**3GPP TSG- WG3 Meeting # *draft* R3-240933**

**Athens, Greece, 26th Feburary – 1st March, 2024**

Agenda Item: 9.3.2

Source: Google (Moderator)

Title: Summary of offlines for CB#32 CRNTI

Document for: Discussions

# 1 Introduction

**CB: # 32\_CRNTI**

**- Check the issue and discuss other candidate solutions**

(moderator - Google)

Summary of offline disc [R3-240933](Inbox\R3-240933.zip)

# 2 Proposals for Chair notes

<TBD>

# 3 Introduction

The Cell RNTI (C-RNTI) currenlty in use between the UE and the base station (CU and DU) can identify a UE context and a RRC connection. It is also used to help validate the UE, for example, in case of RRC connection resumption, RNA update, or RRC connection re-establishment as described in TS 38.331 [1] and TS 33.501 [2] as cited below.

|  |
| --- |
| “The ResumeMAC-I/shortResumeMAC-I is a 16-bit message authentication token, the UE shall calculate it using the integrity algorithm (NIA or EIA) in the stored AS security context, which was negotiated between the UE and the source gNB/ng-eNB and the current KRRCint with the following inputs:  - KEY : it shall be set to current KRRCint;  - BEARER : all its bits shall be set to 1.  - DIRECTION : its bit shall be set to 1;  - COUNT : all its bits shall be set to 1;  - MESSAGE : it shall be set to VarResumeMAC-Input/VarShortInactiveMAC-Input as defined in TS 38.331 [22] for gNB and in TS 36.331 [69] for ng-eNB with following inputs:  *source PCI, target Cell-ID, source C-RNTI*.”  "When the target gNB/ng-eNB receives the RRCResumeRequest message from the UE, the target gNB/ng-eNB extracts the I-RNTI from the RRCResumeRequest message. The target gNB/ng-eNB contacts the source gNB/ng-eNB based on the information in the I-RNTI by sending an Xn-AP Retrieve UE Context Request message with the following included: I-RNTI, the ResumeMAC-I/shortResumeMAC-I and target Cell-ID, in order to allow the source gNB/ng-eNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context.  The source gNB/ng-eNB retrieves the stored UE context including the UE 5G AS security context from its database using the I-RNTI. The source gNB/ng-eNB verifies the ResumeMAC-I/shortResumeMAC-I using the current KRRCint key stored in the retrieved UE 5G AS security context (calculating the ResumeMAC-I/shortResumeMAC-I in the same way as described above).*”* |

|  |
| --- |
| “**The connection re-establishment succeeds if the network is able to** **find and verify a valid UE context** or, if the UE context cannot be retrieved, and the network responds with an *RRCSetup* according to clause 5.3.3.4.” |

|  |
| --- |
| “In order to calculate the token, the source gNB shall use the negotiated NIA-algorithm from the 5G AS Security context from the source gNB with the following inputs: source C-RNTI, source PCI and target Cell-ID, where source PCI and source C-RNTI are associated with the cell the UE last had an active RRC connection with and target Cell-ID is the identity of the target cell where the RRCReestablishmentRequest is sent to.  - KEY shall be set to KRRCint of the source cell;  - all BEARER bits shall be set to 1;  - DIRECTION bit shall be set to 1;  - all COUNT bits shall be set to 1.  The token shall be the 16 least significant bits of the output of the used integrity algorithm.”  “If the target gNB receiving the RRCReestablishmentRequest has a prepared KNG-RAN\* key and token for the specific cell, the target gNB receiving the RRCReestablishmentRequest shall validate the token received in the RRCReestablishmentRequest. However, if the target gNB has not prepared token for the cell, the target gNB extracts the C-RNTI and PCI from the RRCReestablishmentRequest message. The target gNB contacts the source gNB based on PCI by sending an Xn-AP Retrieve UE Context Request message with the following included: C-RNTI, PCI, the token and target Cell-ID, in order to allow the source gNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context. ” |

**Observation 1: Cell RNTI can identify a UE context and a RRC connection. It is also used to help validate the UE.**

It is noticed that the C-RNTI IE is optional in the UE Context Setup Response message and the UE Context Modification Response message. As only receiving side behavior is described for C-RNTI is captured in the current TS 38.473 [3] for the UE context response messages (**i.e., during the preparation phase)**, it is not clear, upon LTM execution, whether and how the CU determines the C-RNTI to use (while keeping the other prepared C-RNTIs for other cell groups for subsequent cell switching) for the UE.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| C-RNTI | O |  | 9.3.1.32 | C-RNTI allocated at the gNB-DU | YES | ignore |

|  |
| --- |
| “If the *C-RNTI* IE is included in the UE CONTEXT SETUP RESPONSE, the gNB-CU shall consider that the C-RNTI has been allocated by the gNB-DU for this UE context.”  “If the *C-RNTI* IE is included in the UE CONTEXT MODIFICATION RESPONSE, the gNB-CU shall consider that the C-RNTI has been allocated by the gNB-DU for this UE context.” |

After several rounds of subsequent LTM cell switching, without a clear guidance how the C-RNTI is determined after each LTM completion, the CU might lose track of the exact C-RNTI and fail in validating a UE during an RRC connection re-establishment or a RRC state transitions.

In the online and offline discussion, most companies generally acknowledged the issue for conditional mobility and some also mentioned immediate mobility. Instead of introducing C-RNTI in other messages (e.g., Access Success or UL RRC Message Transfer), the feedback favors clarifying that, for the mobility use cases, the C-RNTI is obtained by the CU in the UE Context Setup Response message or the UE Context Modification Response message.

It was first suggested by some companies to revise the stage 2 TS 38.401 to cover all the involved cases. However, after checking, in TS 38.401 there are **more than 20 sections** involved mobility and not only the mobility enhancement work items are impacted. It could therefore be difficult for people to check. Therefore, the moderator proposes to address the stage 3 TS 38.473 specification for the clarification.

**Proposal: Clarify how the CU obtains and determines the C-RNTI for mobility case in the TS 38.473.**

There are three general places to address the issue. The draft version of the CRs are in the draft folder as well. Please have a look and provide feedback.

1. Procedure text in the UE Context Setup procedure and the UE Context Modification procedure to clarify that the gNB-CU receives the C-RNTI when the request concerns reconfiguration with sync.
2. Procedure text in the Access Success procedure to clarify that upon reception of the Access Success message, the gNB-CU considers that the corresponding UE Context is active and the C-RNTI is used.
3. Semantics description that the C-RNTI IE is included if the gNB-DU regards the request as a reconfiguration with sync.

**Question: Companies kindly provide your comments below if any.**

|  |  |
| --- | --- |
| **Company** | **Comment** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 4 Conclusion, Recommendations

# 5 References

[1] 3GPP TS 38.331v17.5.0

[2] 3GPP TS 33.501v17.7.0

[3] 3GPP TS 38.473v16.6.0

[4] 3GPP TS 38.473v17.7.0

[5] 3GPP TS 38.473v18.0.0