**n3GPP TSG-RAN WG2 Meeting #121 *R2-230xxxx***

**Athens, Greece, 27 February – 03 March 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **38.300** | **CR** | **0628** | **rev** | **1** | **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 on RRCReject handling | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | R2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NR\_SmallData\_INACTIVE-Core | | | | |  | ***Date:*** | | | 2023-02 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | *RRCReject* can be used by the NW in overload situation to direct the UE back to RRC\_INACTIVE mode after initial *RRCResumeRequest* message by the UE. NW shall not send *RRCReject* after it has scheduled any DL data to the UE but *RRCRelease* shall be used in that case, instead. Otherwise, UE would apply the old security keys upon next access attempt which would create a security threat. With the current specification, an attacker NW could keep the UE in SDT procedure and direct the UE back to RRC\_INACTIVE mode with *RRCReject* successfully completing the SDT procedure even after data transmissions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Requirement for NW is specified that it should not send RRCReject to the UE after it transmitted any DL data.  **Impact analysis**  Impacted functionality: Small Data Transmission.  Inter-operability:   1. If the network is implemented according to the CR and the UE is not, no inter-operability issues. 2. If the UE is implemented according to the CR and the network is not, no inter-operability issues. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Attacker NW could keep a UE in SDT procedure and transmit/receive data from the UE while still be able to succesfully complete the SDT procedure by transmitting *RRCReject* to the UE, ie., without any valid security information. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 18.0 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

*First Modified Subclause*

18 Small Data Transmission

18.0 General

Small Data Transmission (SDT) is a procedure allowing data and/or signalling transmission while remaining in RRC\_INACTIVE state (i.e. without transitioning to RRC\_CONNECTED state). SDT is enabled on a radio bearer basis and is initiated by the UE only if less than a configured amount of UL data awaits transmission across all radio bearers for which SDT is enabled, the DL RSRP is above a configured threshold, and a valid SDT resource is available as specified in clause 5.27.1 of TS 38.321 [6]. Maximum duration the SDT procedure can last is dictated by a SDT failure detection timer that is configured by the network (see clause 6.2.2 of TS 38.331 [12]).

SDT procedure is initiated with either a transmission over RACH (configured via system information) or over Type 1 CG resources (configured via dedicated signalling in *RRCRelease*). The SDT resources can be configured on initial BWP for both RACH and CG. RACH and CG resources for SDT can be configured on either or both of NUL and SUL carriers. The CG resources for SDT are valid only within the PCell of the UE when the *RRCRelease* with suspend indication is received. CG resources are associated with one or multiple SSB(s). For RACH, the network can configure 2-step and/or 4-step RA resources for SDT. When both 2-step and 4-step RA resources for SDT are configured, the UE selects the RA type according to clause 9.2.6. CFRA is not supported for SDT over RACH.

Once initiated, the SDT procedure is either:

- successfully completed after the UE is directed to RRC\_IDLE (via *RRCRelease*) or to continue in RRC\_INACTIVE (via *RRCRelease or RRCReject*) or to RRC\_CONNECTED (via *RRCResume or RRCSetup*); or

- unsuccessfully completed upon cell re-selection, expiry of the SDT failure detection timer, a MAC entity reaching a configured maximum PRACH preamble transmission threshold, an RLC entity reaching a configured maximum retransmission threshold,or expiry of SDT-specific timing alignment timer while SDT procedure is ongoing over CG and the UE has not received a response from the network after the initial PUSCH transmission.

Upon unsuccessful completion of the SDT procedure, the UE transitions to RRC\_IDLE. Network should not send *RRCReject* to complete the SDT procedure if DL data over any radio bearer enabled for SDT is transmitted.

The initial PUSCH transmission during the SDT procedure includes at least the CCCH message. When using CG resources for initial SDT transmission, the UE can perform autonomous retransmission of the initial transmission if the UE does not receive confirmation from the network (dynamic UL grant or DL assignment) before a configured timer expires as specified in clause 5.4.1 of TS 38.321 [6]. After the initial PUSCH transmission, subsequent transmissions are handled differently depending on the type of resource used to initiate the SDT procedure:

- When using CG resources, the network can schedule subsequent UL transmissions using dynamic grants or they can take place on the following CG resource occasions. The DL transmissions are scheduled using dynamic assignments. The UE can initiate subsequent UL transmission only after reception of confirmation (dynamic UL grant or DL assignment) for the initial PUSCH transmission from the network. For subsequent UL transmission, the UE cannot initiate re-transmission over a CG resource.

- When using RACH resources, the network can schedule subsequent UL and DL transmissions using dynamic UL grants and DL assignments, respectively, after the completion of the RA procedure.

While the SDT procedure is ongoing, if data appears in a buffer of any radio bearer not enabled for SDT, the UE initiates a transmission of a non-SDT data arrival indication using *UEAssistanceInformation* message to the network and, if available, includes the resume cause.

SDT procedure over CG resources can only be initiated with valid UL timing alignment. The UL timing alignment is maintained by the UE based on a SDT-specific timing alignment timer configured by the network via dedicated signalling and, for initial CG-SDT transmission, also by DL RSRP of configured number of highest ranked SSBs which are above a configured RSRP threshold. Upon expiry of the SDT-specific timing alignment timer, the CG resources are released while maintaining the CG resource configuration.

Logical channel restrictions configured by the network while in RRC\_CONNECTED state and/or in *RRCRelease* message for radio bearers enabled for SDT, if any, are applied by the UE during SDT procedure.

The network may configure UE to apply ROHC continuity for SDT either when the UE initiates SDT in the PCell of the UE when the *RRCRelease* with suspend indication was received or when the UE initiates SDT in a cell of its RNA.

*End of Changes*