**3GPP TSG-RAN WG2 Meeting #109e *R2-2002xxxx***

**Elbonia, 24 February – 6 March 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **38.300** | **CR** | **0188** | **rev** | **1** | **Current version:** | **15.8.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network | **x** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Security and RRC Resume Request |
|  |  |
| ***Source to WG:*** | Nokia (Rapporteur) |
| ***Source to TSG:*** | R2 |
|  |  |
| ***Work item code:*** | NR\_newRAT-Core |  | ***Date:*** | 2020-03 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-15 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Security requirements for an RRC Resume Request in INACTIVE are not accurate in two instances:1. SRB0 is mentioned as a possibility to reject an RRC Resume Request while Stage 3 (3GPP TS 38.331) specifies that SRB0 is always used for the RRCReject message.
2. Specifying that SRB1 shall be used “with at least integrity protection” hints the possiblity of not using ciphering even when previously configured. This contradicts Stage 3 (3GPP TS 38.331 & 38.323).
 |
|  |  |
| ***Summary of change:*** | The following corrections are made:1. It is clarified that SRB0 is always used when the gNB decides to reject the request right away.
2. The confusing statement is replaced by “with at least integrity protection and ciphering as previously configured for that SRB”

**Impact analysis**Impacted functionality: RRC\_INACTIVE.Inter-operability:1. If the network is implemented according to the CR and the UE is not, no interoperability issues are foreseen.
2. If the UE is implemented according to the CR and the network is not, no interoperability issues are foreseen.
 |
|  |  |
| ***Consequences if not approved:*** | Confusing statements in Stage 2 leading to possible misunderstanding of how security is ensured in RRC\_INACTIVE. |
|  |  |
| ***Clauses affected:*** | 9.2.2.4.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  |  |
| ***affected:*** |  | **x** |  Test specifications |  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

##### 9.2.2.4.1 UE triggered transition from RRC\_INACTIVE to RRC\_CONNECTED

The following figure describes the UE triggered transition from RRC\_INACTIVE to RRC\_CONNECTED in case of UE context retrieval success:



Figure 9.2.2.4.1-1: UE triggered transition from RRC\_INACTIVE to RRC\_CONNECTED
(UE context retrieval success)

1. The UE resumes from RRC\_INACTIVE, providing the I-RNTI, allocated by the last serving gNB.

2. The gNB, if able to resolve the gNB identity contained in the I-RNTI, requests the last serving gNB to provide UE Context data.

3. The last serving gNB provides UE context data.

4/5. The gNB and UE completes the resumption of the RRC connection.

NOTE: User Data can also be sent in step 5 if the grant allows.

6. If loss of DL user data buffered in the last serving gNB shall be prevented, the gNB provides forwarding addresses.

7/8. The gNB performs path switch.

9. The gNB triggers the release of the UE resources at the last serving gNB.

After step 1 above, when the gNB decides to use a single RRC message to reject the Resume Request right away and keep the UE in RRC\_INACTIVE without any reconfiguration (e.g. as described in the two examples below), or when the gNB decides to setup a new RRC connection, SRB0 (without security) is used. Conversely, when the gNB decides to reconfigure the UE (e.g. with a new DRX cycle or RNA) or when the gNB decides to push the UE to RRC\_IDLE, SRB1 (with integrity protection and ciphering as previously configured for that SRB) shall be used.

NOTE: SRB1 can only be used once the UE Context is retrieved i.e. after step 3.

The following figure describes the UE triggered transition from RRC\_INACTIVE to RRC\_CONNECTED in case of UE context retrieval failure:



Figure 9.2.2.4.1-2: UE triggered transition from RRC\_INACTIVE to RRC\_CONNECTED
(UE context retrieval failure)

1. The UE resumes from RRC\_INACTIVE, providing the I-RNTI, allocated by the last serving gNB.

2. The gNB, if able to resolve the gNB identity contained in the I-RNTI, requests the last serving gNB to provide UE Context data.

3. The last serving gNB cannot retrieve or verify the UE context data.

4. The last serving gNB indicates the failure to the gNB.

5. The gNB performs a fallback to establish a new RRC connection by sending *RRCSetup*.

6. A new connection is setup as described in clause 9.2.1.3.1.

The following figure describes the rejection form the network when the UE attempts to resume a connection from RRC\_INACTIVE:



Figure 9.2.2.4.1-3: Reject from the network, UE attempts to resume a connection

1. UE attempts to resume the connection from RRC\_INACTIVE.

2. The gNB is not able to handle the procedure, for instance due to congestion.

3. The gNB sends *RRCReject* (with a wait time) to keep the UE in RRC\_INACTIVE.