3GPP TSG-RAN WG2 Meeting #110-e R2-‎2005962‎

Electronic, June 1 – June 12 2020‎

Source: CATT (rapporteur)

Title: Summary of [706][V2X] 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 #706 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.

* [AT110-e][706][V2X] PDCP issues (CATT)

Discuss and conclude PDCP issues in R2-2005724 (in R2-2005962).

Deadline is 6/8 10:00am (UTC).

# Discussion

## Issues on PDCP PDU format

### Issue 1: MAC-I for SL SRB

In SA3 TS 33.536 [2], it is mentioned the PC5 unicast link shall support activation or deactivation of security based on the security policy similar to Uu‎. The security policy indicates the following:‎

* ‎Signalling integrity protection: REQUIRED/PREFERRED/NOT NEEDED
* ‎Signalling confidentiality protection: REQUIRED/PREFERRED/NOT NEEDED
* ‎User plane integrity protection: REQUIRED/PREFERRED/NOT NEEDED
* ‎User plane confidentiality protection: REQUIRED/PREFERRED/NOT NEEDED

According to SA3 TS 33.536, except for SL SRB0, the integrity and confidentiality protection for SL SRBs can be activated or deactivated.

In current PDCP spec, the MAC-I field is always present for SL SRB1, SRB2 and SRB3. Thus, it’s necessary to discuss how to handle the MAC-I field when the integrity protection for SL SRBs is deactivated. There are two options as following:

* Option 1: To follow Uu SRBs, if integrity protection is not configured for SL SRB1, SRB2 and SRB3, the MAC-I field is still present but should be padded with padding bits set to 0.
* Option 2: To follow SL DRBs, the MAC-I field is present only when the DRB is configured with integrity protection.

Thus, rapporteur‎ encourage companies to provide the views on this issue, i.e., if integrity protection is not configured for SL SRB1, SRB2 and SRB3, whether the MAC-I field is still present or absent based on the above two options.

**Question 1: If integrity protection is not configured for SL SRB1, SRB2 and SRB3, ‎which following option does company prefer for MAC-I field?**

* **Option 1: To follow Uu SRBs, if integrity protection is not configured for SL SRB1, SRB2 and SRB3, the MAC-I field is still present but should be padded with padding bits set to 0.**
* **Option 2: To follow SL DRBs, the MAC-I field is present only when the DRB is configured with integrity protection.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any**  |
| Samsung | Option 2 | BTW, integrity protection is always applied to Uu SRBs except SRB0 so MAC-I field is always present. |
| Ericsson | Option 2 |  |
| OPPO | Option 2 |  |
| ZTE | Option 1 | Keep previous agreement for SL SRBs for MAC-I field and follow Uu SRBs handling. |
| Futurewei | Option 2 | SRB1, SRB2 and SRB3 should always have integrity protection configured, given the agreement that

|  |  |
| --- | --- |
| 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 |

 |
| vivo | Option 1 | For SL SRB 1/2/3, integrity protection, i.e. MAC-I, is needed and configured with high probability. |
| Intel | Option 2 | Slight preference to have uniform SL design |
| CATT | Option 2 | Agree with Samsung, the Uu SRBs are always applied integrity protection. But for SL SRBs, the integrity protection can be actived/deactived, which is different with Uu SRBs. Thus, Option 2 is preferred. |
| Qualcomm | Option 1 | Follow Uu design |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Issue 2: PDCP SN size in SL groupcast and ‎broadcast ‎

In [4], the issue of PDCP SN size in SL groupcast and ‎broadcast was discussed. There are several observations mentioned in [4] as following:

* Observation 1: All the given date rates under different NR V2X scenarios in TS 22.186 could be ‎satisfied when PDCP SN size is 12bits, and having PDCP SN size as 18 bit seems an over design. ‎
* Observation 2: The 6-bit RLC SN length was agreed for NR SL groupcast and broadcast in RAN2 ‎‎#107, based on the companies’ views that the NR SL groupcast and broadcast are not expected to ‎be with ultra-high data requirements. Thus PDCP SN with 18 bits does not match the RLC SN with ‎‎6 bits. ‎
* Observation 3: The motivation to use 18 bit PDCP SN size for the support of security related ‎mechanism (i.e. COUNTER operation) for NR SL groupcast and broadcast is invalid as well, as ‎SA3 concluded that no security mechanism is supported for NR SL groupcast and broadcast.‎

Thus, the previous agreement on a specified 18 bit PDCP SN size in SL groupcast and broadcast was proposed to be revised in [4] based on following options:

* ‎‎Option 1: Change PDCP SN size in SL groupcast and broadcast from 18bits to 12bits.‎
* ‎Option 2: Introduce a PDCP PDU format with 12 bit SN in SL groupcast and broadcast, and ‎use a bit in PDCP header to indicate whether the PDCP SN size is 18 bits or 12 bits.‎

Rapporteur‎ thinks we can first discuss whether 12 bit SN is necessary to be introduced for SL groupcast and broadcast based on the observations in [4]. If majority view is yes, we can further discuss the solutions. If majority view is no, we keep the current PDCP PDU formats for NR SL groupcast and broadcast.

**Question 2: Does company agree to introduce 12 bit SN for SL groupcast and broadcast?**

* **Yes;**
* **No, i.e., keep 18bits PDCP SN size for SL groupcast and broadcast as current PDCP spec.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)****(Yes/No)** | **Comments if any**  |
| Samsung | Yes |  |
| Ericsson | No with comment | We don’t see this as critical issue, so no strong need to revert our previous agreement. We are fine to follow majority view.  |
| OPPO | No | Agree with Ericsson |
| Huawei, HiSilicon | Yes | As elaborated in [4], we justify that the 18 bit PDCP SN length for Gcast and Bcast is an over-design, with the specific reason that the high data rate is not usually required for Gcast and Bcast, and more importantly cannot be really achieved with the restriction of 6-bit RLC SN length. More importantly, from a UE vendor point of view, 18-bit PDCP SN can lead to big complication of UE implementation, especially for the memory consumption needed for PDCP reordering during Bcast/Gcast reception.The problem comes from the “multi-point to point” nature of SL Gcast/Bcast, since a UE has to receive all UEs in proximity for their Gcast/Bcast services, and in typical cases of V2X, the number of the UEs in proximity can be several hundreds. For example, in urban area (e.g. Beijing, Shanghai, etc.) several hundreds of vehicles nearby may need to be received in the communication range of V2X (e.g. radius of about several hundred meters).We think to change 18 bit to 12 bit is just a minor spec change, which may need nearly no difficulty for CR implementation and no more time for further discussion. Especially in the case that there is UE vendor has strong concern on it, it seems necessary to agree on this change.  |
| ZTE | No | 18 bits PDCP SN is workable, no need to revert previous agreement. |
| Futurewei | Yes | Huawei pointed 18 bit SN is not needed and can impose challenge in UE implementation. |
| vivo | Yes | We tend to agree with the above observations. This change is small but it.can aovid consuming UE memory for PDCP reordering. |
| Intel | No | We see Huawei’s point, but at the same time we are not sure if reverting the earlier agreement is really essential either. |
| CATT | No strong view | We understand Huawei’s observations. We can follow the majority view. |
| Qualcomm | No | Agree with above comments to retain current agreement  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 3: If the answer of Q2 is yes, ‎which following option does company prefer to introduce the 12 bit SN for SL groupcast and broadcast?**

* **Option 1: Change PDCP SN size in SL groupcast and broadcast from 18bits to 12bits.‎**
* **‎Option 2: Introduce a PDCP PDU format with 12 bit SN in SL groupcast and broadcast, and ‎use a bit in PDCP header to indicate whether the PDCP SN size is 18 bits or 12 bits.‎**
* **Option 3: Others.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any**  |
| Samsung | Option 1 | We prefer to define one PDCP PDU format for SL groupcast and broadcast. |
| Futurewei | Option 1 |  |
| Huawei, HiSilicon | Option 1 | Very simple change w/o need of any further complicated discussion and w/o nearly any Spec change. |
| vivo | Option 1 |  |
| CATT | Option 1 | If majority view is yes in Q2, we prefer Option 1, which is a simply can clear way in the spec. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issues on security policy related aspects

### Issue 1: ‎Activation/deactivation of the security per SL unicast link

In SA3 TS 33.536 [2], the confidentiality and integrity protection is activated/deactivated per PC5 unicast link for both sidelink SRBs and DRBs‎. The activation/deactivation of signalling and user plane security policy procedures are defined in SA3 TS 33.536 using PC5-S signalings. During the online discussion on RRC during this meeting, it’s agreed as a working assumption that all security configurations on whether to enable/configure ciphering and integrity protection are exchanged in the upper layers via PC5-S signalling and then instructed to the AS, for SL-SRB carrying PC5 RRC signalling and for SL-DRBs.

Thus, how to capture activation/deactivation of the security for PC5 unicast link in AS layer is necessary to be discussed. There are two options.

* Option 1: Capture the activation/deactivation of the security for PC5 unicast link in 38.331;
* Option 2: Capture the activation/deactivation of the security for PC5 unicast link in 38.323.

For Option 1, upon RRC layer receives the security activation indication for a PC5 unicast link from V2X layer, the RRC layer should indicate the security activation to the PDCP layer for each SLRB which belongs to the PC5 unicast link. Then PDCP layer should apply the security function to all PDCP PDUs for SL-SRB and for SL-DRBs.

For Option 2, the V2X layer can directly indicate PDCP layer the security activation for a PC5 unicast link associated with the source and destination ID pair. Then the PDCP layer should apply the security function to all PDCP PDUs for SL-SRB and for SL-DRBs which belong to the source and destination ID pair.

Rapporteur‎ thinks we can firstly discuss which spec is preferred to capture the activation/deactivation of the security. Then we can further discuss the detail text which should be captured in the spec.

**Question 4: Which following option does company prefer to capture activation/deactivation of the security for PC5 unicast link in AS layer‎?**

* **Option 1: Capture the activation/deactivation of the security for PC5 unicast link in 38.331.**
* **Option 2: Capture the activation/deactivation of the security for PC5 unicast link in 38.323.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any**  |
| Samsung | Option 1 | According to TS 33.536, PC5-RRC message is used to configure AS security for DRB.“When establishing or re-configuring the user plane bearer, the initiating UEs shall ensure the configuration of confidentiality and integrity protection in the PC5-RRC message matches the agreed UP security policies for traffic that will be sent on the bearer. The confidentiality and/or integrity protection algorithms are same as those selected for protecting the signalling bearers if confidentiality and/or integrity protection are required for both signalling and user plane.”We think that the security activation/deactivation for SRB can be known to RRC by V2X layer. |
| Ericsson | Option 1 | To keep a clean function split between protocol layers, it should be the RRC entity which configures other protocol layers e.g. PDCP.  |
| OPPO | Option 2 | The activation/deactivation is done via V2X layer instead of RRC layer and both integrity and confidential protection is done in PDCP layer for both SRB and DRB. So the modelling is different from Uu by nature. We think capture security related aspects in PDCP layer is sufficient |
| ZTE | Option 1 | AS security for PC5 unicast link shall be captured in RRC specification. |
| Futurewei | Option 1 | A SLRB’s security is configurated/activated when it is established. SLRB is established/released by RRC, and not all SLRBs are established/released at the same time. The establishing and releasing a SLRB is transparent to V2X layer. |
| Huawei, HiSilicon | Option 2 | We see no problem to imitate LTE SL unicast for D2D, where the logic is the same that the PC5-S exchanges the security related configurations, and directly tells them to the UE’s PDCP. If anyway companies want to make it specified in RRC, we need very specific TP on how to do that (as till now, no such proposal concrete enough is on the table). |
| vivo | Option 1/2 | According to online agreements:*All security configurations on whether to enable/configure ciphering and integrity protection are exchanged in the upper layers via PC5-S signalling and then instructed to the AS, for SL-SRB carrying PC5 RRC signalling and for SL-DRBs.**For both SL-SRB carrying PC5 RRC signaling and SL-DRBs, no signaling exchange or operation in RRC is needed for the security related configurations to enable/configure ciphering and/or integrity protection.*We agree security activation/deactivation should be known by RRC and configured to PDCP. And clarification in PDCP may also be needed. |
| Intel | Option 1 | We think it would be better for the AS layer to control this aspec,t similar to E///’s view. |
| CATT | Option 2 | We initially thinking is to capture the activation/deactivation of the security for PC5 unicast link in 38.323‎, which is simply way in the spec. But if most companies’ thinking is better to capture this security procedure in 38.331, we are fine to follow the majority view. |
| Qualcomm | Option 1 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 5: If the answer of Q4 is Option 1, companies are invited to provide the detail text in RRC spec and maybe also involved PDCP spec for the security activation/deactivation.**

|  |  |
| --- | --- |
| **Company** | **Provided the detail context in RRC (and maybe PDCP) spec** |
| Samsung | In RRC specification, under subclause 5.8.9.1 some texts similar to 5.3.1.2 AS security and 4.2.2 Signalling radio bearers can be specified. For example: 5.8.9.1.X AS SecurityAS security comprises of the integrity protection and ciphering of PC5 signaling (SL-SRB2, SL-SRB3) and user data (DRBs).Once AS security is activated by upper layers, all PC5-S messages on SL-SRB2 and PC5-RRC messages on SL-SRB3 are integrity protected and ciphered by PDCP.PC5-RRC handles the configuration of the AS security parameters which are same as those selected for the signaling bearers, if integrity protection and/or ciphering is activated by upper layers.For PDCP specification, in the section 5.8 Ciphering and deciphering:*The ciphering function is activated for SL SRBs and SL DRBs for a PC5 unicast link by upper layers TS 38.331. When security is activated, the ciphering function shall be applied to all PDCP PDUs in the SL SRBs and SL DRBs which belong to the PC5 unicast link.*For PDCP specification, in the section 5.9 Integrity protection and verification:*The integrity function is activated for SL SRBs and SL DRBs for a PC5 unicast link by upper layers TS 38.331. When security is activated, the integrity protection function shall be applied to all PDUs including and subsequent to the PDU in the SL SRBs and SL DRBs which belong to the PC5 unicast link.* |
| ZTE | In RRC specification, under subclause 5.3.1.2 some texts similar to AS security for Uu can be specified, for example:For unicast of NR sidelink communication, AS security comprises of the integrity protection and ciphering of PC5 RRC signalling (SL-SRBs) and user data (SL-DRBs). The ciphering and integrity protection algorithms and the key (KNPR-sess ID) for a PC5 unicast link are exchanged by PC5-S messages (i.e. Direct Security Mode Command and Direct Security Mode Complete) as specified in TS 33.536 [xx]. NOTE 2: All SL-DRBs related to the same PC5 unicast link have the same enable/disable setting for ciphering and the same enable/disable setting for integrity protection. |
| Futurewei | Reusing Uu approach, as suggested Samsung, is a good baseline. |
| Huawei, HiSilicon | If RAN2 anyway agree to write something in TS 38.331, the below TP is suggested, by incorporating the TPs provided by companies above:*For unicast of NR Sidelink communication, AS security comprises of integrity protection and ciphering of PC5 signaling (SL-SRB2 and SL-SRB3) and user data (DRBs). The ciphering and integrity protection algorithms and parameters for a PC5 unicast link are exchanged by PC5-S messages in the upper layers as specified in TS 33.536 [xx], and apply to the corresponding PC5 RRC connection in the AS. Once AS security is activated for a PC5 unicast link in the upper layers as specified in TS 33.536 [xx], all messages on SL-SRB2 and SL-SRB3 and/or user data on SL-DRBs of the corresponding PC5 RRC connection are integrity protected and/or ciphered by the PDCP.* *NOTE X: All SL-DRBs related to the same PC5 RRC connection have the same activation/deactivation setting for ciphering and the same activation/deactivation setting for integrity protection as in TS 33.536 [xx].*In general, RRC spec does not need to touch the details on the security mechanism and parameters, which, in PC5, are all designed by SA3. What we only need to do is to refer to the SA3 Spec in upper layers, in order to avoid any potential misalignment across Specs and/or descriptions not exact enough in RRC. |
| Intel | We are fine with Huawei’s proposed text  |
| CATT | Share the same view with Huawei for 38.331. For 38.323, we can accept Samsung’s suggestion. The detail wording can be further discussed during the CR discussion. |
| Qualcomm | Agree with above recommendations to use the Uu description as a baseline, with the below suggestionsFor unicast of NR sidelink communication, AS security comprises of the integrity protection and ciphering of PC5 RRC signalling (SL-SRBs) and user data (SL-DRBs). The ciphering and integrity protection algorithms and the key (KNPR-sess ID) for a PC5 unicast link are negotiated ~~exchanged~~ by PC5-S messages (i.e. Direct Security Mode Command and Direct Security Mode Complete) as specified in TS 33.536 [xx]. NOTE 2: All SL-DRBs related to the same PC5 unicast link have the same enable/disable setting for ciphering and the same enable/disable setting for integrity protection, excluding the Direct Security Mode Command, per TS 33.536 [xx]. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Question 6: If the answer of Q4 is Option 2, does company agree to capture the following text in the PDCP spec for the security activation/deactivation?**

In the section 5.8 Ciphering and deciphering:

*For NR sidelink communication, the ciphering function is activated for SL SRBs and SL DRBs, separately, for a PC5 unicast link by upper layers TS 33.536 [14]. When the ciphering function is activated for SL SRBs or SL DRBs for a PC5 unicast link, the ciphering function shall be applied to all PDCP PDUs in the SL SRBs or SL DRBs which belong to the PC5 unicast link.*

In the section 5.9 Integrity protection and verification:

*For NR sidelink communication, the integrity protection function is activated for SL SRBs and SL DRBs, separately, for a PC5 unicast link by upper layers TS 33.536 [14]. When the integrity protection function is activated for SL SRBs or SL DRBs for a PC5 unicast link, the integrity protection function shall be applied to all PDUs including and subsequent to the PDU in the SL SRBs or SL DRBs which belong to the PC5 unicast link.*

|  |  |
| --- | --- |
| **Company** | **Agree or updates the above text, if any**  |
| OPPO | The intention is correct. But both ciphering and integrity protection are not applied to all PDCP PDU. At the beginning of section 5.8 and 5.9 there is some limitation on which kind of PDCP PDU is applied and should be reflected here also e.g. both are not applied for PDCP control PDU. |
| Futurewei | No, it is not clear what does it mean by “*the ciphering function is activated for SL SRBs and SL DRBs, separately”* and *“the integrity protection function is activated for SL SRBs and SL DRBs, separately”*? How can V2X layer take separate action on a particular SLRB?  |
| vivo | There are some special security operation for Direct Security Mode Command message, i.e. only with integrity protection and without ciphering. Hence we propose:*For NR sidelink communication, the ciphering function is activated for SL SRBs and SL DRBs, separately, for a PC5 unicast link by upper layers TS 33.536 [14]. When the ciphering function is activated for SL SRBs or SL DRBs for a PC5 unicast link, the ciphering function shall be applied to all PDCP PDUs except for* Direct Security Mode Command *in the SL SRBs or SL DRBs which belong to the PC5 unicast link.*  |
| CATT | For OPPO’s comments, we think the limitation in the beginning of section 5.8 and 5.9 are also applied to the SL. In Uu downlink and uplink, the related text also mentions “the ciphering function shall be applied to all PDCP Data PDUs indicated by upper layers TS 38.331 [3] for the downlink and the uplink, respectively.”.For Futurewei’s comments, there is an explicit procedures for the handling of signalling security policy proceeds and the handling of the user plane security policy proceeds in the section 5.3.3.1.4.2.3 in TS 33.536‎.For vivo’s comments, we think the issue for Direct Security Mode Command message belongs to SA3 V2X layer. Based on the security policy for signalling, the integrity protection of Direct Security Mode Command message also can be deactived. Thus, we think in PDCP spec, just reference to TS 33.536 is sufficient. |
| Qualcomm | Suggestions to the proposed text: In the section 5.8 Ciphering and deciphering:*For NR sidelink communication, the ciphering function is activated for SL SRBs and SL DRBs~~, separately~~, for a PC5 unicast link by upper layers, as described in TS 33.536 [14]. When the ciphering function is activated for SL SRBs or SL DRBs for a PC5 unicast link, the ciphering function shall be applied to all PDCP PDUs in the SL SRBs or SL DRBs which belong to the PC5 unicast link, in accordance TS 33.536.*In the section 5.9 Integrity protection and verification:*For NR sidelink communication, the integrity protection function is activated for SL SRBs and SL DRBs~~, separately~~, for a PC5 unicast link by upper layers, as described in TS 33.536 [14]. When the integrity protection function is activated for SL SRBs or SL DRBs for a PC5 unicast link, the integrity protection function shall be applied to ~~all~~ PDCP PDUs including and subsequent to the PDU in the SL SRBs or SL DRBs which belong to the PC5 unicast link, in accordance TS 33.536.* |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### Issue 2: ‎‎PDCP re-establishment trigger

Whether the PDCP re-establishment trigger is captured in RRC or V2X layer has been discussed during the last meeting. ‎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 re-keying procedure which is in V2X layer but not ‎RRC layer. In current SA3 and CT1 spec, there is no PDCP re-establishment trigger condition due to ‎re-keying operation. Thus, according to the companies contribution [3][7], Rapporteur suggests to send LS to SA3 and CT1 to capture the PDCP re-establishment trigger due to ‎re-keying operation in V2X layer.‎

**Question 7: Does company agree PDCP re-establishment trigger should be captured in V2X layer?**

* **Yes;**
* **No, please give how to capture the PDCP re-establishment trigger.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)****(Yes/No)** | **Comments if any**  |
| Samsung | No | As for AS security, re-keying can be informed to PC5-RRC by V2X layer. Then PDCP re-establishment can be triggered by PC5-RRC. |
| Ericsson | No | To keep a clean function split between protocol layers, it should be the RRC entity which configures other protocol layers e.g. PDCP. Thus, it should be V2X layer indicates PC5-RRC and PC5-RRC triggers PDCP re-establishment.  |
| OPPO | Yes | Although it looks like a matter of taste, we don’t understand why RRC layer should be broker here. And even RRC could be broker here, V2X layer still need trigger lower layer which is RRC i.e. nothing is saved in V2X layer. |
| ZTE | No | Agree with Samsung and Ericsson |
| Futurewei | No | PDCP reestablishment should be triggered by PC5-RRC: * it needs to be done together with RLC reestablishment and resetting MAC part related to the involved SLRB;
* based on the rekeying procedure specified in TS 33.536, PDCP reestablishment of SRB1 may need to be done at different time moments from other SLRBs.
 |
| Huawei, HiSilicon | Yes | Anyway, the root cause for PDCP reestablishment comes from V2X layer, i.e. rekeying. Please do note that UE’s PC5 RRC layer *cannot autonomously* decide when to do PDCP reestablishment, and this is completely different from Uu, where UE’s RRC layer can determine that via the reception of the PDCP reestablishment indication from RRC signaling (no such indication in PC5).  |
| vivo | No | It may be strange for V2X layer to trigger each PDCP entities re-establishment directly, e.g. how V2X layer knows the number of PDCP entities of this link. Hence it is more natural that V2X layer indicates PC5-RRC and PC5-RRC triggers PDCP re-establishment. |
| Intel | No | PC5-RRC can be used to trigger the PDCP re-establishment. Once the rekeying procedure is completed, we think the V2X layer or the PDCP layer itself (since the key ID is carried in the PDCP header), could inform the RRC which could suggest the PDCP entity to re-establish for a clean approach of AS layer control.  |
| CATT | Yes | We think the main cause of PDCP reestablishment is from re-keying operation in V2X layer. Even though the PDCP reestablishment trigger is capture in RRC layer, how RRC layer knows when the re-keying operation happen. |
| Qualcomm | No |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 8: If the answer of Q7 is yes, does company agree to send LS to SA3 and CT1 to ask them to capture the PDCP re-establishment trigger due to ‎re-keying operation in V2X layer‎?**

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

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)****(Yes/No)** | **Comments if any**  |
| OPPO | Yes |  |
| CATT | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

In SA3 reply LS [8], ‎ the re-keying procedure is per PC5 unicast link‎, which means PDCP re-establishment trigger is per PC5 unicast link‎. For the issue how to capture PDCP re-establishment trigger for PC5 unicast link in AS layer, which is similar as discussed in above issue 1 in Section 2.2, there are also following two options.

* Option 1: Capture the PDCP re-establishment trigger for PC5 unicast link in 38.331;
* Option 2: Capture the PDCP re-establishment trigger for PC5 unicast link in 38.323.

This issue has also been discussed during the email discussion#959. Some companies also prefer Option 2. Thus, the current PDCP running CR already capture a NOTE as follows to clarify the PDCP re-establishment trigger operation.

*Upper layers request reestablishment of transmitting or receiving PDCP entity for PC5 interface as specified in TS 33.536 [14] and TS 24.587‎ [xx].*

However, some companies still have some concerns on Option 2. Thus, Rapporteur‎ thinks we can firstly discuss which spec is preferred to capture the PDCP re-establishment trigger for PC5 unicast link. Then we can further discuss the detail text which should be captured in the spec.

**Question 9: Which following option does company prefer to capture the PDCP re-establishment trigger for PC5 unicast link in AS layer‎?**

* **Option 1: Capture the PDCP re-establishment trigger for PC5 unicast link in 38.331.**
* **Option 2: Capture the PDCP re-establishment trigger‎ for PC5 unicast link in 38.323.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any**  |
| Samsung | Option 1 | We prefer to the same modeling for issue 1 and issue 2 of 2.2. So PC5 RRC can trigger PDCP reestablishment. |
| Ericsson | Option 1 |  |
| OPPO | Option 2 |  |
| ZTE | Option 1 | Some related text specified in RRC specification may be better |
| Futurewei | Option 1 | It is not a correct understanding from the rapporteur that “the re-keying procedure is per PC5 unicast link‎, which means PDCP re-establishment trigger is per PC5 unicast link”. PDCP re-establishment is specified per PDCP entity, or SLRB, as in Section 5.1.2 of TS 38.323.It is not clear if PDCP re-establishment is needed for SL SRB0, and it is possible that SL SRB1 needs to be re-established at different time moments from SL SRB2/3 and SL DRBs. |
| Huawei, HiSilicon | Option 2 | Same as Question 4, if anyway companies want to make it in RRC, we need very specific TP on how to do that (as till now, no such solution is on the table).Specifically, if in RRC, it needs to be something like “if xyz happens, then reestablish PDCP”. One may need to specific what such “xyz” actually is. |
| vivo | Option 1 |  |
| Intel | Option 1 |  |
| CATT | Option 2 | Same as Q4. We are also fine to follow the majority view. |
| Qualcomm | Option 1 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 10: If the answer of Q9 is Option 1, companies are invited to provide the detail text in RRC spec and maybe also involved PDCP spec for the PDCP re-establishment trigger.**

|  |  |
| --- | --- |
| **Company** | **Provided the detail context in RRC (and maybe PDCP) spec** |
| Samsung | In RRC specification, under subclause 5.8.9.1 a new subclause AS security can be specified as an example:5.8.9.1.X AS SecurityThe UE shall reestablish PDCP for PC5 unicast link if re-keying is informed by upper layers as specified in TS 33.536 and TS 24.587.  |
| Futurewei | A general format can be “if abc is indicated by the upper layer, the RRC shall xyz”. For example, for UE-1 at step 4a of rekeying procedure specified in TS 33.536 – If the reception of “Direct Security Mode Command” is indicated by the upper layer, UE shall* for each *slrb-PC5-ConfigIndex-r16* value included in the *slrb-ConfigToAddModList-r16* that is part of the current UE configuration,
	+ re-establish the PDCP entity of this SRB as specified in TS 38.323;
 |
| Huawei, HiSilicon | If anyway RAN2 agree to speechify something in RRC, making the PC5 RRC trigger PC5 PDCP reestablishment, RAN2 may need to be very careful on selecting a precise and correct moment for the UE to apply the new key and thus reestablish the PC5 PDCP entity. Particularly, two aspects may need to be considered in conjunction with the below SA3 figure:* SA3 is clearer than us RAN2 about the exact moment/condition when the two UEs need to apply the new key (which also impacts when to re-establish PC5 PDCP). **Hence, is it helpful and safer that we rely on some forms of indications provided from the upper layers and decided by SA3/CT1, so AS (PC5 RRC) simply follows/refers to that indication and initiates PDCP reestablishment with new key application accordingly?** Anyway, it is SA3 that designed the whole (complicated) procedure, and they should be at the best position to decide the precise moment for when to apply the new key. Hence, this way can avoid the risk that RAN2 ourselves concludes a specific moment/condition that is however not aligned with SA3 intention. If we go for this way, we just need to inform SA3/CT1 and asking them to work on possible impacts in their Specs for the indication; no open question is needed.
* The *delayed new key application* for TX in UE\_2. During pre-meeting email discussion, nobody defied the need of UE\_2 to use the new key for TX, later than for RX. If RAN2 agree to make RRC initiate PDCP reestablishment but don’t agree distinction of TX/RX PDCP entity, perhaps we need some forms of clarification (perhaps in NOTE) on the likeliness of such “delayed” new key application for TX. **As this is related to UP operation, is it helpful that we make some clarifications in PDCP, e.g. a NOTE like “UE determines when to apply the new key for TX and for RX as per TS 33.536 (i.e. this figure)”?** Anyway, the specific moment for UE1/2 to apply new key for TX and for RX is also given by this figure by SA3, so perhaps the safest way is also to point to this figure, instead of determining it by RAN2 ourselves?

Note that, if RAN2 agree to go for RRC, we are open to hear proposals from companies on RRC impacts, as long as the proposals are easy for convergence and work.  |
| Intel | We prefer to keep it simple in RRC and simply refer to SA specs for the detailed procedure as proposed by Samsung. |
| CATT | Share the same view as Huawei. |
| Qualcomm | Agree with Intel |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Question 11: If the answer of Q9 is Option 2, does company agree to capture the following text in the PDCP spec for the PDCP re-establishment trigger?**

In the section ‎5.1.2‎ PDCP entity re-establishment:

*NOTE: Upper layers request reestablishment of transmitting or receiving PDCP entity for PC5 interface as specified in TS 33.536 [14] and TS 24.587‎ [xx].*

|  |  |
| --- | --- |
| **Company** | **Agree or updates the above text, if any**  |
| OPPO | Yes except for the wording “or” between transmitting and receiving PDCP entity. We think re-establishment of TX and RX PDCP entity should be done at same time hence it should be replaced by “and” |
| Futurewei | No, the time of PDCP reestablishment needs to be specified clearly in TS 33.536 and TS 24.587 –* for UE-1, it is at step 4a of rekeying procedure for all SLRBs;
* for UE-2, it is at step 3a for all SL SRB2/3 and SL DRBs, and at step 4b for SL SRB1.
 |
| Huawei, HiSilicon | As above, we need to find some ways to clarify the potential *delayed* new key application for TX PDCP entity, than the RX, if not this NOTE.  |
| CATT | We think the exact time for rekeying procedure is captured in TS 33.536 and TS 24.587. The exact time can be different between the peer UEs. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Issue on PDCP status report

In the last RAN2 meeting, it’s agreed that status report for SL AM DRB is supported for SL unicast. In Uu, for AM DRBs, whether to send a PDCP status report in the uplink‎ is configured per DRB by network. Thus, the PDCP status report is optional supported in Uu interface. We suggest RAN2 to discuss whether the PDCP status report is also optional supported in PC5 interface and if yes, how to configure the status report for SL DRB.

To follow the Uu princple is preferred in [3], i.e., the PDCP status report is also optional supported per SL DRB in PC5 interface. It’s proposed whether the status report is required can be configured by NW or pre-configured to Tx UE, then the Tx UE configures whether the status report is required to Rx UE.

However, always triggering PDCP status report is preferred in [9] and selective retransmission will have better performance. Thus, it’s proposed for SL AM DRBs, a PDCP status report can be triggered without *statusReportRequired* ‎configuration.‎

Rapporteur suggests to discuss whether the PDCP status report is triggered by *statusReportRequired* configuration.

**Question 12: Does company agree the PDCP status report is triggered by *statusReportRequired* ‎configuration?**

* **Yes;**
* **No, i.e., PDCP status report is always enabled for SL AM DRBs.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)****(Yes/No)** | **Comments if any**  |
| Samsung | No | Unlike Uu, the PDCP status report can be always triggered upon PDCP re-establishment.  |
| Ericsson | No with comment | It seems a cleaner solution to trigger PDCP status report once re-establishing PDCP. On the other hand, it depends on whether UE is always capable of selective retransmission.  |
| OPPO | Yes | Not sure why do we deviate from principle over Uu |
| ZTE | No | It is straightforward that PDCP SR is triggered when re-establishing PDCP, otherwise UE may be required for some other capability. |
| Futurewei | No | It should be clarified that this question is about optional configuring PDCP status report upon PDCP reestablishment, not about its being “optionally supported” – it is mandatory for UE to support.As it is already supported by UE, it is not clear why not taking advantage of it to enable selective retransmission.  |
| vivo | No | PDCP status report is more efficient for retransmission triggered by PDCP re-establishment. If mandatory supported by V2X UE, it has better performance. |
| Intel | No strong view | We can follow majority view on this. |
| CATT | No strong view | We initial thinking is to follow Uu behavior. But if most companies prefer that PDCP status report is always enabled for SL AM DRBs, we can follow the majority view. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 13: If the answer of Q12 is yes, does company agree the following procedure for PDCP status report triggerring by *statusReportRequired* ‎configuration?**

* **For CONNECTED UE, whether the status report is required can be configured per SL DRB by RRC dedicated signaling to the Tx UE, then the Tx ‎UE configures whether the status report is required per SL DRB to the Rx UE using PC5 RRC signaling.‎**
* **For IDLE/INACTIVE or OOC UE, whether the status report is required can be configured per SL DRB by SIB or pre-configuration to the Tx UE, then the Tx ‎UE configures whether the status report is required per SL DRB to the Rx UE using PC5 RRC signaling.‎**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)****(Agree or not)** | **Comments if any**  |
| OPPO | Yes |  |
| CATT | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Discard timer

The issue on discard timer was discussed in [9]. In current 38.331, there are separate IEs, *discardTimer*/*discardTimerExt* and *sl-DiscardTimer* to be ‎configured for Uu DRB and SL DRB, respectively. So it’s proposed to add some clarifications in subclause 7.3 in 38.323. ‎There are two following options are proposed to address this issue in [9].

* Option 1: the proposed text in subclause 7.3 in TS 38.323 is as follows.‎

*a) discardTimer*

This timer is configured only for DRBs. The duration of the timer is configured by upper layers TS 38.331[3] with *discardTimer/discardTimerExt* for Uu interface and *sl-DiscardTimer* for PC5 interface. In the transmitter, a new timer is started upon reception of an SDU from upper layer.

* Option 2: to modify the description *sl-DiscardTimer* in 6.3.5 in TS 38.331 as follows.‎

*sl-DiscardTimer*

Value in ms of *~~sl-~~discardTimer* specified in TS 38.323 [5]. Value ms50 corresponds to 50 ms, value ms100 corresponds to 100 ms and so on.

Rapporteur thinks this issue is valid and can be further discussed.

**Question 14: Does company agree the above issue on discard timer is valid?**

* **Yes;**
* **No, i.e., keep the current RRC and PDCP specs as they are.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)****(Yes/No)** | **Comments if any**  |
| Samsung | Yes | The IE should be aligned in both specifications. At least there is no *sl-discardTimer* in 38.323. |
| Ericsson | Yes |  |
| OPPO | Yes |  |
| ZTE | Yes |  |
| Futurewei | Yes |  |
| vivo | Yes |  |
| Intel | Yes |  |
| CATT | Yes |  |
| Qualcomm | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Question 15: If the answer of Q14 is yes, which following option does company prefer to address the above issue on discard timer‎?**

* **Option 1: add some clarifications in subclause 7.3 of TS 38.323.**

*a) discardTimer*

This timer is configured only for DRBs. The duration of the timer is configured by upper layers TS 38.331[3] with *discardTimer/discardTimerExt* for Uu interface and *sl-DiscardTimer* for PC5 interface. In the transmitter, a new timer is started upon reception of an SDU from upper layer.

* **Option 2: to modify the description *sl-DiscardTimer* in subclause 6.3.5 of TS 38.331.**

*sl-DiscardTimer*

Value in ms of *~~sl-~~discardTimer* specified in TS 38.323 [5]. Value ms50 corresponds to 50 ms, value ms100 corresponds to 100 ms and so on.

* **Option 3: Others.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any**  |
| Samsung | Option 2 | This change may be simpler. |
| Ericsson | Option 1 |  |
| OPPO | Option 1 |  |
| ZTE | Option 2 | Both are OK, option 2 may be more clearer. |
| Futurewei | Option 2 | Both would be fine; option 2 is simpler. |
| vivo | Option 2 |  |
| Intel | No strong view | Option 2 seems simpler. However, we can go with majority.  |
| CATT | Option 2 | Both are fine for us. Option 2 may be better. |
| Qualcomm | Option 2 | This seems the simpler approach |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Other Issues

Regarding to other issues mentioned in [1], e.g., order of PDCP SN and Key ID and Key ID size, are already covered in PDCP running CR [6]. Here, companies are invited to provide other technical remaining issues related V2X PDCP, if any.

|  |  |  |
| --- | --- | --- |
| **Company** | **Issues** | **Comments if any**  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 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.

# Reference

1. R2-2005724‎, Summary of PDCP remaining issues on NR V2X, CATT
2. S3-201338 TS 33.536 v1.2.0, Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services
3. R2-2004747, Remaining Issues on PDCP, CATT
4. R2-2005464, Discussion on PDCP SN size for SL groupcast and broadcast in NR V2X Huawei, MediaTek Inc.,HiSilicon
5. R2-2005343, Remaining issues for NR SL PDCP header format, Qualcomm Finland RFFE Oy
6. R2-2004888, 38.323 CR for NR V2X, CATT, CR, 0048
7. R2-2004881, Draft LS on trigger of PDCP reestablishment, OPPO
8. R2-2005727‎, LS reply to RAN WG2 LS on the security related issues for NR SL, SA3, S3-201483
9. R2-2005548, Clarification of SL PDCP Operation, Samsung Electronics Co., Ltd
10. R2-2005045, Discussion on counter check procedure for NR sidelink, Spreadtrum Communications
11. R2-2005055, Remaining issues in PDCP for NR sidelink Nokia, Nokia Shanghai Bell
12. R2-2004577‎ , Discussion on remaining issue related to RRC in NR V2X, ZTE Corporation, Sanechips