3GPP TSG-RAN WG2 #101bis R2-1805353

Sanya, P.R. of China, 16th – 20th April 2018

Agenda Item: 10.4.1.3.2

Source: Ericsson

Title: Summary of [101#37][NR] RRC procedures/messages (Ericsson)

Document for: Discussion

# Introduction

In previous RAN2 meetings before RAN2#101, two main open issues were identified for NR RRC:

* RRC messages and procedures, RRC harmonization, etc.
* NR security framework for RRC\_INACTIVE.

In RAN2#101 in Athens, RAN2 has made enough progress to enable an initial discussion of an draft on connection control. Concerning RRC messages and procedures, the following was agreed for NR connection establishment:

Agreements

1: RRC Connection Request/Setup procedure is not merged to other RRC procedures

The agreement was extended later in the same meeting to other RRC messages and procedures as follows:

Agreements

1 Message and procedure structure will follow the LTE baseline (apart from resume / re-establishment which is being discussed offline). This is not meant to override any previous agreements that have been made

Finally, out of the offline discussion on re-establishment, the following was agreed:

=> Content of the messages will be progressed based on the assumption of separate messages and procedures

=> Resuming the DRBs in re-establishment can be considered further

Concerning the security framework for UEs in RRC\_INACTIVE, the following was agreed:

Agreements

1 Msg3 is protected and verification is performed by the last serving gNB before UE context is transferred to another network node.

FFS Whether it may also be possible that the target gNB can verify the Msg3 in some cases.

=> Include in previous offline whether Msg 3 is protected with old key or new.

2 Msg3 includes a MAC-I in the RRC message as in LTE

FFS Inputs used for MAC-I calculation in order to possibly address the replay attack concern from SA3.

And, for MSG.4 and MSG.3 security, the following was taken as an working assumption (pending SA3 confirmation):

Working assumption:

1 NCC provided when the connection is suspended

2: New key is derived based on the NCC received in the suspend message and used for the calculation of MAC-I in MSG3.

Based on these agreements/working assumptions and agreements from previous meeting, it has been agreed to have the following email discussion:

**[101#37][NR] RRC procedures/messages (Ericsson)**

      Start to draft RRC spec text based on agreements that have been made. Identify FFS points that still need to be resolved.

      Intended outcome: Report to next meeting including identified FFS points and TP.

~~Deadline:  Thursday 2018-03-29~~

      Deadline:  Thursday 2018-04-10

The purpose of this contribution is reporting some of the main assumptions taken by the rapporteur that were commented via email and/or that could benefit from online clarifications/discussions/confirmation without the need of contributions. Very minor issues e.g. editorial ones are not reported here and can be found in the actual CR with comments. The CR on connection control, based on the outcome of the discussion is provided in [1].

Another companion contribution contains the current status of agreements related to connection control. In particular, it describes the open issues before RAN2#101 and how they were addressed in RAN2#101 [2].

Yet another companion contribution contains the FFSs identified by rapporteur and participating companies [3]. In our view, some of these are better addressed in a follow up discussion and/or via contributions.

# Discussion

We have decided to limit the amount of topics to report in the summary and/or discuss online for the sake of progress and efficiency. For example, we have not reported editorial corrections, or issues raised that were later clarified.

As highlighted in the introduction, the draft CR has initially assumed LTE baseline for messages and procedures. One different to be highlighted is perhaps that in LTE we use the term “Connection” for some of these messages, while in NR we have followed the same approach defined for RRCReconfiguration (which is called RRCConnectionReconfiguration in LTE) and have not used these names. The message names proposed by rapporteur and further updated based on inut from other companies were the following:

* *RRCSetupRequest, RRCSetup, RRCSetupComplete;*
* *RRCResumeRequest, RRCResume, RRCResumeComplete;*
* *RRCReestablishmetnRequest, RRCReestablishment, RRCReestablishmentComplete;*
* *SecurityModeCommand, SecurityModeFailure, SecurityModeComplete;*
* *RRCReestablishmentReject;*
* *RRCReject;*
* *RRCRelease* (for connected to idle transition);
* *RRCSuspend* or *RRCSuspend* (for connected to idle transition).

A first open issue that is worth discussing is the **message for the RRC\_CONNECTED to RRC\_INACTIVE transition**. In RAN2#101 in Athens, Ericsson has initially proposed to harmonize Suspend and Release procedures (using Release message) in [R2-1802366](file:///C%3A%5CData%5C3GPP%5CExtracts%5CR2-1802366%20-%20Harmonizing%20of%20the%20RRC%20procedures.docx) [4] which was not agreed. Adding to that the fact we do not really have an obvious LTE baseline for this case (in LTE we have no RRC\_INACTIVE, hence no transition to it), we have assumed separated RRC messages and procedures as that looked cleaner. As rapporteur, that seemed the cleanest implementation (e.g. compared to harmonizing with Release) as a large part of the configuration is anyway specific to RRC\_INATIVE UEs and target state is different from RRC\_IDLE. Also, the amount of common idle and inactive parameters is limited, while one can always define in the future new parameters only applicable for RRC\_IDLE. On the other hand, as some companies seemed to prefer the harmonization of Suspend/Release, it seemed appropriated to keep both options in the CR for the time being. One company also commented that *RRCReconfiguration* could also be considered as a target harmonization. As that did not seem to have support from other companies, we have not implemented in the CR although we suggest to include as part of the online discussion.

Discussion 1 Discuss the following options for RRC\_CONNECTED to RRC\_INACTIVE transition:

* **Option 1/ No harmonization (e.g. RRC Suspend message);**
* **Option 2/ Based on harmonization**
	+ - * **2a/ Release with Suspend configuration;**
			* **2b/ RRC Re-configuration;**

Another open issue that is worth reporting is the **current assumptions in the CR related to RRC Re-establishment**. As shown above, the RAN2#101 in Athens points to an initial assumption based on separated messages and procedures, compared to Resume. However, it seemed quite clear from discussions that a significant number of companies prefer to have some common aspects with the resume procedure e.g. resume of DRBs, usage of same identifiers, etc. To avoid controversial discussions, rapporteur has initially not captured anything. Some companies have expressed support for that approach, but one company preferred to capture LTE baseline as a starting point for the re-establishment discussion, for the sake of progress.From rapproteurs perspective that seemed acceptable as baseline, so that it becames clear what new aspects in addition to LTE are clearly being proposed for NR.

Discussion 2 Confirm that we can discuss re-establishment aspects (e.g. identifiers, bearer reumption, etc.) via contributions (no need to capture anything in chairman’s notes).

Another issue that is worth discussing is **whether we need to define an acronym for I-RNTI or add in definition section.** According to 38.300, I-RNTI is defined as follow: *unique identification used to identify the UE context for RRC\_INACTIVE*.

Discussion 3 Discuss the following options for I-RNTI definition in RRC:

* **Option 1/ Add in the acronym list that I-RNTI is “inactive state RNTI”;**
* **Option 2/ Add in the definitions (aligned with 38.300);**
* **Option3/ Do both 1/ and 2.**

Another issue that is worth reporting is that some companies were not satisfied with the state transition figure with a direct arrow between RRC\_INACTIVE to RRC\_IDLE. As reported by another group of companies, that transition is actually supported as can UE sends an RRC Resume Request and receive a message moving the UE to RRC\_IDLE as response. As multiple companies commented that, it seemed relevant to be clarified.

Discussion 4 Confirm that we keep the figure with the direct transition from RRC\_INACTIVE to RRC\_IDLE (supported via the RNA update in two steps, where UE actually does not enter RRC\_CONNECTED). No need for a NOTE specifically addressing that aspect or FFS opening up a paging based transition (agreed not to be supported).

Another issue that is worth reporting and discussing is how to capture the fact we have RRC\_INACTIVE in LTE and whether that impacts the IRAT aspects of the state transition figure. There were three possible outcomes identified: i) adding NR, LTE connected to 5GC and LTE/5GC (with RRC\_INACTIVE), ii) adding NR and LTE with RRC\_INACTIVE (without describing the CN) or iii) adding NR and LTE (without RRC\_INACTIVE, as not relevant for transitions in Rel-15).

Discussion 5 Discuss how we capture the inter-RAT transitions (no suport for IRAT inactive mobility, as previously agreed):

* **Option 1/ NR, LTE connected to 5GC and LTE/5GC (with RRC\_INACTIVE);**
* **Option 2/ NR and LTE with RRC\_INACTIVE (without describing the CN)**
* **Option 3/ NR and LTE (without LTE RRC\_INACTIVE, as it is not relevant for transitions in Rel-15).**

Another issue worth reporting is about whether early measurement configuration prior to security configuration is needed in NR. In the rapproteur’s understanding, in LTE that was supported in Rel-8 to speed up the availability of measurements during IDLE to CONNECTED transitions. However, in NR, we have not discussed any agreement to optimize that transition, parituxarly because RRC\_INACTIVE to RRC\_CONNECTED transition is the main procedure to optimize in terms of latency. In that sense, as *measConfig* in RRC\_INACTIVE to RRC\_CONNECTED has security activated (transmitted in *RRCResume*), that IDLE to CONNECTED optimization for early measurements was not very straighforward to be assumed without a discussion.

Discussion 6 Discuss whether we need to optimize the IDLE to CONNECTED transition for early measurement configuration (before security) or whether we focus on RRC\_INACTIVE to RRC\_CONNECTED transition.

Another issue worth clarifying relates to the procedure in LTE upon sending the RRC Connection Setup Request message and including an establishmentCause in accordance to the information received from upper layers. It was commented that there was not formal agreement that the NAS provides cause value, but that the mapping is specified in the NAS specification. The rapporteur has not understood the issue and suggest to clarify that online.

Discussion 7 Confirm that NAS provide establishment cause for RRC Setup Request (MSG.3 in connection establishment).

Another issue worth clarifying relates to the name of the field currently used to provide cell reselection priorities to IDLE or INACTIVE UEs. In LTE the name *idleModeMobilityControlInfo* is used, while it has been proposed to use *idleModePriorities* or different field names for INACTIVE and IDLE (although same IE could be used).

Discussion 8 Discuss which name to use for the field providing cell reselection priorities:

* **Option 1/ *idleModeMobilityControlInfo* for idle, *inactiveModeMobilityControlInfo* for inactive (common IE);**
* **Option 2/ *idleModeMobilityControlInfo* for both inactive and idle UEs;**
* **Option 3/ *idleModePriorities* for both inactive and idle UEs;**

Another issue worth discussing is whether we address state mismatch upon transit from RRC\_CONNECTED to RRC\_INACTIVE/RRC\_IDLE as in LTE (i.e. by defining a data inactivity timer) or by another kind of solution. Initally, rapporteur has assumed that the agreement on one-step Release / Suspend would have as direct consequence the definition of that timer. However, it seems there no common understanding yet about that.

Discussion 9 Discuss the following options related to state mismatch in connected to idle/transitions:

* **Option1/ assume LTE solution for state mismatch during Connected to Idle/Inactive transition (i.e. based on Data Inactivty Timer and NAS recovery);**
* **Option 2/ RAN2 will start discussing new solutions in the next meeting for that problem;**
* **Option 3/ RAN2 will not address that potental issue in Rel-15**

Another issue worth discussing is whether we can have a single description of the UE actions upon reception of *RRCSetup* message for the connection establishment and fallback resume, or whether it is cleaner to define the reception in separated sections and, within the Resume procedure, call the procedure in connection establishment.

Discussion 10 Discuss whether we agree on defininig a single procedure for the reception of RRCSetup message or an additional procedure in Resume (simply calling the procedure in establishment) in the RRC specifications.

Another issue worth discussing is how to handle L1/L2 default configurations for MSG.3 (*RRCResumeRequest* and *RRCSetupRequest*). In LTE, default configurations are defined in setion 9 which are called upon iniitating MSG.3 transmission.

Discussion 11 Discuss whether we agree on the principle of defining L1/L2 default configurations for MSG.3 (e.g. *RRCResumeRequest*, *RRCSetupRequest, etc.*).

Another issue worth discussing is whether in Reject we apply the same LTE principle of upon the reception of RRC Reject the UE shall reset MAC and release the MAC configuration. Then, in RRC resume and establishment is says that MAC default configuration applies. In our view, if we do not add that MAC configuration is release and MAC reset, we could end up complicating the description in resume procedure.

Discussion 12 Discuss whether we keep LTE assumption on resetting MAC and release the MAC configuration upon reception of the *RRCReject* message.

Another issue worth discussing is whether we could assume that the FFS we have on the input parameters are mainly related to new parameters in addition to what we already have in LTE (for replay attacks), as rapporteur has assumed.

Discussion 13 Discuss whether we agree that the input parameters for resumeMAC-I will be at least the same as in LTE. FFS possibly new one(s) for replay attack­.

Another issue worth discussing is whether we can assume that SDAP can be suspended and resumed.

Discussion 14 Discuss whether we agree that SDAP configuration can be suspended/resumed.

Another issue worth discussing related to the security framework is whether NCC is resumed.

Discussion 15 Discuss whether we agree that SDAP configuration can be suspended/resumed.

As also highlighted in the introduction, the draft CR has captured security related agreements. In addition, the agreed working assumption has also been captured as that seemed beneficial for progressing (which is the whole point of having a working assumption). A clear FFS was added to capture the fact this requires further confirmation or even revision based on further RAN2 dsicussions and/or SA3 input. Still related to inactive security framework, there has been one comment questioning whether the agreements/working assumption on key refresh upon resume was limited to MSG.3 security or was valid for the whole Resume procedure. The approach taken by the rapporteur (i.e. assuming that it applies for both MSG.3 and MSG.4) is based on the assumption from the offline discussion#33 [5]. Therein, the title of the first section in RAN2#101 in Athens says “Security framework options for MSG.4” and the basic understanding was that i) there is always key refresh in resume procedure (i.e. new keys used in MSG.4) and ii) MSG.4 is always encrypted and IP protected.

# Conclusion

In section 2 we made the following observations:

Discussion 1 Discuss the following options for RRC\_CONNECTED to RRC\_INACTIVE transition:

* **Option 1/ No harmonization (e.g. RRC Suspend message);**
* **Option 2/ Based on harmonization**
	+ - * **2a/ Release with Suspend configuration;**
			* **2b/ RRC Re-configuration;**

Discussion 2 Confirm that we can discuss re-establishment aspects (e.g. identifiers, bearer reumption, etc.) via contributions (no need to capture anything in chairman’s notes).

Discussion 3 Discuss the following options for I-RNTI definition in RRC:

* **Option 1/ Add in the acronym list that I-RNTI is “inactive state RNTI”;**
* **Option 2/ Add in the definitions (aligned with 38.300);**
* **Option3/ Do both 1/ and 2/;**

Discussion 4 Confirm that we keep the figure with the direct transition from RRC\_INACTIVE to RRC\_IDLE (supported via the RNA update in two steps, where UE actually does not enter RRC\_CONNECTED). No need for a NOTE specifically addressing that aspect or FFS opening up a paging based transition (agreed not to be supported).

Discussion 5 Discuss how we capture the inter-RAT transitions (no suport for IRAT inactive mobility, as previously agreed):

* **Option 1/ NR, LTE connected to 5GC and LTE/5GC (with RRC\_INACTIVE);**
* **Option 2/ NR and LTE with RRC\_INACTIVE (without describing the CN)**
* **Option 3/ NR and LTE (without LTE RRC\_INACTIVE, as it is not relevant for transitions in Rel-15).**

Discussion 6 Discuss whether we need to optimize the IDLE to CONNECTED transition for early measurement configuration (before security) or whether we focus on RRC\_INACTIVE to RRC\_CONNECTED transition.

Discussion 7 Confirm that NAS provide establishment cause for RRC Setup Request (MSG.3 in connection establishment).

Discussion 8 Discuss which name to use for the field providing cell reselection priorities:

* **Option 1/ *idleModeMobilityControlInfo* for idle, *inactiveModeMobilityControlInfo* for inactive (common IE);**
* **Option 2/ *idleModeMobilityControlInfo* for both inactive and idle UEs;**
* **Option 3/ *idleModePriorities* for both inactive and idle UEs;**

Discussion 9 Discuss the following options related to state mismatch in connected to idle/transitions:

* **Option1/ assume LTE solution for state mismatch during Connected to Idle/Inactive transition (i.e. based on Data Inactivty Timer and NAS recovery);**
* **Option 2/ RAN2 will start discussing new solutions in the next meeting for that problem;**
* **Option 3/ RAN2 will not address that potental issue in Rel-15**

Discussion 10 Discuss whether we agree on defininig a single procedure for the reception of RRCSetup message or an additional procedure in Resume (simply calling the procedure in establishment) in the RRC specifications.

Discussion 11 Discuss whether we agree on the principle of defining L1/L2 default configurations for MSG.3 (e.g. *RRCResumeRequest*, *RRCSetupRequest, etc.*).

Discussion 12 Discuss whether we keep LTE assumption on resetting MAC and release the MAC configuration upon reception of the *RRCReject* message.

Discussion 13 Discuss whether we agree that the input parameters for resumeMAC-I will be at least the same as in LTE. FFS possibly new one(s) for replay attack­.

Discussion 14 Discuss whether we agree that SDAP configuration can be suspended/resumed.

Discussion 15 Discuss whether we agree that SDAP configuration can be suspended/resumed.

# References

1. R2-1805355, CR on RRC Connection Control, Ericsson, 3GPP TSG RAN WG2 #101bis, Sanya, P.R. of China, 16th – 20th April 2018
2. [R2-1805352](file:///C%3A%5CData%5C3GPP%5CExtracts%5CR2-1805352%20-%20Summary%20of%20agreements%20on%20connection%20control.docx), Summary of agreements on connection control, Ericsson, 3GPP TSG RAN WG2 #101bis, Sanya, P.R. of China, 16th – 20th April 2018
3. R2-1805354, Remaining open issues on RRC Connection Control, Ericsson, 3GPP TSG RAN WG2 #101bis, Sanya, P.R. of China, 16th – 20th April 2018
4. R2-1802366, Harmonizing RRC Connection control messages and procedures, Ericsson, 3GPP TSG RAN WG2 #101, Athens, Greece, February 2018
5. R2-1804014, Offline discussion#33, Intel, 3GPP TSG RAN WG2 #101, Athens, Greece, February 2018