3GPP RAN WG2 Meeting #113bis-e R2-210xxxx

eMeeting April 12th – April 20th, 2021

Agenda Item: 8.6.3

Source: InterDigital (email discussion rapporteur)

Title: [DRAFT] [Post113-e][503][SDT] T319, cell reselection and re-establishment

Document for: Discussion, Decision

# Introduction

This discussion document is intended to define the new T319-like timer for small data transmission, as well as address cell reselection during SDT procedure and related security aspects. The following objectives have been provided by session chair:

* [Post113-e][503][SDT] T319, cell reselection and re-establishment (InterDigital)

 Scope: 1) Extended T319 timer/new handling (option on how to start/maintain timer) 2) how to deal with timer expiry, 3) Cell reselection handling and related security aspects

 Intended outcome: Report to the next meeting.

The following deadlines are provided:

* Initial deadline (for companies' feedback): **Friday 2021-03-26 23:59 UTC**

# Discussion

## SDT failure detection timer

In Rel-16, to detect transmission failure in INACTIVE state UE starts T319 timer upon transmission of *RRCResumeRequest/RRCResumeRequest1*. TS 38.331 [1] defines timer operation as follows:

| Timer | Start | Stop | At expiry |
| --- | --- | --- | --- |
| T319 | Upon transmission of *RRCResumeRequest* or *RRCResumeRequest1.* | Upon reception of *RRCResume,* *RRCSetup, RRCRelease, RRCRelease* with *suspendConfig* or *RRCReject* message, cell re-selection and upon abortion of connection establishment by upper layers. | Perform the actions as specified in 5.3.13.5. |

The current maximum value of T319 may be insufficient to account for multiple small data packets during subsequent small data transmission, possibly leading to unnecessary transmission failure and data loss since the UE transitions into IDLE mode upon timer expiry.

Extending T319 could avoid premature declaration of RRC connection resume failure during subsequent small data transmission. However, as T319 is configured in *ue-TimersAndConstants* in SIB1, the same T319 value applies to all UEs within the cell, which would impact legacy procedures such as RNAU and RRC connection resume by increasing detection time of connection resume failure.

It was therefore agreed in R2#112e to introduce a new timer, **referred to as SDT failure detection timer in this discussion**, to detect and handle failures during the small data procedure [2]:

**Agreements**

Define a new timer. FFS whether it has the same definition as T319 or it is restarted every UL/DL

Considering this timer is intended to detect small data transmission failure, it was proposed in [3, 4] that SDT failure detection timer be started upon initial small data transmission, with [3] further adding reception of DL small data as a start condition.

**Q1: Do you agree SDT failure detection timer starts upon transmission/reception of initial small data PDU?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Additional comments** |
| ZTE | Agree (transmission) For reception case the question is not clear to us | Note that all SDT sessions will be initiated by the transmission of the first UL message (i.e. the CCCH message) at which point the failure detection timer shall be started. So, the failure detection timer should start upon transmitting the first UL message (i.e. at similar point as when the legacy T319 is started). It is unclear to us why the timer shall be started at reception of some message in DL. Perhaps this is related to option 2 in Q3, but since that is being discussed separately, we will provide our views for restarting the timer as part of Q3.  |
| Intel | Agree | We confirm that a new time (like T319) should start at the initiation of the SDT session. We prefer updating the wording “transmission/reception of initial small data PDU” to “SDT session” (or other term) that may not bring ambiguity (e.g. SDT session is only started with an UL transmission). |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

For RRC-based SDT, an RRC message is transmitted along with initial small data. If this RRC message is *RRCResumeRequest* or *RRCResumeRequest1* both SDT failure detection timer and legacy T319 timer would be running simultaneously, which may lead to data loss if T319 is configured with a shorter duration and expires (sending the UE to IDLE) before completion of SDT procedure.

**Q2: Do you agree if *RRCResumeRequest* or *RRCResumeRequest1* is transmitted for the purposes of SDT, legacy T319 timer is not started? (i.e. failure detection relies on new SDT failure detection timer instead)**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Disagree** | **Additional comments** |
| ZTE | Agree | Since the new timer is agreed, the legacy timer doesn’t apply for SDT anymore. |
| Intel | Agree | A new timer will be started instead than T319 with similar purpose. However, we are also ok to further discuss this during stage-3 discussion. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

In [Post112-e][551][SDT], the following FFS details were further captured regarding timer duration:

Option 1) extended T319 like timer, or;

Option 2) timer restarted after each UL/DL.

Proponents of Option 1 state that extending the duration of SDT failure detection timer to accommodate subsequent SDT would be a simple solution, and that having a time bound on subsequent small data transmission (as in LTE EDT) is acceptable considering the target use case for SDT is applications with short and infrequent data.

Proponents of Option 2 note an extended timer restricts the network to configuring a timer duration based on the predicted total/max time for subsequent small transmission. Considering this duration is variable, defining a timer duration which can accommodate all scenarios may be difficult, and result in unnecessary delay to SDT transmission failure detection.

**Q3: What is the preferred SDT failure detection timer handling to accommodate subsequent SDT?**

* **Option 1: An extended timer to accommodate full duration of subsequent SDT;**
* **Option 2: Timer is restarted upon (re)transmission or reception of small data;**
* **Option 3: Other, please describe.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred Option(s)** | **Additional comments** |
| ZTE | Option 1 | We prefer option 1, but if option 2 is the majority view, we think we can reuse something similar to dataInactivityTimer for option 2.  |
| Intel | Option 1 | The benefit of restarting the timer at each UL/DL (with option 2) is that it provides more flexibility and avoids SDT being time bound as the actual time required for SDT cannot be predicted in advance. It also allows a shorter T319’ such as failures can be detected more quickly. On the other hand, the time bound nature of T319’ (with option 1) can be seen as a benefit because, it limits SDT duration and avoids new potential scenarios to address from a long SDT duration. Moreover, SDT mechanism by its very definition should be of short duration. In addition, with option 1, the network can always do a fallback to RRC\_CONNECTED if the UE is running out of timer, which is similar to new data arrival handling. Hence, we don’t see strong motivation to allow long durations of a given SDT session via option 2. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Legacy T319 timer is stopped upon reception of a response RRC message (e.g. *RRCResume*), cell re-selection, or abortion of connection establishment by upper layers. Assuming the network may respond with a similar set of RRC messages, the same stop conditions may also apply to SDT failure detection timer.

**Q4: Which legacy T319 stop conditions are also applicable to SDT failure detection timer?**

* **1: Reception of *RRCResume***
* **2: Reception of *RRCSetup***
* **3: Reception of *RRCRelease***
* **4: Reception of *RRCRelease* with *SuspendConfig***
* **5: Reception of *RRCReject***
* **6: Cell reselection**
* **7: Abortion of connection establishment by upper layers**
* **8: Other, please describe.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Applicable stop condition(s)** | **Additional comments** |
| ZTE | Depends on answer to Q3  | If option 1 is adopted for Q3, then the timer shall be stopped upon all the legacy conditions listed above (i.e. 1-7) |
| Intel | 1 to 7 | 1) 2) would be sent when network fallbacks the UE into RRC\_CONNECTED. 3) 4) would be sent when the network wants to end the SDT session while it keeps the UE in RRC\_IDLE for 3) and in RRC\_INACTIVE for 4).5) could be applicable to SDT similarly to legacy access. This would allow the network to respond reject SDT traffic under congestion situations. Moreover, this scenario might be more critical when gNB is overloaded and cannot fetch the UE AS Context. 6) 7) might require further discussion aiming to prevent data loss and duplication during an SDT session, as explained in R2-2100366.  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Cell re-selection during SDT procedure

As per legacy procedure if cell reselection occurs while T319 is running, UE transitions to IDLE. Adopting similar behaviour while SDT failure detection timer is running (i.e. during ongoing SDT procedure) would lead to interruption of small data transmission and possible data loss.

However, several contributions [5, 10, 12] note cell reselection occurring during an SDT procedure would be rare and transitioning to IDLE and re-attempting the SDT procedure on a new cell is a simple solution with minimal specification impact. Even if UE transitions to IDLE during cell reselection, [4-6] note that UE could recover lost data from higher layers (i.e. PDCP retransmission) without complexity and specification change, and data loss prevention could be left to UE implementation.

Alternatively, proponents of enhancement note subsequent small data would extend the SDT procedure increasing the probability of cell reselection during SDT, and that small data transmission should have a similar reliability to connected mode data transmission. It is further noted in [6] that retransmission based on UE implementation may result in data duplication as the PDCP SN for the data is not maintained in the network and UE when UE goes to IDLE.

**Q5: Which of the following do you agree with:**

1. **The possibility of small data loss during cell re-selection justifies enhancement to existing procedures (i.e. UE should not transition to IDLE as in legacy T319 behaviour)**
2. **Existing recovery mechanisms (e.g. higher-layer retransmission) are sufficient to prevent small data loss even if UE transitions to IDLE during cell reselection;**
3. **Cell re-selection during SDT is a corner case, no enhancement/recovery mechanism is necessary;**
4. **Other, please describe**

|  |  |  |
| --- | --- | --- |
| **Company** | **Supported statement(s)** | **Additional comments** |
| ZTE | Option 1 (unless there are some showstoppers or significant impacts) | We think option 1 should be considered as long as there are no obvious show-stoppers for this. If we identify some critical issues with option 1 then other options can be the fallback solutions.  |
| Intel | 1 | We think UE should continue in RRC\_INACTIVE after cell reselection is triggered during an SDT session, as explained in R2-2100366. If UE stays in RRC\_INACTIVE (instead of transitioning into RRC\_IDLE upon triggering cell reselection during an ongoing SDT session), data loss can be prevented using existing recovery mechanisms (e.g. higher-layer retransmission)On other hand, if a UE transitions into RRC\_IDLE upon triggering cell reselection during an ongoing SDT session, any DL small data would always be lost.  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

An alternative solution to transitioning to IDLE is for UE to remain in INACTIVE and attempt a second RRC Resume to the new cell. However, per TS 33.501 [7] UE is provided with updated I-RNTI and NCC in subsequent *RRCRelease* with *suspendConfig* messages to prevent tracking of UE based on I-RNTI value. This may lead to security concerns if UE attempts the new Resume procedure before completion of the first and does not receive updated I-RNTI and NCC. One option mentioned in [4,6] is to temporarily allow re-use of the NCC and I-RNTI from the former cell to initiate an RRC Resume in the new cell, which could then be updated afterwards.

**Q6a: From RAN2 perspective, if UE remains in INACTIVE during cell reselection can same NCC and I-RNTI be used temporarily for RRC Resume procedure in new cell?**

**Note: A related discussion is ongoing in email discussion [Post113-e][502] [8] for data arriving on non-SDT DRBs. Companies are asked to highlight issues specific to cell reselection, if available.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Additional comments** |
| ZTE | Yes | In general, we think this can be the case. Note that unlike in the same cell case, the same MAC-I will not be repeated (since the physical Cell ID will be different after cell reselection). So, the issue is slightly different to the repetition of CCCH message which is being discussed in the other email discussion. Then our proposal in [11] was to use RRCRestablishment instead of RRCResume (i.e. I-RNTI is not used). RRCResume and RRCReestablishment are both very similar, but if we use RRCRestablishment, upon successful completion UE moves to connected mode directly. In addition, the following differences are worth noting: If RRCResume is used: (i.e. I-RNTI is used as UE ID), then the message is routed to the old anchor and there may be some additional work needed (in RAN3) if there was anchor relocation and since there is no context fetch procedure at anchor gNB upon RRCResume, this procedure might actually fail unless RAN3 defines new procedure to support this. If RRCReestablishment is used: (i.e. the UE ID points to the cell in which reselection happens), then the Reestablishment message is routed to the new gNB, but in this case, if there was no anchor relocation, then again some impact will be there for RAN3 to verify the UE. It would be good to understand the above differences and then if we agree to support some mechanism, we need to first agree which way to go (i.e. RRCResume or RRCReestablishment)?  |
| Intel | Yes | Yes, from RAN2 perspective. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

If temporarily reusing NCC and I-RNTI value in sperate cells is supported from a RAN2 perspective, possible impacts and feasibility should be verified by SA3.

**Q6b: If ‘Yes; to Q6a, is an LS to SA3 necessary?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Additional comments** |
| ZTE | Yes | Once some basic framework is agreed, we should inform SA3 to check whether there are any issues from security perspective.  |
| Intel | Yes | SA3 should be consulted on the risk and, if needed, with possible solutions to mitigate the associated risk. For example, possible approaches are that the network should then move the UE to CONNECTED, or back to INACTIVE (with the suspend and SDT configuration), use horizontal key derivation etc as discussed in [R2-2008992] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

An alternative solution described in [4,6] is to provide UE with a new I-RNTI and NCC while SDT procedure is ongoing. Proponents of this solution are invited to describe how such signalling would work.

**Q6c: Are additional mechanisms (e.g. not relying on RRC Release message) needed to provide an updated I-RNTI/NCC value during SDT procedure? If ‘Yes’, please describe.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Additional comments** |
| ZTE | No | The problem with this approach is that this may still not work because the cell reselection may happen even before the DL message is received. So, there is no guarantee that the above procedure will work for all cases anyway. So, there is no need to optimise for this. Note that we already agreed that the RRC message in DL terminating the SDT procedure will be sent at the end. So, based on this, it seems it is not possible to send a new I-RNTI/NCC midway through the SDT procedure.  |
| Intel | Maybe  | Depending on SA3 response. Additional mechanism may be needed for other security reasons as well regarding network authentication as discussed in last meeting. As we explained in Q6b, possible options could be that in a future SDT session, network could already respond to the 1st UL SDT with *RRCRelease* message included updated *SuspendConfig* (moving back the UE into RRC\_INACTIVE with updated security information) or with a fallback into RRC\_CONNECTED (in order to fully authenticate the UE and update the security). |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

UE in CONNECTED for which AS security is activated with SRB2 and at least one DRB setup may initiate an RRC re-establishment procedure to continue RRC connection. Application of this procedure to cell reselection during SDT could avoid drawbacks of other candidate solutions such as potential data loss if transitioning to IDLE or security concerns of second Resume procedure. However, specification currently defines the re-establishment procedure only for connected mode UEs and would require extension to support INACTIVE UEs with SDT.

NOTE: resumption of SRB2 is currently a working assumption, however, for the purposes of this discussion it can be assumed that SRB2 is resumed during SDT.

**Q7: Assuming SRB2 is resumed, can RRC re-establishment procedure be extended to INACTIVE UEs with ongoing SDT procedure? If ‘No’ please provide technical reason(s) which preclude this.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Additional comments** |
| ZTE | Yes | As explained above (see Q6a), both RRCResume and RRCRestablishment can work but they will have different implications on the network signalling. So, we need to be clear on what are the impacts and we could use the appropriate solution.  |
| Intel | No | Technically speaking re-establishment could be extended, however we do not see this an essential behaviour for SDT session that targets to be a short and simple mechanism. Moreover, enabling re-establishment procedure during an SDT session would end up adding complexity to UE and network side and we think other solutions as discussed above are simpler. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Q8: What is the preferred UE behaviour for cell re-selection during an on-going SDT procedure?**

* **Option 1: UE transitions to IDLE and initiates an SDT procedure on the new cell;**
* **Option 2: UE remains in INACTIVE;**
* **Option 3: UE performs RRC re-establishment procedure;**
* **Option 4: Other, please describe**.

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred Option(s)** | **Additional comments** |
| ZTE | Option 3 | Other options can be investigated if option 3 is not seen as viable.  |
| Intel | 2 | We support staying in INACTIVE when SDT operation is possible in the new cell. Note that legacy transitions from RRC\_INACTIVE to RRC\_IDLE would still be applicable e.g. when re-selecting to LTE. Handling of last data sent in the ongoing SDT session just before triggering cell reselection would be left up to UE implementation aiming to prevent data loss and duplication during an SDT session, as explained in Q4 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## SDT failure detection timer expiry

Current behaviour upon legacy T319 timer expiry is to transition to IDLE. However, enhancements applicable to cell reselection (i.e. higher-layer retransmission, remaining in INACTIVE, or RRC re-establishment) may also be applicable to SDT failure detection timer expiry to prevent small data loss during connection failure.

**Q9: Are the same potential UE behaviours listed in Q8 also applicable to SDT failure detection timer expiry? If ‘No’, please describe aspect(s) specific to timer expiry which would preclude an option(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Additional comments** |
| ZTE | Yes | The failure behaviour should be the same for all possible failure events during SDT |
| Intel | Yes | And, if possible, we should adopt the same solution (whatever the solution adopted is) as for cell reselection scenario.  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Q10: Assuming options described for cell reselection are also applicable for SDT failure detection timer expiry, what is the preferred UE behaviour at SDT failure detection timer expiry?**

* **Option 1: UE performs actions in TS 38.331, section 5.3.13.5 (i.e. transition to IDLE as per legacy T319 timer) and attempts RRC connection setup;**
* **Option 2: UE remains in INACTIVE;**
* **Option 3: UE performs RRC re-establishment procedure;**
* **Option 4: Other, please describe**.

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred Option(s)** | **Additional comments** |
| ZTE | Option 3 |  |
| Intel | 2 | Aligned with our preference for cell reselection. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Q11: Are there any other SDT failure detection timer or cell-reselection related aspects RAN2 should discuss?**

|  |  |
| --- | --- |
| **Company** | **Other Aspects** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Summary

<To be generated pending company feedback>

# Conclusion

<To be generated pending company feedback>

# Contact Information

|  |  |  |
| --- | --- | --- |
| **Company** | **Name** | **Email** |
| ZTE | HuangHe | huang.he4@zte.com.cn |
| Intel | Marta Martinez Tarradell | marta.m.tarradell@intel.com |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# References

1. [TS 38.331 v16.3.1](https://www.3gpp.org/ftp/Specs/archive/38_series/38.331/38331-g31.zip) Radio Resource Control (RRC) protocol specification
2. [R2-2100001](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2100001.zip) Report of 3GPP TSG RAN2#112-e meeting – ETSI MCC
3. [R2-2101578](file:///C%3A%5Cevutukuri%5Cwork%5C5G%5CRAN2%5Cdocs%5CR2-2101578.zip) Small data transmission failure timer – InterDigital, APT, Ericsson, ETRI, FGI, Sharp, Sony
4. [R2-2101184](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2101184.zip) Control plan common aspects for SDT – Huawei, HiSilicon
5. [R2-2101223](file:///C%3A%5Cevutukuri%5Cwork%5C5G%5CRAN2%5Cdocs%5CR2-2101223.zip) Remaining issues on control plane aspects of NR small data transmission – Qualcomm
6. [R2-2100366](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2100366.zip) Common Control plane aspects for SDT – Intel Corporation
7. [TS 33.501 v17.0.0](https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h00.zip) Security architecture and procedures for 5G system
8. [R2-210xxxx](https://www.3gpp.org/ftp/Email_Discussions/RAN2/%5BRAN2%23113-e%5D/%5BPost113-e%5D%5B502%5D%5BSDT%5D%20GeneralOtherCpIssues%28ZTE%29) [Post113-e][502] General and other control plane open issues for SDT (ZTE)
9. [R2-2100147](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2100147.zip) Control Plane Common Aspects of RACH and CG based SDT - Samsung Electronics Co.
10. [R2-2101177](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2101177.zip) CP aspects for SDT – Ericsson
11. [R2-2101161](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2101161.zip) Control plane common aspects of SDT – ZTE Corporation, Sanechips
12. [R2-2100295](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2100295.zip) Considerations on control plane common aspects – CATT
13. [R2-2101369](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Docs/R2-2101369.zip) Control plane aspects on SDT procedure - Apple