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 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### 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 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 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 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Conclusion

In the previous sections we made the following observations:

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

# References

[1]