3GPP TSG-RAN WG2 #131 R2-25xxxxx

**Bengaluru, India, 25th – 29th August 2025**

Agenda Item: x.x.x

Source: Ericsson

Title: List of open issues for mobility phase4

Document for: Discussion

# 1 Introduction

This document is to collect possible remaining open issues to complete the WI.

# 2 Open issues

Companies are invited to mention possible open issues **which are critical** for the conclusion of the WI.

|  |  |  |  |
| --- | --- | --- | --- |
| Company (Name) | Open issue | Justification | Rapporteur comment |
| Fujitsu, NTT DOCOMO | NW should be able to distinguish between CLTM and fast recovery after CLTM failure in order to deal with SN gap caused by SRB COUNT continuation when UE is performing fast recovery. If reordering timer (*t-Reordering*) on NW-side is set for a long duration, because NW must wait for the duration before receiving *RRCReconfigurationComplete* in RRC layer and sending contention resolution to the UE, T304 in the UE may expire, which results in fast recovery failure. In Rel-18, RAN2 agreed to deal with SN gap by NW implementation, and that can be done because LTM and fast recovery can be distinguished. However, in Rel-19, CLTM and fast recovery after CLTM failure cannot be distinguished, which is an open issue. | This issue is critical for operators which configures long reordering timer. If this is not resolved, this leads to failure of fast recovery after CLTM and interruption time longer than the duration of reordering timer. | The understanding is that this could be an issue only when the value of the reordering timer is long, but now I am wondering if we really need to fix this. Anyhow, I would encorauge the companies to bring a contribution to the next meeting and also clarify which are the solutions on the table. |
| Ofinno | According to the current running CR, UE starts performing CLTM condition evaluation only in 2 cases:  Start case 1) if the received LTM-Config includes the field ltm-ServingCellExecutionCondition set to setup  Start case 2) On executing LTM to a candidate cell and ltm-ExecutionCondition is configured within the LTM-Candidate IE for the selected LTM candidate configuration  There are 2 scenarios where the CLTM condition evaluation is stopped:  Stop case 1) During CLTM execution. In this case, the UE restarts performing the CLTM evaluation after applying the candidate cell configuration, according to Start case 2 above.  Stop case 2) On initiating MCG failure information procedure. In this case, the current running CR does not have a procedure for the UE to resume/ start performing the CLTM condition evaluation.  We think the UE should resume CLTM condition evaluation after successful recovery from MCG failure RRC reconfiguration for MCG is received while T316 is running;  Alternatively, the handling of CLTM condition evaluation during MCG failure information procedure can be simplified if the UE ensures that CLTM is only executed when timer T316 is not running. | If this issue is not address, UE will cannot perform CLTM condition evaluation/ CLTM execution until an network sends an RRC reconfiguration message including ltm-config comprising the field ltm-ServingCellExecutionCondition set to setup. | First, I am wondering whether we need to optimize a failure scenario, which can be the one of the MCG failure. But even so, in case of an MCG failure the MCG will most likely changed and this means that the UE would need to reapply anywhay the LTM-Config, which will instruct again the UE to start the execution conditions. Also, I would say that network is totally in control of this for the case of MCG failure, meaning that the network can always uptade the LTM-config.  Therefore, I would say that this is not really an issue and we can simply rely on the network implementation. I don’t expect any contribution on this. |
| LGE | Based on the lateast RRC running CR (i.e., v22), L1 condition for CLTM evaluation is associated with an event for L1 MR (i.e., EventLTM3/4/5). This implies that both L1 MR and CLTM execution are simultaneously triggered if the event is satisfied.  To avoid simultaneous trigger of L1 MR and CLTM execution, it is good to introduce separate events for CLTM evaluation as in CHO (i.e., CondEventLTM3/4/5). | If this open issue is not addressed, UE triggers both L1 MR and CLTM execution simultaneously when the event associated with L1 execution condition is being satisfied. | This issue was already discussed in the WI and we have agreed to not introduce separate events for the case of CLTM.  I think this can be easily solved in the MAC CR discussion. I don’t expect any contribution about this in RRC, because this is not really an RRC problem but a MAC issue (i.e., how to fix the procedure in MAC). |
| LGE | Based on the RRC running CR v22, a redundant secondary key update can happen during subsequent MCG LTM cell switch in DC case.  For example, consider the case where Cell#1 belonging to CU#1 is the current serving cell, Cell#2 and Cell#3 belonging to CU#2 are LTM candidate cells, and DC is configured. In this case, LTM candidiate configuration for Cell#2 and Cell#3 include the sk-Counter for secondary key update during inter-CU MCG LTM. When subsequent LTM cell switch, i.e., Cell#1 🡪 Cell#2 🡪 Cell#3, happens, a redundant secondary key update is performed during the LTM cell switch from Cell#2 to Cell#3.This is because secondary key update during MCG cell switch depends only on whether sk-Counter is included into the target(candidate) configuration.  To address the issue, the procedure 5.3.5.3 should considers that secondary key update during subsequent MCG LTM cell switches with DC (i.e., SN is not changed) is performed only if MN security update is performed during an MCG LTM cell switch. Otherwise, the network should ensure that secondary key update at intra-CU LTM will not happen during subsequent LTM cell switches in mixture of intra-CU LTM and inter-CU LTM with DC (i.e., SN is not changed). | If this open issue is not addressed, a redundant secondary key update can happen during subsequent MCG LTM cell switch in DC case. The redundant secondary key can finally lead to data interruption due to key refresh. | The understanding is that even for the secondary key change, this is always controlled by the Rel-19 IDs we agreed for the security key change. So there should be no issue for this.  Also, even if the cases mentioned happen, as far as the keys match on the UE and network side this is not an issue.  This seems not a critical issue so I would not expect any contributions on this. |
| Nokia | Issue 1 : When Inter-CU LTM is prepared all the candidate cells of target cells are prepared with new security key K-GNB\* based on Target PCI +ARFCN and the NCC value for the target cell. However on switching the candidate cells of target cells need to prepared for intra-CU LTM without security key change. If switching is triggered prior to that UE may assume no-key change as the source and target node have same Rel-19 ID network may still have different keys. RAN2 need to discuss way forward on how to avoid this out-of-sync.  Issue 2: As per RAN2 agreements, Intra-CU LTM and Inter-CU SCG LTM can be supported simultaneously. In this case the RRC Configuration will have LTM-Config and LTM-Config-DC. As LTM switching requires reference configuration in both cases.. Both can have reference config. Running CR have different text in field description in this part.  RAN2 agreement for Inter-SN LTM is that the reference configuration in this case need to have both MCG and SCG parts similar to SCPAC. RAN2 to conclude on changes needed in RRC to reflect the right agreement.  Issue 3:As the NCC value is sent plain text in switching command the switching failure may happen due to NCC mismatch. However, if the network is not aware of this issue the failure will repeat. To enable NW to know the issue. RAN2 to discuss how the UE can indicate the used NCC value to network after switching failure.  Issue 4: In last RAN2 meeting, it was agreed to support Intra-MCG-LTM with SCG as MRDC-Add-Release configuration with possibility to have different SN for each SCG. However the SN-key change needed in this case when Intra-MCG LTM switch is triggered is not discussed clearly. One suggestion was to trigger Master-key update after switching to force SN-key change..However this can happen only after switching. From the time of switching until this reconfiguration there can be security rekeying issue. | Issue 1: Inter-CU and Intra-CU LTM co-existence is valid scenario and if this issue is not resolved there could be mismatch for intra-CU execution. Specification change needed for clear system behaviour.  Issue 2: The running CR does not reflect the agreement related to MCG LTM and Inter-SN SCG LTM.  Issue 3: if NW does not the about the Inter-CU switch failure due to NCC attack the failures will repeat forever. Good to address this issue in specification.  Issue 4: Extending the Intra-MCG LTM with SCG belonging to different SN was quickly agreed without analysis on associated issues. Hence RAN2 to finalise the switching and key change related UE behaviour in this scenario. | Issue 1: The understanding is that when the candidate cell are prepared the key is not derived upfront but only once an LTM cell switch is triggered and the UE applies the new configuration. Therefore, there is no issue if a cell is prepared for inter-CU and then is used for intra-CU. But even so, the network can always re-configure the candidate cells. This does not seems a critical issue so no contributions are expected.  Issue 2: For the case of intra-CU and inter-CU SCG LTM configured together, RAN2 has already agreed that only LTM-ConfigNRDC is used. So there is no case where intra-CU SCG LTM is received within LTM-Config and inter-CU SCG LTM is received within an LTM-ConfigNRDC. No contributions expected for this issue.  Issue 3: The understanding is that the case highlighted is when the NCC is changed by a malicious node/UE and thus there is a NCC mismatch. In such a case the RRC re-establishment procedure can be triggered by the UE, which is also what SA3 has discussed when they agreed that NCC can be send in plain text. We also discussed in RAN2 that we will not agree on any mechanism to handle case when the NCC is tampered. Therefore, I don’t expect any contributions on this issue.  Issue 4: In case of intra-MCG LTM with SCG, the key on the SCG does not need to be changed since the key on the MCG has not changed. If network wants to refresh the security key at the SN, it can always do it after the intra-MCG LTM cell switch is completed. Therefore, I would not expect any contributions on this issue. |
| ZTE | Whether to introduce ltm-Config-r18 in INM CG-Config? Based on current RRC running CR, this new IE is added to CG-Config, and it is supposed to deliver the LTM candidate configuration(s) that to be used at the SCG.  However, based on RAN3 endorsed CR in R3-254010, most IEs of ltm-Candidate are already specified in Xn interface, e.g. TCI-state config, early UL sync config, SSB config, CSI-RS config, complete/full ind, etc. Besides, some other fields are still under discussion in RAN3, for example, noSecurityChangeID.  So, the need of separate ltm-Config IE in CG-Config should be further justified. | If this open issue is not addressed, there will be duplicated parameters defined in RAN2 and RAN3 specs, it will cause confusion, and results in inter-operability issue in future. | When I checked R3-254010 I see that some information is partially there, but some other fields are missing, such as the “attemptLTM-Swith”, the L2 reset IDs, the measured TA IDs, the security IDs.  I guess is safe to keep the current signalling in the INM for the time being and them we can check later on what is missing in RAN3 signalling. Maybe we come back on this after this meeting when we have the post email discussion for RRC. |
| Ericsson | Currently in the LTM execution procedure we have the following:  1> If Rel-19 ID of source and target are different:  2> the UE perform security key change  1> else if no Rel-18 ID are configured for source and target; or  1> if the Rel-18 ID of source and target are different:  2> UE does L2 reset  However, is not clear what happens when the network does not configure the Rel-19 IDs for both the source and target cell. In such a case the UE should still check whether to do L2 reset or not, but now is not clear from the procedural text how the UE will behave.  One way should be to capture this explicitly in the procedural text according to the following:  1> If Rel-19 ID of source and target are different:  2> the UE perform security key change  1> else if Rel-19 ID of source and target are the same; or  1> if Rel-19 ID of source and target are not configured:  2> if no Rel-18 ID are configured for source and target; or  2> if the Rel-18 ID of source and target are different:  3> UE does L2 reset | If this open issue is not solve, it will be not clear what the UE beaviour would be in case the Rel-19 ID are not configured for source and target, which could be a common scenarios for intra-CU LTM.  This may lead to misalignment between UE and network and to failures. | There is no need necessarility for contributions about this, but this issue can be discussed as part of an offline or the RRC email discussion which will happen after the meeting. |

# 3 Conclusion

According to what has what has been discussed in section 2:

1. aaa

# References