**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 our specifications the use of null security algorithms (i.e., in 5GS NEA0 and NIA0) are in fact security algorithms used for integrity and/or ciphering of messages. However, when applied they cannot provide any encryption protection or integrity protection for the control plane signalling messages. So when the null security algorithm(s) are selected and in use the control plane signalling messages will be sent unprotected. In short, in that case security is activated (security context is established and integrity and/or ciphering using Null security algorithm is used) as a result of successful security control mode procedure but the messages are sent unprotected.

CT1 has updated their specification TS 24.587 to clarify the use of null and non-null security 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