3GPP TSG-RAN WG2 Meeting #109bis-e R2-2004078

Electronic, 20 April – 30 April 2020

Source: CATT (rapporteur)

Title: Summary of offline discussion for PDCP remaining issues (CATT)

Agenda Item: 6.4.3.2

Document for: Discussion and Decision

# Introduction

This document is to kick off the offline discussion #705 to discuss the PDCP remaining issues which include the issues and proposals in the V2X PDCP summary document [1]. The scope of this offline discussion in the chairman notes is as following.

* [AT109bis-e][705][V2X] PDCP issues (CATT)

Scope: To discuss summary of PDCP remaining issues

Expected outputs: Proposals and summary in R2-2004078

Deadline: 4/24 10:00 for companies’ feedback and 4/27 10:00 for rapporteur version (UTC)

# Discussion

## Issue 1: LCID usage for integrity and ciphering algorithms

In SA3 reply LS [2], SA3 confirmed that there shall be a 5-bit input for the security algorithms and the triple (Key, Bearer, Counter) are only used once in order to avoid key stream reuse. SA3 ask RAN2 to decide how 5-bit input is derived from a particular LCID.

In 38.321, the values of LCID for SL SRBs and DRBs are from 0 to 19. Thus, using the 5 least significant bits of LCID can differentiate the SL SRBs and DRBs which can satisfy the SA3 properties. Therefore, most companies propose to use the 5 least significant bits of LCID as input to the ciphering/integrity algorithms and reply LS to inform SA3 ([3]- [9]).

**Question 1: Does company agree, from RAN2 perspective, the 5 least significant bits of LCID can be used as 5-bit input to the ciphering/integrity algorithms?**

* **Yes. If Yes is selected, please further clarify whether is it necessary to reply LS to SA3 to inform RAN2 preference;**
* **No. If No is selected, please further clarify the preferred solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes |  |
| OPPO | Yes |  |
| HW, HiSi | Yes | It is necessary to reply LS to SA3, to make sure the 5 least significant bits of LCID is used. |
| MediaTek | Yes | Send LS to SA3 about RAN2 agreements. |
| ZTE | Yes | Since the parameters required by PDCP are provided by upper layer and how the BEARER is set (the mapping of LCID to BEARER) is captured in TS 33.536, RAN2 shall reply LS to SA3 to inform them of the agreements RAN2 made. |
| Ericsson | No | We understand from SA3 that such 5-bit out of 6-bit LCID solution might lead to collision, e.g. two different LCIDs might have the same 5 least significant bits. SA3 is discussing now other alternatives such as letting the initiating UE generate a unique 5-bit input and send to the peer UE.  We shall wait for SA3’s conclusion and come back to this. |
| Nokia | No | We have the same concern as Ericsson, but are fine with setting it as a working assumption, inform SA3 about the potential issues and then make the final conclusion based on their reply. |
| Futurewei | Yes | Though LCID is of 6 bits, only the 5 LSB are used to identify logical channels, as the valid values of LCID for logical channel over SL-SCH are 4 – 19. |
| Spreadtrum | Yes | Agree with Futurewei |
| Apple | Yes |  |
| LG | Yes |  |
| Qualcomm | Yes |  |
| Intel | Yes | As SA3 is requesting a response in this regard, we should provide RAN2 view. |
| CATT | Yes | In SA3 reply LS [2], SA3 ask RAN2 to decide how 5-bit input is derived from a particular LCID. Thus we think it depends on us to decide and send our preference back to SA3. |
| vivo | Yes | The 5 least significant bits of LCID is sufficient and unique, which can meet the security requirement. Send LS to SA3 about RAN2 agreements. |
| Lenovo | Yes | As described in discussion part, only LCID 0-19 are relevant to the input of security algorithm. Thus least 5 bits of LCID is enough. |

Rapporteur's observation:

A clear majority view is using the 5 least significant bits of LCID as 5-bit input to the ciphering/integrity algorithms. We will conclude this issue together with Q2.

According to the answer on Q1, no matter what solution we prefer, rapporteur suggests we need reply SA3 LS to inform our preferred solution.

**Question 2: Does company agree whether it is necessary to reply SA3 LS to inform RAN2 preferred solution based on companies answer to Q1?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes | We are fine with reply LS to SA3 to inform the decision. |
| OPPO | Yes |  |
| HW, HiSi | Yes |  |
| MediaTek | Yes |  |
| ZTE | Yes | Since the parameters required by PDCP are provided by upper layer and how the BEARER is set (the mapping of LCID to BEARER) is captured in TS 33.536, RAN2 shall reply LS to SA3 to inform them of the agreements RAN2 made. |
| Ericsson | No | As commented in Q1, we shall just wait for SA3’s conclusion and come back to this next meeting. |
| Futurewei | Yes | SA3 should be informed of the possible LCID values for logical channel, in order to help them avoid any confusion. |
| Spreadtrum | Yes |  |
| Apple | Yes |  |
| LG | Yes |  |
| Qualcomm | Yes |  |
| Intel | Yes |  |
| CATT | Yes |  |
| vivo | Yes | Other solution is not needed. |
| Lenovo | Yes | SA3 should know the final decision from RAN2 |

**Voting result together with Q1 and Q2:**

**Yes: 14**

**No: 2 (include one company also fine with a working assumption)**

Rapporteur's observation:

A clear majority of companies agree to use the 5 least significant bits of LCID as 5-bit input to the ciphering/integrity algorithms. Thus, Rapporteur suggests following majority views and send LS to SA3 to further check.

**Proposal 1: From RAN2 perspective, the 5 least significant bits of LCID can be used as 5-bit input to the ciphering/integrity algorithms.**

**Proposal 2: Reply LS to SA3 to inform RAN2 preference on LCID usage for integrity and ciphering algorithms.**

## Issue 2: Whether D/C filed and SDU type are necessary for SL SRB?

According to the OPPO’s draft CR [6], the SDU type is unnecessary for SL SRB for unicast and broadcast. Thus, some clarifications need to be captured in the Data PDU format for SLRBs for broadcast, i.e., the unprotected PC5-S message (e.g. Direct Communication Request). Moreover, similar as Uu, D/C filed is also unnecessary for SL SRB. Thus, a separate Date PDU format for SL SRB in unicast is necessary to be added in spec. Rapporteur suggests we can agree D/C filed and SDU type are unnecessary for SL SRBs for unicast and broadcast.

**Question 3: Does company agree D/C filed and SDU type are unnecessary for all SL SRBs for unicast and broadcast messages?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes |  |
| OPPO | Yes |  |
| MediaTek | Yes |  |
| ZTE | Yes |  |
| Ericsson | Yes |  |
| Nokia | Yes |  |
| Futurewei | Yes |  |
| Spreadtrum | Yes |  |
| Apple | Yes |  |
| LG | Yes |  |
| Qualcomm | Yes |  |
| Intel | Yes |  |
| CATT | Yes |  |
| vivo | Yes |  |
| Lenovo | Yes with comments | D/C field and SDU type are not only unnecessary for all SL SRBs for unicast and broadcast message as in question description, but also unnecessary for all SL SRBs for groupcast.  And this is not mean different data PDU format for SL SRB and SL DRB for groupcast and broadcast, i.e. SDU type field is still exist for SL SRB, but not applicable for SL SRB |

**Voting result:**

**Yes: 15**

**No: 0**

Rapporteur's observation:

All companies agree that D/C filed and SDU type are unnecessary for SL SRBs.

**Proposal 3: D/C filed and SDU type are unnecessary for SL SRBs.**

## Issue 3: Data PDU formats for SL unicast

Several companies provide contributions to discuss the Data PDU formats for SL unicast ([1]- [6] and [8]-[12]). Companies have different views on the design of Data PDU formats for SL unicast. Regarding to the Data PDU formats, there are several issues should be discussed as following:

* Issue 3.1: Whether is it necessary to design separate Data PDU formats for SL SRBs and SL DRBs?
* Issue 3.2: Whether is it necessary to carry Key ID in the PDCP PDU header?

For Issue 3.1, based on the discussion in issue 2, for SL SRBs, it is unnecessary to carry D/C field and SDU type field in the PDU header and the MAC-I is always present. Thus, it’s better to have a separate Data PDU format design for SL SRBs [4][6].

**Question 4: Does company agree to adopt separate Date PDU formats for SL SRBs and SL DRBs for unicast?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes |  |
| OPPO | Yes |  |
| HW, HiSi | Yes |  |
| MediaTek | Yes |  |
| ZTE | Yes |  |
| Ericsson | Yes |  |
| Nokia | Yes |  |
| Futurewei | Yes |  |
| Spreadtrum | Yes |  |
| Apple | Yes |  |
| LG | Yes |  |
| Qualcomm | Yes | We agree with the observations made in Q3 [6]. Further, our view is aside from the D/C and SDU fields, the PDU formats should follow the Uu design |
| Intel | Yes |  |
| CATT | Yes |  |
| vivo | Yes |  |
| Lenovo | Yes |  |

**Voting result:**

**Yes: 15**

**No: 0**

Rapporteur's observation:

All companies agree to adopt separate Date PDU formats for SL SRBs and SL DRBs for unicast.

**Proposal 4: Adopt separate Date PDU formats for SL SRBs and SL DRBs for unicast.**

For Issue 3.2, Huawei mentioned that security context confusion duration is very short, in comparison to the total communication duration of the two UEs. So if 16-bit Key ID is always carried in the SLRB PDCP header, it will result in significant radio resource waste, because most of the time the Key ID is not useful for the pair of UEs at all. In addition, it is unfriendly for UE processing to carry 16-bit Key ID in the NR V2X SLRB PDCP header, as this enforces the UE to implement different PDCP header processing mechanisms for SLRB and Uu DRB respectively, which significantly increases UE implementation complexity [10].

Although the Key ID should indeed be concluded by SA3 from a security perspective, SA3 should have taken no consideration on radio resource efficiency as well as the AS implementation complexity when they made the decision, as these are within the expertise of RAN2. Therefore, RAN2 may also need to have a check on whether the 16-bit Key ID concluded by SA3 is acceptable from an AS perspective. Also, an enquiry with SA3 is possible, as the next SA3 meeting is before next RAN2 meeting, giving sufficient time from RAN2 to receive firm conclusion from SA3.

**Question 5: If 16-bit Key ID is always carried in the SLRB PDCP header, does company agree that the above drawbacks which are mentioned in the Huawei’s contribution [10] should be addressed?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | No | We are fine with SA3 decision. This is not new for PC5 since PGK/PTK fields are carried in the PDCP header in LTE-V2X. |
| OPPO | No | We think this is a SA3 issue hence we respect SA3’s decision to keep the key id in the PDCP PDU header as LTE does. |
| HW, HiSi | Yes | 16-bit Key ID in SLRB PDCP header is not necessary, considering the radio resource efficiency and implementation complexity. |
| MediaTek | No |  |
| ZTE | No | This issue also exists in LTE D2D, however, the conclusion is still to carry the Key ID in the PDCP header. We shall follow SA3’s conclusion. |
| Ericsson | No |  |
| Nokia | No | Let us follow SA3’s decision. |
| Futurewei | Yes | If PDCP re-establishment is supported for key refreshing, SA3 should be informed that security context confusion would not occur during rekeying procedure, and Key ID can be removed from PDCP header to reduce overhead. |
| Spreadtrum | With Comments | We have sympathies with Huawei. Whether there will be security in broadcast and groupcast should be taken into consideration too. |
| Apple | No | We share the view with ZTE that the similar discussion for LTE-D2D is concluded to have Key-ID in the header, even with the existence of PC5-S rekeying procedure used. So, we can follow the same solution here. |
| LG | No |  |
| Qualcomm | No | As the current design based on Rel-15 is not broken, it seems prudent not to introduce a different solution to SA3, in particular since SA3 as yet has not reached a conclusion on this issue (including whether there may be unexpected scenarios encountered during the rekey procedure that cannot be accounted for with a single bit). |
| Intel | Yes with comment | Although key ID has been carried in the PDCP header in LTE wherein sidelink operation was generally done on a per-packet basis, we could be more efficient in NR wherein we have bearer/flow-based operation for unicast. We can at the least check with SA3 if the solution suggested by Huawei (to have a one-bit indicator rather than the key ID in the header) can be considered. |
| CATT | Yes with comments | We realize the issues raised by Huawei are valid, but not big problem. At this late stage, we prefer to follow SA3’s decision. |
| vivo | No | This 16-bit Key ID is similar to LTE V2X, which will act as part of COUNT value to participate security operation in LTE. And for NR, this role of this Key ID is under discussion in SA3:  "It is FFS if the length of the counter is 32 bits and if not whether it is the LSB of the counter that is included in PDCP header and if COUNT[0] to COUNT[31] are padded with its of KNPR-sess ID."  Wait for SA3's further conclusion. |
| Lenovo | No | Would like to follow SA3 decision |

**Voting result:**

**Yes: 5**

**No: 11**

Rapporteur's observation:

Majority companies’ view is to follow SA3 decision, while some companies realize the drawbacks which are mentioned by Huawei. We will conclude this issue together with Q6.

According to the preference of Q5, since SA3 already agree the 16-bit Key ID is always carried in the SLRB PDCP header, we need to discuss whether we should follow SA3 guideline or not.

**Question 6: Which following option does company prefer, based on companies answer to Q5?**

* **Option a): Follow the SA3 guideline, which is the 16-bit Key ID is always carried in the SLRB PDCP header for unicast;**
* **Option b): 16-bit Key ID is not carried in the SLRB PDCP header as Huawei’s proposal in [10];**
* **Option c): Send LS to SA3 to ask them for potential guideline.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) |  |
| OPPO | Option a) |  |
| HW, HiSi | Option b) or c) | We need to send LS to SA3, to show RAN2 strong concern, and ask SA3 to re-estimate the necessary to carry 16-bit Key ID in PDCP header from security perspective.  It is also OK for us to send LS to SA3 for potential guidance, if companies think SA3’s help from security’s perspective is needed. |
| MediaTek | Option a) | We are also OK to send LS to SA3. |
| ZTE | Option a) |  |
| Ericsson | Option a) |  |
| Nokia | Option a) |  |
| Futurewei | Options b) and c) | If PDCP re-establishment is supported for key refreshing, SA3 should be informed that security context confusion would not occur during rekeying procedure, and Key ID can be removed from PDCP header to reduce overhead. |
| Apple | Option a) |  |
| LG | Option a) |  |
| Qualcomm | Option a) |  |
| Intel | Option b) or c) with comment | We can send LS to SA3 to provide our suggestion and ask whether the solution still meets the security requirements while being resource efficient. However, if the majority of companies prefer option a), we can be ok with it as well. |
| CATT | Option a) |  |
| vivo | Option a) | We are OK to send LS to SA3. |
| Lenovo | Option a) |  |

**Voting result:**

**Option a): 12**

**Option b): 3 (including one company is also OK for Option a))**

**Option c): 3 (including one company is also OK for Option a))**

Rapporteur's observation:

A clear majority of companies’ view is to follow SA3 decision. Thus, Rapporteur suggests following majority views.

**Proposal 5: To follow SA3, Key ID is necessary to be carried in the PDCP PDU header.**

If option b) is selected in Q6, we need to further discuss how to address the issue on security context confusion in rekeying procedure. In Huawei’s contribution [10], there are two options to address this issue as follows.

* Option 1: No Key ID is carried in NR V2X SLRB PDCP header;
  + In this option, the security context confusion in rekeying procedure is resolved up to UE implementation.
* Option 2: 1 bit indicator is carried in NR V2X SLRB PDCP header to distinguish the old or new security context.

**Question 7: If option b) is selected in Q6, which following option does company prefer to address the issue on security context confusion in rekeying procedure?**

* **Option a): No Key ID is carried in NR V2X SLRB PDCP header;**
* **Option b): 1 bit indicator is carried in NR V2X SLRB PDCP header to distinguish the old or new security context;**
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| HW, HiSi | Option b) | 1 bit is enough to distinguish the old or new security context. |
| Futurewei | Option b) or a) | Option b, if PDCP reestablishment is not supported for rekeying procedure;  Option a, if PDCP reestablishment is supported for rekeying procedure. |
| Intel | Option b) | This solution seems preferable from our perspective. However, we have to check with SA3 for confirmation. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Rapporteur's observation:

Base on the outcome of Q6, there is unnecessary to conclude this question.

## Issue 4: Solution for PDCP COUNT wrap around

For NR SL, whether PDCP re-establishment should be supported was discussed in the last meeting during the offline discussion. Some companies thought PDCP re-establishment is needed for security key refresh, and LS was sent to SA3 to ask whether the re-keying procedure should be introduced for NR V2X unicast.

In SA3 TS 33.536 [17], the re-keying procedure is specified in Section 5.3.3.1.4.4. The re-keying operation shall be done before the counter for a PDCP bearer repeats with the current keys. A re-keying operation shall refresh the KNRP-sess and NRPEK and NRPIK. The KNRP-sess ID is carried in the PDCP header. NRPEK and NRPIK are used in the integrity and ciphering algorithms. According to companies’ contributions, there are two options to address the PDCP COUNT wrap around issue.

* Option 1: SLRB release and addition procedures;
* Option 2: PDCP re-establishment procedure.

Only one company support Option 1 [14], while other four companies prefer Option 2 ([5]- [9] and [13]).

**Question 8: Which following option does company prefer to address the PDCP COUNT wrap around issue in rekeying procedure?**

* **Option a): SLRB release and addition procedures;**
* **Option b): PDCP re-establishment procedure;**
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) | We prefer to use SLRB release and addition procedures to avoid PDCP COUNT wrap around which is same as Uu (i.e., gNB can initiate release/add or full config). From procedure point of view, there is nothing to change in SLRB release and add procedures for this purpose. About triggering this is a separate discussion.  The use of existing Uu PDCP reestablishment has a problem for AM DRB since the COUNT value is not reset to the initial value in the PDCP reestablishment. So, option b) works only for UM DRB and SRB. If we use PDCP reestablishment for RLC AM, then we need to modify the current PDCP reestablishment procedure. |
| OPPO | Option b) | Rekeying procedure itself makes it unnecessary to either change LCID or reset COUNT. Hence PDCP re-establishment is sufficient. Plus Option a) cause more user plane interruption and packet drop. Please note PDCP SN wrap round doesn’t mean PDCP COUNT wrap round i.e. it is different from Uu wrap round issue at all. |
| HW, HiSi | Option c) | Left to UE implementation. |
| MediaTek | Option b) | Agree with OPPO. |
| ZTE | Option a) | It could be avoided by SLRB release and addition procedure by UE implementation. |
| Ericsson | b) |  |
| Nokia | b) | Agree with Ericsson and OPPO |
| Futurewei | Option b) | Release and addition procedure would also have an option of PDCP reestablishment, and full-config would involve clearing full PC5 configuration and performing whole PC5 configuration from scratch, yet still keeping the old security key. |
| Spreadtrum | Option b) | PDCP reestablishment have to be supported for re-keying procedure any way. |
| Apple | Option b) |  |
| Qualcomm | Option b) |  |
| Intel | Option b) |  |
| CATT | Option b) | Agree with OPPO. |
| vivo | Option c) | We think that both option a and option b are allowed just like UU. |
| Lenovo | Option b) | Agree with OPPO. |

**Voting result:**

**Option a): 2**

**Option b): 11**

**Option c): 2 (one company think it can be left into UE implementation; the other company think both Option a) and b) can be allowed)**

Rapporteur's observation:

A clear majority of companies’ view is to support PDCP re-establishment to address the PDCP COUNT wrap around issue in rekeying procedure. Thus, Rapporteur suggests following majority views.

**Proposal 6: PDCP re-establishment is supported in SL unicast.**

If option a) is selected in Q8, Samsung propose that SL DRB release and addition can be triggered by UE’s lower layer, e.g., PDCP layer. The TX UE checks whether TX\_NEXT is approaching to the large COUNT value or not. If so, UE’s PDCP layer indicates it to RRC layer to perform SLRB release and addition procedures.

**Question 9: If option a) is selected in Q8, does company agree that SL DRB release and addition can be triggered by UE’s lower layer, e.g., PDCP layer?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes | We are not that strong in PDCP layer. This can be triggered either PDCP layer or RRC layer.  About V2X layer, unless SA3 defines any requirements, e.g., TX\_NEXT is approaching to the maximum COUNT, it can be up to RAN2. |
| HW, HiSi | No | Refer to Q8 |
| ZTE | No | It is UE implementation. |
| Futurewei | No | SL DRB release and addition is a PC5 RRC procedure. |
| CATT | No |  |
| vivo | No | Just like UU, some guidance should be added.  For example in UU,  The TX UE may e.g. use different RB identities for RB establishments, change the AS security key |
| Lenovo | No | by UE implementation |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Rapporteur's observation:

Base on the outcome of Q8, there is unnecessary to conclude this question.

If option b) is selected in Q8, whether the PDCP re-establishment trigger is captured in RRC or V2X layer should be discussed. Over Uu interface, the trigger of PDCP re-establishment is captured in RRC spec. While over PC5 interface, PDCP re-establishment is only triggered by rekeying procedure which is in V2X layer but not RRC layer. Thus, OPPO suggest to send LS to SA3 to capture the PDCP re-establishment trigger due to re-keying operation in V2X layer.

**Question 10: If option b) is selected in Q8, does company agree the PDCP re-establishment trigger should be captured in V2X layer?**

* **Yes. If Yes is selected, please further clarify whether is it necessary to send LS to SA3 to ask them to capture the PDCP re-establishment trigger due to re-keying operation;**
* **No. If No is selected, please further clarify how to capture the PDCP re-establishment trigger.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | No | It can be up to RAN2 unless SA3 defines any requirements, e.g. TX\_NEXT is approaching to the maximum COUNT. |
| OPPO | Yes | A LS to SA3 is needed to introduce a PDCP reestablishment trigger in V2X layer. |
| HW, HiSi | No | Refer to Q8 |
| MediaTek | Yes |  |
| ZTE | No | It is not appropriate for SA3 to capture the PDCP re-establishment trigger. WE could just capture in PDCP spec that the PDCP re-establishment is triggered by upper layer. |
| Ericsson | Yes |  |
| Nokia | Yes |  |
| Futurewei | No | V2X layer doesn’t have context and control of SLRBs. |
| Spreadtrum | Yes |  |
| Apple | Yes |  |
| Qualcomm | Yes | The LS should be sent to CT1, as CT1 defines V2X layer details |
| Intel | Yes |  |
| CATT | Yes | We need send LS to SA3. |
| vivo | No | Just like UU, some guidance should be added.  For example,  The TX UE may e.g. use PDCP reestablishment prodedure to change the AS security key |
| Lenovo | Yes |  |

**Voting result:**

**Yes: 10**

**No: 5**

Rapporteur's observation:

A clear majority of companies’ views agree the PDCP re-establishment trigger should be captured in V2X layer. It’s necessary to send LS to SA3 to ask them to capture the PDCP re-establishment trigger due to re-keying operation. One company also mentions the LS should also be sent to CT1, as CT1 defines V2X layer details. Thus, Rapporteur suggests following majority views.

**Proposal 7: Send LS to SA3 and CT1 to ask them to capture the PDCP re-establishment trigger due to re-keying operation.**

## Issue 5: PDCP status report

Regarding to the status report, if PDCP re-establishment is supported, it’s better to support status report to maintain loss-less and in-order delivery [8][9].

Therefore, rapporteur suggests RAN2 to discuss whether the status report is necessary to be supported for SL unicast.

**Question 11: Does company agree to support the status report for SL unicast?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes | If PDCP status report is introduced, status report can be used for retransmission. |
| OPPO | No | Since key ID always exists in the PDCP PDU header it is likely that PDCP PDU will not be dropped. Hence PDCP status report doesn’t help too much in this case. |
| HW, HiSi | No | Not necessary if PDCP re-establishment is not supported. |
| MediaTek | Yes |  |
| ZTE | No |  |
| Ericsson | Yes | If PDCP re-establishment is introduced |
| Nokia | Yes | Preferably, but not having it could also be OK |
| Futurewei | Yes | If PDCP re-establishment is supported. |
| Spreadtrum | Yes | If PDCP re-establishment is supported, status report is needed. |
| Apple | Yes |  |
| Qualcomm | Yes |  |
| Intel | Yes | Agree with Ericsson |
| CATT | Yes | We share the majority view that if PDCP re-establishment is supported, status report is needed. |
| vivo | Yes | When PDCP performs re-establishment, PDCP status report is needed. |
| Lenovo | Yes | If PDCP re-establishment is introduced. According to existing spec, status report is triggered |

**Voting result:**

**Yes: 12**

**No: 3**

Rapporteur's observation:

A clear majority of companies’ view is to support the status report for SL unicast, since the outcome of Q8 is to support PDCP re-establishment. Thus, Rapporteur suggests following majority views.

**Proposal 8: Status report is supported for SL unicast.**

## Issue 6: Length of bits for PDU type

According to OPPO and CATT’s contributions ([6] and [8]), there are two options for the length of bits for PDU type:

* Option 1: 3 bits.
* Option 2: 2 bits.

If status report is supported, for SL unicast, there are two types of control PDUs, one is PDCP status report and the other is interspersed ROHC feedback. Thus, similar as Uu, using 3-bits PDU type, i.e., Option 1, is preferred in order to reuse the Uu control PDU formats for SL unicast ([8] and [9]).

2-bits PDU type, i.e., Option 2, is suggested in OPPO’s contribution and a new control PDU format is design for interspersed ROHC feedback for SL unicast [6].

**Question 12: Which following option does company prefer on the length of bits for PDU type?**

* **Option a): 3 bits;**
* **Option b): 2 bits;**
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) | We are fine to follow Uu format |
| OPPO | Option b) | If status report is not introduced then one code point will be wasted if Uu format is to be reused. |
| HW, HiSi | Option a) | 3 bits is better for future extension. |
| MediaTek | Option a) |  |
| ZTE | Option b) | No strong view, but from our understanding, 2-bit is enough. |
| Ericsson | a) or b) | Either way is fine, no strong view |
| Nokia | a) |  |
| Futurewei | a) | Uu format can be reused. |
| Spreadtrum | Option a) | It is fine to follow uu format. |
| Apple | Option a |  |
| LG | Option a) |  |
| Qualcomm | Option a) | Our preference would be to follow the Uu format, unless there is a designated use for the recovered bit |
| Intel | Option a) |  |
| CATT | Option a) | If status report is supported, 3 bits is preferred. |
| vivo | a) | Follow legacy Uu format. |
| Lenovo | a) or b) | Either way is fine, no strong view |

**Voting result:**

**Option a): 14**

**Option b): 4**

Rapporteur's observation:

A clear majority of companies’ view is to support 3-bits length for PDU type and Uu format can be re-used. Since the outcome of Q11 is to support status report, Rapporteur suggests following majority views.

**Proposal 9: The length of PDU type is 3-bits.**

## Issue 7: Initial value of RX\_DELIV

In current 38.323, the initial value of SN part of RX\_DELIV is specified as (x – 0.5 × 2[*sl-PDCP-SN-Size*–1]) modulo (2[*sl-PDCP-SN-Size*]), where x is the SN of the first received PDCP Data PDU. The HFN part is not specified at all and it shall be determined automatically by RX\_NEXT.

Considering the relation with SN of first received PDCP data PDU and RX\_NEXT, Samsung proposes the initial value of RX\_DELIV shall be RX\_NEXT - 0.5 × 2[*sl-PDCP-SN-Size*–1] – 1 [14].

**Question 13: Which following option does company prefer on initial value of RX\_DELIV?**

* **Option a): Keep the current specification in 38.323, i.e., the initial value of SN part of RX\_DELIV is specified as (x – 0.5 × 2[*sl-PDCP-SN-Size*–1]) modulo (2[*sl-PDCP-SN-Size*]);**
* **Option b): The initial value of RX\_DELIV shall be specified as RX\_NEXT - 0.5 × 2[*sl-PDCP-SN-Size*–1] – 1.** Note this option b) will update the current specification;
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option b) | The initial value of HFN part is not specified at all, but it shall be determined automatically by RX\_NEXT. The text proposal is very simple: “**as RX\_NEXT - 0.5 × 2[*sl-PDCP-SN-Size*–1] – 1”**  Note that there is no room for UE implementation. |
| OPPO | Option a) | Nots sure what’s problem of current initial value |
| HW, HiSi | Option b) | Option b) is ok for broadcast and group broadcast. To clarify this question is not related with unicast. |
| MediaTek | Option a) |  |
| ZTE | Option a) |  |
| Ericsson | Option a) slightly preferred | We have a Note in the spec that “NOTE: It is up to UE implementation to select HFN for RX\_NEXT as such that initial value of RX\_DELIV should be a positive value.”  Is it not enough? |
| Nokia | a) or b) |  |
| Futurewei | No strong view |  |
| Spreadtrum | Option a) | To follow uu. |
| Apple | Option a |  |
| Qualcomm | Option a) | Share the views expressed by OPPO and Ericsson |
| Intel | Option a) |  |
| CATT | Option a) | No strong view |
| vivo | Option a) | No need for re-discussion. Current spec is enough. |
| Lenovo | No strong view | Would like to ask clarification question: why there has no room for UE implementation for the initial value? |

**Voting result:**

**Option a): 11**

**Option b): 3**

**No strong view: 2**

Rapporteur's observation:

A clear majority of companies’ views are to keep the current specification in 38.323, i.e., the initial value of SN part of RX\_DELIV is specified as (x – 0.5 × 2[*sl-PDCP-SN-Size*–1]) modulo (2[*sl-PDCP-SN-Size*]). Thus, Rapporteur suggests following majority views that don’t make changes on the current specification. So no further proposal is needed.

## Issue 8: Need of counter-check procedure in PC5

According to the current SA3 specification, the integrity protection can be optional for SL unicast DRBs. If the SL integrity protection is not used, there may be a need to introduce a counter check procedure in PC5 interface, as proposed in [7].

Therefore, rapporteur suggests RAN2 to discuss whether it is necessary to introduce a counter check procedure in PC5 interface for unicast.

**Question 14: Does company agree to introduce a counter check procedure in PC5 interface for unicast?**

* **Option a): Yes;**
* **Option b): No;**
* **Option c): Send LS to SA3 to ask them about the necessity of introducing SL Counter Check procedure.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) | It may help to avoid HFN desynchronization problem. |
| OPPO | Option b) | For this release we don’t need it |
| HW, HiSi | Option b) | Prefer integrity check is always used. |
| MediaTek | Option b) |  |
| ZTE | Option a) | It seems necessary and helpful for PC5 unicast. |
| Ericsson | Option a) |  |
| Nokia | Option b) | Seems like an enhancement |
| Futurewei | Option b) |  |
| Spreadtrum | Option a) |  |
| Apple | Option a) | RAN2 is not sure whether security is always used for SL unicast, At least RAN2 can send a LS to SA3 for triggering discussion on this aspect. |
| LG | Option a) |  |
| Qualcomm | Option a) |  |
| Intel | Option b) |  |
| CATT | Option b) | Share the same view as Huawei. If counter check procedure is needed, the UE can set integrity protection is always enable. Moreover, at this late stage, we prefer not do this. |
| vivo | Option b) |  |
| Lenovo | Option b) | Seems this needs to be determined by SA3 |

**Voting result:**

**Option a): 7**

**Option b): 9**

Rapporteur's observation:

There is no clear majority. Since this is an enhancement, at this late stage, Rapporteur prefers not to discuss such kind of enhancement. Thus, Rapporteur suggests RAN2 to discuss whether it is necessary to introduce a counter check procedure in PC5 interface for unicast.

**Proposal 10: Suggest RAN2 to discuss whether it is necessary to introduce a counter check procedure in PC5 interface for unicast, considering the following options:**

* **Option 1: Do not introduce a counter check procedure in PC5 interface for unicast in R16;**
* **Option 2: Send LS to SA3 to ask them about the necessity of introducing SL Counter Check procedure.**

## Other Issues

Regarding to other details editorial issues, e.g., the detail design in PDU format and some clarifications related ciphering and integrity procedure can be further discussed during the PDCP CR discussion. Here, companies are invited to provide other technical remaining issues related V2X PDCP.

|  |  |  |
| --- | --- | --- |
| **Company** | **Issues** | **Comments if any** |
| OPPO | SL SRB PDCP PDU format | Recently CT1 agreed that Direct Communication Request message can be also sent via Unicast. But this message is not protected. So MAC-I should be optional within SL SRB PDCP PDU format which should be also clarified in table 6.3.2-1  Rapporteur’s comments:  Not sure I do clearly understand this issue. I agree the Direct Communication Request message can be also sent via Unicast. But since this message is the first PC5-S message which still cannot be integrity protected, even though it is sent via unicast. Thus, MAC-I is still not needed in the PDCP PDU format. Moreover, the table 6.3.2-1 is for PDCP SN. I don’t know why we need some clarifications related MAC-I in table 6.3.2-1.  I think for this issue, maybe we can make some clarification in Section 6.2.2.4, i.e., the PDU format for Direct Communication Request message to say that Direct Communication Request message can also be transmitted via unicast. The detail text can be discussed during CR discussion stage.  OPPO:  In our opinion there are two alternatives to define the PDCP PDU format for DCR by unicast:  Alt1: reusing broadcast/groupcast PDCP PDU format with 18bits SN  Alt2: reusing SLRB SRB PDCP PDU format with 12 SN bits  If we go for alt1, then some clarification is needed for the broadcast/groupcast PDCP PDU format that it can be also used for unicast message carrying DCR message  If we go for alt2, then MAC-I should be optional because DCR message is not integrity protected. Then at least one bit in the PDCP header is needed to indicate whether MAC-I exists or not.  After 2nd thought we believe 1st approach is simpler way to resolve the issue which is also aligned with previous agreement that 18bit SN is adopted for PC5-S signaling carrying DCR.  Rapporteur’s comments:  OK, Alt1 is also preferred from Rapporteur’s point of view. Let’s discuss the details during the CR discussion. |
|  |  |  |
|  |  |  |
|  |  |  |

# Conclusion

This contribution summarizes the offline discussion for open issues on V2X PDCP.

Based on companies’ input, the proposals achieved by this offline discussion are shown as follows.

**Proposal 1: From RAN2 perspective, the 5 least significant bits of LCID can be used as 5-bit input to the ciphering/integrity algorithms.**

**Proposal 2: Reply LS to SA3 to inform RAN2 preference on LCID usage for integrity and ciphering algorithms.**

**Proposal 3: D/C filed and SDU type are unnecessary for SL SRBs.**

**Proposal 4: Adopt separate Date PDU formats for SL SRBs and SL DRBs for unicast.**

**Proposal 5: To follow SA3, Key ID is necessary to be carried in the PDCP PDU header.**

**Proposal 6: PDCP re-establishment is supported in SL unicast.**

**Proposal 7: Send LS to SA3 and CT1 to ask them to capture the PDCP re-establishment trigger due to re-keying operation.**

**Proposal 8: Status report is supported for SL unicast.**

**Proposal 9: The length of PDU type is 3-bits.**

**Proposal 10: Suggest RAN2 to discuss whether it is necessary to introduce a counter check procedure in PC5 interface for unicast, considering the following options:**

* **Option 1: Do not introduce a counter check procedure in PC5 interface for unicast in R16;**
* **Option 2: Send LS to SA3 to ask them about the necessity of introducing SL Counter Check procedure.**

# Reference

1. R2-2003774, Summary of PDCP remaining issues on NR V2X, CATT
2. R2-2002541, LS reply to RAN WG2 LS on NR V2X Security issue and PDCP SN size (S3-200478; contact: CATT), SA3, LS in, To:RAN2
3. R2-2002566, Discussion on NR V2X remaining user plane issues, ZTE Corporation, Sanechips
4. R2-2002570, (draft)CR on TS 38.323 for NR V2X on miscellaneous issues , ZTE Corporation, Sanechips
5. R2-2002649, Discussion on PDCP open issues, OPPO
6. R2-2002650, 38323\_CRyyyy\_(REL-16)\_Correct on PDCP for NR V2X, OPPO
7. R2-2002810, Remaining issues on NR V2X PDCP Design, Apple
8. R2-2002833, Remaining Issues on PDCP, CATT
9. R2-2002834, 38.323 draftCR for NR V2X, CATT
10. R2-2003510, Discussion on the SLRB PDCP header format, Huawei, HiSilicon
11. R2-2003511, Draft CR on the PDCP format for NR SL unicast, Huawei, HiSilicon
12. R2-2003535, Draft CR to 38.323 for NR PC5-S and PDCP header, Qualcomm
13. R2-2003668, Remaining PDCP issues, Nokia, Nokia Shanghai Bell
14. R2-2003681, Discussion for SL PDCP open issues, Samsung Electronics Co., Ltd
15. R2-2003682, SL PDCP COUNT wrap around avoidance and initial value of RX\_DELIV, Samsung Electronics Co., Ltd, 38.323
16. R2-2003683 , SL PDCP COUNT wrap around avoidance, Samsung Electronics Co., Ltd, 38.331
17. S3-200528 TS 33.536 v0.3.0, Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services