**3GPP TSG-RAN2 Meeting #121 *R2-23xxxxx***

**Athens, Greece, 27th February – 3rd March 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **38.331** | **CR** | 3926 | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  | | | | | | | | |
| *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:*** | Correction to security protection requirement for ULDedicatedMessageSegment | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Google Inc. | | | | | | | | | |
| ***Source to TSG:*** | R2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | RACS-RAN-Core, NR\_QoE-Core | | | | |  | ***Date:*** | | | 2023-02-17 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 can be 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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The *MeasurementReportAppLayer* can only be sent with security protection. The *ULDedicatedMessageSegment* can be used at transfer of segments of *MeasurementReportAppLayer*. The *ULDedicatedMessageSegment* is allowed to be sent without security protection in the current text. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is clarified that the protection of the *ULDedicatedMessageSegment* is the same as for the message which the *ULDedicatedMessageSegment* is carrying. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There is an inconsistent security protection requirement between the *MeasurementReportAppLayer* and *ULDedicatedMessageSegment* including a segment of the *MeasurementReportAppLayer.*  **Impact analysis**  Impacted functionality:  QoE reporting with segmentation  Interoperability:  As described in section 4.2.2, all messages sent over SRB4 are integrity protected and ciphered. The *ULDedicatedMessageSegment* message including a segment of the *MeasurementReportAppLayer* is sent over SRB4. Therefore, the UE and network should perform security protection on the *ULDedicatedMessageSegment* message sent over SRB4 according to section 4.2.2. There is no interoperability issue foreseen. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

# 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* | - | - | - |  |
| *MeasurementReportAppLayer* | - | - | - |  |
| *MBSBroadcastConfiguration* | + | + | + |  |
| *MBSInterestIndication* | - | - | - |  |
| *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, SRB4, multicast MRBs 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* | + | - | - | The message shall not be sent unprotected before AS security activation if *sl-CapabilityInformationSidelink* information field is included in the message. |
| *SystemInformation* | + | + | + |  |
| *UEAssistanceInformation* | - | - | - |  |
| *UECapabilityEnquiry* | + | - | - | The network should retrieve UE capabilities only after AS security activation. |
| *UECapabilityInformation* | + | - | - |  |
|  |  |  |  |  |
| *ULDedicatedMessageSegment* | NOTE 1 | | | |
| *UEInformationRequest* | - | - | - |  |
| *UEInformationResponse* | - | - | - | In order to protect privacy of UEs, *UEInformationResponse* is only sent from the UE after successful security activation |
| *UEPositioningAssistanceInfo* | - | - | - |  |
| *ULInformationTransfer* | + | - | - |  |
| *ULInformationTransferIRAT* | NOTE 2 | | | |
| *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.  NOTE 2: This message type carries others RRC messages. The protection of an instance of this message is the same as for the message which this message is carrying. | | | | |