3GPP TSG-RAN WG2 #109bis-e R2-20xxxxx

Electronic Meeting, April 20th – 30th 2020

Agenda Item: 5.4.1.1

Source: Qualcomm

Title: [AT109bis-e][007][NR15] Security

Document for: Discussion, Decision

# 1 Introduction

This document is the report of the following email discussion:

* [AT109bis-e][007][NR15] Security (Qualcomm, Nokia, Huawei)

Scope: Treat [R2-2003334](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003334.zip), [R2-2003335](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003335.zip), [R2-2003336](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003336.zip), [R2-2003337](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003337.zip), [R2-2002985](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002985.zip), [R2-2002986](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002986.zip), [R2-2003697](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003697.zip), [R2-2003698](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003698.zip).

Part 1: Determine which issues that need resolution, find agreeable proposals. Deadline: April 23 0700 UTC

Part 2: For the parts that are agreeable, discussion will continue to agree on CRs.

As described above in the scope, the following Tdocs are covered here:

[R2-2003334](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003334.zip) Clarification on avoiding keystream repeat due to COUNT reuse Qualcomm Incorporated, Ericsson, Vodafone, NTT DOCOMO CR Rel-15 38.331 15.9.0 1555 - F NR\_newRAT-Core

[R2-2003335](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003335.zip) Clarification on avoiding keystream repeat due to COUNT reuse Qualcomm Incorporated, Ericsson, Vodafone, NTT DOCOMO CR Rel-16 38.331 16.0.0 1556 - A NR\_newRAT-Core

[R2-2003336](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003336.zip) Clarification on avoiding keystream repeat due to COUNT reuse Qualcomm Incorporated, Ericsson, Vodafone, NTT DOCOMO CR Rel-15 36.331 15.9.0 4257 - F TEI15

[R2-2003337](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003337.zip) Clarification on avoiding keystream repeat due to COUNT reuse Qualcomm Incorporated, Ericsson, Vodafone, NTT DOCOMO CR Rel-16 36.331 16.0.0 4258 - A TEI15

Moved from 5.4.2

[R2-2002985](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002985.zip) Avoiding security risk for RLC AM bearers during termination point change Nokia, Nokia Shanghai Bell, Deutsche Telekom CR Rel-15 38.331 15.9.0 1539 - F NR\_newRAT-Core

[R2-2002986](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002986.zip) Avoiding security risk for RLC AM bearers during termination point change Nokia, Nokia Shanghai Bell, Deutsche Telekom CR Rel-15 36.331 15.9.0 4241 - F NR\_newRAT-Core

[R2-2003697](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003697.zip) Potential issue on the Counter Check in (NG)EN-DC and NR standalone Huawei, HiSilicon discussion Rel-15 NR\_newRAT-Core

[R2-2003698](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003698.zip) Draft LS to SA3 on potential issue of Counter Check Huawei, HiSilicon LS out Rel-15 NR\_newRAT-Core To:SA3

# 2 Discussion

Companies are requested to add their comments for each of the treated documents of this email discussion in the boxes below (one for each document to be treated).

## 2.1 Security risk related to COUNT reuse

### 2.1.1 Discussion on the CRs for Clarification on avoiding keystream repeat due to COUNT reuse, [R2-2003334](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003334.zip), [R2-2003335](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003335.zip), [R2-2003336](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003336.zip), [R2-2003337](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003337.zip)

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Nokia | Agree about the COUNT reuse problem in general | Agree that there is something to clarify but just to confirm once again. Is this a different issue than what we have also identified in R2-2002985, R2-2002986?  [Qualcomm]: The issues are in the same area. However, we think changes are not overlapping, and changes from both sets are needed/beneficial. |
| Qualcomm | Agree to CRs 😊 |  |
| CATT | Agree |  |
| Ericsson | Agree |  |
| Huawei, HiSilicon | CRs are useful but we have comments for the changes and disagree with the coversheets | There is no relation with UL  Valid "reason for change" could be that:  - 36/38.331 rewords requirements from 33.501 on avoidance of keystream repeat without actually referring to 33.501, which could be misunderstood that 38.331 is the reference and result in not respecting the requirements from 33.501  - the meaning of "different RB identities for RB establishments" is not clear  With the change, 38.331 is anyway "misaligned" in the sense that what is quoted here is "e.g." so this is misaligned by definition.  Consequences if not approved could be: "RAN2 specification rewords requirements from 33.501 without quoting the original requirements, which can be misunderstood as replacing the requirements from 33.501".  About the changes:  - in 36.331 and 38.331, suggest removing "different"  - in 38.331: suggest adding "successive" like in 36.331  [Qualcomm v7]: Thanks for the comments. Yes, the above suggestions are helpful. Please find in drafts a revised version (changes in coversheet marked with revision marks and changes in actual text highlighted - highlighting is to be removed later). Hope this takes your concern into account. (Similar changes to be mirrored for other CRs later.) |
| Samsung | Disagree | Change#1 in cover sheet i.e. reference to SA3 specs can be handled by editorial changes by RRC rapporteur.  Nothing is broken in the LTE and NR specs. This is not an essential correction.  [Qualcomm v7] Thank you for the comments. However, we think the changes rise above the level of editorial changes. While nothing is broken, there I possibility of misunderstanding as explained in revised coversheet. |
| Apple | Agree |  |
| Intel | Disagree | The network requirement should be quite clear already and it has been like this since LTE Rel-8. The main requirement is clear from SA3 and the existing text “ The eNB is responsible for avoiding reuse of the COUNT with the same RB identity and with the same KeNB,“. If the keys are not changed, then this clearly requires a RBid that is not used previously. |

### 2.1.2 Discussion on the CRs for Avoiding security risk for RLC AM bearers during termination point change, [R2-2002985](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002985.zip), [R2-2002986](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002986.zip)

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Qualcomm | Agree in general | See comments above in 2.1.1. We agree with the intention. However, there are some minor suggestions to the CR   * “and” should be put in front of the last (added) example and existing “and” to be removed. * In coversheet, other specs impacted, not sure if we need to add 36.xxx in 38.xxx and vice versa, but if yes, then CR numbers missing. * If Agreed, Rel-16 mirrors are required. * It may also make sense to merge this to respective CRs in 2.1.1 above since changes are in the same section but we are fine either way. |
| CATT | Not really needed | We agree with the scenario, but there are a lot of scenarios that will cause similar security risk, e.g. the SN may release the DRB with this very DRB ID and then add another DRB with the same DRB ID, or release the DRB and provide the DRB ID back to the MN by XnAP signalling… We need not list each of them. |
| Ericsson | Agree | The scenario that Nokia describes is relevant, even though fullConfig cannot be signalled for the SCG configuration, this is handled by SN indicating that it is using full configuration to MN and then MN setting endc-ReleaseAndAdd for EN-DC towards the UE, so that the UE releases the old SCG configuration before applying the new one.  Maybe what is described is may sound like a corner case, but it does not hurt to add Nokia’s clarification.  There seems to be a typo though on the cover sheet reason for change. Step #4 should say “that the MN did not yet have a key refresh” |
| Huawei, HiSilicon | Not really needed | Same view like CATT, this is certainly not the only scenario.  If there is strong support, we can accept this but the "consequences if not approved" is certainly unsuitable. |
| Samsung | Partially agree | The scenario is possible in which key stream repetition can happen if MN key is not refreshed at step #4 as explained in cover sheet.  However, at step #3 when full config is applied why the same DRB ID is applied. There is no reason to keep the same DRB ID.  The key stream is avoided if at step #3 the DRB ID is changed.  Instead of the proposed changed, we propose to add a NOTE in RRC that at full config NW should change the DRB ID then the identified scenario can be avoided |
| Apple | Agree | We agree with the intention and fine to add the clarification. |
| Intel | May be | As discussed above, the network requirement is very clear. It is not essential to capture all possible examples. Since this is new scenario for Rel-15, it could be considered more useful. If we are to agree the CR, I think the terminology is PDCP re-establishment rather than reset (or COUNT reset). |

## 2.2 Discussion on the Potential issue on the Counter Check in (NG)EN-DC and NR standalone, [R2-2003697](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003697.zip), [R2-2003698](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003698.zip)

In this discussion paper, following is proposed. A draft LS is also provided.

**Proposal: Send a LS to SA3 to check whether it is acceptable for the counter check procedure to check less than the 25 MSBs and indicate the minimum number of bits to be checked.**

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Nokia | Disagree | Just for our understanding do you consider full scheduling active during the COUNTER CHECK procedure? Can you please confirm. |
| CATT | Disagree | SA3 does not say that any COUNT is provided back by the UE means a traffic-insertion attack (it uses “may” instead). The RAN node can handle it based on its own implementation, e.g. comparing the 23 MSBs of the COUNT provided by the UE with the 23 MSBs of the 25 MSBs it sends.  As per current status, we prefer not adopting any NBC changes unless there is a fatal issue and impossible to be handled based on implementation. |
| Ericsson | Disagree | With the proposed change, the flexibility for a potential attacker would increase and hence should be avoided.  A much better approach to avoid intercepted packets is for the network to enable integrity protection.  This seems like an optimization which is not required. The network could address this by implementation, in our view. |
| Qualcomm v4 | Disagree | This is NBC as UE behavior change is required to accommodate for this CR, as UE will expect now to receive and compare less than 25 MSB. And as commented above, the proposal do not address the potential concerns. |
| Huawei, HiSilicon | Agree | To Ericsson's comment: in EN-DC, integrity protection is NOT supported, this mechanism is the only one available.  To CATT's comment: whether the check is done by the UE or the network, we think SA3 should confirm that this is acceptable.  About NBC UE changes: well, maybe security is a valid reason for some NBC change (potentially with a UE capability).  About Qualcomm's comment "not address the potential concerns": well, the group which can appreciate the concerns is SA3, hence why we would like to hear their views. |
| Samsung | Disagree | Nothing is broken from RRC point of view.  The is no issue with RRC procedure. UE simply reports the COUNT in response if there is mismatch and it is NW decision to take further action. Whether COUNT mismatch within a range is allowed is operator policy.  Since this concerns operator policy, we prefer the proponent raise the issue in SA3 directly instead of the LS |
| Apple | Disagree | We share Samsung’s view that it can be discussed in SA3 directly and we don't think there is any RRC spec impact. |
| Intel | Disagree | Nothing is broken from RAN2 specification point of view. If this is considered a security issue, it should be raised in SA3. |

# Conclusion

In the previous sections we made the following observations:

Based on the discussion in the previous sections following is proposed:

# References

[1]