**3GPP TSG-CT WG1 Meeting #136-eC1-22abcd**

**E-Meeting, 12th – 20th May 2022**

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

Response to: LS (C1-223325/ R5-222035) on V2X PC5 link for unicast communication with null security algorithm from 3GPP RAN WG5

Release: Rel-17

Work Item: -

Source: 3GPP CT WG1

To: 3GPP RAN WG5

Cc: 3GPP SA WG3, 3GPP RAN WG2

**Contact Person:**

Name: Christian Herrero-Veron

E-mail Address: Christian.Herrero at huawei.com

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

Attachments: C1-22edfg

**1. Overall Description:**

CT1 would like to thank RAN5 for their LS on V2X PC5 link for unicast communication with null security algorithms.

CT1 has reviewed the content of the LS and relevant specifications and would like to indicate that according to CT1 specification the use of null security protection algorithm (i.e., in 5GS NEA0 and NIA0) are in fact security protection algorithms used for integrity protecting and ciphering of the PC5 messages. However, when applied they cannot provide any integrity protection or ciphering for the PC5 messages. Therefore if the null security protection algorithms, i.e. integrity protection and ciphering using null security protection, are activated as a result of successful security control mode procedure, the PC5 messages are transmitted unprotected.

CT1 has updated their specification TS 24.587 to clarify the use of null and non-null security protection algorithms in order to avoid any misunderstanding (see attached file).

**2. Actions:**

**To 3GPP RAN WG5 group.**

**ACTION:** CT1 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. Date of Next CT1 Meetings:**

CT1#137e 22th - 26th August 2022 Goteborg, Sweden, EU

CT1#138e 10th - 14th October 2022 e-meeting