Title: DTLS for SCTP next steps and request for input
Response to: Reply LS on SCTP-AUTH and DTLS (S3-233355)

Source:	**IETF Transport Area Working Group (TSVWG)**
To:	**3GPP SA WG3, and 3GPP RAN WG3**
To Contacts:	Peter Schmitt <Peter.Schmitt@huawei.com>
	3GPPLiaison@etsi.org
CC:	Charles Eckel eckelcu@cisco.com
	TSVWG <tsvwg@ietf.org>
Submitted Date:	2023-08-04

Send any reply LS to: statements@ietf.org

Purpose: For action

Deadline: 2023-09-11 Action Needed

1. Description

IETF's Transport Working Group (TSVWG) thanks 3GPP SA3 for "Reply LS on SCTP-AUTH and DTLS" [1]. This LS is a follow up to inform 3GPP SA3 and RAN3 that TSVWG continues its work on a DTLS based security solution for SCTP that should be suitable to the needs of 3GPP for the N2, Xn, F1, and E1 interfaces. TSVWG would like to inform 3GPP how input from 3GPP and its participants can help ensure that the time plan is met.

In the development work of a replacement as reported in the previous liaison statement (Titled: Updated LS to 3GPP regarding SCTP-AUTH and DTLS) [2] the work had run into some security issues. In the continued work to address these security issues there are now two different proposals that TSVWG is attempting to choose between. The first is to continue with the previous solution with DTLS on top of SCTP [3] and relying on an updated version of SCTP-AUTH [4] to ensure the DTLS records are in order per message and no records can be injected into protected message. The second solution is to create an encryption chunk [5] that encapsulates all the payload of SCTP packets, where each SCTP packet's content can be protected by DTLS [6] ensuring confidentiality, source authenticity, and integrity.

These two solutions appear to both to fulfill the security and functional requirements to address 3GPP's needs as understood by TSVWG. The interpretation of the requirements is the following:

- Support message size of larger than 500 kb, which appear to be the approximate theoretical maximum size of Xn (3GPP TS 48.423) messages. Although we note that the original liaison statement from RAN3 [7] refers to SCTP's unlimited message size.

- Enable long lived SCTP association with lifetimes of many weeks.
- Periodic mutual re-authentication of the peers.
- Periodic rekeying with forward secrecy and enable Diffie-Hellman Exchanges forcing an attacker to perform dynamic key-exfiltration after each rekeying.
- Security solution should not be vulnerable to SCTP association availability attacks based on injecting or prevention of delivery of a small number of packets by an on- or off-path attacker.
- Rekeying or re-authentication may not interrupt the SCTP using applications message delivery for any extended time, such as multiple RTTs to drain all transport messages to perform the rekeying.

We also have noted the wording in the reply liaison statement [1], "Since the problem is related to the use of DTLS with SCTP, SA3's understanding is that the solution should be based on DTLS, and the solution should not rely on unsupported DTLS features".

The two proposed solutions have different properties when it comes to robustness (i), requirements on the DTLS implementation (ii), implementation effort in the SCTP stack (iii). There has been IPR disclosures on both proposed solutions [3] and [6], details available in links from referenced web pages. These differences are summarized in this presentation (Slides [8], Recording [9]) to the TSVWG meeting at IETF's 117th Meeting. As many of the differences are related to implementation and requirements on the SCTP and DTLS implementation it would really help if either of the 3GPP WG's or at least its participants would provide input to the TSVWG work on which of the solutions that it would be preferable to pursue by TSVWG. It is requested that SA3 and RAN3 would confirm if implementation possibilities in both userland and kernel implementations of SCTP are required for the solution? And if any additional concerns with implementation of either of the solutions are perceived.

TSVWG's meeting at IETF 117 was unable to make a choice at this time on which solution to pursue due to lack of sufficient breath of input and time for participants to prepare and discuss the differences. To address this and make progress as quickly as possible an online interim meeting of TSVWG has been scheduled on the 19th of September 2023 at 16:00-18:00 CEST where this can be discussed in more depth. TSVWG would like to invite interested parties to participate in this interim meeting which is open to anyone. No registration will be required, however an IETF Datatracker account (https://datatracker.ietf.org/accounts/create/) will be needed to join the session. The session details and a join link will be available from this page: https://datatracker.ietf.org/meeting/interim-2023-tsvwg-01/session/tsvwg

In the discussion at IETF 117 TSVWG meeting, it was requested that 3GPP clarified which SCTP message sizes that a solution is required to support. In other words, are the theoretical maximum message size mentioned above relevant to be supported, or would it be sufficient that a smaller message size is supported? In general, it would be good to have SA3 and RAN3 confirm that the interpretation of the requirements is correct.

TSVWG plans to make a consensus decision on its mailing list after the interim meeting. If a rough consensus is achieved on which solution to pursue, TSVWG should be able to finish its work within a year. Meaning that approved for publication by IESG specifications could be available by the end of 2024, with published RFC within one to two months. However, for this time plan to hold it is necessary that sufficient level of review is achieved. Thus, interested parties needs to be involved in the remaining process in TSVWG.

In case the requirements are not correct, or if either SA3 or RAN3 conclude that the proposed solutions' properties are not usable for 3GPP purposes, TSVWG needs to learn what are those issues. With that input the WG could reconsider the desired properties and requirements, its participant propose alternative solutions, and discuss the proposals on the table. It will also likely delay the work significantly.

2. Actions

For both SA3 and RAN3:

- TSVWG would like to invite interested to participate in the TSVWG Interim meeting on the 19th of September 2023 at 16:00-18:00 CEST.

- TSVWG would like to request that any input on the choice of solution is provided in an LS by 2023-09-11.

- TSVWG would like to request answers to questions given above and confirmation if the interpretation TSVWG has made on requirements are correct to 3GPP.

3. Upcoming Meetings

2023-09-17: Online interim meeting of TSVWG 16:00-18:00 CEST. Details for this meeting: https://datatracker.ietf.org/meeting/interim-2023-tsvwg-01/session/tsvwg

2023-11-03 to 2023-11-10: IETF's 118th Meeting in Prague.

4. References

[1] 3GPP Liaison, "**Reply LS on SCTP-AUTH and DTLS",** 3GPP doc nr: **S3-233355,** https://datatracker.ietf.org/liaison/1847/
[2] https://datatracker.ietf.org/liaison/1806/
[3] https://datatracker.ietf.org/doc/draft-ietf-tsvwg-dtls-over-sctp-bis/
[4] https://datatracker.ietf.org/doc/draft-tuexen-tsvwg-rfc4895-bis/
[5] https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-crypto-chunk/
[6] https://datatracker.ietf.org/doc/draft-westerlund-tsvwg-sctp-crypto-dtls/
[7] https://datatracker.ietf.org/liaison/1723/
[8] https://datatracker.ietf.org/meeting/117/materials/slides-117-tsvwg-71-dtls-in-sctp-00
[9] https://youtu.be/HcjKkhYn08Q?t=2484