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

# 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. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### **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. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 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. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 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.  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 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. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Conclusion