3GPP TSG RAN WG2 Meeting #115-e R2-17xxxxx

**Electronic meeting, 16th-27th August 2021**

**Agenda item:** x.x.x

**Source:** Intel Corporation

**Title:** Report of email discussion [Post114-e][507][SData] Non-SDT data arrival handling

**Document for:**  Discussion and decision

# Introduction

The intention is to discuss the following topics as part of the email discussion “[Post114-e][507][SData] Non-SDT data arrival handling” taking into consideration the related proposals on RAN2#114e TDocs [1]-[22] and in preparation for responses to be received from SA3 and CT1 in relation to previous RAN2 LSs [23][24].

* [Post114-e][507][SData] Non-SDT data arrival handling (Intel)

**Scope:**

* + Phase 1 (identify the open issues/questions) – 5 days
	+ Phase 2 (collect the company views on open issues/questions)
	+ Phase 3 (collect companies view on preferred solution CCCH vs. DCCH with the aim to down-select)

**Email discussion to focus on:**

a. Develop details of both solutions (CCCH and DCCH) and identify any further impacts to other WGs (e.g. RAN3)

b. Develop details of how cell reselection could be handled (considering possible repetition of security material) and check if we could agree to support optimised handling of cell reselection

c. Can consider SA3/CT1 discussions into where appropriate.

**Intended outcome**: Report with agreeable proposals

**Email discussion deadline:** August 6th, 0900 UTC

**Note**: silent period is July 5-30 (may be updated during TSG RAN)

## 2nd Phase: Introdution

The **deadline for the 2nd phase** of this email discussion is **Monday July 26th, 2300 UTC.**

This 2nd phase focuses on collecting companies’ views to better understand the technical details of the proposed solutions. The discussion points addressed during the 1st phase and companies’ responses provided during the 1st phase are **greyed out** to avoid confusions. New questions (marked as Q.x and with a corresponding sub-section header) are added for companies to provide their views during this 2nd phase. Blue color is used to mark changes/inputs done during this 2nd phase.

## 1st Phase

### 1st Phase: Introduction

The **deadline for this 1st phase** of email discussion is **Friday June 18th, 0900 UTC.**

The **1st phase** of this email discussion provides an overview of the discussion points for the above scenarios that were identified in the contributions. Companies are invited to provide inputs on any missing topics/questions that need to also be included. Issues impacting other groups (e.g., RAN3) can also be listed. These issues are to be addressed in more detail with possible solutions during the 2nd phase.

For completion of the solutions and to acknowledge companies’ inputs, observations (with their corresponding description and references) are also included to capture points that seem straight forward (i.e. the suggestion is not to include a related discussion point for them in the 2nd phase).

### 1st Phase: Report

Rapporteur has addressed companies’ responses during the 1st phase in a new column that is added to each table where companies were asked for new points to be addressed. These tables are moved to this 1.2 section aiming to minimize any confusion between the responses provided by companies in the 1st and 2nd phase.

#### New points to section 2 (identified during 1st phase)

Please indicate if there are any other topics/questions that require to be addressed as part of this **section 2** on “General topics: switch from SDT to CONNECTED”.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Companies’ views** | **Rapporteur’s response** |
| ZTE | For 2.1, for option 1.a, we think there should be a question on whether or not we will support any mechanism to prevent data loss in case UE is moved back to INACTIVE state (since in normal RRC release procedure, PDCP suspend operation will be performed and all the data buffered on UE side will be discarded) – perhaps this is also related to section 4.2 (i.e., we may apply uniform handling for all scenarios where there could be an abrupt termination of SDT procedure).  | New question Q1) is added with corresponding new proposal for option 1.a) |
| APT | Similar view with ZTE: a higher-level question like whether to support a mechanism to prevent data loss (especially for the on-going SDT RB) when UE is moved back to RRC\_INACTIVE would be helpful for section 2.1, option 1.a.  | See response to ZTE |
| Huawei, HiSilicon | On Topic#1: The presented solutions are only a subset of the possible approaches, so it is better to focus on the questions that are raised instead of specific solutions for now (probably this is the intention, but we just wanted to underline this). In general, this topic is more in the RAN3 area, so in the end we may just need to ask them to come up with the solution.For Topic#2: Observation 1 is not really an observation – we should perhaps turn it into a proposal and attempt to agree on it.On the comment from ZTE – when the UE moves to RRC INACTIVE and PDCP is suspended the PDCP PDUs are discarded, but not PDCP SDUs. This is how the data loss is avoided (as compared to moving the UE to RRC IDLE). | For Topic #1, the discussion is indeed focusing on the questions.For Topic #2, observation 2 is moved to a new question Q.6) as requested.Added the suggested clarification on the new question Q1) raised by ZTE. |
| TCL | Agree with HW that we should focus on the questions raised and do further studies on them for now, then investigate the possible approaches based on the studies. For section 2.1, option 1.a, we share the same view with ZTE and APT, the service continuation should be considered during the procedure the UE move back to INACTIVE state. | See responses to previous related comments |
| NEC | For Topic#1, we think this should be discussed by RAN3. And we understand that RAN3 haven’t agreed to support the scenario of subsequent SDT without anchor relocation yet. So it is too early to discuss related issue in RAN2.We agree with observation 1 in Topic #2. | For Topic #1, a questionQ.4) is added with potential points to be asked/raised to RAN3 if the scenario were supported.For Topic #2, see response provided to Huawei on this. |

#### New points to section 3.1 (identified during 1st phase)

Please indicate if there are any other topics/questions that require to be addressed as part of this **section 3.1** on “General topics” for “Non-SDT data handling during ongoing SDT session”.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Companies’ views** | **Rapporteur’s response** |
| ZTE | In general, this is fine, but we would like to clarify that the discussion is \*only\* for the case where at least RACH preamble has been transmitted. i.e. we will not need to discuss any UE behaviour for the case when nothing has yet been transmitted. Further, we are not sure whether scenario 1) and 2) needs to be distinguished from RRC perspective, but this can be discussed during the questions... | Description of Topic 3 is updated to explicitly capture the 1st point on RACH preamble |
| CATT | The data arrival on non-SDT bearers could occur even when the SDT session is ongoing. This scenario is not been covered by the listed scenario 1) and 2). Hence Scenario 3: 1st UL RRC message has been sent successfully should also be considered. The scenario is applicable to both RA-SDT and CG-SDT. | The proposed scenario 3 aims to be addressed when explaining how CCCH and DCCH based approaches work in sections 3.2 and 3.3. Clarification text added before section 3.1 on this regard. |
| APT | Another scenario worth considering: Scenario 3) When non-SDT Data becomes available after UE has received the contention resolution corresponding to the 1st RA-SDT transmission, but has not received RRC message from gNB (i.e., in the middle of subsequent SDT transmissions).This scenario is particularly suitable for UE to use the DCCH approach to inform the arrival of non-SDT traffic. In addition, it appears that scenarios 1 and 2 only take RA-SDT into account. For CG-SDT, the following scenarios may need to be considered as well:Revised Scenario 1) When non-SDT Data becomes available after UE has initiated an SDT procedure, but 1st UL RRC message has not been sent yet. **For RA-SDT,** this could be when UE has already sent PRACH preamble when using 4-step RA-SDT. **For CG-SDT, this could be when UE has not sent the initial transmission via CG resource.**Scenario x) When non-SDT Data becomes available after UE has initiated an SDT procedure and has sent the 1st UL RRC message via CG resource, but the feedback has not been received by UE in CG response window. | For scenario 3), see response to CATT’s comment.For CG-SDT, it is clarified that scenarios 1) and 2) target on RA-SDT, and the new scenario x) is added targeting CG-SDT. However, it is not added “For CG-SDT, this could be when UE has not sent the initial transmission via CG resource” as the rapporteur assumes that this can be handled by UE implementation (as UE has not sent anything yet). |
| Huawei, HiSilicon | The answer to this issue will most likely be different for CCCH and for DCCH based approaches, so we suggest to discuss this issue for both approaches separately. | Since this is before SDT initialization, the rapporteur assumes it is the same for both approaches. Instead of moving this to separate sections, rapporteur suggests that companies can provide differences if they see any in phase 2. A sentence is added to the question along these lines. |
| TCL | We are generally fine with the proposal. However, we are wondering whether the subsequent SDT transmission is to be considered in this discussion as APT mentioned. For if there is subsequent SDT transmission, the subsequent SDT transmission may have impact on the handling of the non-SDT transmission. So the following scenario is suggested:Scenario x) When the non-SDT data arrival after the first SDT transmission is finished, and the subsequent SDT is to be performed. | For sub-sequent SDT (i.e. scenario 3), see response to CATT’s comment.  |
| NEC | We also think we need to consider the scenario of non-SDT data arrival during subsequent transmission phase. | For sub-sequent SDT (i.e. scenario 3), see response to CATT’s comment.  |

#### New points to section 3.2 (identified during 1st phase)

Please indicate if there are any other topics/questions that require to be addressed as part of this **section 3.2** on “CCCH-based approach” for “Non-SDT data handling during ongoing SDT session”.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Companies’ views** | **Rapporteur’s response** |
| ZTE | For section 3.2.1.1, in case the UE triggers new RRCResume procedure autonomously after releasing the current SDT session, then according to the current release procedure, the UE has to perform PDCP suspend operation and discard all buffered PDCP PDUs. It needs to be clarified whether this is the intention (in which case we need to understand how to handle data loss prevention etc). In case different operation is intended than legacy release, then it seems NW has to distinguish between the first and second RRCResume procedures and take different action accordingly and these details need to be understood too. Questions to narrow down these options and to understand how the actual procedure works will be useful. Just one other observation is that some of the questions/discussion in the above sections may be inter-related (for instance depending on which node - Anchor/new target - handles the second CCCH message, the security of the second CCCH message should be adjusted accordingly – i.e. these questions are interrelated), other than that, we think the general observations and discussion points have been captured accurately.  | For 3.2.1.1), Added a new discussion to address the open question explained is added. Note that this “new” point is somehow inter-related with the following discussion on section 3.2.4 that addresses the “PDCP COUNT and/or security key to be used”On the point that “some of the questions/discussion in the above sections may be inter-related”, this is indeed the case and companies are encouraged to provide consistent/align view on the inter-related topics. |
| Huawei, HiSilicon | Discussion point 6) is relevant only in case SA3 indicates there is an issue with reusing the security material / existing key (i.e. if they conclude there is no issue, then there seems to be no reason to have option other than 6d)). Hence, we propose to clarify that 6d) is the baseline assumption and discuss only the remaining options, just in case SA3 confirms the issue. Also, we are not sure what option 6a) describes. It can either be understood as option 6b) or option 6d). We propose to remove it, especially that our paper is given as a reference, but what we propose is already captured by option 6d) and 6e). Discussion point 7) – option a) and option b) are not described properly, i.e. the legacy behavior is for the new gNB to send UE CONTEXT RELEASE message to the old anchor:After Path switch and after sending RRCRelease w/ suspend (for RNA update with anchor relocation)1. After Path Switch and after receiving RRCResumeComplete from the UE (for moving the UE to RRC Connected).

This can be seen in TS 38.300 sections 9.2.2.4.1 and 9.2.2.5. | For section 3.2.5, there is indeed some dependency to SA3 but at the same time some of the options discussed there are also related to other topics e.g. previous section 3.2.4. Note that SA3 dependencies already are indicated within section 3.2.5 and also in the new question Q.14). Irrespective of security issue, which key (the one used to derive the previous Resume MAC-I or the one used during the previous data transfer) is used to derive the Resume MAC-I for the 2nd *RRCResumeRequest* msg needs to be discussed from RAN2 protocol point of view as there is no *RRCRelease* message for CCCH option. For DP#6, the understanding is that more than one of the options may be supported in related to how *resumeMAC-I* is generated for this 2nd RRCResumeRequest. For opt.6a), the TDoc reference will be removed. It was assumed as the explained procedure in [12] does not explain any change for this which follows legacy resume operation.For opt.6b), this is a change of legacy resume as horizontal key derivation of the NCC is not done for this kind of scenarios.To be aligned with approach taken in other DP, the aim was to add all options discussed in R2#114e TDocs for companies to provide their preference on those or other new options (if applicable).Description related to DP#7 in section 3.2.6 is updated accordingly. |
| NEC | For Discussion point 6), NCC is used to derive the KgNB key for the transmission at the new cell, not to generate resumeMAC-I. So we wonder if option 6.a), 6.b) and 6.c) is actually intended to be used to solve the issue in Discussion point 5)? In other words, to solve the key stream reuse issue by using different security keys.For Discussion point 7), we agree with Huawei that the legacy behavior is that after sending RRCRelease or receiving RRCResumeComplete, the new gNB indicates the last serving gNB to release UE AS context. So when CCCH is sent to the new gNB, the last serving gNB still have the UE AS context. Therefore there is no issue on UE AS context fetch if we following the existing behavior for CCCH solution.For Discussion point 8), this should be up to SA3 decision. | Rapporteur suggests that companies’ views on expected behaviors are welcome during 2nd phase understanding that 1st phase aimed to capture inputs on new open points to be discussed. |

#### New points to section 3.3 (identified during 1st phase)

Please indicate if there are any other topics/questions that require to be addressed as part of this section 3.3 on “DCCH-based approach” for “Non-SDT data handling during ongoing SDT session”.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Companies’ views** | **Rapporteur’s response** |
| ZTE | One issue that was raised in the past is how to deal with the case where the DCCH message is generated, but the UE is sent back to INACTIVE (i.e. the network releases the SDT session before the UE sends the DCCH message). Our understanding is that this will simply trigger a new resume (i.e. no changes needed), but in any case, should we add one question for this too?  | Proposed new topic is added in a new question Q.22) in a new section 3.3.3 |
| Huawei, HiSilicon | We need to also discuss the following for the DCCH solution:1. What are the contents of DCCH message, e.g. does the resume cause need to be included etc.2. DCCH message delivery failure handling, i.e. what happens if the UE does not receive a confirmation of reception of the message.3. What happens if there is no UL grant to send the DCCH message for non-SDT data indication.4. What the behavior of the UE is if the NW sends an RRRCRelease message before the UE sends the DCCH message. | Proposed topic 1 is covered as part of DP#11, however a new option is added for the resume cause.Added the proposed topic 2 in a new question Q.21) in the new section 3.3.2.2.Added the proposed topic 3 in a new question Q.23) in a new section 3.3.4.Proposed topic 4 is same as the one provided by ZTE, see corresponding response. |
| NEC | We agree with the question proposed by Huawei, and we also need to discuss the following additional aspects:- If a timer is needed for the DCCH message, to avoid frequent triggering of the generating of the DCCH message before receiving network response e.g. RRCResume message. | Rapporteur suggests that this view is provided as part of the response to new question Q.21) added in the new section 3.3.2.2 |

#### New points to section 4 (identified during 1st phase)

Please indicate if there are any other topics/questions that require to be addressed as part of this section 4 on “Failure handling during ongoing SDT session”.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Companies’ views** | **Rapporteur’s response** |
| ZTE | As noted above, for section 4.1, there may be also some other triggers depending on which approach we take (e.g., delayed switch to CONNECTED mode during ongoing SDT without anchor relocation etc), but perhaps the intention here is to collect any other triggers as part of the discussion – and this is fine? | Yes, your understanding is right. I.e., current list is based on RAN2#114e TDoc but companies are welcome to comment and/or add new triggers to be considered (if any) |
| Huawei, HiSilicon | We think we should discuss the preferred behavior for each of the events mentioned in section in 4.1 separately as in some cases it may be preferable to keep the UE in RRC INACTIVE while for others it may be better that UE moves to RRC IDLE. It may not be possible to apply exactly the same behavior for all cases.Another event worth discussing is downlink non-SDT data arrival (especially for the non-anchor relocation case). This is not a failure/abrupt termination case as such, but we need a procedure to handle this scenario. | The scope of this email discussion was the trigger of “cell reselection”, however some companies proposed common failure handling e.g. [4] [18]. Therefore as explained before section 4.1, sections 4.1 and 4.2 aims to understand whether the intention on having a common UE behaviour could be easily agreeable by companies. Otherwise, the suggestion is to focus on cell reselection trigger (as indicated in the scope of this email discussion). |
|  |  |  |

# General topics: switch from SDT to CONNECTED

RAN2 has agreed to support transition from SDT session to RRC\_CONNECTED where that SDT session could be ongoing with and without UE AS Context relocation as shown in related agreements below.

* RAN2#113bis: “*UE switches from SDT to non-SDT in following cases: Case 1 (27/0): UE receive indication from network to switch to non-SDT procedure. Network can send RRCResume. FFS whether network can send indication in RAR/fallbackRAR/DCI to switch to non-SDT procedure.”*
* RAN2#112: “*RAN2 confirm that RACH based SDT is supported with and without UE context relocation*”
* RAN2#111: “*Context fetch and data forwarding with anchor re-location and without anchor re-location will be considered. FFS if there are problems with the scenario “without anchor relocation*”

This section addresses general topics for discussion that are therefore applicable to any scenario where the UE with an ongoing SDT session fallbacks into RRC\_CONNECTED regardless of the trigger condition. Some of those trigger conditions may be because network wants to continue the exchange of the SDT data while having the UE in RRC\_CONNECTED or network detects DL non-SDT data or network is informed that UL non-SDT data is available in UE side.

## Topic #1: Handling to switch from SDT to CONNECTED during an ongoing SDT session without UE AS context relocation

Rel-17 SDT WID captures that “*UL small data transmissions for RACH-based schemes (i.e. 2-step and 4-step RACH)*” will be enabled with “*Context fetch and data forwarding (with and without anchor relocation) in INACTIVE state for RACH-based solutions*”. Whether and how to address the scenario when UE transitions into RRC\_CONNECTED during an ongoing SDT session where UE AS context was not relocated is discussed by [2][6][8][19].



Figure 1. Transition into RRC\_CONNECTED during subsequent SDT without anchor relocation [8]

For the scenario explained above and also shown in the Figure 1, the following approaches are suggested:

1. Network release the UE back into RRC\_INACTIVE (potentially with updated suspend and SDT configurations) [5]. This may lead to additional delay (from the release and initiation of a follow up new attempt), however it may not be an scenario that occurs frequently.
2. A new mechanism is defined by RAN2/3 to update the security keys during the ongoing SDT session (due to the relocation of the UE context during an ongoing SDT session) [6][8][19]. The new procedure would be required to support the key change involving: to provide new NCC to the UE, suspend data transfer, resetting L2, re-establish PDCP, Resume data transfer. In addition, RAN2 will need to also discuss which node triggers the anchor change and which node generates the RRC message with the NCC considering the network architecture (including how the CU DU split is done for anchoring). Open questions are also identified by [19][8]:
3. Which node decides the content of *RRCResume* message (anchor gNB vs serving gNB)?
4. Which node performs ciphering and integrity protection for *RRCResume* message?
5. Handling of the security key update e.g.
	* 1. after receiving the second RRCResumeReq from the same UE, will the anchor gNB generate another new KgNB associated with the same target gNB?
		2. how to ensure security key separation if UL/DL data and *RRCResume* message are treated by anchor gNB with updated security key and then, *RRCResumeComplete* message and subsequent UL/DL are treated by the current serving gNB.
6. Which node decodes *RRCResumeComplete* message

Moreover solution details on the questions listed above and how the new mechanism may look like are also provided by [8][19].

1. How to address the scenario when switching from SDT to RRC\_CONECTED during an ongoing SDT session where the UE context was not relocated by the network. Including questions Q1-Q4 for above option 1.b).

#### Option 1.a) Network releases the UE back into RRC\_INACTIVE when anchor relocation is required in the middle of an SDT session

##### **Q.1) for 2nd Phase**

This Q.1) is created based on previous discussion point and the responses provided during 1st phase.

It is pointed during the 1st phase that in normal RRC release procedure, PDCP suspend operation will be performed and all the data buffered on UE side will be discarded. On other hand, when PDCP is suspended, the PDCP PDUs are discarded, but not PDCP SDUs.

1. For **previous option 1.a)**, is there any mechanism needed to prevent data loss in case UE is moved back to INACTIVE state?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Yes/No** | **Justification** |
| Huawei, HiSilicon | No | As mentioned above, PDCP SDUs are not discarded when the UE moves to RRC INACTIVE, so they can still be transmitted. This is also the whole point of a proposal to keep the UE in RRC INACTIVE after cell reselection during SDT for example. |
| ZTE | Yes with comments  | It is true that PDCP SDUs are not discarded, however, it should be noted that PDCP suspend will be performed when RRCRelease is received and PDCP suspend will result in the following actions: * Transmitter sets the TX\_NEXT to initial value and discards all the stored PDCP PDUs
* Receiver will stop reordering and deliver the PDCP SDUs to upper layers in ascending order of COUNT

Since the PDCP entity will restart with initial COUNT value at next RRCResume, there will be two issues: * redundancy cannot be avoided and
* in order delivery of PDCP PDUs cannot be ensured in this case

It should be noted that lossless delivery as agreed in RAN2, requires also the in order delivery of PDCP SDUs to upper layers. So, the question is whether we should ensure inorder delivery without redundancy in this case. So, there are two options: * **Option 1: If we want to ensure in-order delivery and avoid the redundancy**, then the PDCP suspend operation should not be performed in this case and this may require some changes (e.g. to indicate “*no PDCP suspend*” in RRCRelease and to indicate the same on the transmitter side to the transmitting UP entity – e.g. over E1 interface).
* **Option 2: If we can live with redundancy and no in-order delivery**, then nothing more needs to be done.

From our perspective, we prefer option 1 to ensure the in order delivery and avoid the redundancy. |
| InterDigital | No | If we go for option 1.a, then the existing mechanism should be reused as much as possible. Even if PDCP PDUs are thrown away, the PDCP SDUs can be retained and so lossless operation can be achieved based on the PDCP SDUs rather than PDUs. |

#### Option 1.b) New mechanism that allow performing anchor relocation in the middle of an SDT session in order to switch from SDT to CONNECTED

This section is updated based on the details provided above and by [2][6][8][19].

For this discussion, the term “**anchor gNB**” refers to the gNB where the UE AS Context is stored before UE initiates the SDT session and “**serving gNB**” refers to the gNB where the UE initiates the SDT session.

For **previous option 1.b)**, when switching from SDT to RRC\_CONECTED during an ongoing SDT session where the UE context was not relocated by the network, the following points are raised by companies:

* RLC PDUs are received/processed by the serving gNB [19].
* PDCP entities for SDT operation when anchor gNB is not relocated may be processed by anchor gNB [8], or by serving gNB (as anchor gNB forwards them) [19].
* For the data awareness during SDT operation, the serving gNB is the first aware of the UL data (size and arrival) [2][8], and the anchor gNB is the first aware of DL data arrival [2][8].
* The serving gNB controls SDT operations related to the radio interface, such as, performs the data transmission/reception via radio interface, or set the content of *RRCResume* message related to configurations of radio interface [8].
* Security key in used in relation to this “late” anchor relocation:
	+ During an ongoing SDT session where the UE context was not relocated by the network, the data forwarding between serving gNB and anchor gNB has already been started, and the new security key, derived based on the NCC stored, has already been used by anchor gNB [19]. Therefore UE uses the updated security key (i.e. KgNB associated with the serving gNB, referred as Kserving-gNB) which is updated upon initiation of 1st *RRCResumeRequest* message, to receive any DL data/signalling upon initiating the SDT operation (which includes *RRCResume* message) [8]. Therefore, ciphering and integrity protection for *RRCResume* message should be performed based on that same Kserving-gNB [8].
	+ Based on the SA3 requirement, re-using the same key in two nodes is not allowed. Hence the change of anchor requires a change of security keys [6]. Therefore once the security key has already been used in the anchor gNB (during SDT operation without anchor relocation), the same security key shall not be used in the serving gNB again after anchor relocation is performed [19].
	+ On summary, a new key (other than the key used in the data transmission before anchor relocation) shall be generated and used between serving gNB and UE after anchor relocation [19].
		- The materials for key generation (e.g. AS-SecurityInformation in XnAP, including KgNB\* and NCC) should be generated by anchor gNB, and be sent from anchor gNB to serving gNB (e.g. in RetrieveUEContextRequest or a later message) [19].
		- The key materials (i.e. *MasterKeyUpdate* and *SecurityConfig*) should be sent to UE through a RRC message (e.g. *RRCResume*) generated by serving gNB [19]. This RRC message should be security protected by the SRB PDCP located in anchor node (i.e. the RRC message (e.g. *RRCResume*) generated by serving gNB should be sent to anchor node for security protection operation) [19].
		- The UE shall be configured to CONNECTED mode in the RRC message and reconfiguration with sync shall be used [19].
	+ On other hand, a change of keys requires the L2 to be reset to prevent mix up of data with the old and new keys. Currently, a change of keys is done either when the user plane is suspended/not established (re-establishment, SMC, Resume) or using a RACH procedure+L2 reset as the switch over point if there is ongoing data transfer (handover). A release and add of the RLC bearer could also be used to flush the L2. Additionally, PDCP has to be re-established. However, none of the existing NR procedures support this particular behaviour. [6]
	+ On summary, the support of key change when switching from SDT to CONNECTED may involve: providing new NCC to the UE, suspend data transfer, resetting L2, re-establish PDCP, ensuring identification of data with the old key and new key on the network side, Resume data transfer [6]
	+ Therefore if this scenario is handled similarly to handover procedure [8], the UE sends *RRCResumeComplete* message and subsequent UL/DL data is handled in the current serving gNB but different security keys are used [8].
* Potential issues with RAN3 impact foreseen for this scenario where SDT operation is done without anchor relocation:
	+ Signaling exchange via Xn interface e.g. when deciding/triggering the transition from SDT to CONNECTED [8].
	+ how the CU DU split is done when switching from SDT to RRC\_CONECTED during an ongoing SDT session where the UE context was not relocated by the network [6]
* Potential issues with SA3 impact foreseen for this scenario where SDT operation is done without anchor relocation:
	+ Whether update of the security key is required or not for this scenario and how to ensure security separation between two different gNBs after transaction [8]

The following questions Q.2) to Q.5) are suggested taken into consideration the points explained and asked above:

##### **Q.2) for 2nd Phase**

1. Is the following understanding confirmed: for the scenario where anchor relocation is performed in the middle of an ongoing SDT session, the security key is updated to meet SA3 requirement that the same security key is not re-used in two nodes?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Yes/No** | **Justification (if the response is no)** |
| Huawei, HiSilicon | Worth checking with SA3 whether this is an issue, other approaches than updating the security key for RRCResume exist as well | This case is somewhat different from legacy case to which the SA3 requirement refers to because all the messages are anyway sent over the air interface between serving gNB and the UE (i.e. between the UE and a single gNB, not two different gNBs). It should also be noted that the lack of key separation would happen only for a single message, i.e. RRCResume message. Right after resuming the connection, the serving gNB can perform security key update based on the new NCC received from AMF during Path Switch. It might be then worth clarifying with SA3 whether this is an issue that needs to be addressed. If this is deemed an issue after all, then we would prefer avoiding developing new complicated signaling options. Instead of this, a simple solution would be for the current anchor gNB to end the SDT procedure (i.e. provide RRCRelease message to the UE) and let the UE establish a new non-SDT connection. This way all the potential security issues can be avoided. |
| ZTE | Yes | However, we agree with the views from Huawei above that a simple solution would be preferable (e.g. the anchor gNB to end the SDT procedure and let the UE establish a new connection). Handling of the pending PDCP entity will then need to be performed as per the agreement for the above question.  |
| InterDigital | Yes | The AS keys are associated with the anchor gNB and so the AS keys should be updated upon change of anchoring point. |
|  |  |  |

｀

##### **Q.3) for 2nd Phase**

1. Assuming that RAN2 confirms in previous point in Q.2) (i.e. “the scenario where anchor relocation is performed in the middle of an ongoing SDT session, the security key is updated”), The following points summarize suggested RAN2 solutions to be confirmed for the new mechanism that updates the security key when performing anchor relocation in the middle of an ongoing SDT session. Please indicate your view on the solution points listed below and/or if you propose new ones to consider.
2. Network sends to UE a DL RRC msg (e.g. *RRCResume*) that provides the new NCC at the same time that informs of the switch from SDT to CONNECTED. The security key is used for the transfer of that DL RRC msg (e.g. *RRCResume*) should also be addressed.
3. L2 handling of data during and after the security key change (L2 reset/re-establishment and identification of data with old and new keys) can be addressed via reconfiguration with sync or by RLC bearer release and add with a new LCID.
4. Current anchor gNB terminates and ongoing SDT procedure by sending RRCRelease message to the UE (where NCC is provided). The UE triggers a new non-SDT RRC Resume procedure during which the anchor is relocated to the new serving gNB.

|  |  |
| --- | --- |
| **Company’s name** | **Companies’ views on the solution point(s) and/or****additional new solution options to consider** |
| Huawei, HiSilicon | As mentioned above, this scenario can be addressed by ending an ongoing SDT procedure with RRCRelease message and establishing a new connection via non-SDT RRC resume procedure during which the anchor gets relocated. We add an additional point for this approach above.  |
| ZTE |  We also support solution point 3 above (with slight modification).The UE shall trigger the next resume procedure using normal rules (i.e. the existing rules for SDT vs non-SDT will be used to trigger the next resume procedure) in this case.  |
| InterDigital | Regarding to Point 1), a new NCC should be provided in the DL RRC message and the DL RRC message should be integrity protected with the new key and + previously configured algorithm but not encrypted with the new key. It seems the RRC connection reestablishment procedure has all the toolkit required for the support of the concern scenario thus we suggest applying the RRC connection reestablishment procedure (i.e. follow 38.331 subclause 5.3.7 and 33.501 subclause 6.11) in the middle of the resume attempt and so the DL RRC message should be RRCReestablishment rather than RRCResume.Regarding to Point 2), the same procedures as RRC connection reestablishment procedure should take place. |
|  |  |

##### **Q.4) for 2nd Phase**

1. The following questions/points are suggested to be asked/informed to **RAN3** in order to enable the new mechanism that allows the switching from SDT to RRC\_CONECTED during an ongoing SDT session where the UE context was not relocated by the network (as explained in **previous option 1.b**). Please indicate if you do not agree to include any of them and/or if you propose new questions to be shared with RAN3.
	1. Which node triggers/decides the switch from SDT to CONNECTED.
	2. Which node decides the content of *RRCResume* msg.
	3. Which node performs ciphering and integrity protection for *RRCResume* msg.
	4. Which node decodes *RRCResumeComplete* msg.
	5. Whether and what new signaling exchange is required between anchor gNB and serving gNB to support the switching from SDT to RRC\_CONECTED.
	6. Assuming that RAN2 confirms the following understanding in previous question Q.2) (i.e. “the scenario where anchor relocation is performed in the middle of an ongoing SDT session, the security key is updated”), to define a new mechanism that allows updating the security key when performing anchor relocation in the middle of an ongoing SDT session taken into consideration RAN2 related agreements (if any).

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Questions not to send to RAN3** | **Company’s views on the questions not to send to RAN3 or** **new questions to RAN3 to consider** |
| Huawei, HiSilicon | Q.4.1), Q.4.2), Q.4.3), Q.4.4), Q.4.6) | For Q.4.1) RAN3 already has a working assumption, so it seems there is no need to trigger this in RAN3:* WA: The last serving gNB, i.e., anchor gNB, will be the decision maker on whether to relocate anchor or not. Assistance information provided by the receiving gNB may help on the decision. Details of assistance information are pending future discussion.

Q.4.2), Q.4.3), Q.4.4) and Q.4.6) are only relevant for RRCResume based approach and addressing all these issues may be complicated, especially if the security issue (related to Q.4.3)) would be confirmed by SA3. Therefore, we think we can focus on asking RAN3 to study point Q.4.5). We can potentially list the approaches (RRCResume based and RRCRelease based) and issues discussed in this document and RAN3 can discuss the details. |
| ZTE | Probably no need to ask anything (but TBD based on actual solution chosen) | We think we first need to discuss the solution details. Our preference is to agree a simple solution (e.g. based on RRCRelease per above) and if this is agreeable, then it is obvious that the anchor gNB (which has the security context) will perform the security protection of the RRCRelease message (this already happens today in case of RNAU without anchor relocation, so, we then expect no impact to RAN3 in this case actually from signalling perspective). So, the rest of the questions seems not really needed (i.e. we can simply inform RAN3 then of our decision)If we agree some other more complex solution, then it seems we do need some more detailed communication with RAN3 (e.g. there could be some impact to E1 interface etc per above) |
| InterDigital | Q.4.3)Q.4.4) | We think ciphering can’t be applied for the 1st DL message and the old key should be used for the integrity protection check for the 1st DL message. Thus, the anchor node shall enforce the security. i.e. it’s not RAN3 issue.RAN2 should make a working assumption that the new serving gNB decodes the RRCResumeComplete msg and should tell our WA to RAN3 instead of just asking this question to RAN3. |
|  |  |  |

##### **Q.5) for 2nd Phase**

1. The following questions/points are suggested to be asked/informed to **SA3** in order to enable a new mechanism that allows the switching from SDT to RRC\_CONECTED during an ongoing SDT session where the UE context was not initially relocated by the network during SDT (as explained in **previous option 1.b**). Please indicate if you do not agree to include any of them and/or if you propose new questions to share with SA3.
	1. How to ensure the security key separation between two different gNBs after moving into CONNECTED needs to be resolved (taking into account views provided on Q.3))

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Questions not to send to SA3** | **Company’s views on the questions not to send to SA3 or****additional new questions to SA3 to consider** |
| Huawei, HiSilicon | Q.5.1) (in this form at least) | After moving the UE to RRC Connected, the new gNB can update the security keys by performing reconfiguration with sync and using a new NCC from AMF received during Path Switch procedure. We think we may rather ask the questions similar to the one in Q2), i.e.: whether it is acceptable to use current UE’s K\_RRC key for sending RRCResume message from the serving gNB to the UE for the scenario where anchor relocation is performed in the middle of an ongoing SDT session. However, as we note above, an alternative approach is to terminate an SDT procedure when the anchor needs to be relocated in the middle of SDT procedure and let the UE trigger a new connection resume. This way security issues are avoided and there is no need to involve SA3 at all.  |
| ZTE | Probably no need to contact SA3 (TBD based on actual chosen solution) | Again, we think that if we go with the approach of RRCRelease based solution, then we don’t really need to ask SA3 anything. (Since this is same as the tunneled RRCRelease message in case of RNAU without anchor change). For Rel-17 this seems sufficient.If we support a solution where the UE directly moves to RRCConnected state, then we need some new handling and this needs further discussion (details TBD) |
| InterDigital | - | We are fine to send the query to SA3 with taking into account the Q.3’s RAN2 conclusion. |
|  |  |  |

## Topic #2: Radio bearer handling when switching from SDT to CONNECTED

RAN2 already agreed that SDT RBs are re-established at initiation of SDT procedure and the new security keys are applied then, i.e. there is no need to perform re-establishment second time when *RRCResume* is received as it is done Rel-15 NR. Therefore, when switching from SDT to CONNECTED, the PDCP of non-SDT RBs do not need to be re-established [12]. For this switch/fallback under network control, it is also explained in [6] that it is left up to network implementation that the data exchanged before triggering the fallback to resume is not lost (i.e. UE does not need to retransmit it) and SDT related data traffic can continue after UE gets RRC\_CONNECTED.

1. When UE receives *RRCResume* message during an ongoing SDT session or in response to *RRCResumeRequest* message sent for SDT (i.e. switch from SDT to CONNECTED), the PDCP entities for only the non-SDT RBs are re-established (i.e., SDT RBs are not re-established as were already resumed for the SDT session).
2. When switching from SDT to CONNECTED, it is left up to network implementation that the data exchanged before triggering the fallback to resume is not lost (i.e. UE does not need to retransmit it) and SDT related data traffic can continue after UE gets CONNECTED.

#### Q.6) for 2nd Phase

This Q.6) is created based on previous Observation 1 and the responses provided during 1st phase.

RAN2 has agreed that the PDCP entities of only the SDT DRBs are re-established when initiating an SDT session.

* RAN2#112e: “*For both RACH and CG based solutions, upon initiating RESUME procedure for SDT initiation (i.e. for first SDT transmission), the UE shall re-establish at least the SDT PDCP entities and resume the SDT DRBs that are configured for small data transmission (along with the SRB1). FFS for non-SDT DRBs. FFS on implicit vs. explicit. FFS on whether we a new Resume cause. FFS on whether we need to deal with suppressing PDCP status report*”
1. When UE receives *RRCResume* message during an ongoing SDT session or in response to *RRCResumeRequest* message sent for SDT (i.e. switch from SDT to CONNECTED), how are the PDCP entities handled?
2. PDCP entities for only the non-SDT RBs are re-established (i.e., SDT RBs are not re-established as were already resumed for the SDT session) [6][12].
3. PDCP of non-SDT RBs do not need to be re-established
4. Other approaches

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | It depends | The answer to this question depends on the scenario and the solution applied in non-anchor relocation scenario:- For anchor relocation case or in case serving gNB is already an anchor when SDT is triggered, option 2.a) applies- For non-anchor relocation case, if new keys are going to be used, then all RBs need to be re-established. With RRCRelease basaed approach this would happen automatically as the UE would just follow legacy RRC Resume procedure.  |
| ZTE | Option 2.a, but | In general option 2.a should be the baseline. And for non-anchor relocation case, if some special handling is needed per above, we think reconfiguration with sync will be used and the network can set the PDCP reestablishment flag accordingly for this case. The existing signalling already supports this.  |
| InterDigital | 2.c) | Only the non-SDT RBs are re-established unless any new keys are derived during the switch from SDT to CONNECTED. Or, all RBs are re-established for the case that a new key is generated during the switch (e.g. for the case that UE context is transferred from anchor to a new serving gNB in the middle of switch.) |
|  |  |  |

# Non-SDT data handling during ongoing SDT session

The discussion for the “non-SDT data handling” is split in three parts:

* Section 3.1 addresses any general topics during the “start” of the SDT session. These topics seem independent on whether CCCH or DCCH based approach are used.
* Section 3.2 focuses on CCCH-based approach when the SDT session is ongoing.
* Section 3.3 focuses on DCCH-based approach when the SDT session is ongoing.

## General topics

### Topic #3: non-SDT Data available when “starting” an SDT session

Another scenario to address is the desirable behaviour is non-SDT Data is available when “starting” an SDT session, before UE sends the 1st UL RRC message or before contention resolution which is discussed by [16][18][20]. It might be important to discuss separately both scenarios, as well as, a new one suggested by the responses provided during 1st phase:

* Scenario 1) When non-SDT Data becomes available after UE has initiated an SDT procedure (i.e. UE sends RACH preamble), but 1st UL RRC message has not been sent yet. This could be when UE has already sent PRACH preamble when using 4-step RA-SDT. Scenario 1) only targets RA-SDT.
* Scenario 2) When non-SDT Data becomes available after UE has initiated an SDT procedure and has sent the 1st UL RRC message + data successfully, but contention resolution has not been received by UE in Msg.4/Msg.B. Scenario 2) only targets RA-SDT.
* Scenario x) When non-SDT Data becomes available after UE has initiated an SDT procedure and has sent the 1st UL RRC message + data via CG resource, but UE has not received any feedback during the CG response window. Scenario x) only targets CG-SDT.
1. The expected UE behaviour when non-SDT Data becomes available after UE has initiated an SDT procedure for: scenario 1) 1st UL RRC message has not been sent yet and scenario 2) contention resolution has not been done.

The following Q.7) to Q.9) are created based on previous discussion point and the responses provided during 1st phase.

#### Q.7) for 2nd Phase

1. What is the expected UE behaviour for **scenario 1)** when non-SDT Data becomes available after UE has initiated an SDT procedure (i.e. RACH preamble is sent) but 1st UL RRC message has not been sent yet?

|  |  |
| --- | --- |
| **Company’s name** | **Companies’ views** |
| Huawei, HiSilicon | The UE should terminate the current RACH procedure and initiate a new one, i.e. send a non-SDT RACH preamble and CCCH/RRCResumeRequest message. |
| ZTE | Firstly, we think non-SDT data arriving after RACH has been sent but before getting a network response (e.g., before RAR/contention resolution) is a real corner case and there should not be a complicated optimization to handle this situation. For CCCH solution the UE will terminate the existing RACH procedure and initiate a new RRCResume Procedure. However, this is not needed in case of DCCH solution. In case of DCCH solution, we can follow the existing procedure, i.e. today once the UE sends RACH preamble, it simply listens to DL for network response even if some new trigger happens in the meanwhile. Thus, in case of non-SDT-data arrival, we think UE simply can continue to follow the current RACH procedure. Even if a new RACH procedure is triggered, UE will need to send yet another RACH preamble and wait for network response anyway (i.e. it is in the same situation as before any way).  |
| InterDigital | We share ZTE view on the corner case and so we are not willing to optimise this case with any complicated solution.Regarding to the original question, UE should terminate the existing RACH procedure and initiate the non-SDT resume procedure from the beginning (i.e. initiating the resume from the non-SDT preamble transmission.) |
|  |  |

#### Q.8) for 2nd Phase

1. What is the expected UE behaviour for **scenario 2)** when non-SDT Data becomes available after UE has initiated an SDT procedure and has sent the 1st UL RRC message + data successfully, but contention resolution has not been received by UE in Msg.4/Msg.B?

|  |  |
| --- | --- |
| **Company’s name** | **Companies’ views** |
| Huawei, HiSilicon | The same as in Q7, i.e. the UE should terminate the current RACH procedure and initiate a new one, i.e. send a non-SDT RACH preamble and CCCH/RRCResumeRequest message. |
| InterDigital | Same as Q7 |
|  |  |

#### Q.9) for 2nd Phase

1. What is the expected UE behaviour for **scenario x)** when non-SDT Data becomes available after UE has initiated an SDT procedure and has sent the 1st UL RRC message +data via CG resource, but UE has not received any feedback during the CG response window?

|  |  |
| --- | --- |
| **Company’s name** | **Companies’ views** |
| Huawei, HiSilicon | Similar as in Q7, i.e. the UE should terminate the ongoing SDT procedure and initiate a RACH procedure, i.e. send a non-SDT RACH preamble and CCCH/RRCResumeRequest message. |
| ZTE |  Same as Q7. In this case, it makes even more sense to wait for network response since only contention resolution is pending.  |
| InterDigital | Same as Q7. |
|  |  |

## CCCH-based approach

This section aims to clarify how CCCH-based approach works to enable the switch from an ongoing SDT session to non-SDT operation considering the related inputs provided in [5][9][12][13][14][18][20]. Note that some of the topics are inter-related with the ones discussed as part of previous general sections 2 and 3.1.

### [CCCH point (1)] Detection of non-SDT data

Upon UE detects non-SDT data available during an ongoing SDT session, this section discusses initial UE’s actions associated with CCCH-based approach.

#### [CCCH point (1.1)] UE autonomous release

For CCCH-based approach, It is clarified in [5] that UE autonomously triggers the end or the release of the ongoing SDT session upon detecting the non-SDT data.

1. For CCCH-based approach, UE autonomously triggers the end or the release of ongoing SDT session upon detecting the non-SDT data.

The following details and Q.10) are created based on the responses provided during 1st phase.

During current release procedure to suspend, the UE performs PDCP suspend operation and discard all buffered PDCP PDUs as it is also discussed in next section 3.2.4. For CCCH-based approach, it needs to be clarified whether this operation is maintained or not when UE autonomously ends the ongoing SDT session and initiates the new CCCH message.

1. Legacy behaviour - PDCP is suspended, and PDUs flushed. If PDCP suspend operation is done upon UE autonomously triggers the end or the release of ongoing SDT session, UE/network may not be able to detect data duplication and prevent data loss. This is also explained by Observation 6 in next section 3.2.4. This is also related to the discussion in next section 3.2.4.
2. New behaviour - PDCP suspend operation is not done or changed upon UE autonomously triggers the end or the release of ongoing SDT session. PDCP SN is not reset and PDUs are not flushed. If so, it needs to be clarified if network needs to distinguish between the 1st and 2nd *RRCResumeRequest* msg. and the corresponding different actions would need to be addressed. This is related to Discussion point 3) in next section 3.2.3.
3. Legacy behaviour with horizontal key derivation using the key derived after the first RRCResume as the base key - PDCP is suspended and PDUs flushed, the UE and RAN derive new KgNB\* horizontally, which is used for new UP and CP keys calculation. This way issue mentioned in section 3.2.4 is avoided.

##### **Q.10) for 2nd Phase**

1. For CCCH-based approach, upon UE autonomously triggers the end or the release of ongoing SDT session, what is the expected “PDCP suspend operation” considering previous options 1.x or new ones? please justify your response and provide further details on the corresponding open points.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | Option 1.c) | Option 1c) allows to reuse legacy behaviour when it comes to PDCP entities handling, but avoids the issue of reusing the COUNT value with the same security key by calculating new security keys horizontally. As mentioned in our answer to Q.1), since only PDCP PDUs are discarded and the PDCP SDUs are not discarded during this procedure, there is no data loss (same applies to option 1.a)) |
| ZTE | Option 1.b) | It should be noted that UE will derive a new KgNB after triggering RRCResume procedure. So, firstly, we should have a common understanding on which key is used as base key for the key derivation for second RRCResume procedure: * Is it the key in the UE INACTIVE AS context (this is how it works currently if we assume second RRCResume works exactly same as the first RRCResume) or
* Is it the key derived after first RRCResume procedure?

The figure below shows these options… It should be noted that the current RRCResumeProcedure is according to option 1 (since it uses the stored UE Inactive AS context to derive the new KgNB to be used). However, as pointed out, the problem is that if we stick with the current RRCResume procedure (i.e. option 1), then the key will not change after the second RRCResumeProcedure (i.e. KgNB2 is generated again since the input key has not changed and all other inputs to KDF are also the same). Hence, since the COUNT is reset, then we do need a new mechanism to derive the key after the second RRCResume procedure (i.e. the base key now is not anymore the key stored in the UE INACTIVE AS Context). Now, this is in option 2 above. This is also what is mentioned above as option 1.c in our understanding. It is worth being clear on this procedure to avoid any mis-understanding here:1. For the initial RRCResume procedure, the base key is the key stored in the UE INACTIVE AS context
2. For the second RRCResume procedure (i.e. upon non-SDT data arrival and if CCCH message is to be used), then the UE has to derive a new key but for this key derivation, the base key is **NOT** the key stored in UE AS context (it is the key that id derived in step a) above. This procedure needs to be updated in RRCResume.

Then, horizontal key derivation (i.e. Option 1.c) does not work in all cases. The problem is that there could be cases where the network may not have received the first RRCResume message and the keys between network and UE will go out of sync in this case. For instance, if the UE autonomously terminates the RACH procedure and derives a new set of security keys, then it could be the case that the first RRCResumeRequest message is not received at the network and hence the network will not be able to derive the same security key in this case.. So, even if we want to go through option 1.c), we need to ensure at least that the network has received the first UL message. In this case, we need two different solutions: * Before contention resolution, if the UE terminates the ongoing RACH procedure, then it is unclear which keys shall be used on the UE side. Horizontal key derivation will not work in this case because the network will not be aware of the first RRCResume. This needs to be clarified in this solution.
* After contention resolution, then, option 1.c) can work, but then it means that the UE may have to adopt different solution based on whether or not contention resolution has happened.

 Based on this we would like to note the following observation: Observation: the CCCH solution should adopt one of the following options: **Option 1**: If the horizontal key derivation based on the initial derived key is used for the second RRCResumeProcedure, then an indication is needed in the RRCResumeReq to indicate that this is the second RRCResumeReq (to enable the network to also calculate the key correctly – if not, there should be a requirement that horizontal key derivation can only be used after contention resolution and prior to contention resolution, UE has to use same key and we need to check if this is okay)**Option 2**: If the key stored in the UE Inactive AS context is used as the base key for the second key derivation, then the same key is derived in first and second RRCResume. In this case, the COUNT should not be reset (i.e. the existing RRCResume procedure is not applicable – UE has to keep continue the count to ensure no count reuse with same key). Also in this case, there is no need for the new kgNB to be included in UEContextResponse message from anchor gNB. We need to decide which option to choose for CCCH solution.  |
| InterDigital | 1.x) | If new keys are derived in the middle of the switch, then PDCP should be re-established to apply the new keys. Otherwise, PDCP is retained without any suspension/release as data transmission continues after the switch. |
|  |  |  |

### [CCCH point (2)] RACH, UAC associated with the 2nd resume proc.

It is explained that CCCH-based approach [5] may require additional signalling to the network (e.g. RACH) and applies again UAC same as any UE in RRC\_INACTIVE in order to send non-SDT data

1. When switching from SDT to non-SDT via CCCH-based approach, AS applies UAC and initiates random access procedure same as any legacy UE in RRC\_INACTIVE.

### [CCCH point (3)] Resume cause

This point (3) discuss the proposal that this 2nd *RRCResumeRequest* message uses a new resume cause value (for the network to differentiate it) [20].

1. When switching from SDT to non-SDT via CCCH-based approach, whether a new value of the resume case is defined to differentiate the UE that had an ongoing SDT session and is sending a 2nd *RRCResumeRequest*.

#### Q.11) for 2nd Phase

This Q.11) is created based on previous discussion point.

1. When switching from SDT to non-SDT via CCCH-based approach, is there any needed for the network to differentiate that this UE had an SDT session ongoing and is sending a 2nd *RRCResumeRequest* msg., for example by including a new value of the resume cause?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Yes/No** | **Justification** |
| Huawei, HiSilicon | Yes, but no new indication is required | gNB will be able to detect that the RRCResumeRequest is coming from the same UE by reading the I-RNTI included in the message. There is no need for a new resume cause nor any other new indication when switching from SDT to non-SDT via CCCH-based approach. |
| ZTE | Yes | As noted above the gNB may not have received the first RRCResumeRequest (since the UE can terminate the 1st RRCResume Procedure autonomously). So, a new indication will be needed if the UE uses horizontally derived key for the 2nd RRCResume message. This means that we likely need a new CCCH message for the 2nd RRCResumeReq even in case of option 1.c |
| InterDigital | No | We share Huawei’s view.NW knows whether the same UE had any SDT session before or not for a particular UE and if the UE signals the non-SDT resumption request, then NW knows it’s switch from SDT to non-SDT operation. Thus, any additional information doesn’t need to be signalled. |
|  |  |  |

### [CCCH point (4)] PDCP COUNT and/or security key to be used

This section discusses the details of the 2nd *RRCResumeRequest* msg or the corresponding behaviour in UE and network side to support switching to non-SDT data during an ongoing SDT session for CCCH-based approach considering the inputs provided in [4][5][8][9][12][13][14][16][18][20].

References from legacy Resume/Suspend procedure are included below to show that the PDCP COUNT for all RBs are always reset. For example, this is done when *RRCRelease* is received including *suspendConfig* as shown below on the references taken from TS 38.331 § 5.3.8.3 and TS 38.331 § 5.1.4.

**5.3.8.3** **Reception of the RRCRelease by the UE**

The UE shall:

*\*\*\*text omitted\*\*\**

1> if the *RRCRelease* includes *suspendConfig*:

*\*\*\*text omitted\*\*\**

2> suspend all SRB(s) and DRB(s), except SRB0;

2> indicate PDCP suspend to lower layers of all DRBs;

*\*\*\*text omitted\*\*\**

***5.1.4 PDCP entity suspend***

*When upper layers request a PDCP entity suspend, the transmitting PDCP entity shall:*

*- set TX\_NEXT to the initial value;*

*- discard all stored PDCP PDUs;*

*When upper layers request a PDCP entity suspend, the receiving PDCP entity shall:*

*- if t-Reordering is running:*

*- stop and reset t-Reordering;*

*- deliver all stored PDCP SDUs to the upper layers in ascending order of associated COUNT values after performing header decompression;*

*- set RX\_NEXT and RX\_DELIV to the initial value.*

Current Release with suspend and Resume Request procedure resets the PDCP COUNT for all RBs as shown above. Since the CCCH method does not involve the RRC Release message, it is not clear if the COUNT for the RBs is reset for the second RRC Resume request.

On summary, the handling of the PDCP COUNT and the security key when switching from SDT to non-SDT should be clarified for CCCH-based approach as explained by [6][8][12][15][19]. Therefore, CCCH-based approach requires some level of update to resume procedure considering the points here discussed.

1. When switching from SDT to non-SDT via CCCH-based approach, understand whether the PDCP COUNT is (or not) reset.

#### Q.12) for 2nd Phase

This Q.12) is created based on previous discussion point.

1. When switching from SDT to non-SDT via CCCH-based approach, is the current behavior of resetting the PDCP count for RBs during the resume procedure applicable after the 2nd *RRCResumeRequest* msg?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Yes/No** | **Justification** |
| Huawei, HiSilicon | OK to reuse | We are OK to reuse this behaviour, but this would require applying either option 1c) mentioned for Q10 or requiring the network to update the security keys right after the connection is resumed, i.e. when the UE is already in RRC\_CONNECTED state, but before transmits/receives any data. |
| ZTE | Yes, but with new key only  | According to the current procedure, PDCP count will be reset but this means: * New key is derived at the UE using Horizontal key derviation for second RRCResume (note this either needs new indication in the second RRCResume per above)
* Since PDCP count is reset, we need new solution to ensure lossless data (i.e. in order delivery without redundancy).

For DCCH solution, no new key is needed and PDCP count will simply continue.  |
| InterDigital | Depend-on new key derivation | COUNT can be reset only when a new key is applied and so it’s up to the key handling during the switch. If any new keys are derived during the switch, then COUNT should be reset. Otherwise, COUNT value should be retained. |
|  |  |  |

TS 38.331 § 5.3.1.2 explains that same PDCP COUNT cannot be reused with the same security key as shown below:

“*It is not allowed to use the same COUNT value more than once for a given security key.*”

Note that further related details are discussed in the following sections of this email discussion.

1. The mechanism to be defined that enables the switch from SDT to non-SDT shall meet the following NR requirement: the same PDCP COUNT value is not used more than once for a given security key.

If the PDCP COUNT is reset for the CCCH based approach and as the UE has not received a new key, how to satisfy the above requirements for the RBs should be discussed [6][8][12][15][19].

1. When switching from SDT to non-SDT via CCCH-based approach and if the PDCP COUNT is reset, how to prevent the reuse of the same PDCP COUNT and the same security key for the RBs.

#### Q.13) for 2nd Phase

This Q.13) is created based on previous discussion point.

1. When switching from SDT to non-SDT via CCCH-based approach and if the PDCP COUNT is reset, how can the reuse of the same PDCP COUNT and the same security key for the RBs be prevented?

|  |  |
| --- | --- |
| **Company’s name** | **Explanation** |
| Huawei, HiSilicon | The security keys can be either derived horizontally when the second RRCResumeRequest is triggered (option 1c) as indicated in section 3.2.1.1) or the network may be required to update the security keys right after the second resume procedure is finalized i.e. when the UE is already in RRC\_CONNECTED state, but before transmits/receives any data.  |
| ZTE | Using same COUNT value more than once for the same key is definitely not allowed and hence we have to use something similar to Horizontal key derivation but this needs new indication in the CCCH message or new procedure at the UE before and after contention resolution as noted above.  |
| InterDigital | The discussion should be other way around. If any new key derivation is required by SA3, then PDCP COUNT should be reset. Otherwise the COUNT should be retained. |
|  |  |

If PDCP count is reset upon detecting non-SDT data during an ongoing SDT session for CCCH-based approach, UE/network may not be able to detect data duplication and prevent data loss after transitioning into RRC\_CONNECTED.

1. When switching from SDT to non-SDT via CCCH-based approach, if the PDCP count is reset upon detecting non-SDT data during an ongoing SDT session, the UE/network may not be able to detect data duplication and prevent data loss during the transitioning into RRC\_CONNECTED.

### [CCCH point (5)] security associated resume MAC-I (dependent on SA3 outcome)

This sub-section discuss how *resumeMAC-I* is calculated for this 2nd *RRCResumeRequest* msg and some of it is dependent on SA3 outcome. For reference, it is shown below related actions from TS 38.331 on this:

*1> set the* ***resumeMAC-I*** *to the 16 least significant bits of the MAC-I calculated:*

*2> over the ASN.1 encoded as per clause 8 (i.e., a multiple of 8 bits) VarResumeMAC-Input;*

*2> with the* ***KRRCint key in the UE Inactive AS Context*** *and the previously configured integrity protection*

*algorithm; and*

*2> with all input bits for COUNT, BEARER and DIRECTION set to binary ones;*

Therefore, the suggested options are in relation to the NCC and the KRRCint key in used.

Irrespective of the security issue that SA3 is addressing, RAN2 can still discuss whether the key used for generating the *ResumeMAC-I* – for example, is it the one that is currently in use for the SDT data transfer or the one used for generating the *ResumeMAC-I* of the first *RRCResumeRequest*. Proposals were also made to address the security issue related to the reuse of key for generation of the ResumeMAC-I. The proposals for key to use for generating ResumeMAC-I include:

* + 1. NCC provided in last *RRCRelease* message i.e. same as for legacy *RRCResumeRequest* which was also used when the SDT session was started (before initiating ongoing switch to non-SDT).
		2. Horizonal key derivation from current NCC [5] [14] [18].
		3. New NCC that was provided by the serving gNB in the 1st DL message after UE sends the 1st UL SDT msg (i.e. upon initiating the SDT session) [5].
		4. UE’s KRRCint key stored in UE Inactive AS Context i.e. same as for legacy *RRCResumeRequest* which was also used when the SDT session was started (before initiating ongoing switch to non-SDT) [12] (this may depend on the SA3 conclusion).
		5. UE’s new KRRCint key i.e. the one calculated when triggering SDT [12].
1. When switching from SDT to non-SDT via CCCH-based approach, which key is used for generating the *resumeMAC-I* for the 2nd *RRCResumeRequest* msg.

#### Q.14) for 2nd Phase

This Q.14) is created based on previous discussion point.

1. When switching from SDT to non-SDT via CCCH-based approach, which previous option 6.x or new option is preferable to calculate the key used for generating the *resumeMAC-I* for the 2nd *RRCResumeRequest* msg. (understanding that some of this is dependent on SA3 outcome)?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option(s)** | **Justification** |
| Huawei, HiSilicon | Option 6.d) if SA3 concludes security material can be reused for this.Option 6.e) or 6.c) if SA3 concludes security material should not be reused. | The answer to this question depends on the SA3 reply to RAN2 LS. We think option 6.d) is a baseline behaviour, but if SA3 concludes this would cause a security issue, then option 6.e) is the simplest. In this case the security key which is used would be the same as for DCCH message in the DCCH-based non-SDT data arrival indication. Option 6.c) is another viable option, but more complex and would require more specifications changes. |
| ZTE | Option 6.d) | If there is no security issue, then option 6.d is the baseline. Other options are complex and unnecessary and have other issues and there is no time to pursue these at this time. |
| InterDigital | 6.x | COUNT=2 is used for resumeMAC-I calculation for the 2nd RRCResumeRequest (Note: see 33.501 subclause 6.8.2.1.3, COUNT=1 is currently always used for the resumeMAC-I calculation).Alternatively, COUNT=1 is used for the CCCH message of the non-SDT data indication (and the regular resumption case) and COUNT=2 is used for the SDT operation. |
|  |  |  |

### [CCCH point (6)] Identification of UE AS context in the network

For legacy resume procedure, the release of the UE context from the anchor gNB0 is done upon completion of the path switch with the AMF and the serving gNB. However for SDT option, when to release the UE AS context from the anchor gNB may require further discussion considering inputs in [6][19][11][17]. The possible options are the following (as shown in Figure 2):

1. UE AS Context is released from anchor gNB after doing the Path Switch during the ongoing SDT session. The drawback is that the I-RNTI stored in the UE during an SDT session points to the UE context in the anchor gNB when this has already been deleted.
2. UE AS Context is released from anchor gNB after serving gNB provides a new NCC and I-RNTI to the UE (i.e. at the end of the SDT session). The drawback is that serving gNB needs to inform anchor gNB when SDT session successfully ends in order to delete the corresponding UE AS Context.



Figure 2. SDT with anchor relocation from [19] but updated to include both options as explained in [6]

Upon initiation of the corresponding SDT session, the I-RNTI stored in the UE points to the UE context in the anchor/old gNB while the UE AS Context may be released from the anchor gNB after serving gNB completes the path switch with the AMF at the beginning of the SDT session.

On summary, during an ongoing SDT session, UE only has an stored/available I-RNTI that points to the anchor gNB. Therefore, if UE had an ongoing SDT session in a serving gNB that is different than the anchor gNB, the identifier to be included in this 2nd *RRCResumeRequest* message and how it can identify the UE context should be discussed. Some possible options also discussed in the contributions were:

1. I-RNTI i.e. same as for legacy *RRCResumeRequest* message which was also used when the SDT session was started (before initiating ongoing switch to non-SDT). This option would route the 2nd *RRCResumeRequest* message to the anchor/old gNB.
2. New I-RNTI that is provided by the serving gNB in the 1st DL message after UE sends the 1st UL SDT msg (i.e. upon initiating the SDT session) [6][14]. This option would route the 2nd *RRCResumeRequest* message to the serving gNB where the SDT session was ongoing.
3. When switching from SDT to non-SDT via CCCH-based approach and for the scenario where the ongoing SDT session is with UE AS context relocation, how serving gNB can locate the UE AS Context in the network for the 2nd *RRCResumeRequest* msg based on the I-RNTI available in the UE that may point to a released UE context in the anchor gNB.

#### Q.15) for 2nd Phase

This Q.15) is created based on previous discussion point.

1. When switching from SDT to non-SDT via CCCH-based approach and for the scenario where the ongoing SDT session is with UE AS context relocation, which previous option 7.x or new option is preferable for the serving gNB to locate/identify the UE AS Context in the network for the 2nd *RRCResumeRequest* msg.?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | Both option 7a) and option 7b) work | We think both options work. Option 7a) should be the baseline and option 7b) can be used on top of this if it is agreed to support a new DL RRC message, e.g. to handle potential security issues for other cases. |
| ZTE | Option 7a | We think we should not further discuss new solutions if there are security issues we should simply go with DCCH solution.  |
| InterDigital | 7.a) | The 2nd RRCResumeRequest message would be processed by the anchor gNB and so it makes more sense to use the I-RNTI used for the ongoing SDT session. New I-RNTI makes sense only after the context relocation and so 7.b) can’t be the option here.This applies for the DCCH solution as well. |
|  |  |  |

### [CCCH point(7)] Network handling of the 2nd RRCResumeRequest and the RRCResume messages.

When the anchor/old gNB has/keeps stored the UE AS Context, after receiving the 2nd *RRCResumeRequest* msg from the same UE, it needs to be discussed whether anchor gNB generates or not another new KgNB associated with the same target gNB, as explained in Figure 3 below from [18].



Figure 3: Key generation after the second CCCH message [18]

1. When switching from SDT to non-SDT via CCCH-based approach with anchor gNB, after network receives the 2nd *RRCResumeRequest* msg, whether anchor gNB generates (or not) another new KgNB associated with the same target gNB. The following were raised in [18]:
* Will the second RRCResumeReq (i.e., in step 7) be routed to the old anchor gNB regardless of anchor relocation or not?
* After receiving the second *RRCResumeRequest* msg from the same UE, will the anchor gNB generate another new KgNB associated with the same target gNB?

#### Q.16) for 2nd Phase

This Q.16) is created based on previous discussion point.

1. When switching from SDT to non-SDT via CCCH-based approach with anchor gNB, after network receives the 2nd *RRCResumeRequest* msg, does the anchor gNB generate another new KgNB associated with the same serving/target gNB? please justify your response and provide further details on any open points not addressed here or in other questions in relation to this scenario.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Yes/No** | **Justification** |
| Huawei, HiSilicon | It depends on SA3 | This is similar issue as in question Q.2) and it is common for both CCCH and DCCH based solutions. In our opinion it can be consulted with SA3 whether new KgNB\* has to be used, but if it has to be, then with CCCH-based solution it can be derived horizontally as presented above. |
| ZTE | See Q10 | The situation is different between DCCH and CCCH solutions. In case of DCCH solution, the difference is that the DCCCH RRC message will always be routed to the node that terminates the RRC layer and hence the response message (i.e. RRCResume) can be generated by this node. Count continues in both DL and UL and there is no interruption to data and no new keys are derived during the process. In case of CCCH message, the message is always routed to the node identified by the I-RNTI (i.e. the old anchor gNB). However, the old anchor gNB does not terminate the RRC layer in case of anchor relocation. So, the old anchor gNB needs to process the received second RRCResumeReq and the generate new key and provide the new key to the new anchor gNB (although anchor relocation would have happened) and the new gNB would then have to start using the new keys. This needs a new procedure for anchor relocation case (i.e. the old anchor gNB will have to send the new key without UE context in this case and the old anchor gNB would need to retain the UE context even after the UE anchor relocation to support this case). Then, further question is which key is used as the base key for the 2nd key derivation? Is it the key in the stored UE AS security context or is it the first key (generated after the first RRCResume procedure) and this issue is then same as Q10 above. The final question is handling of COUNT. It seems the proponents want to reuse the existing RRCResume procedure, in which case count will be reset, however, when count is reset, there will be out of order packets and/or redundancy in the DL (similar to UL). Further, any packets transmitted in DL during the interaction with the old anchor gNB on Xn, will be lost and will need to be recovered at PDCP level.  |
| InterDigital | Yes | When the UE context is moved from the anchor to a new serving gNB, then new keys should be derived as the old keys are associated with an anchoring point and the anchoring point is moved to the other gNB for this case.This applies for the DCCH solution as well. |
|  |  |  |

## DCCH-based approach

This section aims to clarify how DCCH-based approach work to enable non-SDT switching from an ongoing SDT session considering the inputs provided by companies [3][5][12][18][20][22].

### [DCCH point (1)] Detection of non-SDT data

For DCCH-approach, it is assumed that the PDCP COUNT is maintained as the SDT session fallbacks into CONNECTED upon gNB sends *RRCResume* message during the ongoing SDT session.

1. When switching from SDT to non-SDT via DCCH-based approach, the PDCP COUNT is maintained for SDT DRBs (i.e. the SDT session fallbacks into CONNECTED upon gNB sends *RRCResume* message during the ongoing SDT session).

The sub-section below discusses how/what information the UE shares with the network when non-SDT data becomes available during an ongoing SDT session when using DCCH-based approach.

#### [DCCH point (1.1)] NAS/AS trigger

On new data arrival for the DCCH approach, the following options were proposed:

1. AS triggers the DCCH indication/request from UE to transition into RRC\_CONNECTED when non-SDT data becomes available during the SDT session [18].
2. NAS trigger new DCCH indication/request to AS for UE to move to RRC\_CONNECTED state when non-SDT data becomes available during the SDT session [18].
3. When detecting non-SDT data during ongoing SDT via DCCH-based approach, whether AS layer can initiate the indication/request to the network.

##### **Q.17) for 2nd Phase**

This Q.17) is created based on previous discussion point.

1. From RAN2 point of view, when detecting non-SDT data during ongoing SDT via DCCH-based approach, which previous option 9.x or new option is preferable for AS or NAS layer to trigger the DCCH indication/request to the network?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | Depends on CT1 reply | In our understanding NAS will trigger another request for the UE to move to RRC CONNECTED state and based on this AS will trigger DCCH message transmission. In any case NAS behaviour is not for RAN2 to decide and we have already asked a relevant question to CT1 in R2-2104644. |
| ZTE | Option 9.b (based on latest CT1 status) | Based on latest status in CT1, our understanding is that NAS will trigger a new request this NAS request should trigger the DCCH message in AS.  |
| InterDigital | Depends on CT1 reply | We share Huawei/HiSilicon’s view. |

#### [DCCH point (1.2)] non-SDT notification to network

For DCCH-based approach, how UE sends the indication/request to switch into RRC\_CONNECTED when non-SDT becomes available during an ongoing SDT session, the following options were proposed to provide the indication to the network:

1. New UL RRC message [3].
2. Re-using legacy UL RRC message e.g. *UEAssistanceInformation* message [3].
3. For DCCH-based approach, how UE sends the indication/request to switch into RRC\_CONNECTED when non-SDT becomes available during an ongoing SDT session.

##### **Q.18) for 2nd Phase**

This Q.18) is created based on previous discussion point.

1. For DCCH-based approach, which previous option 10.x or new option is preferable for UE to send the indication/request to switch into CONNECTED when non-SDT becomes available during an ongoing SDT session?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | Option 10.b) | In case we proceed with this approach, we prefer to reuse an existing message and UEAssistanceInformation would fit the purpose well in our opinion. |
| ZTE | no strong view | We are fine with either. However, if NAS triggers the new request, it seems we can define a new message too (including the contents from NAS).  |
| InterDigital | 10.b) | The existing message plus a new IE, which tells gNB that UE requests the switch from SDT to non-SDT. |
|  |  |  |

Additionally, it was also proposed to provide the following information to the network in the indication:

1. List of one or more RB IDs for which data is arrived [3].
2. Data volume per RB or cumulative can also be indicated [3].
3. Resume cause.
4. For DCCH-based approach, which information is provided by UE to indicate/request the switch into RRC\_CONNECTED when non-SDT becomes available during an ongoing SDT session.

##### **Q.19) for 2nd Phase**

This Q.19) is created based on previous discussion point and the responses provided during the 1st phase.

1. For DCCH-based approach, which previous option 11.x or new option is preferable for the information to be provided by UE to indicate/request about the switch into CONNECTED when non-SDT becomes available in UE during an ongoing SDT session?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option(s)** | **Justification** |
| Huawei, HiSilicon | Option 11.c) | Since this will be based on another request from NAS layer, we understand the resume cause will also be provided (pending CT1 response). If this is confirmed by CT1, then we think resume cause needs to be included. There is no need to include 11.a) nor 11.b) – such information will be known via usual means, i.e. BSR. |
| ZTE | Mandatory: 11.cOptional others | Resume cause can be included for sure, the remaining are nice to have and can be further discussed (leave to stage-3).  |
| InterDigital | At least 11.c) | Resume cause should be provided. We are open to other options. |
|  |  |  |

### [DCCH point (2)] switch from SDT to CONNECTED

For DCCH approach, the switch from SDT to CONNECTED is under network control, therefore after UE informs the network that non-SDT data is available, UE continues with the SDT session ongoing until network informs otherwise to UE. For example, network may respond at some point with *RRCResume* or *RRCRelease*. Upon UE receives *RRCResume* message, UE only re-establishes/resumes the non-SDT DRBs (as SDT RBs were already re-established/resumed upon initiating the SDT session) [3][5][12][18].

1. For DCCH approach, after UE informs the network that non-SDT data is available, UE continues with the SDT session ongoing until network informs otherwise to UE (i.e. by transitioning the UE into RRC\_CONNECTED or releasing the UE into legacy RRC\_INACTIVE or RRC\_IDLE). Upon UE receives *RRCResume* message, only the PDCP of non-SDT DRBs are re-established and resumed (as SDT RBs were already re-established/resumed upon initiating the SDT session).

For DCCH-based approach, the topic addressed in Discussion point 1) on how to handle the scenario when switching from SDT to CONNECTED during an ongoing SDT session where the UE context was not relocated by the network at the beginning of the SDT session is also applicable.

1. When switching from SDT to non-SDT (i.e. CONNECTED) via DCCH-based approach and for the scenario where the ongoing SDT session is without UE AS context relocation, previous Discussion point 1) is applicable (and would also need to be addressed).

#### Q.20) for 2nd Phase

This **Q.20)** is created based on previous discussion point.

1. When switching from SDT to non-SDT (i.e. CONNECTED) via DCCH-based approach and for the scenario where the ongoing SDT session is without UE AS context relocation, previous Q.1) to Q.5) and the responses are expected to be applicable. Please indicate if your responses provided for previous Q.1) to Q.5) are not applicable when using DCCH-based approach and if so, please explain the different behaviour/operation.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Q.1) to Q.6) with responses not applicable to DCCH**  | **Justification on the different behaviour/operation for the specific question with DCCH-based approach** |
| Huawei, HiSilicon |  | Our replies to Q.1-Q.6 may apply for this approach.  |
| ZTE |  | yes, our replies Q 1-6 apply here too.  |
| InterDigital | - | Our replies for Q.1-6 apply for the DCCH-based approach too. |
|  |  |  |

#### Q.21) for 2nd Phase

This Q.21) is created based on the responses provided during the 1st phase.

1. What is the expected UE behaviour after UE sends DCCH message during an ongoing SDT session? consider the following options.
2. UE continues with the SDT session ongoing until network informs otherwise to UE by transitioning the UE into RRC\_CONNECTED or releasing the UE into legacy RRC\_INACTIVE or RRC\_IDLE. UE does not expect receiving an explicit confirmation for the reception of the DCCH message.
3. UE expects receiving a confirmation of reception of the DCCH message. If so, clarify the details of this confirmation and the expected UE behaviour when not received.
4. Other options.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | Option 16.2 | Option 16.1 is not acceptable in our opinion. The newly arrived data can be related to latency sensitive applications, e.g. emergency call, and the UE cannot just wait for the SDT procedure to end in case DCCH message was not received by the network. The safest approach would be for the UE to fallback to legacy RRC Resume procedure in case the network does not reply with RRCResume within a certain time (this is why we believe CCCH-based solution makes more sense from the beginning). Alternative could be to move the UE to RRC IDLE, but this would further delay the connection establishment. |
| ZTE | 16.1 or 16.2 | We are not sure if 16.1 and 16.2 are mutually exclusive. Our understanding is also that a network response is needed, but the response will be RRCResume message in DL.With regards to latency of DCCH approach, we don’t think this is any worse than CCCH. There are two cases: * Case1: If there is UL grant available, DCCH message eliminates the need for RACH and RAR (due the unnecessary RACH procedure needed in case of CCCH). Thus it is quicker than CCCH in this case.
* Case 2: If there is no UL grant, both DCCH and CCCH approach will trigger RACH procedure and the MSG3 includes the request to move to RRC\_CONNECTED state

So, in fact, the DCCH approach is at least as good as the CCCH based approach and is better in case there is UL grant to include the DCCH message.  |
| InterDigital | 16.3 | UE should terminate the SDT operation upon data arrival from the non-SDT DRBs. If that’s agreeable, then we don’t need to worry about the UE behaviour of SDT session while in non-SDT session initiation. |
|  |  |  |

### [DCCH point (3)] release from SDT to INACTIVE

#### Q.22) for 2nd Phase

This Q.22) is created based on the responses provided during the 1st phase.

1. When UE generates DCCH message to inform that non-SDT data is available during an ongoing SDT session, what is the expected UE behaviour if the network releases the SDT session before the UE can send the generated DCCH message considering the following options?
2. UE triggers a new RRC Resume procedure (i.e. no changes needed)
3. Other approaches

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Option** | **Justification** |
| Huawei, HiSilicon | Option 16.1) with comments | We are not sure if we can assume no changes are needed. In our understanding (pending confirmation from CT1), NAS will trigger another resume request to AS layers when non-SDT data arrives. This request will trigger the UE to generate the DCCH message. Then the question arises whether another RRC Resume procedure can be triggered based on the same NAS request or we need to indicate a failure to NAS and wait for another request? In both of these cases, some changes to the current specifications will be most likely needed. |
| ZTE | Option 16.1) | When RRCRelease is received and there is pending data at NAS, then NAS will trigger a new RRCResumeRequest (this is same as today and needs no further discussion). Since new NCC will be there in the RRCRelease message, the next RRCResume can be done normally.  |
| InterDigital | 16.2 | We share Huawei/HiSilicon’s view. |
|  |  |  |

### [DCCH point (4)] UL grant availability

#### Q.23) for 2nd Phase

This Q.23) is created based on the responses provided during the 1st phase.

1. What is the expected UE behaviour if there is no UL grant for a UE to send the DCCH message for non-SDT data indication during an ongoing SDT session?

|  |  |
| --- | --- |
| **Company’s name** | **Companies’ views** |
| Huawei, HiSilicon | In this case the UE needs to trigger SR via RACH procedure. This again makes the whole procedure similar to CCCH-based solution and it would be more straightforward to apply it from the beginning in our opinion. |
| ZTE | Yes, in this case RACH procedure will be triggered. * So, if there is no UL grant, then DCCH message will incur an extra RACH procedure (same as CCCH)
* If there is UL grant DCCH approach will avoid the unnecessary RACH procedure, but CCCH approach always requires a RACH procedure and hence the extra latency associated with the RACH procedure to move to connected state.
 |
| InterDigital | UE should trigger a SR (which will end up in RACH procedure initiation) if UE doesn’t have any valid grant for the DCCH message of non-SDT data indication. It needs to be discussed how to uniquely identify the UE from a DCCH message included in Msg3 or MsgA. |
|  |  |

# Failure handling during ongoing SDT session

This section aims to understand how failure of an SDT connection could be handled. The main focus of this email discussion is in a failure due to cell reselection during a given SDT session, however companies are invited to provide their inputs in first sections aiming to understand whether a common UE behaviour could be defined regardless of the kind of trigger of the abrupt SDT failure.

## Triggers to an abrupt termination/failure of an SDT session

The following triggers were identified by companies as potential triggers that lead to an abrupt termination or failure of an ongoing SDT session:

1. Cell reselection [4][7][8][9][14][18]
2. Expiry of failure detection timer [4][8][18][20]
3. Lower layers indication [4][9]
4. Maximum number of retransmissions is reached in RLC [15][18]
5. Reject reception during SDT [9]
6. Abortion of connection establishment by upper layers (need FFS) [9]
7. Other events
8. Identify the trigger events that leads to an abrupt termination or failure of an ongoing SDT session.

#### Q.24) for 2nd Phase

This Q.24) is created based on previous discussion point.

1. Which previous trigger events or new ones can lead to an abrupt termination or failure of an ongoing SDT session?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Events(s)** | **Comments, if any** |
| Huawei, HiSilicon | 1, 2, 3, 4 | Cell reselection is not a failure as such, but we need to specify some UE behaviour for this case. Events 2 and 4 can be treated as SDT failure and also require some UE behaviour to be specified. Event 3 would require to specify some form of RS monitoring in lower layers, e.g. to detect beam failure and we think RAN1 should investigate this. Event 5 can be handled as per legacy behaviour and we do not see it as an “SDT failure”. For RRC Resume abortion it was concluded during the last meeting that it should not be captured in specifications, so we can keep it the same way for SDT. |
| ZTE | 1, 2, 3, 4 | Same view as Huawei on Event 6). Then for Event 5), we have some comments: Considering the data packet may be included in the first UL message (and this is different from legacy reject case), this may lead to some issues with key reuse and hence we propose to not support RRC Reject for SDT. We can discuss this further at next meeting. Events 1-4 seems to be agreeable.  |
| InterDigital | See comment | We think each event has different expected behaviour.1. Cell reselection [4][7][8][9][14][18] [IDC] For cell reselection during ongoing SDT procedure, UE should remain in INACTIVE and transmits an RRC Resume Request at the new cell (still subject to SA3 confirmation)
2. Expiry of failure detection timer [4][8][18][20][IDC] Upon SDT failure detection timer expiry, the UE follows the same procedure as T319 expiry (e.g. UE transitions to IDLE as in the case of expiry of the T319 timer and attempts RRC connection setup).
3. Lower layers indication [4][9][IDC] Upon Lower layer’s failure indication, the UE follows the same procedure as T319 expiry (e.g. UE transitions to IDLE as in the case of expiry of the T319 timer and attempts RRC connection setup).
4. Maximum number of retransmissions is reached in RLC [15][18] [IDC] It should be handled similar way as RLF. So UE should iniate a cell search and is camped on the suitable cell and then initiate the SDT operation at a new serving cell.
5. Reject reception during SDT [9][IDC] UE aborts the SDT operation and performs the legacy procedure for the case of RRCReject reception  (clear keys and stays in INACTIVE)
6. Abortion of connection establishment by upper layers (need FFS) [9][IDC] ditto
7. Other events[IDC] DL data arrival event at gNB also needs to be addressed.
 |
|  |  |  |

## UE’s action upon detecting an abrupt termination/failure of an SDT session

It is also discussed by [4][18][8] whether a common UE behaviour when any of the applicable trigger events from previous Discussion point 13) that lead to an abrupt termination/failure of an SDT session.

1. Having a common UE behaviour when any of the applicable trigger events from previous Discussion point 13) lead to an abrupt termination/failure of an SDT session.

### Q.25) for 2nd Phase

This Q.25) is created based on previous discussion point.

1. Do you support aiming to have a common UE behaviour when any of the applicable trigger events from previous Q.24) lead to an abrupt termination/failure of an SDT session?

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Yes/No** | **Justification** |
| Huawei, HiSilicon | Yes | CCCH-based approach can easily be reused to handle at least cases 1, 2 and 4. This is not possible with DCCH-based approach as DCCH message needs to be sent over a dedicated grant and requires having a stable radio connection. How to handle event 3 depends on the details of lower layers indication, e.g. how much it resembles the current beam failure indications etc. (which should be decided by RAN1). |
| ZTE | Yes | The common UE behaviour should be either:1. UE moves to IDLE mode and informs NAS (e.g. NAS recovery is performed) or
2. UE stays in RRC\_INACTIVE state and initiates PDCP reestablishment based approach.

We prefer option 2). However, we are now a bit concerned that the time remaining in Rel-17 may not be enough for us to solve all the open issues associated with option 2. If we cannot reach a quick consensus on how to handle this, we may have to live with option 1 in Rel-17 |
| InterDigital | No | See our comment for Q.24). |
|  |  |  |

The following approaches are proposed when having to handle abrupt termination/failure of an SDT session:

1. UE transitions autonomously into RRC\_IDLE.
2. UE remains in RRC\_INACTIVE.

For example, for cell reselection trigger event, approach 1) is proposed by [16][14] and approach 2) by [7][12][13][18][20][21][4][10]. The following sub-sections aims to clarify how each approach may work taken into consideration the inputs from proposing companies. The following sub-sections aims to clarify how the approach 2) may work taken into consideration the inputs from proposing companies.

### Approach 2) UE remains in RRC\_INACTIVE

This section aims to clarify how approach 2) would work like, i.e. UE remains in RRC\_INACTIVE upon detecting an abrupt termination/failure of an SDT session. The motivation to enable this mechanism is to guarantee data continuity, and minimize/prevent data loss and duplication of the ongoing SDT session. Upon detecting this failure, the UE shall immediately initiate a sub-sequent access. It is important to keep in mind that the feasibility of this approach 2) depends on the inputs to be provided by SA3 in relation to the security related LS [23] sent by RAN2.

1. Upon UE detects an abrupt termination/failure of an SDT session and remains into legacy RRC\_INACTIVE, the UE shall immediately initiate a request to resume the suspended RRC connection or to (re)start the SDT session

This sub-sequent access after the failure (referred for this discussion as “recovery solution”) is explained by supporting companies from different angles and levels of details. For example:

* **Recovery solution 0)** UE suspends SDT DRBs and PDCP entities upon failure and performs SDT/RRC Resume procedure in the reselected new cell [12][20][7][13].
* **Recovery solution 1)** serving gNB provides a new NCC and I-RNTI upon initiating any SDT mechanism (i.e. 1st DL SDT msg) for future use after current SDT session ends or terminates [4][14].
* **Recovery solution 2)** gNB provides new NCC/RNTI immediately after an abrupt termination of the SDT session with UE’s behaviour aligned with RRC Reestablishment message operation continuing the SDT session in RRC\_INACTIVE [4].
* **Recovery solution 3)** UE uses horizonal key derivation for the recovery mechanism after an abrupt termination of an SDT session (where data uses this new key but short MAC-I may still be calculated based on the stored key) [4].
* **Recovery solution 4)** Assuming that SA3 informs that NCC and I-RNTI can be reused in a different cell, the recovery solution for cell reselection case works as follows [14][18]:
	+ The *RRCResumeRequest* is routed to the old anchor gNB and the old anchor gNB shall be able to verify the UE and generate new keys irrespective of whether anchor relocation and path switch happens before in the SDT session – needs to be checked with RAN3
	+ The new key is derived for the new cell (using the same NCC and the KgNB in the stored UE inactive context, but using new PCI/ARFCN)
	+ PDCP based recovery mechanism is used to recover the lost/unacknowledged data whilst the UE Stays in RRC\_INACTIVE state

On summary, the recovery solutions 1)-4) explained above aim to define a mechanism that address the following concerns:

* Security concerns, such as, b.1) if new NCC is not provided after the failure of the SDT session, b.2) the NCC to be used for the follow up *RRCResumeRequest* in the recovery, and b.3) if the Data PDCP COUNT reset as the same key cannot be used with same count.
* Concerns of additional delay or even confusion when looking for the gNB where UE’s context was previously stored. I.e. I-RNTI stored in UE points to the anchor gNB when the new serving gNB has a copy of the UE AS context or is actually already relocated.

These concerns are common to some of the ones discussed in previous section sections, therefore the suggestion is to discuss them for the failure handling scenario keeping in mind the details/options provided in the corresponding previous points.

1. When a UE detects a failure of an ongoing SDT session and remains in RRC\_INACTIVE, UE shall initiate immediately a recovery mechanism (e.g. via SDT or resume) and the following sub-topics needs to also be addressed for this specific scenario (in relation to the 2nd resume procedure):
	1. Previous Discussion point 3) Resume Cause value for the 2nd *RRCResumeRequest* msg.
	2. Previous Discussion point 4) and Discussion point 5) on the PDCP COUNT and/or security key to be used.
	3. Previous Discussion point 6) on which key is used for the generation of the *resumeMAC-I*.
	4. Previous Discussion point 7) on the identification of UE AS context in the network when the ongoing SDT session is with UE AS context relocation.
	5. Previous Discussion point 8) on the network handling of the 2nd *RRCResumeRequest* and the *RRCResume* messages.

#### Q.26) for 2nd Phase

This Q.26) is created based on previous discussion point.

1. When a UE detects a failure of an ongoing SDT session and remains in RRC\_INACTIVE, UE shall initiate immediately a recovery mechanism (e.g. via SDT or resume). Please indicate if your responses provided for previous Q.11) to Q.16) are not applicable for this specific scenario (in relation to the 2nd resume procedure) and if so, please explain the different behaviour/operation.
	1. Previous Q.11) Resume Cause value for the 2nd RRCResumeRequest msg.
	2. Previous Q.12) and Q.13) on the PDCP COUNT and/or security key to be used.
	3. Previous Q.14) on which key is used for the generation of the resumeMAC-I.
	4. Previous Q.15) on the identification of UE AS context in the network when the ongoing SDT session is with UE AS context relocation.
	5. Previous Q.16) on the network handling of the 2nd RRCResumeRequest and the RRCResume messages.

|  |  |  |
| --- | --- | --- |
| **Company’s name** | **Q.11) to Q.16) with responses not applicable here** | **Justification on the different behaviour/operation for the specific question**  |
| Huawei, HiSilicon |  | All our replies are applicable to this case as well and the common approach can be used for both non-SDT data indication, cell reselection and potentially other “failure” cases in case CCCH-based solution is used. |
| ZTE |  | Our answers are also applicable here. Then, if we go with a solution to support for all these Events, then we need to discuss whether the UE needs to send an UL message to indicate the failure case and we need to agree on the contents of this UL message (e.g. indicating the event that caused the error – e.g. event 1), 2), 3) 4)), other information included in this message etc. Then we can decide which message to use.  |
| InterDigital |  | Our replies are applicable for the scenario. |
|  |  |  |

# Summary report and proposals

<Section to be updated by Rapporteur>

This report summarizes the views of xx companies ().

Aiming to help with the meeting discussion/progress, the proposals are categorized starting with:

* [To agree] when there is large support and hence proposed for easy agreement.
* [To discuss] when there is substantial level of support and agreement may be possible.
* [FFS] when there is low support or companies propose new solutions or options to possibly consider further e.g. if there is sufficient support (understanding that these topic have not been discussed by all companies when providing their views in the different discussion points).

The proposals also start with a number: for the format [x], ‘x’ represents the number of supportive companies (i.e. these solutions are marked as FFS as the proposed solutions were not discussed by all companies) and, for the format [x/y], ‘x’ represents the number of supportive companies, and (y-x) the number of companies with different view.

1. **[To agree]** xxx
2. **[To discuss]** xxx
3. **[FFS]** xxx
4. xxxx.

# Conclusion

The observations captured are the following:

**Observation 1.** xxxx.

The proposals captured are the following:

**Proposal 1.** xxx

The following list shows the proposals above organized based on the suggested priority aiming to help during its meeting discussion:

**Proposals for easy agreement**

xxx

**Proposals for discussion (1st priority) or to be captured as FFS**

xxx

**Proposals for discussion (2nd priority) or to be captured as FFS**

xxx

# Annex: companies’ point of contact

|  |  |  |
| --- | --- | --- |
| **Company** | **Point of contact** | **Email address** |
| Intel Corporation | Marta Martinez Tarradell | marta.m.tarradell@intel.com |
| ZTE Corporation | Eswar Vutukuri | eswar.vutukuri@zte.com.cn |
| APT | Ming-Hung Tao | MingHungTao@fginnov.com |
| Huawei | Dawid Koziol | dawid.koziol@huawei.com |
| TCL | Hejun Wang | hejun.wang@tcl.com |
| NEC | Wangda | wang\_da@nec.cn/wangda@labs.nec.cn |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Reference

1. R2-2104771, Discussion on common control plane issues of SDT, OPPO
2. R2-2104772, on RACH-based SDT, OPPO
3. R2-2104785, Control Plane Common Aspects of RACH and CG based SDT, Samsung Electronics Co., Ltd
4. R2-2104881, Failure and successful handling for an SDT session, Intel Corporation
5. R2-2104882, CP-SDT remaining open issues, Intel Corporation
6. R2-2104883, RA-SDT remaining open issues, Intel Corporation
7. R2-2105101, Control plane aspects on the SDT procedure, Apple
8. R2-2105281, Consideration on CP issues, CATT
9. R2-2105448, Control plane aspects of SDT, NEC
10. R2-2105549 on RACH-based SDT, Spreadtrum Communications
11. R2-2105574, Small data transmission with RA-based schemes, Huawei, HiSilicon
12. R2-2105575, Control plane common aspects for SDT, Huawei, HiSilicon
13. R2-2105691, Discussion on subsequent SDT in NR, timer handling, and support for SRB1/2, Sony
14. R2-2105760, Common aspects for SDT, Ericsson
15. R2-2105810, Consideration on CP issues for small data transmission, Lenovo, Motorola Mobility
16. R2-2105885, Discussion on open issues of SDT, Qualcomm Incorporated
17. R2-2105886 on open issues for RACH based SDT, Qualcomm Incorporated, R2-2103433
18. R2-2105928, Control plane common aspects of SDT, ZTE Corporation, Sanechips
19. R2-2105929, Open issues for RACH based SDT, ZTE Corporation, Sanechips, Rel-17
20. R2-2106050, SDT CP and configuration aspects, InterDigital
21. R2-2106132, Discussion on CP aspects of SDT, China Telecomunication Corp.
22. R2-2106256, Anchor relocation and context fetch, CMCC
23. R2-2104401, LS to SA3 on Small data transmissions, Interdigital, April 2021.
24. R2-2104644, LS to CT1 on Small data transmissions (Ccing SA2), Intel Corporation, April 2021.