3GPP TSG-RAN WG2 Meeting #109bis-e R2-2004083

Electronic, 20 April – 30 April 2020

**Title:** [Draft] LS response to SA3 on the security related issues for NR SL

**Response to:**

**Release:** Rel-16

**Work Item:** 5G\_V2X\_NRSL-Core

**Source:** CATT [to be RAN2]

**To:** SA3

**Cc:**

**Contact Person:**

#### **Name:** Da Wang

#### **E-mail Address:** wangda@catt.cn

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

**Attachments:**

# **1. Overall Description**

RAN2 would like to thank SA3 for the reply LS on NR V2X Security issue and PDCP SN size ([S3-200478](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_98e/Docs/S3-200478.zip)) to inform RAN2 of the security related fields/information for AS ciphering and integrity protection.

1. Regarding 5-bit input for the security algorithms derived from a specific LCID, RAN2 has made following working assumption.

1: Working assumption: the 5 least significant bits of LCID can be used as 5-bit input to the ciphering/integrity algorithms. Working assumption will be RAN2 agreement if there is no SA3 concern until next RAN2 meeting.

Please note that the 5 least significant bits of LCID can uniquely identify SLRB, as specified in TS 38.321:

* **Table 6.2.4-1 Values of LCID for SL-SCH**

|  |  |
| --- | --- |
| **Index** | **LCID values** |
| 0 | SCCH carrying PC5-S messages that are not protected |
| 1 | SCCH carrying PC5-S messages "Direct Security Mode Command" and "Direct Security Mode Complete" |
| 2 | SCCH carrying other PC5-S messages that are protected |
| 3 | SCCH carrying PC5-RRC messages |
| 4-19 | Identity of the logical channel |
| 20-61 | Reserved |
| 62 | Sidelink CSI Reporting |
| 63 | Padding |

1. RAN2 agreed PDCP re-establishment is triggered for re-keying procedure. In order to better understand the impact on AS layer, RAN2 respectfully asks SA3 following question:

**Question 1:** What is the granularity of the re-keying procedure, e.g., per PC5 unicast link or per SLRB?

**Question 2:** Does the re-keying procedure require reset of the PDCP 32-bit COUNT in SL unicast?

1. Regarding Counter Check procedure, RAN2 would like to ask SA3 following question:

**Question 3:** Is Counter Check procedure needed in PC5 interface for SL unicast DRB?

1. To follow SA3, RAN2 agreed that Key ID is necessary to be carried in the PDCP PDU header.

**2. Actions:**

RAN2 respectfully asks SA3 to take the above information into account for subsequent specification work and provide their feedback for question 1 and question 2:

**3. Date of Next RAN2 Meetings:**

TSG-RAN WG2 Meeting #110 1 – 12 June 2020 Electronic

TSG-RAN WG2 Meeting #111 24 – 28 August 2020 Toulouse, France