**3GPP TSG-RAN WG2 Meeting #113e *R2-2102175***

**Electronic Meeting, January 25th - February 5th, 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **38.331** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **16.3.1** |  |
|  |
| *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:***  | T400 expiry in timer table and protection of RRC messages |
|  |  |
| ***Source to WG:*** | vivo |
| ***Source to TSG:*** | R2 |
|  |  |
| ***Work item code:*** | 5G\_V2X\_NRSL-Core |  | ***Date:*** | 2020-02-01 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-16 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | **Issue 1: T400 expiry in timer table**In the informative table of section 7 for the timer T400, it is stated that when the timer expires, the sidelink reconfiguration failure procedure need to be performed. However, the mentioned procedure is not correct and what should be performed is the NR sidelink RLF related actions as specified in section 5.8.9.3.**Issue 2: Protection of RRC messages**In the Annex B.1 for protection of RRC messages, the security requirement for sending *SidelinkUEInformationNR* and *ULInformationTransferIRAT* messages are missing, which are defined according to the outcome of Offline-702 at RAN2#113e meeting. Specifically, the UE shall never send the two messages unprotected, and the UE only send the two messages protected after AS security activation. |
|  |  |
| ***Summary of change:*** | **Section 7.1.1*** Clarified that when T400 expires, the UE should perform the sidelink RLF procedure as specified in 5.8.9.3.

**Annex B.1*** Added the security requirement for sending *SidelinkUEInformationNR* and *ULInformationTranferIRAT* messages in the list.

**Impact Analysis**Impacted 5G architecture options: Sidelink Impacted functionality:Sidelink RRC reconfiguration procedure and protection of RRC messagesInter-operability:1. If the network is implemented according to the CR and the UE is not, there is no inter-operability issue,
2. If the UE is implemented according to the CR and the network is not, there is no inter-operability issue.
3. If one UE is implemented according to the CR and another UE is not, there is no inter-operability issue.
 |
|  |  |
| ***Consequences if not approved:*** | 1. When T400 expires, the UE may trigger a wrong procedure.
2. Not clear on the security requirement for sending *SidelinkUEInformationNR* and *ULInformationTranferIRAT* messages.
 |
|  |  |
| ***Clauses affected:*** | 7.1.1, Annex B.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*START OF CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 7.1 Timers

### 7.1.1 Timers (Informative)

*[unrelated Timers skipped.]*

| Timer | Start | Stop | At expiry |
| --- | --- | --- | --- |
| T400 | Upon transmission of RRCReconfigurationSidelink | Upon reception of RRCReconfigurationFailureSidelink or RRCReconfigurationCompleteSidelink | Perform the Sidelink radio link failure related actions as specified in 5.8.9.3. |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*START OF NEXT CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# B.1 Protection of RRC messages

The following list provides information which messages can be sent (unprotected) prior to AS security activation and which messages can be sent unprotected after AS security activation. Those messages indicated "-" in "P" column should never be sent unprotected by gNB or UE. Further requirements are defined in the procedural text.

P…Messages that can be sent (unprotected) prior to AS security activation

A – I…Messages that can be sent without integrity protection after AS security activation

A – C…Messages that can be sent unciphered after AS security activation

NA… Message can never be sent after AS security activation

| Message | P | A-I | A-C | Comment |
| --- | --- | --- | --- | --- |
| *CounterCheck* | - | - | - |  |
| *CounterCheckResponse* | - | - | - |  |
| *DedicatedSIBRequest* | + | - | - |  |
| *DLDedicatedMessageSegment* | NOTE 1 |
| *DLInformationTransfer* | + | - | - |  |
| *DLInformationTransferMRDC* | - | - | - |  |
| *FailureInformation* | - | - | - |  |
| *LocationMeasurementIndication* | - | - | - |  |
| *MCGFailureInformation* | - | - | - |  |
| *MIB* | + | + | + |  |
| *MeasurementReport* | - | - | - | Measurement configuration may be sent prior to AS security activation. But: In order to protect privacy of UEs, *MeasurementReport* is only sent from the UE after successful AS security activation. |
| *MobilityFromNRCommand* | - | - | - |  |
| *Paging* | + | + | + |  |
| *RRCReconfiguration* | + | - | - | The message shall not be sent unprotected before AS security activation if it is used to perform handover or to establish SRB2 and DRBs. |
| *RRCReconfigurationComplete* | + | - | - | Unprotected, if sent as response to *RRCReconfiguration* which was sent before AS security activation. |
| *RRCReestablishment* | - | - | + | Integrity protection applied, but no ciphering. |
| *RRCReestablishmentComplete* | - | - | - |  |
| *RRCReestablishmentRequest* | - | - | + | This message is not protected by PDCP operation. However, a *shortMAC-I* is included. |
| *RRCReject* | + | + | + | Justification for A-I and A-C: the message can be sent in SRB0 in RRC\_INACTIVE state, after the AS security is activated. |
| *RRCRelease* | + | - | - | Justification for P: If the RRC connection only for signalling not requiring DRBs or ciphered messages, or the signalling connection has to be released prematurely, this message is sent as unprotected. *RRCRelease* message sent before AS security activation cannot include *deprioritisationReq, suspendConfig, redirectedCarrierInfo, cellReselectionPriorities* information fields. |
| *RRCResume* | - | - | - |  |
| *RRCResumeComplete* | - | - | - |  |
| *RRCResumeRequest* | - | - | + | This message is not protected by PDCP operation. However, a *resumeMAC-I* is included. |
| *RRCResumeRequest1* | - | - | + | This message is not protected by PDCP operation. However, a *resumeMAC-I* is included. |
| *RRCSetup* | + | + | + | Justification for A-I and A-C: the message can be sent in SRB0 in RRC\_INACTIVE or RRC\_CONNECTED states, after the AS security is activated. |
| *RRCSetupComplete* | + | NA | NA |  |
| *RRCSetupRequest* | + | NA | NA |  |
| *RRCSystemInfoRequest* | + | + | + | Justification for A-I and A-C: the message can be sent in SRB0 in RRC\_INACTIVE state, after the AS security is activated. |
| *SIB1* | + | + | + |  |
| *SCGFailureInformation* | - | - | - |  |
| *SCGFailureInformationEUTRA* | - | - | - |  |
| *SecurityModeCommand* | + | NA | NA | Integrity protection applied, but no ciphering (integrity verification done after the message received by RRC). |
| *SecurityModeComplete* | - | - | + | The message is sent after AS security activation. Integrity protection applied, but no ciphering. Ciphering is applied after completing the procedure. |
| *SecurityModeFailure* | + | NA | NA | Neither integrity protection nor ciphering applied. |
| *SidelinkUEInformationNR* | - | - | - |  |
| *SystemInformation* | + | + | + |  |
| *UEAssistanceInformation* | - | - | - |  |
| *UECapabilityEnquiry* | + | - | - | The network should retrieve UE capabilities only after AS security activation. |
| *UECapabilityInformation* | + | - | - |  |
| *ULDedicatedMessageSegment* | + | - | - |  |
| *UEInformationRequest* | - | - | - |  |
| *UEInformationResponse* | - | - | - | In order to protect privacy of UEs, *UEInformationResponse* is only sent from the UE after successful security activation |
| *ULInformationTransfer* | + | - | - |  |
| *ULInformationTransferIRAT* | - | - | - |  |
| *ULInformationTransferMRDC* | - | - | - |  |
| NOTE 1: This message type carries segments of other RRC messages. The protection of an instance of this message is the same as for the message which this message is carrying. |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*END OF CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*