3GPP TSG RAN WG2#109-e R2-2001977

Electronic meeting, 24th February - 6th March, 2020

Agenda Item: 6.4.3.2

Source: CATT (rapporteur)

Title: Summary of offline discussion for open issues on V2X PDCP (CATT)

Document for: Discussion, Decision

# Introduction

This document includes the offline discussion #707 on the related issues and proposals which were discussed in the PDCP email discussion and summary contribution submitted in R2-2000214 and R2-2002017 [1][2]. The scope of this offline discussion in the chairman notes is as following.

R2-2000214 Summary of Email discussion [108#102][V2X] Remaining issues on PDCP CATT discussion Rel-16 5G\_V2X\_NRSL-Core

* Proposal 3 and 4 are agreed with the removal of “Only” and “types of”.
* Proposal 5, 6, 7, 8, 10, and 12 are agreed.
* [Offline Disc#707]: To discuss proposal 1, 2, 9, 11, 13, 14, and 15.
* [Offline Disc#708]: To prepare draft LS to SA3 to inform RAN2 agreements made this e-meeting (CATT, R2-2001973) (Comeback next Wed.)

Agreements on PDCP:

1: Capture which SLRB need confidentiality protection in TS 38.331. The specific functionalities for confidentiality protection (e.g. parameters needed, procedures, etc.) are captured in TS 38.323.

2: Capture which SLRB need integrity protection in TS 38.331. The specific functionalities for integrity protection (e.g. parameters needed, procedures, etc.) are captured in TS 38.323.

3: For SL DRBs of groupcast and broadcast, the MAC-I field is not present.

4: For SL DRBs of unicast, if the integrity protection is not configured, the MAC-I field is not present.

5: For the first PC5 Signalling, i.e., Direct Communication Request, the MAC-I field is not present.

6: Except for Direct Communication Request, the MAC-I field is always present in the PDCP format for other PC5 Signallings and SL RRC signallings.

7: The D/C field is not present and the corresponding bit is present as a Reserved bit in data PDU format for groupcast and broadcast.

8: 4 different LCIDs are allocated for the following SL SRBs:

- The PC5-S signalling that is not protected, e.g., Direct Communication Request.

- The PC5-S signalling to activate security, i.e., Direct Security Mode Command and Direct Security Mode Complete.

- Other PC5-S signallings that are protected.

- PC5-RRC signallings that are protected.

R2-2002017 Summary of PDCP remaining issues on NR V2X CATT discussion Rel-16 5G\_V2X\_NRSL-Core

* Proposal 1 (Note will be captured in 38.323)
* Include the discussion of proposal 2, 3, 4, 5, 6, 7, 8, and 9 into offline disc#708.

# Discussion

## Issue1: HFNs of RX\_NEXT and RX\_DELIV

In the email discussion [1], there are two proposals for HFNs of RX\_DELIV and RX\_NEXT:

Proposal 1: Add a Note that the HFN part of RX\_NEXT can be left to UE implementation as such that initial value of RX\_DELIV should be a positive value.

Proposal 2: Add a Note that the HFN part of RX\_DELIV can be left into UE implementation.

Futurewei [3] and Samsung [4] prefer to either Proposal 1 or Proposal 2, but not both. Futurewei [3] prefers to agree Proposal 2. But the majority view in the email discussion is to agree both proposals.

**Question 1: Regarding the issue of HFNs of RX\_DELIV and RX\_NEXT, which option does company prefer?**

1. **Option a: Only one note is needed. The note needs to clarify that it’s up to UE implementation to select HFN for RX\_NEXT and guarantee the initial value of RX\_DELIV should be a positive value.**
2. **Option b: Only one note is needed. The note needs to clarify that it’s up to UE implementation to select HFN for RX\_DELIV.**
3. **Option c: Add two notes:**
   * **One note is to clarify that it’s up to UE implementation to select HFN for RX\_NEXT and guarantee the initial value of RX\_DELIV should be a positive value;**
   * **The other note is to clarify that it’s up to UE implementation to select HFN for RX\_DELIV.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Option a |  |
| OPPO | Option a | We intend to agree with Futurewei and Samsung |
| Samsung | Option a | Just one note either option a) or option b) is enough.  About option c), since RX\_NEXT and RX\_DELIV are tightly coupled and HFN for each other should not be independently determined, two notes for the two parameters would cause a problem of PDCP receive operation. |
| ZTE | Option a |  |
| LG | Option a | Share the view that a note can better clarify the initial value of the HFN part of RX\_DELIV. |
| Intel | Option a |  |
| Nokia | Option a |  |
| Ericsson | Option a with comment | We agree the HFN part of RX\_NEXT and RX\_DELIV are related, it is a chicken-egg problem to set which first. Regarding how the Note should be formulated, we propose the following:   * Note: it is upon UE implementation to set the initial value of HFN part for RX\_NEXT and RX\_DELIV, both should be equal or larger than 0 |
| vivo | Option a | Just one note is needed since the difference between RX\_NEXT and RX\_DELIV initial values is fixed, i.e. half of SN window. And the SN and HFN part for RX\_NEXT are deduced firstly but it should guarantee the initial value of RX\_DELIV is a positive value. Hence option a is preferable. |
| CATT | Option a | Agree with Futurewei and Samsung. One note is enough. |
| MediaTek | Option a |  |
| Qualcomm | Option a |  |
| Apple | Option a |  |
| Futurewei | Option b | We have slight preference of Option b, as Option a would have a note on RX\_NEXT refer to RX\_DELIV as well, while Option b would only state the need for RX\_DELIV. But we can go with majority. |

**Voting result:**

**Option a: 13 (Seems one company prefers option c based on the comments)**

**Option b: 1**

**Option c: 0**

Rapporteur's observation:

A clear majority of companies agreed with Option a. Thus, Rapporteur suggests following majority views to capture only one Note as option a.

Proposal 1: Capture one Note that it’s up to UE implementation to select HFN for RX\_NEXT as such that initial value of RX\_DELIV should be a positive value.

## Issue2: PDCP SN size of Direct Communication Request message

In the email discussion [1], there is slight majority view with 12 bit PDCP SN size of Direct Communication Request, i.e., 8 companies prefer 12bits, while 5 companies prefer 18bits. Rapporteur suggests we can agree with a working assumption with 12 bit PDCP SN size and send it to SA3 for further check.

**Question 2:** **Regarding to the PDCP SN size of Direct Communication Request message, which option does company prefer?**

1. **Option 1: Agree 12 bit PDCP SN size of Direct Communication Request as a working assumption and send this to SA3 for further check;**
2. **Option 2: Agree 18 bit PDCP SN size of Direct Communication Request as a working assumption and send this to SA3 for further check;**
3. **Option 3: Don’t agree anything in this meeting, just ask SA3 the question on the PDCP SN size of Direct Communication Request message;**
4. **Option 4: Don’t agree anything in this meeting, just wait for SA3 progress;**
5. **Other options: Please provide the detail solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Option 1 |  |
| OPPO | Option 2 | First of all SA3 has confirmed that no protection is needed for Direct Communication Request message hence RAN2 should make decision. Then as we explained in our paper [5] the benefit for SN=18 bits is to save one more PDCP PDU format since same PDCP PDU format for broadcast/groupcast can be reused to make the spec simple. |
| Samsung | Option 2 | Same view as OPPO |
| ZTE | Option 2 | Share the same view as OPPO |
| LG | Option 1 | Share the view to maintain the SL-SRB design, |
| Intel | Option 2 | We agree with OPPO’s view |
| Nokia | Option 2 | Same view as OPPO, we should try to simplify |
| Ericsson | option 1 | Both 12bits and 18btis can work, we prefer to keep it same as other SRBs. |
| vivo | Option 1 | Firstly both 12 bit SN and 18 bit SN can work. If 12 bit is chosen, common SRB formats will be maintained. If 18 bit is used, broadcast/groupcast formats will be unified.  From our view, 12 bit is enough. |
| CATT | Option 2 | Share the same view as OPPO. |
| MediaTek | Option 1 |  |
| Qualcomm | Option 1 |  |
| Apple | Option 2 | We think this is mostly a broadcast message, so it is ok to align it to other SL broadcast message formats. |
| Futurewei | Option 1 | As agreed, direct communication message would be carried on SL-SRB. Hence, 12 bit SN can have consistent PDCP format for SL-SRB. |

**Voting result:**

**Option 1: 7**

**Option 2: 7**

**Option 3: 0**

**Option 4: 0**

Rapporteur's observation:

7 companies think 12-bit PDCP SN size for Direct Communication Request message is enough and will be align with other SL SRBs, while other 7 companies think 18-bit PDCP SN size can align it to other SL broadcast message formats. Rapporteur thinks the PDU formats for broadcast and unicast is different due to the D/C field. Thus, as OPPO mentioned the benefit for SN=18 bits is to save one more PDCP PDU format since same PDCP PDU format for broadcast/groupcast can be reused to make the spec simple. We need to move forward. Rapporteur suggests we can agree with a working assumption with 18-bit PDCP SN size and send LS to SA3 for further check.

Proposal 2: Working assumption: The PDCP SN size of Direct Communication Request message is 18 bits. Send LS to SA3 to further check.

## Issue3: LCID usage in protection algorithms

In the email discussion [1], the issue for LCID usage in protection algorithms had been discussed. There is no clear majority view on the solution. 5 companies prefer to use the 5 least significant bits of LCID, while other companies want to further check SA3 or wait SA3 progress.

**Question 3:** **Regarding to the LCID usage in the integrity algorithms and ciphering algorithms, which option does company prefer?**

1. **Option 1: Agree as a working assumption that from RAN2 perspective, the 5 least significant bits of LCID can be used as input to the ciphering/integrity algorithms. Send this to SA3 for further check;**
2. **Option 2: Don’t agree anything in this meeting, just ask SA3 the question on the LCID usage in the ciphering/integrity algorithms;**
3. **Option 3: Don’t agree anything in this meeting, just wait for SA3 progress;**
4. **Other options: Please provide the detail solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Option 1 |  |
| OPPO | Option 1 with comment | To us it is very straight forward to agree 5 LSB of LCID now in RAN2 but we are fine to further check with SA3 |
| Samsung | Option 2 with comment | Since SA3 might not be informed about that LCID size of NR PC5 is 6 bits, we think that RAN2 should inform SA3 that the length of LCID is 6 bits in NR SL and ask the usage of LCID in ciphering and integrity algorithms. |
| ZTE | Option 2 | We agree to send LS to check with SA3. But from our understanding, to use whole bits of LCID for ciphering and integrity algorithms seems reasonable, since it follows LTE D2D principle. |
| LG | Option 2 | We could inform SA3 via an LS in order to align with them on the size of the LCID. |
| Intel | Option 2 |  |
| Nokia | Option 2 | Agree with ZTE |
| Ericsson | Option 2 with comment | We can send LS to SA3 only if they don’t discuss/conclude in this meeting. |
| vivo | Option 2 | We are fine to send LS to SA3. |
| CATT | Option 2 | We are also ok to just send the question to SA3, if companies cannot agree to use the 5 least significant bits of LCID. |
| MediaTek | Option 1 |  |
| Qualcomm | Option 1 | 5-bits is the guidance from SA3. Adhering to their recommendation seems the most straight-forward approach. |
| Apple | Option 2 | Maybe SA3 can explain to us why only 5 bits are needed in ciphering algorithm. |
| Futurewei | Option 2 | Given the adjusted R16 workplan (April meeting is still dedicated to R16 completion), it’d be better just to inform SA3 the current status and request their input. |

**Voting result:**

**Option 1: 4**

**Option 2: 10**

**Option 3: 0**

Rapporteur's observation:

4 companies think it is straight forward to agree 5 LSB of LCID in RAN2, but some of them are also fine to check with SA3. Thus, Rapporteur suggests we can go with Option2 to send LS to check with SA3 view.

Proposal 3: Send LS to SA3 including the issue on LCID usage in the ciphering/integrity algorithms.

## Issue4: PDCP re-establishment and status report

In NR Uu, during handover procedure, the existing PDCP will be re-established according to configuration from the new cell and PDCP status report will be sent to the new cell so that NW can understand which PDCP PDUs are in the list waiting for transmission. However, in SL, such scenario does not exist that a UE is switching from one UE to anther UE, thus there is no need to consider PDCP re-establishment and status report transmission. Ericsson and OPPO propose NR sidelink does not consider PDCP re-establishment and status report [5][6].

**Question 4: Does company agree that NR sidelink does not support PDCP re-establishment and status report?**

1. **Yes;**
2. **No, if select “No”, please give the reason in the comments.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Yes |  |
| OPPO | No | After second thought, we think PDCP re-establishment is needed at least for rekeying procedure. Following is rekeying procedure:  UE\_1 will re-establishment PDCP after receiving Direct Security Mode Command and start to transmit/receive with new keys including Direct Security Mode Complete message. UE\_2 will re-establish PDCP upon receiving Direct Security Mode Complete message.  As for Status report ,we have no strong opinion i.e. either way is fine. |
| Samsung | Yes |  |
| ZTE | Yes |  |
| LG | Yes |  |
| Intel | Yes |  |
| Nokia | No | We agree to OPPOs statement that re-establishment may be required in NR Sidelink due to especially re-keying issues if using i.e. a 12 bit SN field. |
| Ericsson | Yes | PDCP re-establishment and status report is for handover scenario in Uu, which is not applicable for SL. |
| vivo | Yes |  |
| CATT | Yes | In this release, we can keep it simple to not support PDCP re-establishment and status report. |
| MediaTek | Yes with comments | For NR Uu interface, re-keying is supported. The gNB runs the key change on-the-fly procedure with the UE. During this procedure the gNB shall indicate to the UE that a key change on-the-fly is taking place.  The procedure used is based on an intra-cell handover, and hence the same Key derivation steps shall be taken as in a normal handover procedure. During this procedure, the PDCP entity shall be re-established.  It should be noted that the AS Key re-keying is subject to the full control of AMF. The conditions to trigger re-keying over Uu may not be existing over PC5 anymore.  For Sidelink operation between two NR UEs, it is not clear if SA3 can define a re-keying mechanism between two UEs at Rel-16. SA3 should be consulted for this issue before any agreement within RAN WG2. There is no support for LTE V2X UEs as there was only broadcast based transmission. |
| Qualcomm | No | We agree that PDCP re-establishment is not required for UE handover. However, as noted by OPPO, in the event or rekey, PDCP re-establishment is required. |
| Apple | No | Agree with OPPO. |
| Futurewei | No | When there is PDCP SN wrap-around, security key refresh would be needed. If PDCP reestablishment is supported, status report should be supported as well to maintain loss-less and in-order delivery.  What would be the complexity of porting Uu PDCP reestablishment procedure to PC5? |

**Voting result:**

**Yes: 9**

**No: 5**

Rapporteur's observation:

5 companies think PDCP re-establishment is needed as for security key refresh. Other companies think PDCP re-establishment isn’t necessary and maybe depend on SA3 progress. Since it is the first time and this issue wasn’t discussed in the previous meeting, Rapporteur suggests postponing this discussion to a long email discussion or to the next meeting.

Proposal 4: Suggest RAN2 to further discuss whether PDCP re-establishment and status report is supported or not, considering the security impact.

## Issue5: Length of bits for PDU type

According to the Issue 2, if PDCP status report is not needed, only one control PDU for ROHC feedback is supported in NR SL. Hence 3 bits is bit luxurious for PC5 interface. OPPO proposes to use 2 bits for PDU type [5].

**Question 5: Does company agree that 2 bits PDU type is used for NR sidelink?**

1. **Yes;**
2. **No, if select “No”, please give the preference in the comments.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Yes |  |
| OPPO | Yes |  |
| Samsung | Yes |  |
| ZTE | Yes |  |
| LG | Yes |  |
| Intel | Yes |  |
| Nokia | Yes |  |
| Ericsson | Yes |  |
|  |  |  |
| vivo | No with comment | 2/3 bits PDU type will not impact on the overhead, i.e. just different number of R bits. 3 bits will help for future features without any cost.  But we can accept majority's view. |
| CATT | Yes |  |
| MediaTek | Yes |  |
| Qualcomm | No | As noted by vivo, there is no reduction in the overall field size, and hence no over-the-air savings by reducing the PDU type to 2 bits. Absent an identified purpose/application of this bit, it seems a bit unnecessary to remove it, particularly when weighed against the future extensibility it provides. Accept majority view on this |
| Apple | No | I think 3-bit works fine too. So to be future-proof, we slightly prefer to keep it as 3-bit |
| Futurewei | No | Agree with Vivo, and can also go with majority. |

**Voting result:**

**Yes: 10**

**No: 4**

Rapporteur's observation:

4 companies prefer 3-bit PDU type, but also can go with majority view. Thus, Rapporteur suggests we can agree 2-bit PDU type as follow majority view.

Proposal 5: PDU type for NR sidelink is 2 bits.

## Issue6: Length of bits for SDU type

The SDU type length is already agreed in the last meeting as 2bits.

Qualcomm recommend RAN2 revisit the decision and change the decision of the length of the SDU Type length from 2-bits to 3-bits [7].

There are several reasons are mentioned by Qualcomm as following:

* Reducing the PDCP SDU Type length from 3 bits to 2 bits in Rel-16 reduces the flexibility compared to Rel-14, limiting the ability to address expected SDU types.
* Release-17 is expected to include additional types, potentially including Discovery message and Relay, both of which are neither IP nor non-IP.
* A Release-17 UE in PC-5 may use IPv4, and in groupcast or broadcast may send ARP messages. Since an ARP header differs from non-IP, it cannot be differentiated in PDCP if the PDCP SDU type non-IP is used.
* Release-17 is expected to require more than two additional PDCP SDU types beyond IP and non-IP. Ensuring future extensibility implies the PDCP SDU type field should be greater than 2-bits

Therefore, Qualcomm suggests for future flexibility and backward compatibility, RAN2 use 3-bits PDCP SDU type.

**Question 6: Does company agree to change PDCP SDU type from 2-bits to 3-bits? Note this will convert the previous agreement.**

1. **Yes;**
2. **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Yes | Both are OK, from a forward compatibility view, as either we occupy one more bit for SDU type field or we leave it as an “R” bit for future use. |
| OPPO |  | Either way is fine for us |
| Samsung | Yes | We are fine with 3 bits for future flexibility. |
| ZTE | Yes | Considering forward compatibility, it seems reasonable |
| LG | Yes |  |
| Intel |  | We are ok with either way |
| Nokia | Yes | OK either way |
| Ericsson | No | We don’t see the necessity to change 2bits to 3bits. No strong view though. |
| vivo | Yes | Similar with the above question 5. 2/3 bits PDCP SDU type will not impact on the overhead. 3 bits will help for future features without any cost. |
| CATT | Yes |  |
| MediaTek | Yes | Prefer 3 bits as in LTE for its future extensibility. |
| Qualcomm | Yes | Per the arguments presented in the rapporteur’s summary. |
| Apple | Yes | Agree with the majority view |
| Futurewei | Yes | Though no strong view, we have some sympathy on Qualcomm’s analysis. |

**Voting result:**

**Yes: 13 (Some companies can go with either way)**

**No: 1**

Rapporteur's observation:

A clear majority view prefers 3-bit SDU type. Thus, Rapporteur suggests we can agree 3-bit SDU type as follow majority view.

Proposal 6: Change the previous agreement for SDU type in NR sidelink from 2-bits to 3-bits.

## Issue7: The size of Key ID carried by PDCP header

In the email discussion [1], Rapporteur (CATT) thinks we need to handle the issue of Key ID size. There are two options:

* Option1: RAN2 assume a size for the Key ID, e.g., 16bits, which is following LTE D2D. Send LS to check SA3’s view.
* Option2: RAN2 send LS to SA3 to ask the size of Key ID.

OPPO prefers Option2, since the issue is also related with the content of SA3 Counter with different PDCP SN sizes [5].

**Question 7:** **Regarding to the Key ID size in the PDCP header, which option does company prefer?**

1. **Option 1: Agree as a working assumption that the size of the Key ID is 16bits. Send this to SA3 for further check;**
2. **Option 2: Don’t agree anything in this meeting, just ask SA3 the question on the size of the Key ID;**
3. **Option 3: Don’t agree anything in this meeting, just wait for SA3 progress;**
4. **Other options: Please provide the detail solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Preferentially Option 3; if not achievable, then Option 1. | Note that not only the size of the Key ID, but also sizes of MAC-I, PTK identity and PGK index are needed for us to draw the PDCP PDU format for NR SL. From our SA3 colleague’s feedback, they are discussing these parameters in this meeting. Therefore, we first await SA3 progress, with the hope that they’ll inform us before the PDCP running CR email discussion gets over, and capture the corresponding things (wherever needed) directly in the PDCP running CR (Option 3). If this is not achievable, we can assume the Rel-13 D2D sizes for all above parameters, and capture the related things in the PDCP running CR based on our assumption (especially for the SL PDCP PDU format) (Option 1). In the latter case, we can tell SA3 what we assumed in the LS. From our SA3 delegate’s information, there is big possibility that the Rel-13 D2D mechanism will be reused for the above parameters; so it seems the latter case is not going to result in big problems.  It is improper to leave just a blank for the NR SL PDCP PDU format without capturing anything in the approved PDCP CR, so we anyway need to find a way out to avoid such things happening. |
| OPPO | Option 2 | We think the Q7 and Q10 are linked together. What RAN2 need to know is the detail content of COUNT[0~31] which could consist of bits of PDCP SN and/or HFN and key ID. In the LS to SA3 RAN2 need indicate that the PDCP SN length could be 12bits or 18bits and HFN is aligned between TX side and RX side for unicast and ask SA3 what’s their opinion on the content of COUNT[0~31] including the length of Key ID. |
| Samsung | Option 2 | RAN2 should inform SA3 that SA3’s input is necessary to resolve the issue. |
| ZTE | Option 2 | SA3 should make the final decision of security aspect of issues, rather than RAN2. Thus, RAN2 should check with SA2. |
| LG | Option 2 | We could inform SA3 via an LS in order to align with them on the size of the Key ID. |
| Intel | Option 2 | To us, this seems like an issue which would require SA3 input, so it is better to consult them before making any agreement |
| Nokia | Option 2 | Seems as if we are missing several inputs from SA3. Some might be because SA3 does now know the exact questions we are awaiting answers on. Hence, it is better to send a specific LS. |
| Ericsson | Option 2 with comment | We can send LS to SA3 only if they don’t discuss/conclude in this meeting. |
| vivo | Option 2 | Security design is totally up to SA3. An LS is needed. |
| CATT | Option 2 | If companies cannot agree to re-used the LTE mechanism as a working assumption, to send LS to SA3 may be a best choice. |
| MediaTek | Option 2 |  |
| Qualcomm | Option 2 |  |
| Apple | Option 2 |  |
| Futurewei | Option 2 | It is sensible to ask SA3 on security related issues, if we don’t have sufficient input from them. |

**Voting result:**

**Option 1: 1**

**Option 2: 13**

**Option 3: 1**

Rapporteur's observation:

A clear majority view prefers Option 2. Thus, Rapporteur suggests we can go with Option2 to send LS to check with SA3 view.

Proposal 7: Send LS to SA3 including the issue on the Key ID size in the PDCP header.

## Issue8: The size of MAC-I carried by PDCP header

Similar as the size of Key ID, in the email discussion [1], Rapporteur (CATT) thinks we need to handle the issue of MAC-I size. There are two options:

* Option1: RAN2 assume a size for the MAC-I, e.g., 32bits, which is following LTE D2D. Send LS to check SA3’s view.
* Option2: RAN2 send LS to SA3 to ask the size of MAC-I.

**Question 8:** **Regarding to the MAC-I size in the PDCP header, which option does company prefer?**

1. **Option 1: Agree as a working assumption that the size of the MAC-I is 32bits. Send this to SA3 for further check;**
2. **Option 2: Don’t agree anything in this meeting, just ask SA3 the question on the size of the MAC-I;**
3. **Option 3: Don’t agree anything in this meeting, just wait for SA3 progress;**
4. **Other options: Please provide the detail solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Preferentially Option 3; if not achievable, then Option 1. | See comments for Issue 7. |
| OPPO | Option 2 | RAN2 is not expertise of MAC-I size |
| Samsung | Option 2 | RAN2 should inform SA3 that SA3’s input is necessary to resolve the issue. |
| ZTE | Option 2 |  |
| LG | Option 2 |  |
| Intel | Option 2 |  |
| Nokia | Option 2 |  |
| Ericsson | Option 2 with comment | We can send LS to SA3 only if they don’t discuss/conclude in this meeting. |
| vivo | Option 2 |  |
| CATT | Option 2 |  |
| MediaTek | Option 2 |  |
| Qualcomm | Option 2 |  |
| Apple | Option 2 |  |
| Futurewei | Option 2 | It is sensible to ask SA3 on security related issues, if we don’t have sufficient input from them. |

**Voting result:**

**Option 1: 1**

**Option 2: 13**

**Option 3: 1**

Rapporteur's observation:

A clear majority view prefers Option 2. Thus, Rapporteur suggests we can go with Option2 to send LS to check with SA3 view.

Proposal 8: Send LS to SA3 including the issue on the MAC-I size in the PDCP header.

## Issue9: PDCP SN value when security protection is not used

This issue is raised by OPPO in the email discussion [1].

In solution#12, TR 33.836 says

“If the configuration is not to use any PDCP protection for one-to-one communication user plane bearers, then the UE sets the values of the security information (Key ID and Counter) to zero in the header of the user plane PDCP packets.

For the signalling messages that are not protected, the Key ID and Counter in PDCP format are set to zeros in the header of the PDCP packet.”

Counter is PDCP SN here. But it should be used for PDCP reordering i.e. it should not be zero regardless of security protection. Maybe we should remind SA3 about this.

**Question 9: Does company agree to inform SA3 in the LS that the PDCP SN cannot be always set to zeros if security protection is not used?**

1. **Yes;**
2. **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Maybe No | We think the SA3’s description is only from a security point of view, but the use of PDCP SN for reordering is an independent aspect that may have no impact to SA3 design. To this end, as long as RAN2 take care about this aspect and specify the PDCP SN in a correct way in TS 38.323, there seems to be no other problem. So telling SA3 about this seems to have no additional value. If companies anyway want this to be as precise as possible to their SA3 delegates, maybe they can tell their SA3 delegates respectively. |
| OPPO | Yes | Without PDCP SN, PDCP layer can’t maintain the receiving window. |
| Samsung | Yes | SA3 should be informed about the issue |
| ZTE | Yes |  |
| LG | Yes |  |
| Intel | Yes |  |
| Nokia | Yes |  |
| Ericsson | Yes | We can send LS to SA3 only if they don’t discuss/conclude in this meeting. |
| vivo | Yes |  |
| CATT | Yes |  |
| MediaTek | Yes |  |
| Qualcomm | Yes |  |
| Apple | Yes | There is no harm to remind SA3 about the multi-purpose nature of SN in PDCP in PC5 interface. |
| Futurewei | Yes | It can be beneficial to update SA3 the progress in RAN2, which is different from their understanding. |

**Voting result:**

**Yes: 13**

**No: 1**

Rapporteur's observation:

A clear majority view prefers to send LS including this issue. Thus, Rapporteur suggests we can go with majority view.

Proposal 9: Send LS to inform SA3 that the PDCP SN cannot be always set to zeros if security protection is not used.

## Issue10: Security counter in PDCP header

SA3 COUNT in the Solution #12 in TR 33.836 follows LTE one to one sidelink communication which uses only PDCP SN. For NR SL unicast, PDCP COUNT value which consisting of SN and HFN is maintained between two UEs. So both PDCP SN and HFN can be considered for security counter in SL unicast which is same as NR Uu. Samsung think that this also should be informed to SA3 [8].

**Question 10: Does company agree to inform SA3 in the LS that PDCP SN and HFN are aligned between UEs for NR SL unicast and both can be considered in security counter for NR PC5 as NR Uu?**

1. **Yes;**
2. **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Huawei | Yes | This could be informed to SA3 from a RAN2 perspective, so as to make them take into account. Considering that they might not consider this issue in this meeting, if they later make some modifications by considering our information, we can see whether their changes have potential RAN2 impacts and revise our Spec accordingly (if needed) in future meetings. |
| OPPO | Yes | See comment to Q7 |
| Samsung | Yes | RAN2 should inform SA3 that NR SL unicast follows the principle of NR Uu and is different from LTE D2D and receive SA3’s input on which mechanism between LTE D2D and NR Uu can be applied for NR PC5. |
| ZTE | Yes | Agree with Huawei. |
| LG | Yes | RAN2 should send LS to check SA3’s view on whether HFN part can also be used in security counter, besides PDCP SN. |
| Intel | Yes |  |
| Nokia | Yes |  |
| Ericsson | Yes | We can send LS to SA3 only if they don’t discuss/conclude in this meeting. |
| vivo | Yes |  |
| CATT | Yes |  |
| MediaTek | Yes |  |
| Qualcomm | Yes |  |
| Apple | Yes |  |
| Futurewei | Yes | It can be beneficial to update SA3 the progress in RAN2, which is different from their understanding. |

**Voting result:**

**Yes: 14**

**No: 0**

Rapporteur's observation:

A clear majority view prefers to send LS including this issue. Thus, Rapporteur suggests we can go with majority view.

Proposal 10: Send LS to SA3 including the issue whether HFN together with PDCP SN can be considered in security counter for NR PC5.

# 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.

**Follows as “*potential easy agreement*”:**

**Proposal 1: Capture one Note that it’s up to UE implementation to select HFN for RX\_NEXT as such that initial value of RX\_DELIV should be a positive value.**

**Proposal 5: PDU type for NR sidelink is 2 bits.**

**Proposal 6: Change the previous agreement for SDU type in NR sidelink from 2-bits to 3-bits.**

**Proposal 3: Send LS to SA3 including the issue on LCID usage in the ciphering/integrity algorithms.**

**Proposal 7: Send LS to SA3 including the issue on the Key ID size in the PDCP header.**

**Proposal 8: Send LS to SA3 including the issue on the MAC-I size in the PDCP header.**

**Proposal 9: Send LS to inform SA3 that the PDCP SN cannot be always set to zeros if security protection is not used.**

**Proposal 10: Send LS to SA3 including the issue whether HFN together with PDCP SN can be considered in security counter for NR PC5.**

**Follow proposal is related with sending SA3 LS, but no clear majority view on this issue. Suggest we can further discuss it during the online discussion.**

**Proposal 2: Working assumption: The PDCP SN size of Direct Communication Request message is 18 bits. Send LS to SA3 to further check.**

**Follows as “*need further discussion*”, suggest we can postpone this discussion into a long email discussion or to the next meeting.**

**Proposal 4: Suggest RAN2 to further discuss whether PDCP re-establishment and status report is supported or not, considering the security impact.**

# Reference

1. R2-2000214 Summary of Email discussion [108#102][V2X] Remaining issues on PDCP CATT discussion Rel-16 5G\_V2X\_NRSL-Core
2. R2-2002017 Summary of PDCP remaining issues on NR V2X CATT discussion Rel-16 5G\_V2X\_NRSL-Core
3. R2-2001308, Initialization of HFNs of RX\_DELIV and RX\_NEXT, Futurewei
4. R2-2001499, Initial Value of RX\_DELIV and RX\_NEXT, Samsung
5. R2-2000201, Discussion on PDCP open issues, OPPO
6. R2-2000945, On PDCP re-establishment, Ericsson
7. R2-2001544, PDCU SDU Type Length, Qualcomm Finland RFFE Oy
8. R2-2001340, Security impact in SL PDCP, Samsung Electronics Co., Ltd