**3GPP TSG-SA3 Meeting #112** ***S3-23xxxx***

**Goteborg, Sweden, 14 - 18 August 2023**

**Title:** **Reply LS on DTLS for SCTP**

**Response to:** **(S3-234132) DTLS for SCTP next steps and request for input from IETF TSVWG**

**Release:** **-**

**Work Item:** **-**

**Source:** **3GPP SA WG3**

**To:** **IETF Transport Area Working Group (TSVWG)**

**Cc:** **3GPP RAN WG3**

**Contact person:** **Mohsin Khan**

**Mohsin dot khan at ericsson dot com**

**Send any reply LS to:** **3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** **None**

# 1 Overall description

SA3 would like to thank IETF Transport Area Working Group (TSVWG) for notifying SA3 of the current situation at IETF TSVWG about resolving the vulnerabilities related to SCTP-AUTH and DTLS over SCTP.

The LS, sent by IETF TSVWG to SA3, has listed the architectural and security requirements that IETF TSVWG has taken into consideration towards developing a solution. The LS says IETF TSVWG is trying to choose a solution from two candidate solutions: (i) DTLS on SCTP and relying on an updated version of SCTP-AUTH (ii) using DTLS to protect the payload of SCTP packets in an encryption chunk.

SA3 has extracted the questions that IETF TSVWG has asked SA3. In the following, SA3 articulates the questions and provides answers.

**Question 1:** Is the IETF TSVWG’s interpretation of the architectural and security requirements correct?

**Answer 1:** All the security requirements are preferred by SA3. This is because all the security requirements are generic best-practice properties of a security protocol.

Regarding the architecture requirement of supported message size, RAN3 is the right authority to respond. According to the RAN3 LS [1], supporting longer message lengths seems to be an important requirement. However, from the SA3 perspective, maintaining SCTP capability for large or unlimited message sizes is important to avoid future limitations if the application protocols using SCTP need to be extended.

**Question 2:** Does SA3 have any additional concerns with the implementation of either of the candidate solutions?

**Answer 2:** Solution (i) requires changes in the existing SCTP, SCTP-AUTH standards, implementation, and DTLS library. Therefore, Solution (i)’s implementation effort appears to be higher than Solution (ii).

**Question 3:** Which of the two candidate solutions is preferable to SA3?

**Answer 3:** SA3 prefers Solution (ii) due to the answer to the previous question.

**References**

1. R3-211274, "[Remove the user message size limitation for DTLS over SCTP](https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2021-03-05-o3gpptsgran3-tsvwg-remove-the-user-message-size-limitation-for-dtls-over-sctp-attachment-1.docx)"

# 2 Actions

**To** IETF Transport Area Working Group (TSVWG)

**ACTION:**  SA3 kindly asks IETF Transport Area Working Group (TSVWG) to take the above information into account and expedite the decision process so that a solution is ready by the envisioned time.

# 3 Dates of next TSG SA WG 3 meetings

SA3#113 6 -10 November 2023 Chicago, US

SA3#114 22 -26 January 2024 EU (TBD)