3GPP TSG-RAN WG2 Meeting #116bis Electronic R2-220xxxx

Elbonia, 17 – 25 January 2022

**Agenda item: 8.6.3**

**Source: Nokia (Rapporteur)**

**Title: Report of [Post116-e][510][SDT] CCCH and DCCH (Nokia)**

**WID/SID: NR\_SmallData\_INACTIVE - Release 17**

**Document for: Discussion and Decision**

# 1 Introduction

This document is the report of the following email discussion:

* [Post116-e][510][SDT] CCCH and DCCH (Nokia)

 Scope: Aim to have CRs describing each solution and discuss technical points on the two solution such that a decision can take place next meeting.

 Deadline: Long

# 2 Contact Points

Respondents to the email discussion are kindly asked to fill in the following table.

|  |  |  |
| --- | --- | --- |
| Company | Name | Email Address |
| Nokia (Rapporteur) | Samuli Turtinen | samuli.turtinen@nokia.com |
| ZTE | He Huang | Huang.he4@zte.com.cn |
| Samsung | Anil Agiwal | anilag@samsung.com |
| Intel | Marta Martinez Tarradell | marta.m.tarradell@intel.com |
| OPPO | Xue Lin | linxue@oppo.com |
| CATT | Chandrika Worrall | Chandrika@catt.cn |
| Huawei, HiSilicon | Dawid Koziol | dawid.koziol@huawei.com |
| Fujitsu | Ohta, Yoshiaki | ohta.yoshiaki@fujitsu.com |
| Sharp | Chongming Zhang | Chongming.zhang@cn.sharp-world.com |
| Xiaomi | Yumin Wu | wuyumin@xiaomi.com |
| LG Electronics | SeungJune Yi | seungjune.yi@lge.com |
| Interdigital | Keiichi Kubota | keiichi.kubota@interdigital.com |
| China Telecom | Jincan Xin | xinjc@chinatelecom.cn |
| Henrik Enbuske | Henrik Enbuske | Henrik.enbuske@ericsson.com |
| Qualcomm | Ruiming Zheng | rzheng@qti.qualcomm.com |
| NEC | Wang Da | wang\_da@nec.cn |
| vivo | Yitao Mo (Stephen) | yitao.mo@vivoo.com |
| Sony | Anders Berggren  | Anders.Berggren@sony.com |

# 3 Discussion

Agreeing on a solution option between CCCH- and DCCH-based solution for the non-SDT data arrival during SDT procedure has been challenging and open for several meetings already. Details of the solutions and related issues have been discussed, e.g., in [1-7] in the previous RAN2#116-e meeting.

The intention of this discussion is to gather companies’ views on the presented issues for both solutions to guide the discussion on agreeing on a solution basis for the long-lasting issue.

Since solution opponents for both solutions provided specific issues of the solutions, it seems fair to ask what companies think about these issues as online discussion was mainly about debating that there are open issues in both solutions without solid answers if the issues were actually meaningful in terms of specification effort. The intention would be also to describe how the issue is solved in the solution option, ie., more details of each solution should be described.

Even though both solutions on high level have been clear for pretty much everyone, they are shortly recapped hereinafter for convenience:

 When SDT procedure is ongoing (ie., SDT has been initiated by RRC layer) and data arrives into a buffer of at least one SRB/DRB not configured for SDT, the UE

* DCCH solution: triggers a transmission of an RRC message over SRB1 (tbc.) indicating the availability of data in the buffer of the SRB(s)/DRB(s) not configured for SDT. The RRC message is transmitted as SDT data in the SDT procedure. Based on the RRC message, the NW may bring the UE into CONNECTED mode.
* CCCH solution: terminates the SDT procedure and triggers an RRC resume procedure (non-SDT). Based on the *RRCResumeRequest*, the NW may bring the UE into CONNECTED mode.

## 3.1 Questions on DCCH based solution

[2, 6] provides a set of open issues wrt. DCCH-based solution. These issues are discussed hereinafter.

Firstly, it should be discussed whether a new resume cause is needed, e.g. if non-SDT is triggered by RNA update or signalling while SDT was triggered for data etc. The CT1 reply on this aspect provided in [8] is not completely clear but seems to assume that for suspended resources, NAS will require Service Request procedure to be initiated and NAS will need to provide UAC parameters based on the reason for that Service Request. This may need to be further clarified from CT1.

**Question 1**: Do you agree that resume cause needs to be indicated in the RRC message for non-SDT data indication for DCCH based solution? Further, should this be confirmed from CT1 with an LS?

|  |
| --- |
| Answers to Question 1 |
| Company | Yes/No | CT1 LS: Yes/No | Technical Arguments |
| ZTE | No | No | Firstly, we think this discussion is common to CCCH and DCCH solutions. We need to design the solution to work independent of NAS triggers for both CCCH and DCCH case. Then, we want to point out that none of this is new (i.e., even in legacy resume, new data or new NAS procedure can arrive whilst T319 is running). The current behaviour is that once a resume procedure is initiated (i.e. T319 is running), AS doesn’t respond to any new triggers from NAS except NAS abort procedure. This legacy behaviour should not be changed in Rel-17 just for SDT! If we change this behaviour for SDT, then we will have two procedures in AS (when SDT is running, AS will respond to new triggers from NAS whilst when SDT is not running, AS will continue with existing resume procedure and such a situation is not good). Hence, the non-SDT data arrival indication should be fully handled within AS without any need for NAS triggers both for CCCH and DCCH solutions.  Thus, for non-SDT data arrival, we don’t think the resume cause is needed in the DCCH message. In our view, non-SDT data arrival indication is a RAN level indication used to indicate to the network that there is new data which is for non-SDT RBs. This is consistent with the feedback from CT1 [8] that “once small data transmission is initiated the UAC parameters (access category and access identity) for subsequent UL data for non-SDT DRBs to use will be the same as those for UL data for SDT DRBs”, it seems the resume cause will not change during the SDT, thus there is no need to include the resume cause again in the DCCH message.Even further, we think if there is some ambiguity here, we should actually clarify it for legacy resume first! But, we think the AS procedure here is fairly clear (i.e. once there is an ongoing resume procedure, AS doesn’t respond to any further triggers from NAS until the previous resume procedure is complete and this legacy behvaiour should not be changed).  |
| Samsung | No | No | We do not see any need to indicate resume cause. |
| Intel | No | No | On the RNA topic, how RNAU is handled in relation to an SDT procedure needs to be discussed by RAN2 independently on which solution is chosen to handle the non-SDT traffic during an SDT session. We explained in R2-2109620 that two possible behaviours are proposed by companies:* Option 1) T380 is stopped upon start of the SDT session.
* Option 2) T380 continues running upon of the SDT session. T380 will be restarted as legacy on receipt of RRC Release message.

Our preference is that periodic RNAU timer (T380) continues running during the SDT procedure. However, if T380 expires during an ongoing SDT proc., UE does not need to notify the network as UE already communication ongoing with the network while SDT procedure is ongoing. Therefore, there is no need to send RNAU cause value to the network while the SDT session is ongoing.On the NAS/CT1 topic, CT1 did not have consensus on the NAS handling during SDT procedure as captured in their LS C1-215152. In our understanding, there is no need to contact CT1 on this again. If CT1 reaches consensus in future meetings and agrees on the cause, RAN2 could easily incorporate it in the UL DCCH msg in used. On summary, from RAN2 point of view, it seems sufficient to notify the network that non-SDT data is available as explained in [1]. |
| OPPO | No | No | The RRC message itself can be used as the indication of non-SDT data arrival. |
| CATT | See comments | No  | If NAS provides resume cause to AS layer when new data/signalling arrives during SDT, resume cause can be included in the RRC message for DCCH based solution. But if NAS doesn’t provide resume cause to AS layer for the case, resume cause doesn’t need to be included in the RRC message. We don’t think we need to contact CT1 on this again. And share the same view with Intel, if CT1 reaches consensus on cause value in future meetings, RAN2 can include it in DCCH message. |
| Huawei, HiSilicon | Yes | Yes | We think it is important to indicate the resume cause, e.g. in case the access is for emergency call, it is important that this is treated by the network with very high priority (e.g. move the UE to RRC Connected right-away, without waiting for the ongoing transmissions to be acknowledged). If the network assumes the same resumeCause which is most likely mo-Data, then the transition to RRC Connected can happen later, e.g. after the ongoing transmissions are finalized.CT1 reply to RAN2 LS was quite confusing as it seems CT1 described a case which is different than the one RAN2 asked about, so not sure how much we can rely on this. It would be better to clarify with CT1.Regarding RNA update during an ongoing SDT procedure our view is that UE does not need to perform RNAU during an SDT procedure as there is already an ongoing communication between the UE and the network |
| Fujitsu | Yes | Yes | New cause in *RRCResumeRequest* would be introduced. This is useful for the gNB processing in terms of identifying of the purpose of *RRCResumeRequest*. Otherwise, it increases the complexity of the gNB. |
| Sharp | Yes with comments | No | According to the CT1 LS, the resume cause is not always provided from upper layer. So we think if it is provided, it could be included in the RRC message, otherwise, there is no need to include it. |
| Xiaomi | No | No | The DCCH RRC message itself is sufficient. |
| LG | Yes | Yes | Companies who answered “No” seem to assume that a new RRC procedure is used, as can be seen in [4]. But, our assumption is that the existing RRC Resume procedure is reused, which can minimize the spec impact. If a new RRC procedure is introduced, it means that we have two different procedures for the same purpose, i.e. new procedure and RRC Resume procedure, depending on whether there is ongoing SDT procedure or not. Considering that non-SDT data arrival during short-period SDT procedure is not frequent case, introducing a new procedure for not frequent case is too much.To rely on the existing procedure and apply the same RRC message construction, a new resume cause is needed, as shown below.1> else if the resumption of the RRC connection is triggered by upper layers:2> if the upper layers provide an Access Category and one or more Access Identities:3> perform the unified access control procedure as specified in 5.3.14 using the Access Category and Access Identities provided by upper layers;4> if the access attempt is barred, the procedure ends;2> if the resumption occurs after release with redirect with *mpsPriorityIndication*:3> set the resumeCause to mps-PriorityAccess;2> else:3> set the *resumeCause* in accordance with the information received from upper layers; |
| Interdigital | Yes | Yes | Non-SDT data resumption is supposed to be equivalent to the legacy resumption and so the resume cause should be informed to gNB upon non-SDT resumption.Regarding to the CT1 reply LS, CT1 didn’t get what RAN2 wanted to know and so it’s better to clarify things to get a right answer from them. |
| China Telecom | Yes | Yes | It is better to indicate the resume cause to gNB to respond to the non-SDT data arrival more correctly. |
| Ericsson | Yes | Yes | We believe a resumption cause is needed and agree with other on that the priority of the cause is required. Additionally the RRC message is not a new message as pointed out by LG. As a result we think this must be the base-line also as it aligns with the legacy principle for the RRCResume procedure. |
| Qualcomm | No | No | For now, we don’t think it is needed to indicate resume cause. And this question is for both DCCH solution and CCCH solution. The concern raised for such as emergency call is also for CCCH solution. CT1 LS C1-215152 statement is clear at least for this issue. ‘once small data transmission is initiated the UAC parameters (access category and access identity) for subsequent UL data for non-SDT DRBs to use will be the same as those for UL data for SDT DRBs’. Per our understanding, it means resume cause is not changed hence it is no need to indicate again. For other CT1 mentioned cases, those are separate issues which might be further discussed in CT1, thus no need to send LS to CT1 again. |
| Nokia, Nokia Shanghai Bell | Yes | Yes | Agree with Huawei. |
| NEC | Yes | Yes | If NAS layer provide resume cause to the AS layer upon non-SDT data arrival, we think it is necessary for the UE to provide this resumeCause to the gNB to help the network to understand the cause of the second RRC Resume procedure. It is not clear if the NAS layer provide resume cause to the UE due to non-SDT arrival based on the CT1 reply LS R2-2109308, so it is better that we need to send LS to CT1 to confirm this.About RNA update during SDT, RAN2 has discussed on the similar issue and agreed at the main session of RAN2#113bis-e that “The UE should not start the 2nd RRC resumption procedure when there is a RRC resumption procedure ongoing (no spec change required)”, therefore a seond RRC Resume procedure for RNA update should not be triggered during SDT. |
| vivo | No | No | If the DCCH solution is adopted, we assume the newly introduced RRC message can only be reported when there is non-SDT arrival during SDT procedure. The NW can identify the UE situation upon the reception of this RRC message. We fail to see the motivation.  |
| Sony | No | No | See no need to indicate resume cause in this case |

**Summary 1**: TBD.

**Proposal 1**: TBD.

Regardless of the responses to Question 1, the details of the content of the RRC message for non-SDT data indication should be discussed. For instance, is there a need to include further information on top of the indication, like SRB(s)/DRB(s) information with data, *resumeCause* (see previous question), amount of data, etc.

**Question 2**: What information should be included in the RRC message for non-SDT data indication for DCCH based solution?

|  |
| --- |
| Answers to Question 2 |
| Company | Technical Arguments |
| ZTE | Since UE only needs to inform NW the arrival of non-SDT data, we don’t see the need to have any extra information besides the message itself (i.e. an empty message as proposed in [4] is sufficient). |
| Samsung | Non SDT data indication is sufficient. |
| Intel | UE only needs to notify to the network that non-SDT data is available. This can be done via a new UL RRC message as shown in drafted CR of [4], or as a new container defined within the *UEAssistanceInformation* message as shown in the drafted CR of [7]. As we explained in previous Q1, from RAN2 point of view, there is no strictly need for UE to provide any additional information. |
| OPPO | Share same view as ZTE. No extra information needs to be included in RRC message. |
| CATT | Same as Q1, currently it is enough to only indicate non-SDT data indication in DCCH based solution. But if CT1 reaches consensus that NAS provides resume cause to AS layer when new data/signalling arrives during SDT, it can be included. |
| Huawei, HiSilicon | As mentioned above, we think resumeCause should be included. We do not see the need for any other information, e.g. the amount of data can be signalled via BSR as for normal connection resume. In theory, as an alternative to resumeCause, the information about which RB triggered the indication could be used, but we still prefer to rely on resumeCause as for legacy. |
| Fujitsu | If something is useful, RAN2 can discuss it. |
| Sharp | Further information is better, however, they are kind of optimization which could be discussed for future. |
| Xiaomi | Agree with ZTE. |
| LG | We think existing RRCResumeRequest message should be used. |
| Interdigital | resumeCause needs to be present in the non-SDT data arrival indication. |
| China Telecom | We think the resumeCause should be included. |
| Ericsson | See Q1. AS we see a RRC procedure aligned w legacy we assume resume cause is used. |
| Qualcomm | Currently, non-SDT indication is enough like the CR in [4]. If CT1 further reaches more agreements such as new resume cause, it can be further discussed. |
| Nokia, Nokia Shanghai Bell | We think the resumeCause on top of the non-SDT data indication is required, and this should be sufficient. |
| NEC | Other information besides resumeCause can be seen as optimization, should be deprioritized. |
| vivo | We share the same view with ZTE. |
| Sony | Basically, it would be enough with an empty RRC message. |

**Summary 2**: TBD.

**Proposal 2**: TBD.

Another issue is whether a new UL RRC message would be defined, or an existing UL RRC message (like *UEAssistanceInformation*) could be utilized for the purpose.

**Question 3**: Do you prefer to introduce a new UL RRC message for the non-SDT data indication for DCCH based solution? If not, which existing UL RRC message is preferred to be utilized and why?

|  |
| --- |
| Answers to Question 3 |
| Company | Yes/No | Technical Arguments |
| ZTE | Yes, but no strong view | We have slight preference to use a new DCCH message, which can minimize the impact on specs. But if majority want to use the existing message, it is also fine. We don’t think this is a critical issue, and we can simply follow the majority view. |
| Samsung | Yes but | Slightly prefer new message as it has less overhead. However, if majority view is to use legacy message, we are ok to use *UEAssistanceInformation* |
| Intel | Yes | We have slightly preference to define a new UL RRC msg. as it seems cleaner and with less overhead (with corresponding drafted CR in [4]). However, if majority view prefers reusing an existing UL RRC msg, we are open to use *UEAssistanceInformation* message (with corresponding drafted CR in [7]).  |
| OPPO | Yes but | We prefer to use a new RRC message but we are also fine to reuse UEAssistantInformation. |
| CATT | Yes but no strong view |  |
| Huawei, HiSilicon | No | For DCCH, we would prefer to reuse ReleasePreference indication from UEAssistanceInformation, with an extension to include resumeCause as this IE already serves a similar purpose. |
| Fujitsu | Abstain | Before going into details, our priority would be to decide which solution RAN2 will go for. |
| Sharp | - | No strong opinion, we can go with majority view. |
| Xiaomi | No strong view | We slightly prefer a new RRC message, as a clean solution. |
| LG | No | According to the CT1 LS, the NAS is agnostic to DRBs, and NAS will request RRC resume as in legacy even if non-SDT becomes available during SDT procedure.*if new UL data or NAS message becomes available for which non-SDT radio bearers are not established, the current behaviour (of NAS in 5GMM\_CONNECTED mode with inactive indication) applies**, i.e. any new pending UL data associated with a PDU session with no suspended user plane resources, will require the Service Request procedure to be initiated and NAS will need to provide UAC parameters based on the reason for that Service Request.*This is same as legacy RRCResume procedure, and the UE should reuse existing RRCResumeRequest message. |
| Interdigital | No | UAI with an extension of resumeCause |
| China Telecom | Yes but | Slightly prefer to introduce a new RRC message. But we are fine to reuse the existing message if majority prefer.  |
| Ericsson | No | We agree w LG. If to use DCCH message, we think existing messages can be re-used. |
| Qualcomm | Yes | *UEAssistanceInformation* is also acceptable for us. |
| Nokia, Nokia Shanghai Bell |  | No strong view, both can work. |
| NEC | No strong view | Either is fine for us. |
| vivo | No | We also think the existing preferredRRC-State (i.e. ENUMERATED {idle, inactive, connected, outOfConnected}) can be used.  |
| Sony | Yes | Prefer a new message, no strong view |

**Summary 3**: TBD.

**Proposal 3**: TBD.

The error recovery for DCCH based solution is also unclear, unlike in CCCH based solution where T319 is started when the resume procedure is initiated. While the details of the SDT failure timer are yet unclear, generally it has been agreed to be longer than T319 to account the unknown time required to complete the SDT procedure. Hence, the SDT failure timer applicability for non-SDT data arrival is questionable, for instance, in case the non-SDT data is high priority traffic, e.g. an emergency call.

**Question 4**: Do you agree the SDT failure timer is not sufficient for error handling in case of non-SDT data indication for DCCH based solution? If yes, what should be the UE behaviour in case the network is not responding for the DCCH based non-SDT data indication?

|  |
| --- |
| Answers to Question 4 |
| Company | Yes/No | Technical Arguments |
| ZTE | No | We think SDT failure timer is sufficient.First of all it is unclear why the UE aborting the ongoing connection and initiating a new RACH procedure (which may or may not succeed) has a better chance of success than UE sending a DCCH message using dedicated resources in the ongoing connection (radio conditions won’t change just because UE decides to ignore dedicated resources such as dedicated UL grant etc). The point is that if there is some problem on the Uu, (and hence the UE finds itself in a condition where UL DCCH message is not going through), initiating a new RACH procedure (which then relies on RACH, RAR, contention resolution and then providing the same information as the original information seems to provide no advantage at all! Hence, we don’t think any additional mechanism is needed. RLC retransmission can ensure the DCCH message can reach NW successfully, and we can rely on the NW to ensure the DCCH message can be treated correctly.  |
| Samsung | No | Share ZTE’s views |
| Intel | No | We understand that SDT failure timer is defined to determine any error handling during an ongoing SDT session. Moreover, we do not understand why special error handling is required for UL RRC msg notifying that non-SDT data is available in comparison with other UL SDT signaling/data that could be sent during an ongoing SDT session. If for any failure cases, there was no response, this scenario is also equally possible/applicable to the new connection for CCCH solution. So we see no difference between the two failure cases. In addition, for the example mention of high priority traffic (e.g. an emergency call), there is no special handling defined either for a UE in RRC\_CONNECTED. On other hand, as explained in previous Q1, if CT1 were to agree that corresponding cause information is critical, RAN2 could easily incorporated it in the UL DCCH msg to be used. |
| OPPO | No | Share the same view as ZTE. |
| CATT | No | RLC retransmission for DCCH based solution is enough to ensure that the network can receive the message successfully. Then it is up to network implementation when and how to response to the UE. |
| Huawei, HiSilicon | No | There are multiple mechanisms built into RA procedure to ensure that it succeeds, i.e. preamble retransmission, power ramping etc. which makes CCCH solution more reliable. For DCCH on the other hand, we have to rely only on RLC retransmissions, which can take longer time and it should be noted that dedicated resources in SDT are much less reliable than in RRC Connected as we do not have beam management, RLM etc. In our opinion all these mechanism makes DCCH solution actually less reliable than CCCH approach. However we tend to agree it does not seem to make sense to optimize DCCH solution for this as that would require quite some additional work.  |
| Fujitsu | No | SDT failure timer should handle all errors. |
| Sharp | No | Share the same view with ZTE. |
| Xiaomi | No | Share ZTE’s views. |
| LG | Yes | The SDT failure timer is used for detection of failure of the SDT procedure. However, the non-SDT data indication is a separate procedure, as can be seen in draft CR [4]. As this is a separate procedure from the SDT procedure, the SDT failure timer is not applicable. We think the non-SDT data indication is a RRCResume procedure, and T319 could be used for this. |
| Interdigital | No | The DCCH message is sent with ARQ operation and the SDT failure timer would be sufficient to handle the case that the transmission fails. |
| China Telecom | No | Share the same view as ZTE. |
| Ericsson | No | Agree with Huawei |
| Qualcomm | No | SDT failure timer is sufficient. The purpose of the whole design is just to inform network non-SDT data arrival. It is quite complicated to let UE aborting the normal SDT procedure and initiate a new RACH to just send a CCCH message. We don’t understand why using RACH can provide more reliability or short latency than RLC retransmission, which is obviously a normal error handling scheme. |
| Nokia, Nokia Shanghai Bell | Yes | Random Access procedure error recovery plays no role here if there is a grant for UE to transmit the non-SDT data indication. The SDT failure timer can be very long compared to T319 for instance given the nature of the SDT procedure since its length is not know in advance by neither UE or NW. We think the T319 can be used for the purpose of non-SDT data arrival indication for DCCH solution – the same would be applied for CCCH solution as well. |
| NEC | No | To make it simple, any timer enhancement for the DCCH solution is less preferred.Actually the question is not very clear to us, if the concern is that the DCCH is sent, but the network is not able to response before SDT timer expiry, what is the UE behaviour, we think the same UE behaviour upon SDT timer expiry should be applied, which is UE goes to IDLE mode. |
| vivo | No | DCCH-based reporting is just a sub-procedure of SDT. When the SDT failure timer expires, it means the whole SDT procedure fails. Then some recovery behavior will be performed. We don’t see the strong motivation to have separate recovery behavior is needed for DCCH solution (i.e. a unified UE recovery solution is preferred).  |
| Sony | Yes | We prefer to define a new timer, in order to operate independently for small data RACH procedure. The reason is that available data for SDT is variable in size and its delivery will also be variable in time due to subsequent transmissions. |

**Summary 4**: TBD.

**Proposal 4**: TBD.

For CCCH based solution, the NW can respond with existing RRC messages as specified. For DCCH based solution, however, this is not completely clear. For instance, can the NW respond with *RRCReject* based on the RRC message for the non-SDT data indication and would the UE go to RRC\_INACTIVE mode based on it? Furthermore, would the UE terminate the ongoing SDT procedure or continue with it?

**Question 5**: Do you agree that the NW can respond with *RRCReject* for the RRC message for the non-SDT data indication? If yes, what should be the UE behaviour in this case?

|  |
| --- |
| Answers to Question 5 |
| Company | Yes/No | Technical Arguments |
| ZTE | No | The UE has already sent an RRCResumeRequest message. So, if the network may have already retrieved the UE context and once the UE context is available, there is actually no need to use RRCReject anymore. The purpose of RRCReject is when the UE context is not yet retrieved. Of course, if the UE context has not been retrieved (or network is unable to identify the UE etc, then the network can send RRCReject to the UE – this is legacy behaviour). So, whether or not RRCReject is used depends on whether or not network is able to retrieve the UE context. This has nothing to do with CCCH or DCCH solution to be used! The actual UE behaviour upon receiving the RRCReject is also the same as legacy and needs no changes (as this can only happen in case UE context is not retrieved).  |
| Samsung | No | Share ZTE’s views |
| Intel | No | We understand that RRCReject msg can only be used in respond to the RRCResumeRequest msg. When UE has an ongoing SDT procedure with UL/DL SDT data being exchanged, we understand that network should not respond with RRCReject. If there is a congestion situation, network can always choose to send RRCRelease msg to terminate the SDT procedure similarly to legacy operation in RRC\_CONNECTED. |
| OPPO | No | RRCReject is one of the responses to RRCResumeRequest/RRCSetupRequest. We do not think this message can be used as the feedback for a DCCH message. In addition, RRCReject can be sent after RRCResumeRequest is received for overload balancing, it is unreasonable to send an RRCReject message in an ongoing SDT procedure. |
| CATT | No | Share the same view with ZTE. |
| Huawei, HiSilicon | Yes | RRCReject can be used by the network, e.g. in case it cannot handle the requested connection, e.g. due to overload and wants to use waitTime. In our understanding, upon receiving RRCReject, the UE goes to RRC INACTIVE and should not continue the SDT session. |
| Fujitsu | Yes/No | This is up to NW implementation. |
| Sharp | No | If the intention is to make the UE go to INACTIVE mode or terminate the procedure, RRC release is enough.If the intention is to continue with the ongoing SDT, no response is necessary. |
| Xiaomi | No | Share ZTE’s views. |
| LG | Yes | In the legacy RRCResume procedure, after sending RRCResumeRequest message, the UE can receive one of RRCResume, RRCSetup, RRCRelease, and RRCReject. Which message is received is all up to network implementation. The UE behavior when RRCReject is received is well specified in 5.3.15 in RRC specification. |
| Interdigital | Yes | We assume that the non-SDT resumption would be equivalent to the legacy resumption. Even if the current serving gNB had enough capacity for SDT operation, that doesn’t mean the gNB would have enough capacity for the non-SDT operation. Thus, gNB should have a means to reject the non-SDT resumption like legacy. |
| China Telecom | No | Share the same view with ZTE. |
| Ericsson | Yes | This is up to NW implementation. |
| Qualcomm | No | Why network just sends the RRCRelease message which also can meet the same purpose, especially for an ongoing SDT session. |
| Nokia, Nokia Shanghai Bell | Yes | NW may have not retrieved context before the UE sends the non-SDT data indication and NW may want to reject it due to overload. However, it should be discussed if the SDT procedure should continue or not in this case. |
| NEC | No | RRCReject means the network is not able to accept the request, for DCCH solution, “do not response” has the almost the same effect as sending RRCReject message, and no specification impact.  |
| vivo | Yes | In our understanding, the NW, by implementation can send RRC Reject due to congestion control. We failed to see the motivation to limit the NW implementation. |
| Sony | No | Share the view with ZTE |

**Summary 5**: TBD.

**Proposal 5**: TBD.

Another case described in [6] is in case the NW initiates the transmission of *RRCRelease* message before receiving the RRC message for non-SDT data indication from the UE, what would be the UE behaviour. Naturally, the UE does not know if the NW received the non-SDT data indication before or after triggering the RRC Release.

**Question 6**: What should be the UE behaviour in case it receives *RRCRelease* message after transmitting the RRC message for non-SDT data indication to NW?

|  |
| --- |
| Answers to Question 6 |
| Company | Technical Arguments |
| ZTE | No matter non-SDT data indication has been send or not, once RRC release message is received and there is data still buffered on UE side, the UE will initiate another resume procedure accordingly, which is the same as the current resume procedure triggered by DL Non-SDT data in case SDT without anchor relocation.By the way this exact case can happen today in connected mode as pointed out multiple times! i.e. UE is in connected mode, new pending data or NAS procedure is initiated, but, network sends RRCRelease to the UE (before the new procedure is completed). Then what is the UE behaviour in the above case? The same behaviour would also apply for this case too.  |
| Samsung | UE will process the RRC Release in same manner irrespective of whether it has send non-SDT data indication or not. After processing the RRC Release, if there is data in buffer, UE will initiate resume procedure as usual. |
| Intel | As we explained in [7], if this happens there will be pending data or NAS procedure and hence a new connection will be triggered by NAS. Further, it should be noted that this can happen anyway even today for a UE in RRC\_CONNECTED. For example, UE may be in connected mode and may receive *RRCRelease* msg just when the upper layers in UE initiates some new procedure (which the network is not yet aware of). And we don’t say that the UE terminates the ongoing procedure autonomously in this case. Moreover, even in CCCH case, if the UE sends second *RRCResumeRequest* message, the network can still send RRCRelease for the ongoing SDT session before the gNB can decode the 2nd *RRCResumeRequest* message. The consequences of such collision case for CCCH solution could be even worse. If the network sent an *RRCRelease* msg just as the UE is aborting the SDT session (or just after), the UE will not receive the *RRCRelease* msg (as it is not monitoring the C-RNTI of the aborted SDT session). The network is not aware of UE’s aborting actions (i.e. not monitoring of the PDCCH) neither that the UE has not received the *RRCRelease* msg of the SDT procedure successfully terminated. Now if the UE sends the second *RRCResumeRequest*, the network will treat this as a normal Resume request and the second *RRCResumeRequest* for non-SDT data will fail. Recovery from this is unclear and might probably results for the UE having to go through RRC IDLE.  |
| OPPO | UE goes into normal RRC\_INACTIVE state and then trigger a new RRC resume procedure. |
| CATT | When the UE receives RRCRelease message but the UE still has UL data to be transmitted, the UE will initiate another resume procedure. This doesn’t only happen when the UE transmits the RRC message for non-SDT data indication to NW, but also happen with CCCH-based solution and legacy RRC resume procedure. We don’t see there is any special handling or discussion with DCCH based solution. |
| Huawei, HiSilicon | The problem with DCCH solution is that it is unclear what the trigger of the resume would be after receiving RRCRelease as the UE already indicated the willingness to resume the connection via DCCH message. It might need to be clarified in NAS specifications that the connection request has to be sent again in such case. RRCRelease message uses RLC AM, so the issue mentioned by Intel will not happen (i.e. the network will know the UE did not receive the RRCRelease as there is no confirmation of reception). |
| Fujitsu | The intended UE behaviour would be that UE goes into normal RRC\_INACTIVE state and then trigger a new RRC resume procedure. But, if the UE is instructed to move on to RRC\_IDLE, the UE moves on to RRC\_IDLE.  |
| Sharp | UE is expected to initiate a new RRC resume procedure as legacy. |
| Xiaomi | Agree with ZTE. |
| LG | This is the problem of DCCH solution.1. The UE does not know whether the non-SDT data indication is correctly received by the NW.2. It is not clear how the buffered data can trigger a new RRCResume procedure. In current specification, there is no trigger for this case.*The UE initiates the procedure when upper layers or AS (when responding to RAN paging, upon triggering RNA updates while the UE is in RRC\_INACTIVE, or for NR sidelink communication/V2X sidelink communication as specified in sub-clause 5.3.13.1a) requests the resume of a suspended RRC connection.*3. There may not be non-SDT data stored in the PDCP buffer. It is agreed in RAN2#116 that the NAS may or may not submit non-SDT data to the AS. It’s up to UE implementation.1. The NAS data can arrive at PDCP layer even if the RB is suspended. When does the NAS deliver UL data to AS is up to UE implementation. No spec changes are needed

If NAS didn’t submit non-SDT data to AS (i.e. only request AS to resume the RRC connection), how the UE triggers a new RRCResume procedure? |
| Interdigital | We have the same concern as Huawei/HiSilicon. It’s not clear what triggers another non-SDT data arrival indication. The current 38.331 specifies "The UE initiates the (resume) procedure when upper layers or AS requests the resume of a suspended RRC connection" and so it currently relies on the exiplicit request by NAS or AS. Thus, the expected UE behaviour should be specified somewhere in NAS or AS spec. |
| China Telecom | When the UE receives the RRCReject message but there is still data buffered, the UE will initiate another RRC resume procedure, no matter with the non-SDT indication transmission. |
| Ericsson | This is still very unclear for the DCCH solution and needs to be discussed and specified and thus is one of the more complex topics as it may also impact other specifications/layers. |
| Qualcomm | No matter whether UE sends non-SDT indication to network or not, when UE receive the RRCRelease, if UE still has data in the buffer, UE will initiate a new RRC resume procedure just as legacy. |
| Nokia, Nokia Shanghai Bell | Agree with Huawei. |
| NEC | If UE receives RRCRelease message, the AS layer will inform the NAS layer suspension/ release of the RRC connection. And if the NAS layer still want to send the new UL data, the NAS layer will trigger the AS layer to initiate RRC Resume/Setup again. |
| vivo | No specific enhancement is expected in this case. The UE behavior is the same as that in the case where non-SDT data indication is not indicated. |
| Sony | Should be legacy procedure, where UE will initiate a new resume procedure |

**Summary 6**: TBD.

**Proposal 6**: TBD.

RAN3 has agreed that the last serving gNB decides whether to relocate the UE context or not when the SDT procedure is initiated. However, in case the RRC message for non-SDT data indication is received by the receiving gNB, the context shall be transferred to the receiving gNB in case the UE is brought into RRC\_CONNECTED mode. This would be no longer a decision of the last serving gNB.

**Question 7**: Do you agree that the receiving gNB shall be able to indicate to the last serving gNB and force UE context relocation in case of RRC message for non-SDT data indication is received by the receiving gNB (ie., against current RAN3 agreement)?

|  |
| --- |
| Answers to Question 7 |
| Company | Yes/No | Technical Arguments |
| ZTE | No/Question is based on wrong assumption | The question seems to be based on wrong assumption that there will be context relocation in this case. But, we already agreed that this will not happen. The anchor gNB in this case will not relocate the context, but will simply send RRCRelease message (per the agreement below). So, we should not discuss this again (note there is nothing against RAN3 agreement here because the anchor gNB is still in-charge but it just sends the UE back to INACTIVE in this case). * “No new solution is defined to prevent data loss or duplication for the scenario where the anchor relocation is required in the middle of an SDT session, i.e. network can release UE back into RRC\_INACTIVE”
 |
| Samsung | No | As already agreed context relocation is not performed in the middle of the SDT procedure.  |
| Intel | No | The RAN3 agreement is when UE initiates an SDT session and not in the middle of SDT session.In addition, RAN2 already agreed that when SDT procedure is done without relocating the context, this would not be relocated in the middle, as shown in corresponding RAN2 agreement below. Reference to RAN2#115e related agreement: *“No new solution is defined to prevent data loss or duplication for the scenario where the anchor relocation is required in the middle of an SDT session, i.e. network can release UE back into RRC\_INACTIVE*”Therefore, we do not agree that it is required in Rel-17 to “*indicate to the last serving gNB and force UE context relocation in case of RRC message for non-SDT data indication is received by the receiving gNB*”. |
| OPPO | No | In our understanding, the question is focused on anchor without relocation solution. First of all, we agree with ZTE and Samsung that context relocation in the middle of SDT is precluded. In addition, we do not think receiving gNB is able to decode this DCCH message since the PDCP entity is located at anchor gNB. It is up to anchor gNB to determine whether there is non-SDT data arrival by receiving DCCH message. |
| CATT |  | The question is not clear. In our understanding, with DCCH solution the receiving gNB forwards the received PDCP PDU to the last serving gNB if the last serving gNB decides not to relocate the UE context and handle the PDCP layer by itself. Thus in this case the last serving gNB, not the receiving gNB, handles the received RRC message and decides how and when to response. This is aligned with the current RAN3 agreements. |
| Huawei, HiSilicon | No | The RRC message for non-SDT data indication cannot be decoded by the receiving gNB and it will have to be passed to the last serving gNB. Hence last serving gNB will be decision maker even in this case and this is in line with the RAN3 agreements. Furthermore, we should follow the agreement that we made in RAN2, i.e. the anchor gNB will send RRCRelease. This means that for non-anchor relocation case the DCCH solution will take longer time as the UE has to be first release to RRC INACTIVE and afterwards the UE needs to initiate RACH anyway. |
| Fujitsu | Yes/No | This is new case and not discussed previously. Maybe, further consultation with RAN3 is needed. |
| Sharp | No | It is the Anchor gNB to deal with the received RRC message indicating the non-SDT data arrival and decide the response.  |
| Xiaomi | No |  |
| LG | Not sure | The non-SDT data indication is a new procedure, and we don’t have a clear picture on this. Anchor relocation issue needs to be discussed later after the non-SDT data indication procedure becomes clear. |
| Interdigital | No | We have the same understanding as CATT and Huawei/HiSilicon that the receiving gNB just forwards the SRB1 PDCP PDU without knowing the content of the PDU to the last serving gNB and then the last serving gNB makes a decision.Then, the DCCH message tells the last serving gNB that non-SDT data becomes available and so UE needs to move into CONNECTED mode. It’s obvious that the non-SDT data can’t be processed remotely and so the anchoring point has to be moved to the receiving gNB. We don’t think this issue was discussed before and so we are not sure if the abovementioned RAN2 agreement in ZTE reply applies for this case.We are fine to stick to the RAN2 agreement but as Huawei/HiSilicon said, the non-SDT resumption will take longer time. This conclusion may be not good idea especially for the case of emergency MO call. |
| China Telecom | No | First of all, the context relocation during the SDT procedure is precluded. In addition, with DCCH solution, if the UE context is not relocated to the serving gNB, the serving gNB will forward the received PDCP PDU to the last serving gNB. |
| Ericsson | No | This is an additional topic that needs to be discussed. We do not agree that this was part of the conclusion as stated by ZTE.We agree with Huawei and others that the PDCP PDU is forwarded and that it is still expected that the anchor relocation is performed. |
| Qualcomm | No | We already discussed this before, and RAN2 has conclusion in #115e meeting |
| Nokia, Nokia Shanghai Bell | No | Agree with Huawei. This makes the DCCH solution performance quite non-optimal as the NW has to release the connection in this case.  |
| NEC | No | As RAN2 agreed, the RRCRelease message should be sent to the UE for this case. But the final decision should be up to RAN3. |
| vivo | No | We prefer not to revert the agreements. In this case, the anchor node can release the UE back in INACTIVE again or the receiving node can send the UE to RRC CONNECT and transmit the non SDT-data via APP retransmission. |
| Sony | No |  |
|  |  |  |

**Summary 7**: TBD.

**Proposal 7**: TBD.

Finally, DCCH based solution is described to overperform CCCH based solution since the link between the UE and the NW is already “available”. However, since the SDT procedure is considered to be fairly short, the likelihood that the RA procedure for initial SDT transmission has not been completed upon the non-SDT data arrival into the UE buffer can be regarded also meaningful, ie., most of the time in the SDT procedure is spent in the RA procedure in case the SDT data can be included in the MSGA/Msg3 completely. Same applies for CG-SDT transmission, ie., NW may have not responded to the UE (or the UE even transmitted the initial CG transmission) before the non-SDT data arrival. Since the payload size of SDT Msg3/MsgA/CG is generally thought to be larger, the probability for it to succeed compared to regular RA procedure Msg3/MsgA could be thought to be lower – also since the UE may be moving away from cell centre.

**Question 8**: Do you agree CCCH solution would generally outperform DCCH solution when RA procedure for RA-SDT is not completed or when no response is received for initial CG-SDT transmission?

|  |
| --- |
| Answers to Question 8 |
| Company | Yes/No | Technical Arguments |
|  | No | Since RACH procedure has already been initiated, we don’t see any benefit to cancel the ongoing RACH/CG transmission and initiate another RACH procedure. Furthermore, in case of legacy RACH procedure, we don’t do this. i.e. if the RRC has initiated a RACH procedure for resume, and then if some other trigger comes from higher layer (before RACH procedure is completed), RRC doesn’t abort the ongoing RACH procedure. So, is the intention of the moderator to make the SDT procedure somehow different to the legacy RACH procedure? Seems if we go this way, we should also discuss the legacy RACH procedure then and to us it seems strange (otherwise, we will have different UE behaviour for RACH completion with and without SDT and this is not good). In addition, a new CCCH procedure will interrupt the ongoing SDT data transmission, which will lead to the lost of data over Uu and waste of resource (i.e. new CCCH is not aware of DU, and DU will schedule UE continuously for retransmission). |
| Samsung | No | First we do not agree that non SDT data indication will occur often while the initial RA procedure for SDT is ongoing. Even if it occurs, continuing RA procedure is better than terminating and initiating a new RACH procedure. |
| Intel | No to Q8 (CCCH is even worse) | We are confused by the logic used in the question.We share the view that SDT procedure should aim to be short and if so, the likelihood for non-SDT data to arrive during an ongoing SDT procedure should be very low. Just because SDT session is short, it does not increase the chance of non-SDT data arrival during RACH. The chance of non-SDT data arrival during RACH is dependent on RACH duration and the data arrival rate and does not increase because the duration of SDT session is short. Further, aborting an ongoing RACH procedure which is likely to succeed (success is more likely than failures in a system) and starting a new RACH procedure will result in longer delay for CCCH solution and worse performance.So not only do we not agree with the question but also believe that CCCH handling for this scenario is even worse. |
| OPPO  | No | For the case described above, it is confusing why UE does not wait for the feedback of the UL transmission but terminates a well-going procedure. Even for CCCH solution, we think UE can wait until the confirmation of first UL is received. Based on this understanding, we think the case can not explain why CCCH solution is more effective than DCCH solution. |
| CATT | No | We support subsequent SDT transmission which means the duration of SDT may be longer than legacy RRC connection resume procedure. Hence, we share the same view with Samsung that we don’t agree that new SDT data arrival will occur often while RA procedure for RA-SDT is not completed or when no response is received for initial CG-SDT transmission. |
| Huawei, HiSilicon | Yes | DCCH solution cannot be actually used in case contention resolution has not been done, so CCCH solution obviously outperforms it for this case. In DCCH, the UE has to wait until RA procedure is finalized while this may last some time as the payload in such procedure will be larger and the UE may need to perform more transmissions of msg3/msgA before they are successful. We also do not think the case of legacy RA and RA-SDT are comparable as suggested by ZTE. The purpose of legacy RACH is in general the same, i.e. the UE gets into RRC Connected with all RBs resumed. For RA-SDT, even after successful RACH, only SDT RBs are resumed, so it makes more sense to interrupt such RACH procedure in case the UE has non-SDT data to send. |
| Fujitsu | Yes | We whare the view with the rapporteur.(1) RA procedure cancellation/aborting has been already allowed in MAC specification. We don’t see any complexity and problem with it.(2) DCCH solution cannot be performed before RA completion.(3) We don’t think that SDT procedure should be aimed to be short. If so, why failure handling like T319 timer is agreed?  |
| Sharp | Yes | In our understanding, when RA procedure for RA-SDT or CG-SDT is initiated but no confirmation/response is received, if there is non-SDT data arrival, legacy resume procedure should be triggered. |
| Xiaomi |  |  |
| LG | Yes | DCCH solution can only be used after successful contention resolution. In addition, it is already supported by the current specification that ongoing RACH procedure can be stopped by another RACH procedure. |
| Interdigital | Yes | The DCCH solution can be initiated after a successful contention resolution while the CCCH can be initiated in the middle of another RA procedure. The non-SDT data arrival indication is obviously higher priority action over any operation served by SDT and so the benefit of the CCCH solution is appreciated. |
| China Telecom | No | We do not think the new data arrival will occur often while the initial RA procedure for RA-SDT is ongoing. Even it happens, it is better to continue the ongoing RACH procedure other than terminating and initiating a new RACH procedure.  |
| Ericson | Yes | Agree with others on that a CCCH procedure can be initiate not only after contention resolution. This is an important aspect in the discussion. |
| Qualcomm | No | It is undesirable for UE to terminate the ongoing RACH and initiate a new RACH. And such interruption may cause data loss. We have similar view with ZTE. This is the similar case with the legacy RACH, i.e. RRC doesn’t abort the ongoing RACH if some other triggers come from higher layer. |
| Nokia, Nokia Shanghai Bell | Yes |  |
| NEC | Yes | DCCH message can only be sent during subsequent transmission phase. If the new data arrival during initial transmission phase, the UE has to wait, it may introduce longer delay for the new non-SDT traffic. |
| vivo | Comments | From the latency performance perspective, the answer might be Yes, as the CCCH UE does not need to wait for the next available scheduling resources or next CG resources (i.e. the CCCH UE can immediately re-initiate anchor legacy resume procedure and wait for RRC connection resumption).  |
| Sony | No | Not sure about this question, and how mobility within the cell has any vital impact on the procedure |

**Summary 8**: TBD.

**Proposal 8**: TBD.

## 3.2 Questions on CCCH-based solution

[5] lists number of issues for CCCH based solution. These issues are discussed hereinafter.

Firstly, security issues are described. [5] indicates that UE autonomous horizontal key derivation when switching from SDT procedure to RRC resume procedure would violate security principles. This may need to be clarified from SA3.

**Question 9**: Do you see a concern in UE autonomous horizontal key derivation when switching from SDT procedure to RRC resume procedure? Further, should this be confirmed from SA3 with an LS?

|  |
| --- |
| Answers to Question 9 |
| Company | Yes/No | SA3 LS: Yes/No | Technical Arguments |
|  | Yes | Yes | Firstly the key derivation during RRCResume is specified in SA3 specs. There will be changes needed in this procedure (please see some details provided below in section 3.3 – for draft CRs required). So, at least to get these changes done on SA3 side, we should send an LS to SA3 (otherwise, it is unclear how SA3 will update their specs).Then, we do have concern on the UE autonomous horizontal key derivation based solution since SA3 have said such autonomous horizontal key derivation is not allowed in case of reestablishment – of course they might conclude this case is different but we are not sure if RAN2 can simply make such assumption and proceed. What we want to avoid is that we proceed with this assumption when companies block this solution in SA3! This is the main reason whey we are a bit concerned about proceeding with CCCH only approach. Then, we need to agree the following details first and we are not sure which group should agree these (these details are captured in SA3 spec (see 33.501 – extract below in section 3.3). * How to understand the UE autonomous horizontal key derivation here. Whether the UE autonomous horizontal key derivation will be made based on the key stored in INACTIVE UE context (the one used before UE enter INACTIVE state), or the new one derived in the SDT operation.
* How to handle the mismatch between UE side and NW side in case the original CCCH has not been confirmed before the new CCCH procedure is initiated.
* Which NW entity will do the UE verification and key derivation in case the UE context has been relocated in SDT operation, whether new RAN3 procedure will be required?
 |
| Samsung | Yes | Yes | RAN2 cannot decide this aspect. This should be discussed in SA3 |
| Intel | Yes | Yes | By default, we check with SA3 when we make any security related changes. As we explained in [7], we understand that this point hence needs to be checked with SA3 as the usage of horizontal key derivation on UE side creates potential new risks on SA3 security requirement for forward security. In previous SA3 LS S3-182541, the proposal (in case of reestablishment) was that the UE autonomously derives a new key (after reestablishment) and this new key is horizontally derived according to the solution on the table at that time and SA3 did not allow such mechanism at that point (quoting the above violation). Simple horizontal key derivation is not the only issue, the issue is also that the network may have a new {NH, NCC} pair whilst the UE is autonomously performing horizontal key derivation despite this. |
| OPPO | Yes | Yes | Similar issue has been ever discussed for legacy RRC resume procedure. When T319 expires or cell is re-selected during an ongoing RRC resume procedure, UE will go to IDLE. One of the reasons why UE does not keep in RRC\_INACTIVE and trigger another RRCresume procedure is there is no NCC to derive a new security key. Consecutive horizontal key derivation has also been discussed but was not adopted. We think it is better to follow the results of previous discussion otherwise RAN2/SA3 has to revisit what have been agreed. |
| CATT | yes | yes | This is an enhancement on security. We need to be careful and get the confirmation from SA3. |
| Huawei, HiSilicon | No | OK to send | We do not agree there are changes required in SA3 specifications. As can be seen in the fragment copied by ZTE in section 3.3, the gNB uses stored key to verify resumeMAC-I. Hence, this can be handled in the same way as in the UE side in the proposed CR, i.e. the gNB updates the key stored in UA AS Inactive context. Such behaviour can be described in 38.300 and/or RAN3 specifications (up to RAN3). There is no need to involve SA3 and introduce changes in SA3. They already mentioned in their previous LS that changing a KEY is one of the ways to deal with resumeMAC-I repetition. But we are OK to inform the solution we choose to SA3 and they can get back to us if they see any concern. |
| Fujitsu | No | Yes | [6] in Issue2 already mentioned that this is not an issue. If needed, RAN2 can ask SA3. |
| Sharp | Yes | Yes | The KEY issue should be confirmed by SA3. |
| Xiaomi | Yes | Yes | This should be discussed in SA3 |
| LG | No | Yes | The previous SA3 already indicates that KEY change is one of available solution. We don’t see any issue with changing the KEY. After RAN2 makes decision, RAN2 should send an LS to SA3 to inform our decision. |
| Interdigital | No | Fine to send | The SA3 reply LS suggested us to change one of the integrity protection input parameters (KEY, COUNT, MESSAGE, DIRECTION, BEARER) to avoid any key replay attack. Thus, we can assume KEY change for the subsequent CCCH message is acceptable for SA3. But if majority prefer to send the LS to SA3, we are fine to send the LS. |
| China Telecom | Yes | Yes | It is better to ask SA3 for confirmation.  |
| Ericsson | No | OK to confirm | We have already a preliminary response on this from SA3, but it could be useful to verify the intended solution. |
| Qualcomm | Yes | Yes | This security issue/enhancement is in SA3 scope and should be discussed in SA3, hence LS to SA3 is needed. We cannot say whether this security change/ enhancement changes the SA3 spec or not in RAN2. |
| Nokia, Nokia Shanghai Bell | No | OK to ask |  |
| NEC |  | Yes | We think we need to check with SA3 on this anyway. |
| vivo | No | No | SA3 has already confirmed this issue.From the security perspective, there is no issue as mentioned in SA3 LS since horizontal key derivation (for a new key) can be performed. The only concern is the gNB might not know the UE has already updated the key. If the network vendors think blind decoding complexity is not a concern, from UE perspective, we cannot see any concern. |
| Sony | Yes | Yes | Needs confirmation from SA3. |

**Summary 9**: TBD.

**Proposal 9**: TBD.

[5] further indicates that same security key would be used by two NW nodes in case the KgNB used to cipher the UL data during the SDT procedure is used as input key for the *resumeMAC-I* generation for the *RRCResumeRequest* used for the non-SDT data indication. This may need to be clarified from SA3.

**Question 10**: Do you see a concern in using the same KgNB used to cipher the UL data during SDT procedure for *resumeMAC-I* generation for the *RRCResumeRequest* used for non-SDT data indication? Further, should this be confirmed from SA3 with an LS?

|  |
| --- |
| Answers to Question 10 |
| Company | Yes/No | SA3 LS: Yes/No | Technical Arguments |
|  | Yes | Yes | We presume this question is about the key reuse issue identified with horizontal key derivation. From what we understand, the CCCH proponents are arguing that although the same key is used in two different nodes, it is okay because one key is used just for resumeMAC-I verification in the anchor node whilst the same key is used for integrity protection in the other node. May be this argument can satisfy SA3, but may be this won’t. From our side the main concern is that if we rule out DCCH solution (which will of course have no such issues), and if SA3 says that this is not allowed, then we will be in a situation where we have nothing for this! This situation should be avoided. In any case, SA3 should be consulted on the overall new security framework regardless of what we decide (not only to check it but also to implement it as noted above).  |
| Samsung | Yes | Yes | Whether same key can be used in two different nodes should be be discussed in SA3 |
| Intel | Yes | Yes | As we explained in [7], we understand that SA3 needs to be at the minimum contacted to confirm that there is no issue as this scenario has never done before. There are two points that should be confirmed with SA3:1. The same KgNB is used by two different network nodes, firstly by the current gNB for data before the new CCCH message (i.e. during the ongoing SDT procedure) and then by the old gNB to verify the *ResumeMAC-I* for the second CCCH message (i.e. after the non-SDT data is detected and UE autonomously terminates the ongoing SDT procedure).
2. KgNB key is specific to a cell and the cell ARFCN-DL is used to derive the key [TS33.501§A.1]. The solution will require the key that is specific to the UE’s current cell now being used by the old cell to verify *ResumeMAC-I* for the second CCCH message
 |
| OPPO | Yes | Yes | Check with SA3 |
| CATT | yes | yes | The network may decide to perform anchor relocation during SDT. Then the same KgNB will be used in current serving gNB for UL/DL data during SDT and in the last serving gNB for verification of resumeMAC-I in the RRCResumeRequest used for non-SDT data indication. We need to check with SA3 if it is allowed. |
| Huawei, HiSilicon | No | OK to send | There are different keys used for user plane data and for RRC signalling, so the statement in the question is imprecise. It is rather unclear whether the key will actually be used by the serving gNB as it is unclear whether any RRC messages can be sent during the SDT procedure. Furthermore, it should be noted that:1. KgNB key is generated by the anchor gNB so it is known at anchor gNB anyway.
2. The key is used over the air interface only between UE and a single gNB.
3. After the connection is resumed, the gNB may update the keys again if it wants to, similarly as in HO case.

Hence, it is unclear what the security issue would be. We are OK to inform the solution we choose to SA3 and they can get back to us if they see any concern.  |
| Fujitsu | No | Yes | [6] in Issue4 already mentioned that this is not an issue. If needed, RAN2 can ask SA3. |
| Sharp | Yes | Yes | The KEY issue should be confirmed by SA3. |
| Xiaomi | Yes | Yes | This should be decided by SA3. |
| LG | No | Yes | Same comments as in Q9. |
| Interdigital | No | Fine to send | The keys involved in the scenario of the question are different keys. Please note that keys for SRB and keys for DRBs are independent. Moreover a key for integrity protection and a key for encryption are independent. So two different nodes don’t re-use any key in the abovementioned scenario.If companies want to consult this issue with SA3, we are fine to send an LS to them. |
| China Telecom | Yes  | Yes | If is better to check with SA3. |
| Ericsson | No | Yes | Agree with Huwaei |
| Qualcomm | Yes | Yes | Whether same security key would be used by two NW nodes should ask SA3. |
| Nokia, Nokia Shanghai Bell | No | OK to ask |  |
| NEC | No | Yes | Because we understand the key reuse issue is only for the traffic over the air. So it is better that we consult with SA3. |
| vivo | Yes with comments | No | SA3 has already confirmed this issue.Besides, according to the current spec, the UE will update the key. |
| Sony | Yes | Yes | Check with SA3 |

**Summary 10**: TBD.

**Proposal 10**: TBD.

On the other hand, it was not completely clear if the horizontally generated key would be used for the *resumeMAC-I* generation for the *RRCResumeRequest* used for non-SDT data indication. Or whether another solution is intended.

**Question 11**: What key should be used and which input parameters for the *resumeMAC-I* generation for the *RRCResumeRequest* used for non-SDT data indication?

|  |
| --- |
| Answers to Question 11 |
| Company | Yes/No | Technical Arguments |
|  | TBD | Firstly different solutions will have different consequences and different implications on other groups. Unless we have a fixed solution on the table that we can all agree on as the CCCH candidate, it is impossible to evaluate all implications. Our main concern is that we are now running out of time to discuss all solutions. So, we think we should just stick with one flavour (perhaps the horizontal key derivation one) and check if this works or not.  |
| Intel | Discussion with SA3 required before a solution can be finalized by RAN2 | This depends on how CCCH approach works which is still not fully clear to us as different proposals were described in [2] and during the corresponding online discussions. Our understanding from [2] is that * (1) Resume MAC-I calculation/inputs needs to be updated for the 2nd RRCResumeRequest msg. Different inputs of the resumeMAC-I can be updated by using for example
	+ (a) The KRRCint key used during the SDT proc. (instead of the one stored in the UE AS Inactive Context before initiating the SDT proc); or,
	+ (b) The COUNT is updated in TS 33.501 to start in 2 (instead of 1)
* (2) Horizonal key derivation for subsequent data is done as proposed in CCCH solution.

With CCCH solution, the security risk of re-use of the same I-RNTI across two SDT sessions needs to be verified with SA3 as previous LS response from SA3 (R2-2109065) was not clear on this regard. In normal Resume procedure, a different I-RNTI is allocated for each Resume so the same I-RNTI is not used across two sessions to prevent tracking the UE. Another related open item raised during email disc. 507 is about which *source-c-RNTI* should use when calculating the *VarResumeMAC-Input*  for the 2nd *RRCResumeRequest.* E.g. should this be the one used when UE was previously CONNECTED or new on in used during the SDT operation.*VarResumeMAC-Input  ::=     SEQUENCE* *{    sourcePhysCellId                        PhysCellId,*  *targetCellIdentity                      CellIdentity,*  *source-c-RNTI                           RNTI-Value }*This last topic requires coordination with SA3 as it was not asked in previous LS. |
| OPPO | Up to SA3 inputs |  |
| CATT | Depending on SA3 discussion |  |
| Huawei, HiSilicon |  | The approach based on the horizontally derived key is the simplest to us. The security concerns that are raised are rather far-fetched, but can be verified by SA3 if companies insist. |
| Fujitsu | SA3 | We are fine with asking SA3. |
| Sharp | Up to SA3 inputs |  |
| Xiaomi | Up to SA3 inputs |  |
| LG | TBD | One of the input parameter to *resumeMAC-I* can be changed. Once the CCCH direction is agreed, we can discuss further which parameter should be changed. |
| Interdigital | Either KEY, COUNT, MESSAGE, DIRECTION or BEARER | As SA3 reply LS stated, one of the input parameters (KEY, COUNT, MESSAGE, DIRECTION or BEARER needs to be changed.If companies are reluctant to go for the KEY change, then either COUNT, MESSAGE, DIRECTION or BEARER should be changed.As SA3 has already informed us the guidance, we don’t see much point to consult this issue with SA3 but if majority prefer to consult with SA3, we are fine to do that. |
| China Telecom | Up to SA3 inputs |  |
| Ericsson | ACC. to SA3 input | Agree with IDT. |
| Qualcomm |  | Check with SA3 |
| Nokia, Nokia Shanghai Bell |  | The horizontally derived key should work. |
| NEC | SA3 | We prefer the same key used for *resumeMAC-I* for the *RRCResumeRequest* in SDT procedure but different COUNT value, which is easier for the network to verify the UE. Otherwise, besides KgNB, the last serving gNB has to generate KRRCint for the new gNB to check the resumeMAC-I value. But we can leave it up to SA3 to make decision. |
| vivo | New derived gNB key | We are fine to check with SA3 again. |
| Sony | TBD | SA3 |

**Summary 11**: TBD.

**Proposal 11**: TBD.

Next issue described is that the security keys between UE and network may go out of sync (e.g. if the 2nd *RRCResumeRequest* used for non-SDT data indication using the new key is sent before the contention resolution of the 1st *RRCResumeRequest* is completed, ie., in the SDT procedure). On the other hand, it seems the UE could take this into account already when terminating the SDT procedure and initiating the RRC resume procedure for non-SDT data indication in which case it could use the initial key which should work as in legacy.

**Question 12**: Do you agree the UE can use the initial key (the same key used for *resumeMAC-I* for the *RRCResumeRequest* in SDT procedure) for deriving the *resumeMAC-I* for the *RRCResumeRequest* used for non-SDT data indication in case the RA procedure of the SDT procedure is not completed?

|  |
| --- |
| Answers to Question 12 |
| Company | Yes/No | Technical Arguments |
|  | No | Since RRC layer has no idea whether the RACH procedure is completed in MAC or not. Even in case the RACH procedure is still ongoing, UE has no idea whether first CCCH message has been received by NW successfully or not.In addition, SA3 highlight in the LS that such kind of repetition should be avoided. Hence, we think the UE behaviour should be independent of the success or failure of the previous RACH procedure. So, UE should always derive a new key after sending RRCResumeRequest first time. Of course the consequence of this is that if the first CCCH message is not received, then the resume may not succeed. This is a suboptimality that we need to live with in case we go this way.  |
| Samsung | No | Prefer to have same solution irrespective of whether RA procedure is completed or not. |
| Intel | No (see comment) | We understand there are multiple network/UE synchronization scenarios to be discussed. The respond to Q12 would depend on the response in previous Q11 (i.e. which input is modified to the resumeMAC-I calculation of the 2nd RRCResumeRequest), and on when the UE is allowed to abort the RA procedure associated with an SDT procedure to initiate the non-SDT data. If the UE is allowed to abort it during the first RA-SDT RACH attempt, it can result in a mismatch between UE and network as the network is expecting the first *RRCResumeRequest* while the UE is sending the second non-SDT data *RRCResumeRequest* with a potentially different calculation of the resumeMAC-I. In addition, UE might perform horizontal key derivation for the subsequent data while the network is not aware of the key being used by the UE. |
| OPPO | No | Why not wait until RACH procedure is completed? |
| CATT | No  | Prefer to have a unified solution irrespective of whether RA procedure is completed or not. |
| Huawei, HiSilicon | No strong view | Both ways work:1. If we use the original key, from security perspective, it could be seen in the same way as retransmission of msg3 (since we do not know whether msg3 was already received by the network)
2. If we use a new key, then if the network did not receive the original msg3, the network might not be able to verify shortMAC-I. In this case there will be a fallback to RRC Setup.

If there are concerns with using the original key, then we are OK to go with the horizontal one. It will happen extremely rarely that the original CCCH message is not received and fallback to RRC Setup in such rare cases is not a problem. This is still better than in case of DCCH which cannot handle the case of data arrival before contention resolution at all. |
| Fujitsu | Yes | The main question is the case where “the security keys between UE and network may go out of sync”, instead of triggering new RA procedure before previous RA completion. On this point, we share the rapporteur’s view. Having said that, this question may depend on Q11. |
| Sharp | Up to SA3 inputs |  |
| Xiaomi | No | Agree with the concerns provided by ZTE |
| LG | Comments | We also prefer to have same solution irrespective of whether RA procedure is completed or not. Even for DCCH solution, we prefer to have same solution irrespective of whether SDT procedure is ongoing or not. |
| Interdigital | No | It’s much simpler to have a unified solution. In other words, UE always derives a new key for the case of non-SDT data arrival indication.Regarding to the confusion of key selection, gNB has only 2 choices either the initial key or a new key to verify the resumeMAC-I and so a smart gNB implementation can address the issue. |
| China Telecom | No  | Prefer to have a unified solution irrespective of whether RA procedure is completed or not. |
| Ericsson |  | This is a broader discussion not limited to SDT and a common solution on the UE behaviour is in general needed. There is a similar topic already under discussion in SA3. |
| Qualcomm | No | We have concern on the kind of repetition (reuse the same key used for resumeMAC-I for the RRCResumeRequest) and also aborting the ongoing RACH. |
| Nokia, Nokia Shanghai Bell | Yes  | As the NW may not have received the previous RRCResumeRequest from SDT RA procedure, this seems to work similarly to legacy and hence can be used. |
| NEC | Comments | We prefer to use the same security key but different COUNT value for deriving the resumeMAC-I regardless contention resolution is finished or not, because it is easier for the network to verify the UE. Otherwise, besides KgNB, the last serving gNB also need to generate KRRCint for the new gNB to check the resumeMAC-I value. |
| vivo | No | To circumvent replay attacks, the reuse of resumeMAC-I should be avoided, as suggested by SA3 in S3-213034. |
| Sony | No | Agree with comment from ZTE. |

**Summary 12**: TBD.

**Proposal 12**: TBD.

Data loss is indicated in [5] to be a bigger concern compared to DCCH based solution as the NW may be transmitting DL SDT data and UL SDT data in the UE could be lost. While the DL data is more for NW implementation to handle, the UL data loss should be discussed. Currently, the UE discards all stored PDCP PDUs upon suspend procedure while the PDCP SDUs should be kept. In that sense, it seems the UL data loss should be less of an issue.

**Question 13**: Do you agree the PDCP entity retains the PDCP SDUs in the buffer upon PDCP entity suspend and, hence, the data loss in UL should basically not happen in case of CCCH based solution? Do you see a concern in DL data handling?

|  |
| --- |
| Answers to Question 13 |
| Company | UL data Yes/No | DL data Yes/No | Technical Arguments |
| ZTE | No | No | One issue is whether the COUNT value will be reset or not in PDCP suspend operation. If PDCP Count is reset (current behaviour in PDCP suspend operation), then there is no way to ensure the lossless transmission since there is no way to ensure the in order transmission without redundant packet. In addition, the data packet for UM DRB will be lost. Although the data lost in UM DRB is allowed, it should be avoided as much as possible. |
| Samsung |  |  | In DL data loss can occur for UM DRBs. In UL, whether to reset COUNT or not should be discussed. |
| Intel | See comment | See comment | We agree that UL and DL SDT data when not acknowledge would be buffered in UE and network side. The specifications need to be updated to guarantee that the UE (re)transmits that UL SDT data. However, we understand there might be problems to (re)transmit the corresponding DL SDT data unless new mechanism are defined. To address this, RAN2/RAN3 would require discussion and coordination on their work as normally the network does not associate a new connection request with the data from the old one. In addition, RAN3 impact might be larger than just stage-2 impact e.g. old\_ anchor gNB performs MAC-I verification for the 2nd RRCResumeRequest when the serving gNB already has a UE context and UL/DL data in its buffers, therefore the relocation of the UE context requires some update at the minimum to perform *ResumeMAC-I* verification and not to lose the DL data already available in UE’s buffers. How this may be done should be discussed by RAN3On top of the data loss, there could also potentially be duplication of data (due to PDCP suspend operation). By suspending PDCP, the PDCP SNs are reset and hence it is not possible to detect and discard duplicates if the network and UE were to re-tx from the last acked packet before the second CCCH message. In addition, duplicates could be just as disruptive to TCP as data lost and this does not occur in case of DCCH which is a key difference. Another concern with the data handling is that the DL SDT data unnecessarily sent and loss over Uu when the network keeps sending it whilst the UE is in the middle of a new UL procedure after autonomously had aborted a previously good SDT procedure (which the network is not aware of).  |
| OPPO | No | No | Depends on whether COUNT is reset and the security key used for the newly triggered RRC resume procedure. |
| CATT | See comment | See comment | Data loss will occur for UM DRBs. In addition, the network continues scheduling UL and transmitting DL data to the UE as it has no knowledge that the UE has already aborted the current SDT procedure. |
| Huawei, HiSilicon |  |  | UL: We have already discussed the COUNT issue in the previous e-mail discussion and the overall conclusion was that in case new key is used, there is no need to reset COUNT. DL: We do not see any applications applicable to SDT (e.g. in the justification section of the WID) that would utilize UM DRBs, so the loss will happen extremely rarely. And even if it does, such loss would not be an issue for SDT applications. |
| Fujitsu | Yes | Yes | We share the view with the rapporteur.For RLC UM, the application is accepting the data loss, so that RLC UM is set up. If the data loss over RLC UM is problem, application can perform retransmission in application layer. |
| Sharp | No | No | We share the view with ZTE. |
| Xiaomi | No | No | Agree with ZTE. |
| LG | Yes | Yes | We are discussing the case when a new RRCResume procedure is triggered due to non-SDT data transmission while the SDT procedure is ongoing. In this case, there is no RRCRelease message received when triggering the new RRCResume procedure. According to current specification, the RRC indicates “PDCP suspend” only when RRCRelease message including suspendConfig is received. As there is no RRCRelease message received, the PDCP suspend is not triggered when the new RRCResume procedure is triggered. Thus, the PDCP COUNT is not reset. We don’t understand why some companies think that PDCP COUNT is reset in this case. |
| Interdigital | Yes | Yes | As long as SDU is buffered, we are fine.Regarding to the UM data, as Huawei/HiSilicon said, we don’t see any clear use-case, which requires UM in SDT operation and use of UM DRB has already implied a potential data loss and so even if the data is lost, that shouldn’t be end of the world for the application. |
| China Telecom | No | No | We share same view with ZTE. |
| Ericsson | Yes | Yes | Agree with LG |
| Qualcomm |  |  | We have similar view with Intel |
| Nokia, Nokia Shanghai Bell | Yes | Yes | We think regardless of the solution (whether to reset COUNT or not), the data loss should not happen. |
| NEC | Yes | Yes | Agree with LG that if PDCP suspend is not performed, there will be no such issue for RLC AM. For RLC UM, we think there is no problem as packet loss it acceptable. |
| vivo | Comment | Comment | We think firstly we need to discuss whether the resumed SDT RBs will be suspended or not when CCCH solution is performed. If so, then, only for AM DRB and SRB2, the data in PDCP that is suspended will be kept and the data loss issue can be handled by PDCP retransmission. For UM DRB, we think we can reuse the legacy behavior.  |
| Sony | No | No | Share view with ZTE |

**Summary 13**: TBD.

**Proposal 13**: TBD.

Another issue is how the NW would identify the *RRCResumeRequest* used for non-SDT data indication, e.g., in the case the NW did not know the UE attempted SDT before the RRC resume procedure. For instance, is there a need to specify a new *resumeCause* for the purpose, does the UE indicate this in an LCID in the MAC layer (similarly to RedCap identification indication), is the UE provisioned with different I-RNTI to use in this case, or is this left to NW implementation.

**Question 14**: Do you agree the UE shall indicate to NW the *RRCResumeRequest* is used for non-SDT data indication? If yes, which solution should be specified for this purpose?

|  |
| --- |
| Answers to Question 14 |
| Company | Yes/No | Technical Arguments |
| ZTE | Depends | It depends on the detailed solution. If the existing CCCH procedure can be reused as it is, then there is no need to indicate this; otherwise, if different CCCH approach is expected from legacy resume procedure, then NW has to distinguish the two cases. From our point of view, the main intention of CCCH solution is to reuse the existing CCCH approach. If we introduce a new CCCH procedure, then the benefit of CCCH solution is gone and we are just left with all the disadvantages (such as lost data over Uu, extra latency in providing non-SDT data arrival indication etc). |
| Samsung |  | Prefer to reuse the existing procedure. |
| Intel | Depends | We understand that the network needs to be able to differentiate that this is a 2nd *RRCResumeRequest* msg that was initiated in the middle of the SDT procedure, however how this is done depends on how CCCH solution is modelled. Therefore, the solution may depend on the response in previous Q11 i.e. which input is modified to the *resumeMAC-I* calculation of the 2nd *RRCResumeRequest*. Alternatively, it was mentioned during email discussion 507, that the I-RNTI could be used by network to detect this. On this topic, it is important to mention, that previous SA3 LS was not clear on whether I-RNTI needed to also be updated as discussed during August online session. |
| OPPO |  | Depends on the outcomes of above questions and inputs from SA3. If the security keys used for first and second RRC resume procedure are same, including the ones applied for the generation of resumeMAC-I and data ciphering, there is no need to make the distinguish. Otherwise, it is important for the network to know whether this is the second RRCResumeRequest in order to decide the security to use. |
| CATT | See comment | It depends on the detailed solution if the UE shall indicate to NW the RRCResumeRequest is used for non-SDT data indication. And if needed, prefer to extend existing RRCResumeRequest message. |
| Huawei, HiSilicon | No | We do not think this is needed as the second Resume Request can be identified via I-RNTI that is included. But even if companies prefer to add such indication, it does not mean we need a whole new CCCH procedure – two options were mentioned already in previous documents, i.e. new resumeCause or new logical channel ID. Neither of these solutions requires new procedure. |
| Fujitsu | Yes | New cause in *RRCResumeRequest* would be introduced. This is useful for the gNB processing in terms of identifying of the purpose of *RRCResumeRequest*. Otherwise, it increases the complexity of the gNB. |
| Sharp | No | Not clear about the question.When UE initiates SDT procedure, the dedicated RA-SDT or CG-SDT resource could be used to identify the SDT and non-SDT procedure.The *RRCResumeRequest* for non-SDT data indication could be transmitted via T319 for SDT is running. So the NW could identify the case. |
| Xiaomi |  | Prefer to reuse the existing procedure. |
| LG | No | The NW can identify the second RRCResumeRequest based on I-RNTI. We think legacy RRCResume procedure can be used as it is. |
| InterDigital | See comment | We don’t see any strong need to differentiate SDT case and non-SDT case but if majoriy prefer to distinguish them, a new LCID can be introduced. On our understanding, even if a new LCID is introduced, it won’t change any procedure. |
| China Telecom |  | Prefer to reuse the existing procedure. |
| Ericsson | No | Resume cause gives the condition for the resume req. Additional information adds another layer and complexity. |
| Qualcomm |  | The solution is related to the answer of Q11/Q12. The new CCCH procedure is not preferred. |
| Nokia, Nokia Shanghai Bell | No | This basically depends on whether different keys are used in case the NW did not receive the RRCResumeRequest from SDT-RA procedure:If the NW did receive the RRCResumeRequest from SDT RA procedure, then the NW can identify the UE from the I-RNTI to be performing non-SDT data indication and new key can be applied. While if the NW did not receive the RRCResumeRequest from SDT RA procedure, and new key would be applied, this would be problematic for the NW. However, if the UE applies the old key in case SDT RA procedure is not completed, there should be no issue in this case either. |
| NEC | Depends | Depends on if the same security key is used for generation of resumeMAC-I for non-SDT indication. If different, it is better that network can be indicated that this is for non-SDT such that the network can prepare a different security key to verify the resumeMAC-I; otherwise, it is possible to not indicate in the RRCResumeRequest message. |
| vivo | No | We also think the legacy procedure can be reused. And then the NW can identify the UE situation via BSR reporting in RRC CONNECTED. |
|  |  |  |

**Summary 14**: TBD.

**Proposal 14**: TBD.

Similarly to DCCH based solution wrt. Question 7, some RAN3 impact may be foreseen when the new *RRCResumeRequest* used for non-SDT data indication is received by the NW. For instance, whether the UE context shall not be released by the last serving gNB only after the SDT procedure for the UE is completed (either by moving the UE into CONNECTED mode or directing back to INACTIVE mode). On the other hand, if the context was already relocated, would it not be possible for the receiving gNB to perform the UE integrity check in this case; while, in case the context was not already relocated, then the last serving gNB obviously has the context and could do the check.

**Question 15**: Do you see that there may be some RAN3 impact with the CCCH solution? If yes, what impact is foreseen, and do you see a concern with it?

|  |
| --- |
| Answers to Question 15 |
| Company | Yes/No | Technical Arguments |
| ZTE | Yes | We need to first decide which node performs the verification. Since IRNTI will be used, our assumption is that the verification of the second CCCH message is done by the old anchor gNB. Then when there was anchor relocation up front, there will be some impacts to RAN3 in this case as noted above. Moderator seems to indicate that the new target gNB can do the verification, may be this is possible, but this also needs some changes in RAN3 since we assume the old I-RNTI always points to the old anchor gNB. If we want the target gNB to verify the new resumeMAC-I, then it seems we need some new behaviour here (also some restriction is needed in the network to say that the I-RNTI shall not be reused until the UE is released). Seems this is needs some RAN3 discussion.  |
| Samsung | Yes | As per current procedure resumeMAC-I is always verified by old anchor gNB. If same is followed for resume for non SDT data indication, UE context needs to be stored in old anchor gNB even after the context is transferred to serving gNB during the SDT procedure. If resumeMAC-I is verified by new GNB , this is a new behaviour and needs to be discussed and specified by RAN3. |
| Intel | Yes | Expected RAN3 impacts are:* (A) Old\_ anchor gNB needs to keep the UE context after the actual UE context is transferred to the current/serving gNB for the ongoing SDT session. This is because:
	+ 1) To perform Resume-MAC-I verification of the second CCCH message even after the UE context is transferred to the current gNB.
	+ 2) The I-RNTI in the second CCCH message is the old I-RNTI from the old anchor gNB
* (B) RAN3 also needs to discuss when and how this UE context in the old anchor gNB can eventually be released.
* (C) Old anchor gNB needs to differentiate the 2nd *RRCResumeRequest* message and use the new gNB key to verify the ResumeMAC-I.
* (D) The inputs to the *ResumeMAC-I* calculation is not decided. If it is based on the current C-RNTI (of the new gNB) used during the SDT data transfer before the second CCCH message, RAN3 has to discuss and define a mechanism to transfer that C-RNTI to the old anchor gNB. If it is the old C-RNTI used in the anchor gNB, RAN3 has to define a mechanism to ensure that this is reserved and not used by another UE (this will also require changes to UE handling to store the use the C-RNTI of the old anchor gNB)
* (E) Old anchor gNB needs to indicate to the new anchor gNB using new Xn message to move a UE (w/ context previously relocated) to RRC\_CONNECTED state. This would allow the serving gNB not to lose that DL data already available in buffers (i.e. stored during the SDT procedure that was terminated by UE autonomously).
 |
| OPPO | Yes | Share same view as Samsung. |
| CATT | Yes | If the verification for the new RRCResumeRequest used for non-SDT data indication is handled by the last serving gNB, the UE context shall not be released by the last serving gNB even if anchor relocation is performed for SDT. RAN3 needs to be impacted.If the verification for the new RRCResumeRequest used for non-SDT data indication is handled by the current serving gNB, RAN3 also needs to be involved. For example: Will the current serving gNB find the UE context based on previous I-RNTI allocated by the last serving gNB? |
| Huawei, HiSilicon | Possibly yes | We think it is simplest that the verification is always done in the last serving gNB. As can be seen in the CR agreed by RAN3 in R3-216070, in the anchor relocation case, the context is released from the old anchor only at the end of SDT procedure, so there is no issue with missing context. This is already clear and no discussions in RAN3 are needed as claimed, e.g. by (A) and (B) in Intel’s reply. (C) can be decided in RAN2, no need to involve RAN3. (D) is the same as in legacy so not sure what new impacts are meant. (E) is not needed, data loss will happen only for UM DRBs which are unlikely to use SDT and for which this will be acceptable anyway.The only change in RAN3 specifications that might be needed is to capture that the gNB should update the key in the UE INACTIVE AS CONTEXT after receiving the first CCCH message, so that the new key is used for the verification of the second request. |
| Fujitsu | Yes | As indicated in [6] of Issue 8, this is again “business as usual”, i.e. of course the solution will have to be described in the relevant specifications. The verification aspect can be asked to RAN3. |
| Sharp | Yes | We share the same view with Samsung. |
| Xiaomi | Yes | If resumeMAC-I is verified by new gNB, this is a new behaviour and needs to be discussed and specified by RAN3. |
| LG | Yes | The resumeMAC-I should be verified by anchor gNB. We don’t see any critical issue here.  |
| Interdigital | Yes | We also assume that the last serving gNB verifies the message. If we go for KEY change, the UE INACTIVE AS CONTEXT needs to be updated accordingly. |
| China Telecom | Yes | Share same view as Samsung. |
| Ericsson | Yes |  |
| Qualcomm | Yes | Same view with ZTE. |
| Nokia, Nokia Shanghai Bell | Maybe | Agree with Huawei |
| NEC | Maybe | Agree with HW that it is simplest that the verification is always done in the last serving gNB. Maybe it is also possible for the new gNB based on implementation. We are OK to check with RAN3 on this. |
| vivo | Maybe | We share a similar view with Huawei. |
| Sony | Yes |  |

**Summary 15**: TBD.

**Proposal 15**: TBD.

Last question in [5] considers cell re-selection during SDT procedure. This should generally not be the decision point to select between DCCH and CCCH based solution since regardless of the CCCH solution, the cell re-selection case may not be specified. However, it would be good to get an understanding if companies would prefer this case to be specified in case the CCCH solution is selected.

**Question 16**: Would you agree to specify to specify solution based on the CCCH based solution for cell re-selection during SDT procedure (in case CCCH based solution is agreed to be specified)?

|  |
| --- |
| Answers to Question 16 |
| Company | Yes/No | Technical Arguments |
|  | No | Our concern is that this is now getting too late to specify this solution in Rel-17 in any case and there seems to be no willingness to specify this in the first place unfortunately. We thought we could do this in Rel-18 but seems this will not happen either. Overall, we think companies believe that this is not important anymore. Hence, we are concerned that it is too late now to consider this case. Then, if majority of companies prefer to now also cover this solution for cell reselection, then we could use CCCH solution only for cell reselection. If it is only the cell re-selection, then we can simply reuse the same key for the previous RRC Resume Request to derive the resume MAC-I for the second CCCH, and there will be no security issues for such case (since the cell ID will be different). However, RAN3 impact will still be there, and more discussion is required to understand the whole picture of the solution. We are not sure if this is really feasible now with the time left.  |
| Samsung | No | We have already agreed that UE transition to RRC\_IDLE upon cell reselection. No need to re-open this discussion.  |
| Intel | See comment | RAN2 already agreed not to enable cell reselection scenario in Rel-17 as baseline.*“3. Events that trigger a termination or failure of an ongoing SDT session 1) cell reselection, 2) expiry of the SDT failure detection timer, 3) when Max retx is reached in RLC. RLC AM max retransmission functionality remains unchanged.* *4. When a UE detects a failure of an ongoing SDT session, UE transitions autonomously into RRC\_IDLE (as baseline solution). If time allows or have a ready solution we can consider further optimizations.”*Therefore, we prefer focus RAN2 limited work to enable the solution required to handle non-SDT data during an SDT procedure without adding other scenario that will increase the work load. If time is available for this WI after concluding the other solution, we are open to discuss the required solution to handle cell reselection scenario. However, from Rel-18 SDT discussions, we understand that this was not an scenario supported by majority of companies. |
| OPPO | No |  |
| CATT | No | No need to re-discuss this. |
| Huawei, HiSilicon | Yes | We have already agreed that in case CCCH solution is agreed for non-SDT arrival, we can consider using it for other failure cases. In fact, it can be readily used with minimal additional effort. Since the SDT session can last as long as several seconds (even 10 seconds was proposed previously for the duration of the new SDT timer), the cell reselection can happen quite often, which will degrade the QoS/QoE for applications using SDT as compared to the same applications not using SDT. The fact that this can be handled by CCCH solution is its big advantage even though the proponents of DCCH solution will say it is unimportant.  |
| Fujitsu | Abstain | As the rapporteur is suggested, we also think that cell-reselection aspect is the main driver to decide one of solutions between CCCH and DCCH. Before going into details, our priority would be to decide which solution RAN2 will go for. |
| Sharp | No | We prefer to deal with cell reselection as legacy. |
| Xiaomi | No |  |
| LG | Postpone |  |
| Interdigital | Yes | The CCCH base solution can be applied to address the cell reselection case very easily. It’s still aligned with the RAN2 agreement made in RAN2#115-e as that’s a ready solution.1. When a UE detects a failure of an ongoing SDT session, UE transitions autonomously into RRC\_IDLE (as baseline solution). If time allows or have a ready solution we can consider further optimizations.

  |
| China Telecom | No | No need to re-discuss this. |
| Ericsson | Yes | Rare case that have been discussed and in our understanding we have a baseline UE behaviour. |
| Qualcomm | No | RAN2 already has discussions and agreements.  |
| Nokia, Nokia Shanghai Bell | Yes | If CCCH solution is adopted, we should consider this optimization. |
| NEC |  | Not discuss this now. We can discuss this if CCCH solution can be agreed. |
| vivo | No | As agreed, cell reselection will lead to the termination of the ongoing SDT procedure. As long as the SDT procedure is ended, any related procedure for CCCH solution should be ended as well, this is because CCCH solution is only a part of the whole SDT procedure.  |
| Sony | Yes | Agree that there may be benefit with the CCCH solution supporting the rare case of a potential UE initiated cell reselection during the ongoing SDT procedure |

**Summary 16**: TBD.

**Proposal 16**: TBD.

## 3.3 Draft CRs

In the previous meeting, [2] (Annex) and [4] presented initial RRC CRs for the CCCH based solution and DCCH based solution, respectively. Given the above issues not resolved, complete CRs could not be presented before the issues are resolved. However, companies are being asked if the above CR drafts can be used as baseline for both of the solutions and start from those when further details are clarified based on the questions.

**Question 17**: Do you agree to use [2] (Annex) and [4] CR drafts as baseline CRs for the CCCH based solution and DCCH based solution, respectively? If not, what are the issues?

|  |
| --- |
| Answers to Question 17 |
| Company | CCCHYes/No | DCCHYes/No | Technical Arguments |
|  | Further changes needed (see comments) | Yes | We are fine with the DCCH CR and if any updates are needed based on the majority views above, this can be done within RAN2 for this approach. For the CCCH CR, further discussion is needed for the following aspect:* Since the PDCP suspend operation is performed for each DRB, lossless transmission can not be ensured (out of order packet and redundant packet can not be avoided).
* The security part need to be confirmed by SA3 first.
* Since NAS layer will not distinguish the SDT DRB and Non-SDT DRB, the triggering of second CCCH procedure should be captured in RAN (e.g. the second CCCH shall only be triggered in case there is data available for non-SDT DRB).

We also think the CR needs some further changes as noted below: Then for SA3 specs, we need to change the following too and there may be other changes need… (up to SA3). The actual changes will depend on the solution chosen… for the horizontal key derivation, we need SA3 to modify the following procedure (assuming SA3 are okay with this).  |
| Samsung | No | Yes | Agree with changes suggested by ZTE for RRC CR. Security aspects and related impact to SA3 spec can be discussed by SA3. |
| Intel | Functional changes are missing | Yes (see comment) | For DCCH, if majority of companies prefer using a new UL RRC msg, the draft CR is available in [4], however for *UEAssistanceInformation* message, the draft CR is available in Annex of [7].For CCCH, many details still need to be confirmed with SA3 and RAN3 with regard to the feasibility of the actual solution. Or even if another option is chosen for the security and network handling. For the specific version of the CCCH solution proposed in the CR, we understand that this CR is not capturing all required details to enable the actual solution. Some of the issues and/or missing parts are the following:* (A) Aborting of the ongoing SDT session on non-SDT data arrival is not captured.
* (B) Potential data loss, out of order delivery and interruption as PDCP is suspended which results on a reset of the PDCP COUNT (issue #6 of [5]). There would be needed to capture something on RAN2/RAN3 TS e.g. UP for the handling of the DL data stored in gNB’s buffer.
* (C) It is not captured how 2nd *RRCResumeRequest* message is differentiated e.g. different calculation of the *resumeMAC-I*.
* (D) It is not captured how UE autonomously performs the horizonal key derivation for subsequent data (after the 2nd *RRCResumeRequest* message).
* (E) FFS if any change is needed to the information stored in the UE AS Context e.g.
	+ 1) C-RNTI in used during the SDT proc. and this depends on RAN3 decisions on whether C-RNTI can be stored in the old gNB or new C-RNTI can be provided to the old gNB. so, FFS whether there is any impact in old anchor gNB when having to decode the 2nd *RRCResumeRequest* message.
	+ 2) I-RNTI used in the second CCCH-message. FFS whether I-RNTI needs to be updated for the 2nd CCCH msg, this might need to be checked again with SA3 as previously explained.
* (F) FFS if any new mechanism to guarantee that the security keys between UE and network are not go out of sync (e.g. if the 2nd *RRCResumeRequest* using the new key is sent before the contention resolution of the 1st *RRCResumeRequest* is completed or if the 2nd *RRCResumeRequest* using the new key is sent when network has sent the *RRCRelease* msg associated to the successful termination of the SDT proc.).
 |
| OPPO | No | Yes | Agree with ZTE. |
| CATT | See Comment | yes | According to the CR [2] for CCCH based solution, the UE needs always to perform the unified access control procedure again. That means the new RRCResumeRequest message may not be initiated if the result of UAC for the new RRC Resume procedure is not barred. But for DCCH based solution, the procedure is always allowed. This is another drawback for CCCH based solution. |
| Huawei, HiSilicon | Yes | No | **With relation to both CCCH and DCCH:** We are not sure about the interpretation of the CT1 LS from ZTE. In our understanding, since UP resources for non-SDT data are suspended, then NAS will trigger another resume request. This might need to be verified with CT1 again.**With relation to CCCH solution:** As mentioned in replies to previous questions, we do not see any SA3 impacts. Everything can be handled in RAN specification. When it comes to the changes suggested by ZTE for RRC, they assume no new resume request arrives from NAS layer, which is not our understanding (and CT1 LS did not answer this question). As mentioned above, regardless of the solution chosen, we should clarify this with CT1. In any case, the changes suggested by ZTE are OK in general in case ZTE’s interpretation turns out correct. When it comes to impacts mentioned by Intel, we do not agree any of this is needed (please see our clarification in Q14).**With relation to DCCH:** As we mentioned above, we think resumeCause is needed in DCCH message (or DRB indication), so that the network knows the general priority of the traffic that arrived. We also think it is better to reuse ReleasePreference IE from UE Assistance Information message instead of specifying a new message. Last thing is that we need to clarify with CT1 whether any resume request will arrive during ongoing SDT procedure which may also have an impact on the CR. |
| Fujitsu | Yes | No | Those CRs can be considered as a good baseline, but details can be discussed after one of solutions would be decided. |
| Sharp | Yes | Yes |  |
| Xiaomi | No | Yes | Agree with ZTE. |
| LG | Yes | No | For DCCH draft CR, many aspects are still unclear.1. How does the RRC trigger the non-SDT data indication procedure without request from NAS? The draft CR says that the new procedure is triggered “when data mapped to non-SDT radio bearers becomes available”. However, as commented in Q6, the NAS data may not arrive at PDCP buffer because when to submit non-SDT data to AS is up to UE implementation. How can the new procedure be triggered if non-SDT data is not available in PDCP?2. Before successful completion of RACH procedure, the RRC should not submit DCCH message to lower layer. It is not clear how the RRC knows the status of the ongoing RA-SDT procedure.3. It is not clear how the RRC triggers a new RRCResume procedure when RRCRelease message is received before DCCH message is transmitted. 4. The DCCH message uses SRB1, and it should be security protected. It is not clear how the ciphering and integrity protection is applied to the DCCH message.5. The non-SDT indication is a new RRC procedure, and the UE action should be clearly specified for reception of different messages, i.e. RRCResume, RRCRelease, RRCSetup, RRCReject, similar to RRCResume procedure. |
| Interdigital | Yes | No | DCCH CR requires to be updated to handle the case that UE receives RRCSetup, RRCRelease and RRCReject. Besides, resumeCause and UAC handling mentioned in the CT1 reply LS also need to be addressed in the CR. |
| China Telecom | No | Yes | Agree with ZTE. |
| Ericsson | Yes | No | We agree with the points made from LG and IDT. In any case, the CRs need some work to complete any solution, but a base-line should be in place. |
| Qualcomm | No | Yes | Agree the comments of CCCH solution by ZTE. We also share the similar comments with CATT, i.e. UAC |
| Nokia, Nokia Shanghai Bell | Yes  | Depends | We think both can be used as baseline but need to be enhanced based on the discussion. However, for DCCH, in case existing message is used, this would need to be changed completely. |
| vivo | Comment | Yes | We prefer ZTE’s CR in the first screenshot. |
| Sony | TBD | Yes | Agree with ZTE  |

**Summary 17**: TBD.

**Proposal 17**: TBD.

## 3.4 Preferred option(s) & possible compromise

The selection process between DCCH and CCCH based solutions have been in a deadlock for a while and a compromise proposal to specify both solutions was presented in the previous meeting. For instance, such that the CCCH based solution is used in case the RA procedure for the SDT procedure has not been completed or no NW response has been received for the initial CG-SDT transmission; and DCCH based solution is used after this point. Naturally, this would require more discussion after the above issues are resolved if the compromise would be preferred by most of the companies.

In the following, companies are asked still to provide their preferred option(s) from the following:

 - Option 1: DCCH solution

 - Option 2: CCCH solution

 - Option 3: Compromise solution (ie., both)

If you are OK with both options individually **but not with compromise solution** please indicate Option 1/2.

**Question 18**: Which option(s) do you prefer?

|  |
| --- |
| Answers to Question 18 |
| Company | Option(s) | Technical Arguments |
|  | Option 1 | Option 1 should be adopted for Non-SDT data arrival. Option 3 can be considered for cell re-selection case, but only if we have a consensus to support this (this is probably too late otherwise). |
| Samsung | Option 1 |  |
| Intel | Option 1  | Our first preference is option 1 but we are not opposed to consider option 3 in certain scenarios. As we mentioned earlier, apart from the performance issues with CCCH solution, the other main issue with the CCCH solution is the impact on RAN3 and SA3 which will take time to resolve and makes it difficult to complete in Rel-17. Considering the limited time left for Rel-17, another alternative compromise could be to introduce the DCCH solution for Rel-17 and the CCCH solution in Rel-18 along with the failure recovery handling where SDT session ends abruptly i.e. without UE control. |
| OPPO | Option 1 |  |
| CATT | Option 1 |  |
| Huawei, HiSilicon | Option 2 | CCCH can cover all the use cases, i.e. non-SDT indication before and after contention resolution as well as cell reselection and SDT failure cases. We could accept DCCH solution as an optimization on top, but the issue that it addresses (i.e. potential data loss for UM DRBs) is not really worth the effort in our opinion, considering that such indication would rather be an infrequent event. |
| Fujitsu | Option 2 | Not support Option 3. |
| Sharp | Option 3 |  |
| Xiaomi | Option 1 |  |
| LG | Option 2 | There are many issues related to DCCH solution, and it is not worth to introduce a new procedure to cover the rare case. |
| Interdigital | Option 2 | CCCH solution can address any corner cases and future proof in terms of mobility support. |
| China Telecom | Option 1 |  |
| Ericsson | Option 2 | We still think there are many secondary issues that are likely to surface also after resolving some of the unclarities with the DCCH solution and compared to reusing a fundamentally specified legacy procedure and message structure would be the logical choice. |
| Qualcomm | Option 1 | Option 1 is adopted for Rel-17. CCCH solution still needs more discussions and to check with other WG SA3/RAN3. |
| Nokia, Nokia Shanghai Bell | Prefer Option 2, OK with Option 3 |  |
| NEC | Option 2 or Option 3 | Option 2 can cover the case that non-SDT data arrival before contention resolution. We are also OK with Option 3 as compromise. |
| vivo | Option 3 | It seems the company positions are the same as the previous meeting, so option 3 might be the only way forward.  |
| Sony | Option 1 |  |

**Summary 18**: TBD.

**Proposal 18**: TBD.

# 4 Conclusion

TBD.

# References

[1] [R2-2109617](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2109617.zip) DCCH-based indication of non-SDT data arrival, Intel Corporation, ZTE corporation, Sanechips, Samsung, CMCC, Qualcomm, OPPO, Sharp, Xiaomi, Sony, CATT, FGI, Asia Pacific Telecom, Radisys

[2] [R2-2110596](file:///C%3A%5Cevutukuri%5Cwork%5C5G%5CRAN2%5Cdocs%5CR2-2110596.zip) Non-SDT data arrival, Huawei, HiSilicon, InterDigital, LGE, Ericsson, ASUSTeK, Nokia, Nokia Shanghai Bell, Google, Rakuten Mobile, Fujitsu, NEC

[3] [R2-2109619](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2109619.zip) DCCH vs CCCH based approach for indication of non-SDT data arrival, Intel Corporation, ZTE corporation, Sanechips, Samsung, Qualcomm, OPPO, Sharp, Xiaomi, Sony, CATT, Apple

[4] [R2-2109618](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2109618.zip) Draft CR for introduction of DCCH solution for non-SDT data arrival, ZTE corporation, Sanechips, Intel Corporation, Samsung, CMCC, Qualcomm, OPPO, Sharp, Xiaomi, Sony, CATT, FGI, Asia Pacific Telecom, Radisys

[5] [R2-2111275](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2111275.zip) Comments on the proposed CCCH solution for non-SDT data arrival, Intel Corporation, Apple, ZTE

[6] [R2-2111509](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2111509.zip) Further clarifications on non-SDT arrival solutions, Huawei, HiSilicon, InterDigital, LGE, Ericsson, ASUSTeK, Nokia, Nokia Shanghai Bell, Google, NEC, Fujitsu, Rakuten Mobile

[7] [R2-2111523](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2111523.zip) Comments to [R2-2111509](file://D://__%E4%BC%9A%E8%AE%AE%5C2021%5C202111_RAN2%5CTSGR2_116-e%5CDocs%5CR2-2111509.zip) for non-SDT data arrival, Intel Corporation, ZTE corporation, Sanechips, Samsung, Xiaomi, Qualcomm, Apple, Radisys

[8] [R2-2109308](file:///C%3A%5Cevutukuri%5Cwork%5C5G%5CRAN2%5Cdocs%5CR2-2109308.zip), Reply LS on Small data transmission, Source: CT1