3GPP TSG-RAN WG2 Meeting #115 Electronic R2-210xxxx

Online, August, 2021

**Agenda item: 8.22**

**Source: Apple**

**Title: [AT115-e][032][NR17] Security protection RRC Resume (Apple)**

**Document for: Discussion and Decision**

# 1. Introduction

This document attempts to summarize the following offline discussion.

* [AT115-e][032][NR17] Security protection RRC Resume (Apple)

 Scope: Treat papers under 8.22 on Security protection for RRC resume (this section), Determine agreeable points, Reply LS and Draft CRs.

 Intended outcome: Report, Approved LS out, Agreed-in-principle CRs

 Deadline: CB Friday, at least for the report.

# 2. Contact Points

Respondents to the email discussion are kindly asked to fill in the following table.

|  |  |  |
| --- | --- | --- |
| Company | Name | Email Address |
| ZTE | Eswar Vutukuri | eswar.vutukuri@zte.com.cn |
| MediaTek | Nathan Tenny | Nathan.Tenny@mediatek.com |
| Lenovo, MotM | Prateek Basu Mallick | pmallick@lenovo.com |
| Ericsson | Antonino Orsino | antonino.orsino@ericsson.com |
| Xiaomi | Rao Shi | shirao@xiaomi.com |
| OPPO | Shukun Wang | wangshukun@oppo.com |

# 3. Discussion

SA3 LS Reply (R2-2106977/S3-212349) informs RAN2 on their FBS solution#17 which is about the security protection on the RRCResumeRequest , and SA3 requests RAN2 to check the capability negotiation issue between UE and NodeBs and answer the following questions.

|  |
| --- |
| **SA3 would like to ask RAN2 the following questions:** 1. For the capability negotiation method between UE and gNB/ng-eNB as mentioned above, if there are other preferable alternatives from RAN2 perspective?
2. Is there any mechanism for the source gNB/ng-eNB to know the target gNB/ng-eNB capabilities?
3. The possibility of specifying the solution in RAN2 specification in Rel-17 timeframe, if the solution is concluded by SA3.
 |

Amongst the three SA3 Questions, Q1 and Q2 are about the capability negotiation, and Q3 is about the standards timeline issue.

## 3.1. Capability negotiation

For the capability negotiation issue Q1 and Q2, companies proposed reply are provided as follows:

|  |
| --- |
| **SA3 would like to ask RAN2 the following questions:** 1. For the capability negotiation method between UE and gNB/ng-eNB as mentioned above, if there are other preferable alternatives from RAN2 perspective?
2. Is there any mechanism for the source gNB/ng-eNB to know the target gNB/ng-eNB capabilities?
 |

|  |  |  |
| --- | --- | --- |
|  | [R2-2107299](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107299.zip) Discussion and Response on SA3 LS on new ResumeMac-I calculation Intel | 1. For the capability negotiation method between UE and gNB/ng-eNB as mentioned above, if there are other preferable alternatives from RAN2 perspective?

At the time of processing the *ResumeMac-I*, the old gNB has the UE capability needed to know whether the UE supports the feature and there is no need for the new gNB to be aware of the UE capability. There is no need for any additional UE capability signalling during Resume procedure if this capability can also be included as part of the UE radio capability that is retrieved after AS security activation.Both the old gNB and new gNB should support the new mechanism to use it. UE should combine the support in both the old gNB and new gNB and use the new calculation only if both these indicate support of the ResumeMac-I new calculation. The SIB indication in the old cell or a dedicated signalling and SIB indication in new cell can be used for that purpose respectively. 1. Is there any mechanism for the source gNB/ng-eNB to know the target gNB/ng-eNB capabilities?

Current Xn specification does not seem to provide the full ResumeRequest message to the old gNB for it to calculate the ResumeMac-I using the new method. Hence the new gNB needs to be updated to provide the full ResumeRequest message over Xn. This could, for example, serve as an implicit indication to old gNB of support of the new calculation by the new gNB. Details should be discussed by RAN3.There is no need for the new gNB to be aware of whether the old gNB supports this feature. |
|  | [R2-2107483](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107483.zip) On the security protection of RRCResumeRequest message ZTE, Sanechips | The anchor gNB (i.e. the gNB that would have generated the preceding RRCRelease message) would also verify the security token coming from the UE. Thus, the anchor gNB can configure the UE to use the new security mechanism (e.g. by including an indication in the dedicated message – e.g. in the RRCRelease message if both the anchor gNB and the UE support the new feature). Hence, this doesn’t need an SIB indication or a new mechanism to negotiate the capability between UE and gNB or between gNBs. |
|  | [R2-2107572](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107572.zip) DRAFT LS Reply on security protection on RRCResumeRequest message Apple [To be RAN2] LS out | **Response to Q1:**RAN2 agreed with the SA3’s capability negotiation method between UE and gNB/ng-eNB on the UE capability indication. For the gNB/ng-eNB’s capability indication, RAN2 understanding is that gNB/ng-eNB indicates its capability in both SIB1 and the RRC dedicated signaling (i.e. RRCRelease with SuspendConfig):* When gNB/ng-eNB is the target node (i.e. the the receiving node), it indicates the capability in SIB1, which means the target node can forward the new MAC-I and the associated input information to the source node;
* When the gNB/ng-eNB is the source node (i.e. the last serving node), it indicates the capability to UE via the RRC dedicated signaling (i.e. RRCRelease with SuspendConfig), which means the source node supports the enhanced MAC-I verification.

UE only uses the new MAC-I for RRCResumeRequest message when both the source and target nodes support the feature. If either one of nodes doesn’t support this feature, UE will not send the new MAC-I.**Response to Q2:**There is no mechanism needed for the capability negotiation between the target node and the source node. The target node doesnot need to know the source node’s capability. If the target node supports the feature, it always forwards the new MAC-I indication and the new added input for the MAC-I calculation/verification in X2 message (RETRIEVE UE CONTEXT REQUEST) to last serving gNB. The source node can identify the capability of the target node based on the presence of the new indication in the X2 message.  |
|  | [R2-2107842](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107842.zip) Draft LS reply on security protection on RRCResumeRequest message vivo LS out | * Q1: For the capability negotiation method between UE and gNB/ng-eNB as mentioned above, if there are other preferable alternatives from RAN2 perspective?

Ans1: As the new capability of is used only after network releases UE to RRC INACTIVE mode, there is no need for UE to report this capability before UE RRC connection complete. Existing UE capability reporting procedure is reused to report this capability.* Q2: Is there any mechanism for the source gNB/ng-eNB to know the target gNB/ng-eNB capabilities?
1. Ans2: the capability can be indicated between gNB/ng-eNB by means of Xn setup procedure, Xn configuration update procedure.
 |
|  | [R2-2108216](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2108216.zip) Extended MAC-I for RRCResumeRequest MediaTek | * RAN2 understand that the target gNB/ng-eNB could indicate its support in SIB1. For the source gNB/ng-eNB, it could indicate its support in the *RRCRelease*/*RRCConnectionRelease* message when the UE is sent to RRC\_INACTIVE.
* RAN2 do not see an obstacle to having the target gNB/ng-eNB indicate its support of the enhancement to the source gNB/ng-eNB, but the details of this procedure are in RAN3 scope and RAN2 cannot give an authoritative answer.
 |
|  | [R2-2108348](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2108348.zip) Discussion on security enhancement for RRCResumeRequest Xiaomi | Proposal 3: The UE reports its capability bit of supporting the security enhancement for RRCResumeRequest message. Proposal 4: If the method of system information for capability is introduced, UE should be restricted that only the capability broadcasted from the last used cell can be used.Proposal 5: RRC release message can be used to indicate the gNB capabilty of supporting the security enhancement for RRCResumeRequest message. |
|  | [R2-2108621](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2108621.zip) Security protection on RRCResumeRequest message Huawei, HiSilicon | * From RAN2’ point of view, to support SA3’s solution on RRC resume protection in Q1 and Q2 is feasible with the following potential RAN impact:
* RAN2 impact: to specify the capability negotiation procedure between UE and gNB and potential impacts includes:
* UE's capability reporting on support of new type ResumeMAC-I
* gNB capability indication of new type ResumeMAC-I by system information.
* RRC configuration to enable the UE to use the new type ResumeMAC-I via RRC release message sending by last serving gNB.
* RAN3 impact: to specify how to make the last serving gNB know the capability of the source serving gNB, e.g.
* if resume cause is not periodic RNAU, resume cause in RETRIEVE UE CONTEXT REQUEST message could be used to indicate the current serving gNB capability implicitly;
* if resume cause is periodic RNAU, additional indication information could be included in RETRIEVE UE CONTEXT REQUEST message to RETRIEVE UE CONTEXT REQUEST message to indicate the capability of current serving gNB.
 |

<which entities’ capability to be considered? >

To enable the new ResumeMAC-I feature, some companies indicate that it requires the support of the UE, the anchor gNB and the new serving gNB.

* UE is required to support the new ResumeMAC-I generation;
* The anchor gNB is required to perform the new ResumeMAC-I verification;
* The new serving gNB is required to forward the new ResumeMAC-I indication and the new added input for MAC-I calculation to the anchor gNB via RETRIEVE UE CONTEXT REQUEST.

#### **Question 1: Do you agree that the newResumeMAC-I feature requires the support of the UE, the source gNB and the target gNB?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Agree, with comments | It is true that the serving gNB needs to forward the ResumeMAC-I indication to the anchor. However, this happens today already. The only additional information that the serving gNB needs to send is the resumeCause. Note that this is already in the Xn signalling but is sent when RNAU is initiated. Depending on the final solution chosen, there may or may not be any need for further updates to the target gNB (see answers to questions 2a and 4) |
| MediaTek | Agree | For this feature to work, the target gNB must forward the resumeCause in all cases, not just the RNAU case as currently specified, so there is impact to the target gNB. We don’t see that it is possible to specify a solution without such impact. |
| Lenovo, MotM | Agree |  |
| Ericsson | Agree |  |
| Xiaomi | Agree with comments | Since UE has already negotiated with anchor gNB for the capability, maybe the new serving gNB doesn’t need to know UE and anchor gNB’s capability, it is enough to just simply send an enhanced Xn message RETRIEVE UE CONTEXT REQUEST to anchor gNB.It means no matter what capability gNB have, the Xn message should be enhanced anyway. |
| OPPO | Agree  |  |

<UE capability>

For the UE capability indication, almost all companies indicate that new UE AS capability should be introduced to indicate the UE support of this feature.

#### **Question 2: Do you agree that new UE AS capability should be introduced to indicate the support of the feature?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Yes |  |
| MediaTek | Yes |  |
| Lenovo, MotM | Agree |  |
| Ericsson | Agree |  |
| Xiaomi | Agree |  |
| OPPO | Agree  |  |

#### **Question 2a: Do you agree that the UE should only enable the new ResumeMAC-I feature when it knows that both source and target gNB support it?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Discussion needed | This depends on the solution. There could be two options: Option 1: Anchor gNB only configures the new mechanism when all gNBs within the RNA support the new security mechanismOption 2: Anchor gNB configures the new security mechanism regardless of the support of the feature in the neighbouring gNBsIf we go with option 1, then it seems there is no need to discuss the support of the target gNB since the feature is supported within the RNA and if the UE moves outside the RNA, RNAU based RRCResumeRequest is generated (for which ResumeCause is already included in the Xn message). If we go with option 2, then UE needs to know whether target gNB supports it or not and this needs SIB signalling. We think RAN3 can discuss whether option 1 or option 2 is appropriate for this feature.  |
| MediaTek | Yes (see comment) | Considering ZTE’s comment, we agree that it could be possible for the source gNB to configure this feature only when it knows all potential target gNBs support it, and then the UE would not have to check explicitly. This seems a bit overly restrictive compared to a 1-bit flag in SI, and we would prefer to take the simpler solution, but in any case the UE must only use the new MAC-I when it is guaranteed that the source and target gNBs support it. |
| Lenovo, MotM | Agree |  |
| Ericsson | Agree |  |
| Xiaomi | See comments | We think the target gNB doesn’t need to care about UE and anchor gNB’s capability if Xn message is enhanced to carry the new added input for MAC-I calculation anyway. The anchor gNB know UE’s capability, once receiving RETRIEVE UE CONTEXT REQUEST, it can choose appropriate way to perform verification. |
| OPPO | Agree  |  |

<The anchor gNB capability>

To indicate the anchor gNB’s capability, majority view is that if the anchor gNB supports the feature it can configure the new ResumeMAC-I feature to the UE based on UE capability via the RRCRelease with SuspendConfig message when setting the UE in INACTIVE state.

#### **Question 3: Do you agree that the anchor gNB can configure the new ResumeMAC-I feature via the RRCRelease with SuspendConfig message to the UE based on UE and anchor gNB’s capability?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Agree |  |
| MediaTek | Agree |  |
| Lenovo, MotM | Agree but… | From Q4 it would be clear that “any” gNB supporting the new ResumeMAC-I feature would need to broadcast this support. So, the RRCRelease need not carry this information again…i.e., broadcasting is sufficient. |
| Ericsson | Agree |  |
| Xiaomi | Agree | We think RRCrelease is a fine solution as it is from anchor gNB which the verification is always done here. |
| OPPO | Agree  |  |

#### **Question 3a: Do you agree that the anchor gNB only perform the new ResumeMAC-I verification under the following two conditions:**

1. **When the UE is configured with the new feature; and**
2. **The new serving gNB forwards all the associated input for the new ResumeMAC-I.**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Agree |  |
| MediaTek | Agree, but | For the RNAU case, the source gNB must know whether the target gNB supports the new MAC-I. This is because the resumeCause will be included in the Xn message in any case, and the content over which the MAC-I should be computed depends on whether the target gNB supports the new MAC-I. So this capability of the target gNB needs to be indicated to the source; RAN3 can discuss how best to do this. |
| Lenovo, MotM | Agree |  |
| Ericsson | Agree |  |
| Xiaomi | Agree |  |
| OPPO | Agree  |  |

<The new serving gNB capability>

To indicate the new serving gNB’s capability, companies proposes that the new serving gNB should broadcast it’s support via the SIB signaling.

#### **Question 4: Do you agree that the new serving gNB should indicate the support of the new ResumeMAC-I via SIB?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Depends on the solution (see Q2a) | If we assume support for the feature within entire RNA, then there is no need for SIB indication. If we assume support for a subset of gNBs, then SIB indication is needed. The actual architecture option to be chosen should be decided in RAN3.  |
| MediaTek | Yes | We don’t see a good tradeoff in restricting the applicability of the feature in order to save a 1-bit flag in SI as suggested by ZTE. |
| Lenovo, MotM | Yes | And in more general terms – this should apply for “any” gNB since new serving gNB could be an anchor gNB for another UE. |
| Ericsson | Agree |  |
| Xiaomi | See comments | Does this mean when a UE which already indicate the anchor gNB for supporting new resumeMAC-I reselect to a new serving gNB which doesn’t support new resumeMAC-I via broadcast, the UE will use old resumeMAC-I？then the new serving gNB inform anchor gNB to use old resumeMAC-I calculation？it is true that this scheme can work. If majority agree on this, we can follow.But we still think a simple way is that the new serving gNB doesn’t need to care about the capability of UE and anchor gNB. No matter what capability they have, the new serving gNB always send an enhanced Xn message and that is enough. |
| OPPO | Yes  |  |

About how to inform the new serving gNB’s capability to the anchor gNB, some companies propose to indicate the capability in the X2 setup procedure, but other companies indicate that the capability can be explicitly or implicitly indicated via the X2 RETRIEVE UE CONTEXT REQUEST message.

#### **Question 5: Which options do you prefer to indicate the new serving gNB’s capability to the anchor gNB?**

**Option 1: The new serving gNB’s capability is indicated via the X2 setup procedure;**

**Option 2: The new serving gNB’s capability is explicitly or implicitly indicated via the X2 RETRIEVE UE CONTEXT REQUEST message.**

**Option 3: Others?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Leave to RAN3 | As noted above, apart from these two options, there is a further option to assume support within entire RNA and all these can be discussed and decided in RAN3.  |
| MediaTek | Leave to RAN3 |  |
| Lenovo, MotM | Leave to RAN3 |  |
| Ericsson | Leave to RAN3 |  |
| Xiaomi | Leave to RAN3 | If majority think new serving gNB’s capability should be known to the anchor gNB. |
| OPPO | Leave to RAN3 |  |

## 3.2. The possibility of specifying in R17

For the SA3 Q3, companies proposed reply are provided as follows:

|  |
| --- |
| **SA3 would like to ask RAN2 the following questions:** 1. The possibility of specifying the solution in RAN2 specification in Rel-17 timeframe, if the solution is concluded by SA3.
 |

|  |  |  |
| --- | --- | --- |
|  | [R2-2107299](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107299.zip) Discussion and Response on SA3 LS on new ResumeMac-I calculation Intel | Since this feature impacts both RAN2 and RAN3, it will require a dedicated WI as per RAN plenary guidance and be discussed in RAN plenary. |
|  | [R2-2107483](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107483.zip) On the security protection of RRCResumeRequest message ZTE, Sanechips | RAN2 answer to Q3: As noted above, RAN2 can specify an additional indication in the RRCRelease message to indicate the UE to use the new mechanism to generate the ResumeMAC-I upon next RRCResume. This work is feasible within Rel-17 time frame. However, RAN2 would like to point out that additional information related to the RRCResume procedure is conveyed to the network via the RACH resource and this information is not protected even if entire contents of the RRCResumeRequest as proposed in SA3 solution is covered by the rrcResumeMAC-I. The e.g. information that is not included in the RRCResumeRequest but is conveyed as part of the overall procedure using the RACH resource includes the following: * + Until Rel-16: Selected SSB, Payload size and
	+ Rel-17 onwards: RAN slice information, SDT cause, REDCAP indication, Coverage extension indication).
 |
|  | [R2-2107572](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107572.zip) DRAFT LS Reply on security protection on RRCResumeRequest message Apple [To be RAN2] LS out | It’s possible for RAN2 to specify the solution in R17 if SA3 makes the conclusion to support it in R17. |
|  | [R2-2107842](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2107842.zip) Draft LS reply on security protection on RRCResumeRequest message vivo LS out | ANS 3: From RAN2 perspective, based on SA3 conclusion on this solution, RAN2 can specify the necessary RRC procedure in Rel-17 timeframe |
|  | [R2-2108216](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2108216.zip) Extended MAC-I for RRCResumeRequest MediaTek | The proposed solution is feasible from RAN2 perspective, and RAN3 should be consulted about impact to the context retrieval procedure. |
|  | [R2-2108348](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2108348.zip) Discussion on security enhancement for RRCResumeRequest Xiaomi | N/A |
|  | [R2-2108621](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_115-e%5CDocs%5CR2-2108621.zip) Security protection on RRCResumeRequest message Huawei, HiSilicon | Whether to support this solution in Rel-17 or Rel-18 should be decided by SA3. RAN2 can perform further evaluation based on further SA3 request. |

For the possibility to specify this feature in SA3, all companies think the solution is feasible from RAN2 perspective. 1 company indicates that RAN3 should be consulted about impact to the context retrieval procedure, and other companies indicate that it’s possible for RAN2 to specify the solution in R17 if SA3 makes the conclusion to support it in R17.

#### **Question 6: Do you agree that the solution is feasible from RAN2 perspective?**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Discuss | From a pure signalling point of view, it may be feasible. However, we are not sure what the intention of SA3 is with this modification. As such, if the intention is to protect the resumeCause, SA3 should be aware that resumeCause is not just conveyed within the RRCResumeRequest, but is included in RACH resource implicitly (for a number of features within Rel-17).  SA3 should investigate the overall feasibility and actual use of the solution taking into account the above aspect.  |
| MediaTek | Yes |  |
| Lenovo, MotM | Yes |  |
| Ericsson | Yes |  |
| Xiaomi | Yes |  |
| OPPO | Based on discussion | We share the same view with ZTE. It is not clear why the current mechanism is not enough and need to considier all information in MSG3? Why the new method is better?So RAN2 should know the intention clear when we decide something. |

#### **Question 7: Do you agree that it’s possible for RAN2 to specify the solution in R17 if SA3 makes the conclusion to support it in R17.**

|  |  |  |
| --- | --- | --- |
| Company | Agree or not? | Comments |
| ZTE | Agree, but | But SA3 should be aware of the fact that protecting the contents of RRCResumeRequest doesn’t necessarily protect the ResumeCause (since it is provided out of the resumeRequest message in some cases for Rel-17 onwards).  |
| MediaTek | Yes | We have no objection to indicating to SA3 that the resumeCause is in some cases indicated elsewhere, but it seems orthogonal to the solution they’re asking about. Note that this is about integrity protection, not encryption, so the objective is not to prevent an attacker from learning the resumeCause—it’s to guarantee that an attacker cannot imitate the resume signalling from a legitimate UE. Creating a RACH request that appears to be related to a specific resume cause, but that then cannot be followed up with a valid RRCResumeRequest message, would be a different attack, which SA3 could discuss but which seems not likely to affect the solution discussed here. |
| Lenovo, MotM | Yes |  |
| Ericsson | Yes |  |
| Xiaomi | Yes |  |
| OPPO | Yes  |  |

# 4 Conclusion

TBD.