**3GPP TSG-SA3 Meeting #107Ad-hoc-e *S3-221535-r3***

e-meeting, 27 June – July 1st 2022

**Title: DRAFT Reply LS on V2X PC5 link for unicast communication with null security algorithm**

**Response to: LS (S3-221317/ R5-222035) on V2X PC5 link for unicast communication with null security algorithm from TSG RAN WG5**

**Release: Rel-17**

**Work Item: eV2XARC**

**Source: Lenovo [to be 3GPP SA WG3]**

**To: 3GPP RAN WG5**

**Cc: 3GPP CT WG1, 3GPP RAN WG2**

**Contact person: Andreas Kunz**

**akunz at Lenovo.com**

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

**Attachments:** 2

# 1 Overall description

SA3 would like to thank RAN5 for their LS on V2X PC5 link for unicast communication with null security algorithms.

SA3 has reviewed the content of the LS and relevant specification and would like to provide clarification on the usage of the NULL security algorithms.

The wording of “no security” is misleading in the current specification of TS 33.536, i.e. the NULL security algorithms for encryption and integrity are still security algorithms, but without any protection of the content of the messages. Put another way, the selection of NULL algorithms means that the PC5 messages are considered protected for the purposes of being allowed to be sent or received (even if in effect there is no protection of the messages).

Furthermore SA3 would like to confirm that the key establishment procedures in clause 5.3.3.1.3 of TS 33.536 can be skipped if the receiving UE chooses NULL PC5 integrity protection algorithm for the PC5 signalling integrity protection.

# 2 Actions

**To 3GPP RAN WG5 group.**

**ACTION:** SA3 kindly asks RAN5 to take the above information into account in their discussion about formal conformance testing of the null security algorithms for V2X.

# 3 Dates of next TSG SA WG 3 meetings

<https://www.3gpp.org/DynaReport/Meetings-S3.htm>