**3GPP TSG-RAN WG2 Meeting #113e *R2-2102188***

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **36.331** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Protection of sidelinkUEInformation and ULInformationTransferIRAT |
|  |  |
| ***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:*** | In the Annex A.6 for protection of RRC messages, the security requirement for sending *ULInformationTransferIRAT* messages is updated based on the outcome of Offline-702 at RAN2#113e meeting. Specifically, the UE shall never send thismessage unprotected, and the UE only send this message protected after AS security activation. |
|  |  |
| ***Summary of change:*** | **Annex A.6*** Correct the security requirement for sending *SidelinkUEInformation* and *ULInformationTranferIRAT* messages in the list.

**Impact Analysis**Impacted 5G architecture options: Sidelink Impacted functionality: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:*** | The protection for sending *ULInformationTranferIRAT* messages may be wrongly implemented. |
|  |  |
| ***Clauses affected:*** | Annex A.6 |
|  |  |
|  | **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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## A.6 Protection of RRC messages (informative)

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

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

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

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

NA… Message can never be sent after security activation

| Message | P | A-I | A-C | Comment |
| --- | --- | --- | --- | --- |
| CSFBParametersRequestCDMA2000 | **+** | **-** | **-** |  |
| CSFBParametersResponseCDMA2000 | + | - | - |  |
| CounterCheck | - | -  | -  |  |
| CounterCheckResponse | - | -  | -  |  |
| DLDedicatedMessageSegment | NOTE 1 |
| DLInformationTransfer | + | - | - |  |
| FailureInformation | - | - | - |  |
| HandoverFromEUTRAPreparationRequest (CDMA2000) | - | -  | -  |  |
| InDeviceCoexIndication | - | -  | -  |  |
| InterFreqRSTDMeasurementIndication | - | - | - |  |
| LoggedMeasurementsConfiguration | - | - | - |  |
| MasterInformationBlock | + | + | + |  |
| MasterInformationBlock-MBMS | + | + | + |  |
| MBMSCountingRequest | + | + | + |  |
| MBMSCountingResponse | - | - | - |  |
| MBMSInterestIndication | + | - | - |  |
| MBSFNAreaConfiguration | + | + | + |  |
| MeasReportAppLayer | - | - | - |  |
| MeasurementReport | - | - | - | Measurement configuration may be sent prior to security activation. But: In order to protect privacy of UEs, MEASUREMENT REPORT is only sent from the UE after successful security activation. |
| MCGFailureInformation | - | - | - |  |
| MobilityFromEUTRACommand | - | -  | - |  |
| Paging | + | + | + |  |
| ProximityIndication | - | - | - |  |
| PURConfigurationRequest | + | - | - | Except if the UE is using Control plane CIoT EPS/5GS optimisation, the message is only sent from the UE after successful security activation. |
| RNReconfiguration | - | - | - |  |
| RNReconfigurationComplete | - | - | - |  |
| RRCConnectionReconfiguration | + | - | - | The message shall not be sent unprotected before security activation if it is used to perform handover or to establish SRB2, SRB4 and DRBs |
| RRCConnectionReconfigurationComplete | + | - | - | Unprotected, if sent as response to RRCConnectionReconfiguration which was sent before security activation |
| RRCConnectionReestablishment | - | + | + | This message is not protected by PDCP operation. |
| RRCConnectionReestablishmentComplete | - | - | - |  |
| RRCConnectionReestablishmentReject | - | + | + | One reason to send this may be that the security context has been lost, therefore sent as unprotected.  |
| RRCConnectionReestablishmentRequest | - | - | + | This message is not protected by PDCP operation. However, a short MAC-I is included. |
| RRCConnectionReject | + | + | + | Except for resumption of an RRC connection after early security reactivation in accordance with conditions in 5.3.3.18, A-I and A-C are NA. |
| RRCConnectionRelease | + | - | - | 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.For resumption of an RRC connection after early security reactivation in accordance with conditions in 5.3.3.18, the message is only sent after successful security activation.*RRCConnectionRelease* message sent before security activation cannot include *rrc-InactiveConfig, redirectedCarrierInfo, idleModeMobilityControlInfo* information fields when UE is connected to 5GC. |
| RRCConnectionRequest | + | NA | NA |  |
| RRCConnectionResume | - | - | + | When this message is transmitted, security is activated but suspended. Integrity verification is done after the message received by RRC.For resumption of an RRC connection after early security reactivation in accordance with conditions in 5.3.3.18, the message is only sent after successful security activation.For RRC\_INACTIVE state or after early security reactivation, the message is protected with both integrity and ciphering. |
| RRCConnectionResumeRequest | - | - | + | This message is not protected by PDCP operation. However, a short MAC-I is included. |
| RRCConnectionResumeComplete | - | - | - |  |
| RRCConnectionSetup | + | NA | NA |  |
| RRCConnectionSetupComplete | + | NA | NA |  |
| RRCEarlyDataRequest | + | NA | NA |  |
| RRCEarlyDataComplete | + | NA | NA |  |
| SCGFailureInformation | - | - | - |  |
| SCGFailureInformationNR | - | - | - |  |
| SCPTMConfiguration | + | + | + |  |
| SecurityModeCommand | + | NA | NA | Integrity protection applied, but no ciphering (integrity verification done after the message received by RRC) |
| SecurityModeComplete | - | NA | NA | Integrity protection applied, but no ciphering. Ciphering is applied after completing the procedure. |
| SecurityModeFailure | + | NA | NA | Neither integrity protection nor ciphering applied. |
| SidelinkUEInformation | + | - | - |  |
| SystemInformation | + | + | + |  |
| SystemInformationBlockType1 | + | + | + |  |
| SystemInformationBlockType1-MBMS | + | + | + |  |
| UEAssistanceInformation | - | - | - |  |
| UECapabilityEnquiry | + | - | - | Except if the UE is using Control plane CIoT EPS optimisation, E-UTRAN should retrieve UE capabilities only after AS security activation. |
| UECapabilityInformation | + | - | - |  |
| UEInformationRequest | - | - | - |  |
| UEInformationResponse | - | - | - | In order to protect privacy of UEs, UEInformationResponse is only sent from the UE after successful security activation |
| ULDedicatedMessageSegment | + | - | - |  |
| ULHandoverPreparationTransfer (CDMA2000) | - | - | - | This message should follow HandoverFromEUTRAPreparationRequest |
| ULInformationTransfer | + | - | - |  |
| ULInformationTransferIRAT | - | - | - |  |
| ULInformationTransferMRDC | - | - | - |  |
| WLANConnectionStatusReport | - | - | - |  |
| 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*