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

Electronic Meeting, 17–25 Jan 2022

Agenda Item: 8.24.3

Source: NTT DOCOMO, INC.

Title: Summary of [AT116bis-e][044][NR17] RRC resume security (NTT DOCOMO)

# Introduction

This document is to summarize the following email discussion.

RRC Resume Security

Offline only

* [AT116bis-e][044][NR17] RRC resume security (NTT DOCOMO)

 Scope: Reply to LS in R2-2200154. Consider R2-2201506, R2-2201161, R2-2201162 (chair comment: pl consider also that R2 doesn’t need to reply to aspects typically in R3 domain).

 Intended outcome: Approved LS out

 Deadline: EOM

Although the deadline of the whole discussion is EOM, companies are invited to provide their inputs to the email discussion document by Friday 0800 UTC to ensure enough time for checking the draft LS in Week 2.

# Contact Points

|  |  |  |
| --- | --- | --- |
| Company | Name | Email |
| Docomo (moderator) | Masato Taniguchi | masato.taniguchi.mf@nttdocomo.com |
| Ericsson | Antonino Orsino | antonino.orsino@ericsson.com |
| Google | Frank Wu | frankwu@google.com |
| vivo | Boubacar Kimba | kimba@vivo.com |
| Qualcomm | Ozcan Ozturk | oozturk@qti.qualcomm.com |
| Apple | Fangli XU | fangli\_xu@apple.com |
| Huawei, HiSilicon | Rui Wang | wangrui46@huawei.com |
| CATT | Rui Zhou | zhourui@catt.cn |
| MediaTek | Felix Tsai | chun-fan.tsai@mediatek.com |
| Nokia | Jarkko Koskela | Jarkko.t.koskela@nokia.com |
| Intel | Sudeep Palat | Sudeep.k.palat@intel.com |
| OPPO | Shi Cong | shicong@oppo.com |
|  |  |  |

# References

[1] [R2-2200154](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_116bis-e%5CDocs%5CR2-2200154.zip) LS Reply on security protection of RRCResumeRequest message (S3-214539; contact: NTT DOCOMO) SA3 LS in Rel-17 FS\_5GFBS To:RAN2, RAN3

[2] [R2-2201506](file:///D%3A/Documents/3GPP/tsg_ran/WG2/RAN2/2201_R2_116bis-e/Docs/R2-2201506.zip) Security protection on RRCResumeRequest message (SA3 LS) Huawei, HiSilicon discussion Rel-17 FS\_5GFBS

[3] [R2-2201161](file:///D%3A/Documents/3GPP/tsg_ran/WG2/RAN2/2201_R2_116bis-e/Docs/R2-2201161.zip) Clarifications on security protection of RRCResumeRequest message Ericsson discussion Rel-17 FS\_5GFBS

[4] [R2-2201162](file:///D%3A/Documents/3GPP/tsg_ran/WG2/RAN2/2201_R2_116bis-e/Docs/R2-2201162.zip) [Draft] Reply LS on security protection of RRCResumeRequest message Ericsson LS out Rel-17 FS\_5GFBS To:SA3, RAN3

# Discussions

## Error cases that can lead to deletion of context

The first question from SA3 is on error cases that can lead to deletion of context. Two contributions analysed the cases.

In [2], Huawei makes the following proposal (as Proposal 1). According to the contribution, whether UE context is deleted is not in the scope of RAN2, and assuming if the UE context is deleted then RRC setup can be performed at the serving gNB.

**Proposal 1: Answer to Q1: if RRC Resume Request message is modified by attacker, whether this will lead to deletion of UE context is not clear to RAN2 and RAN3 could provide answer to it. And if assuming UE context will be deleted in this case, the RRC setup can be performed at the serving gNB and RAN2 see no extra work to handle this case.**

In [3], Ericsson makes the following proposals. The contribution discusses that deletion of the UE context may happen in some cases, and if the UE context is deleted, then the old gNB can release the UE and the UE can perform cell (re)selection in order to resume in a different (new) gNB. The contribution also proposes replying that deletion of the UE context does not represent a showstopper for solution 17 in SA3.

1. A failure in the Retrieve UE context procedure it may happen if the old gNB has (physically) crashed or the integrity protection contained in the RETRIEVE UE CONTEXT REQUEST message is not valid, or, that the old gNB decided not to provide the UE context to the new gNB.
2. In case the new gNB fails to retrieve the UE context procedure, the old gNB can release the UE and this UE can perform a cell (re)selection in order to resume in a different (new) gNB.
3. RAN2 to reply to SA3 that the deletion of the UE context at the old gNB may happen if the old gNB has (physically) crashed or the integrity protection contained in the RETRIEVE UE CONTEXT REQUEST message is not valid, or, that the old gNB decided not to provide the UE context to the new gNB.
4. RAN2 to reply to SA3 that even if the UE context is deleted at the old gNB, there is already a procedure standardized in RAN3 (i.e., in TS 38.423) to handle this case.

Taking these proposals into account, companies are invited to answer the following questions.

### **Q1: Which reply do you prefer on cases that leads to deletion of UE context? Any suggestion for improvement?**

Option 1: If RRC Resume Request message is modified by attacker, whether this will lead to deletion of UE context is not clear to RAN2 and RAN3 could provide answer to it.

Option 2: The deletion of the UE context at the old gNB may happen if the old gNB has (physically) crashed or the integrity protection contained in the RETRIEVE UE CONTEXT REQUEST message is not valid, or, that the old gNB decided not to provide the UE context to the new gNB.

|  |  |  |
| --- | --- | --- |
| Company | Option 1/Option 2/other | Comments |
| Ericsson | Either Option 1 or Option 2 | As source company of [R2-2201161](file:///D%3A/Documents/3GPP/tsg_ran/WG2/RAN2/2201_R2_116bis-e/Docs/R2-2201161.zip) we believe that, even in case of a deletion of the UE context, there is not a real issue for supporting solution 17 of TR 33.809 because the current RAN3 specification already handle this case.However, if company prefer to wait for a reply from RAN3 we are also fine to go for Option 1. |
| Google | Other | We understand that if the last serving gNB verifies that the resumeMAC-I of the UE is invalid, the last serving gNB can delete the UE context and transmit a RRCSetup message to the UE. The resumeMAC-I can be invalid, because the RRC Resume Request message is modified by attacker or the last serving gNB is reset due to a crash. However, we think Q1 is about gNB implementations so it is more in the RAN3 domain. Therefore, we prefer to let RAN3 answer Q1. |
| vivo | Option 2 | Wait for a reply from RAN3 |
| Qualcomm | Other | Also think RRC Setup procedure can work but better wait for RAN3 since this also involves interaction between the gNBs, which is in RAN3 domain. |
| Apple | Option 2 | We can also leave this question to RAN3.  |
| Huawei, HiSilicon | Proponent of Option 1 | After reading above company’s comments, we feel they are quite aligned, i.e. RAN2 procedure of RRC setup responding RRCResumeRequest could work in case of the RRCResumeRequest is modified by attacker, as the last serving gNB can consider this is a security context check failure. But UE context release is relevant to RAN3 as well, so it would better to leave to RAN3. |
| ZTE | - | We also think we should wait for RAN3 feedback. We would like to point out that the I-RNTIs are sent in RRCRelease message which is encrypted and hence an attacker cannot have ready access to valid I-RNTIs. The I-RNTI sent in clear on the air is not reused and hence it seems that the attacker can only blindly guess random I-RNTIs. If an invalid I-RNTI is used then the target will not be able to identify a valid anchor node.  |
| Docomo | Other | Though we agree with Option 2, we feel it is in the domain of RAN3. |
| CATT | Option 1 | It is better to leave it to RAN3. |
| Mediatek |  | We think both option 1 and option 2 are correct but prefer to wait RAN3’s reply. |
| LGE | Option 1 | This is the RAN3 scope. |
| Nokia | Option 1 | We agree with Huawei |
| Intel | See comments | Combination of both options. RAN2 specifications support the case that UE context is not available. The reason why it is not available is a network implementation aspect and the reasons listed above is mostly valid but we do not capture it In RAN2 spec. We would also like to add that deleting the UE context on integrity failure may not always be the right thing to do as it can lead to prevent potential denial of service attack. We can reply that RAN2 does not specify the scenarios when network may delete the UE context and that specifications already support recovery in case of deletion of UE context. |
| OPPO | Option1 | We tend to share the view from Intel. |

### **Q2: Do you agree to the following reply regarding what happens if the context is deleted? Any suggestion for improvement?**

(1) RRC setup can be performed at the serving gNB and RAN2 see no extra work to handle this case.

(2) The old gNB can release the UE and this UE can perform a cell (re)selection in order to resume in a different (new) gNB

|  |  |  |  |
| --- | --- | --- | --- |
| Company | Agree with (1)? | Agree with (2)? | Comments |
| Ericsson | Agree | Agree | When the retrieve of the UE context fail the source gNB may send an RRC release to the UE that is delivered transparently by the target gNB. According to this, the UE may perform RRCSetup, or eventually do a cell (re)selection and select a new target gNB. This is already quite clear from TS 38.423. |
| Google | Yes | No | RRC release message is transmitted via SRB1 with security protection. In case the old gNB (i.e., the last serving gNB) deletes the UE Context because of the invalid resumeMAC-I, security keys (i.e., KRRCenc and KRRCint) derived by the old gNB may not be the same as security keys derived by the UE. In this case, the UE may not be able to correctly obtain the RRC release message from the PDCP PDU received on SRB1.RRC setup message is transmitted via SRB0 without security protection. Therefore, the UE can always receive the RRC setup message in the case described above. |
| vivo | Agree | Agree | UE can perform RRCSetup, or cell (re)selection and select a new target gNB |
| Qualcomm | Yes but | No | Better wait for RAN3 confirmation on using RRC Setup. Agree with Google on RRC Release. |
| Apple | Agree | Agree | Both have been covered by current specs. |
| Huawei, HiSilicon | Yes | No | Agree with Google about the issue on sending RRC release. |
| ZTE | Yes (from protocol perspective) | No | We think in general, RRCSetup is a fallback mechanism which comes with additional overhead. We should not just increase the cases of fallback unnecessarily as this will reduce the attractiveness of INACTIVE state in the first place and increase the signalling overhead since unnecessary SMC procedure will be needed.  |
| Docomo | Yes | Not sure | Google’s concern makes sense to us. |
| CATT | Agree | No | If the intention of (2) is the same as in [3], the analysis by Google applies. |
| MediaTek | Yes | Not sure |  |
| LGE | Yes | No | Agree with Google. The UE cannot receive RRCRelease message because it is security protected. |
| Nokia | Yes | No | Agree with Google |
| Intel | Yes | No | We agree with Google comment on Release. Further, we don’t have any specified mechanism for using the Release message for this case to trigger a cell selection to another cell (UE does cell selection after Release but that may result in the same cell).While we agree that RRCSetup can be used for recovery, it causes more interruption and delay. It is useful to provide this to SA3 so they can evaluate any potential denial of service attack. |
| OPPO | Yes | No | Share google’s comment on RRC release |

## Behaviour of UE with suspended RRC connections

The second question from SA3 is on the behaviour of UE with suspended RRC connections in case this feature is activated or deactivated in gNBs.

In [2], Huawei analyses cases where the feature is deactivated at the gNB and makes the following observation and proposal.

**Observation 1: capability negotiation between UE and network are supported in solution from SA3.**

**Proposal 2: Answer to Q2: there is no additional RAN2 spec impact foreseen assuming this feature could be activated or deactivated in gNBs dynamically.**

In [3], Ericsson also analyses the interoperability and sees no issue if the UE has the system information of both gNBs. Accordingly, they have prepared a reply LS in [4].

Proposal 4: RAN2 to reply to SA3 that the UE before sending the RRCResumeRequest message with the new or old version of the ResumeMAC-I/shortResumeMAC-I needs to have stored latest system information of the gNBs in order to check whether both support the new version of the ResumeMAC-I/shortResumeMAC-I or not.

### **Q3:Which approach of reply do you prefer ([2] or [4])? Any suggestion for improvement?**

|  |  |  |
| --- | --- | --- |
| Company | [2] or [4] | Comments |
| Ericsson | 2 and 4 | We think that [2] and [4] basically reach the same conclusion i.e., there is no RAN2 impact foreseen if the feature can be activated/deactivated or not by the gNB.This is because when sending the RRCResumeRequest the UE needs to have anyway the latest version of SIB1 from the target gNB and, eventually, also from the source gNB.Further, if the gNB cannot activate/deactivate this feature, we see that there is no issue at all. |
| Google | [2] | The following is excerpted from TR 33.809*The UE and the network negotiate/learn each other’s capability/support of using the newer version of ResumeMAC-I/shortResumeMAC-I as below:**- UE’s capability is part of an RRC message (i.e., AS SMComplete).**- gNB/ng-eNB should indicate its capability of supporting the new version of ResumeMAC-I in SI message (i.e., SIB1, refer to a closely related feature called useFullResumeID in SIB1).* *- gNB/ng-eNB should also indicate its capability of supporting the new version of ResumeMAC-I in RRCRelease message with SuspendConfig, which is sent after AS SMC thus protected.*The SA3’s solution (i.e., solution 17) is clear so we can simply indicate that there is no issue foreseen with solution 17 in TR 33.809 in case this feature is activated or deactivated in gNBs. |
| vivo | 2 | 2 is enough |
| Qualcomm | Comments | Both 2 and 4 seem to consider the case when the feature is activated/de-activated at the resume cell. We should also analyse the case of last serving cell. |
| Apple | [2] | This case can be covered by the capability negotiation between UE and gNB, which has been captured in SA3 TR on the solution#17 description.  |
| Huawei, HiSilicon | Proponent of 2 | On Qualcomm’s comment, we have discussed the case that last serving gNB deactivate this feature after releasing the UE with the configuration of this feature in [2]. In our understand, the UE configuration is supposed to be stored in the UE AS inactive context, and the last serving gNB is aware of the configuration of this feature from the UE context even though the gNB has disabled this feature and changed the network capability in SIB, thus the last gNB should be able to check the shortMAC-I using new method. And even though we assume the last gNB cannot perform the new method after it disable the feature, the worst case is security check failure which leads to fallback to RRC setup. No big issue. |
| ZTE | 4, with comments | We think it should be guaranteed that the anchor and target both support and activate the feature when the UE is performing resume as already agreed previously. Otherwise, the feature shall not be used. When the RAN node activates this feature, only resume procedure using this new feature should be accepted by this node. It is unclear to us how it can be guaranteed that the UE knows what the anchor’s current mechanism is if this can dynamically change. [4] seems to suggest that UE shall know the latest SIB information. However, although this is possible in the target node this is not possible in the anchor node. So, we are not sure how the mechanism is supposed to work in this case. We disagree with the point that RRCSetup can always be used. This is not preferable option since it increases the signalling overhead. So, if anchor node can dynamically activate and deactivate the feature, it seems some coordination will be needed to ensure there is no mismatch between the UE and the anchor node and this needs discussion.  |
| Docomo | [2] | We agree with Huawei’s comment that the last serving gNB can use an appropriate way (new or old) of resume MAC-I validation by using the information about whether the feature was activated or not when the UE went to RRC\_INACTIVE. |
| CATT | [2] | It is already covered by the capability negotiation between UE and gNB. |
| MediaTek | [2] | [2] is enough.  |
| LGE | 2 | 2 is enough. |
| Nokia | 2 | we see no reason to more than 2 |
| Intel | Either 2 or 4, with comments | UE has to check that both source and target gNB supports this feature before using it. UE only knows the source SIB while it was last in the source cell. If source gNB dynamically turns off this feature later, it is not clear what that means – can it still perform verification of new ResumeMAC-I from a UE performing ResumeRequest in another cell as suggested by Qualcomm? If so, it should be OK, but the SA3 LS is not clear this is the case. So we think 2 on its own is not sufficient and if we agree to option 2, we should also state the assumption mentioned by Qualcomm in the LS. |
| OPPO | [2] |  |

## Cell selection procedures potentially prioritising availability of this feature

In [2], Huawei makes the following proposal. The background is that, in the current NR spec, cell selection/reselection mainly is based on signal measurement.

**Proposal 3: Answer to Q3: RAN2 does not expect any impact on cell selection/reselection mechanism brought by this feature.**

In [3] Ericsson makes the following proposal. The background is that a cell that supports the new feature does not necessary means that is also the cell that gives the best performance for the UE.

Proposal 6: RAN2 to reply SA3 that UE behaviour during cell (re)selection is not impacted by solution 17 of TR 33.809 and that no prioritization rule will be introduced for the UE to prioritize a cell that support the new feature.

Although the background seems different, neither of the contributions sees any impact on RAN2 specifications. Hence the moderator suggests simply replying with the assumption of no RAN2 impact.

### **Q4: Do you agree to mention the following in the reply LS? Any suggestion for improvement?**

**- RAN2 does not expect any impact on cell selection/reselection mechanism brought by this feature.**

|  |  |  |
| --- | --- | --- |
| Company | Agree? | Comments |
| Ericsson | Agree | We do not see any impact on the cell (re)selection procedure. Also, a cell that supports the new feature does not necessary means that is also the cell that gives the best performance for the UE.  |
| Google | Yes | We also don’t see any impact to the cell selection/reselection procedures. |
| vivo | Agree |  |
| Qualcomm | Disagree | If the UE re-selects cells without the feature, the resume will fail. So, there should be a way to prioritize these cells. |
| Apple | Agree | We donot see any impact on the cell (re)selection procedure. |
| Huawei, HiSilicon | Agree | On Qualcomm’s comment, if UE reselect to a cell not supporting the new method, UE can know the network capability via SIB, and it will set the shortMAC-I using legacy method according to the SA3 solution. No misalignment will happen between UE and network.We also understand there are always new features introduced in a later release, and the basic principle is that UE selects cell according to signal quantity, we do not see why this new feature should impact cell (re)selection.  |
| ZTE | Discuss | We are not sure about cell reselection, but there should some discussion on avoiding unnecessary fallbacks. Firstly, we are not sure whether dynamic on and off of this feature is a prerequisite and if this is agreed in SA3, we should discuss mechanisms to ensure unnecessary fallbacks are avoided.  |
| Docomo | Agree |  |
| CATT | Agree | Agree with companies above that there should be no impact to cell selection/reselection. |
| MediaTek | Agree |  |
| LGE | Agree |  |
| Nokia | Agree |  |
| Intel | Agree | We should not impact cell selection/reselection. It is up to network to use this feature in the cells if it considers that this security is important.  |
| OPPO | Agree |  |

## General

In [3] and [4], Ericsson proposes to explicitly mention that there is no showstopper for Solution 17 from RAN2 point of view.

### **Q5: Do you agree to mention the following in the reply LS? Any suggestion for improvement?**

**- RAN2 does not see the concerns expressed by SA3 in the LS in R2-2200154 as a showstopper for implementing solution 17 of TR 33.809.**

|  |  |  |
| --- | --- | --- |
| Company | Agree? | Comments |
| Ericsson | Agree | As we also discussed in R2-2107574, we think that the introduction of this new security feature in RAN2 is minimum and we see no problem of supporting it. |
| Google | Yes | We don’t see the concerns as well. |
| vivo | Agree |  |
| Qualcomm | Disagree | Not clear “no showstopper” means. RAN2 has previously responded to SA3 on the necessary changes and commented that this would need a Work Item since it also has impact on RAN3. That conclusion still holds. For Rel-17, it is impossible to have a new WI since there is no time left. It is sufficient to respond to the actual questions. |
| Apple | Agree | The “no showstopper” means the solution is technically feasible. In RAN2#115e we discussed the solution and agreed that the solution is technically feasible. For the timing issue, if there is no time to implement it in R17 timeframe, it can be implemented in R18.  |
| Huawei, HiSilicon | Agree | We understand the intention of this sentence is not to say this solution can be specified in Rel-17, since indeed there is not sufficient time as Qualcomm comments, but just to confirm the feasibility of the solution.Considering in last RAN2 LS R2-2109121, it says “The solution is technically feasible from RAN2 perspective.”, we are ok to double confirm that those questions from SA3 will not change the RAN2 conclusion on the feasibility. |
| ZTE | Disagree | In general, we are also not sure what is meant by no show stoppers. With regards to the dynamic nature of this feature, in our view, this needs a bit more discussion on how to ensure unnecessary fallbacks are avoided as pointed above. We agree with Qualcomm that a WI will be needed anyway as previously agreed.  |
| Docomo | See comment | We are ok either way, but we sympathize with QC and ZTE on WI management. If we are to say “no showstopper”, the reply should focus on technical point of view. |
| CATT | Agree | Agree with Huawei that we are just confirming the feasibility. |
| MediaTek | Disagree | We should just reply the technical points and avoid saying “no showstopper” |
| LGE | Disagree | We should just reply that RAN2 does not see any impact.  |
| Nokia | Disagree | It would be very unfortunate to state that this is no showstopper – I guess It would be showstopper to require multi WG changes at this point of time. We just state what are impacts. |
| Intel | Disagree | While we agree it looks technically feasible, we still need to understand the full details of the final agreed SA3 solution. And then we need consider the impact to our specifications and check if this can be completed in Rel-17. |
| OPPO | Disagree | Prefer to not mentioning “no showstopper” as mentioned by other companies, R17 may not have enough time for new WI. |

# Conclusion