCTP Traffic using DTLS
draft-tuexen-tsvwg-sctp-dtls-req-00

Michael Tüxen (tuexen@fh-muenster.de), Editor
Design Team Participants

• Marcelo Ricardo Leitner
• Xin Long
• John Mattsson
• Claudio Porfiri
• Tirumaleswar Reddy.K
• Zahed Sarker
• Hannes Tschofenig
• Michael Tüxen
• Magnus Westerlund
Context

• RFC 6083bis required.
• Currently using IPSec.
• With the upcoming deployment of signaling nodes in the cloud, this is not sufficient anymore.
• 3GPP requirements.
Generic Requirements

• Protocol mechanisms should not limit availability of communication or result in message loss.

• User message sizes of at least 1 GB (0.5 MB currently in use) supported, if unlimited is not feasible.
Functional Requirements for SCTP

• Features from the base specification
  • Ordered reliable transmission of user messages
  • Multihoming, but no dynamic address reconfiguration
  • Restart procedure

• Parametrization
  • At least two SCTP streams available to the application
Implementation Considerations for SCTP

- User message sizes must not be limited by a protocol implementation
- For some participants it is preferred to be able to use open-source kernel SCTP implementations
Security Requirements

• An on-path attacker being able to replay messages, insert messages, or modify messages is considered.

• Fundamental
  • Mutual authentication
  • Privacy and integrity is required for user data

• Best practices for long lived sessions
  • Periodic re-authentication, for example allowing a certificate update
  • It must the possible to run DH once per hour or every 100GB

• Availability
  • Replay or injection must not affect the availability of the association.
  • In particular, the SCTP restart procedure must not allow to take over an SCTP association by an attacker.
Implementation Considerations for DTLS

• Focus on DTLS 1.3
• For some participants it is preferred to use unmodified DTLS implementations