**3GPP TSG-RAN WG2 Meeting #113e R2-2102089**

**eMeeting, 25th Jan – 5th Feb 2021**

**Title:** LS on small data transmissions in NR

**Response to:** -

**Release:** Release 17

**Work Item:** NR\_SmallData\_INACTIVE-Core

**Source:** TSG SA WG3

**To:**

**Contact Person:**

#### Name: xxx

E-mail Address: xxx

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**1. Overall Description:**

RAN2 has started work on the NR Small Data Enhancements WI (RP-201305). The objectives of this WI include solutions for RACH based small data transmission (RA-SDT) and Configured Grant based small data transmissions (CG-SDT). RAN2 would like to highlight the following agreements reached so far and respectfully request SA3 to provide any feedback from security perspective on these agreements.

|  |
| --- |
| Some relevant agreements:  1  1 For both RACH and CG based solutions, upon initiating RESUME procedure for SDT initiation (i.e. for first SDT transmission), the UE shall re-establish at least the SDT PDCP entities and resume the SDT DRBs that are configured for small data transmission (along with the SRB1)  2 The first UL message (i.e. MSG3 for 4-step RACH, MSGA payload for 2-step RACH and the CG transmission for CG) may contain at least the following contents (depending on the size of the message):  - CCCH message (needs to be included)  LCP can be used to determine to priority of the content below that may be included  - DRB data from one or more DRBs which are configured by the network for small data transmission  3 In case of RRC-based solution, for both RACH and CG based solutions, the CCCH message contains ResumeMAC-I generated using the stored security key for RRC integrity protection – i.e same as Rel-16.  4 For both RACH and CG based solutions, new keys are generated using the stored security context and the NCC value received in the previous RRCRelease message (i.e. same as legacy procedure) and these new keys are used for generating the data of DRBs that are configured for SDT.  5 UL/DL transmission following UL SDT without transitioning to RRC\_CONNECTED is supported  6 RAN2 design assumes that RRCRelease message is sent at the end to terminate the SDT procedure from RRC point of view. |

As noted above, for small data transmissions, the first UL message:

1. includes the CCCH message (which contains the ResumeMAC-I generated using the stored security key for RRC integrity protection – same as Rel-16) and
2. may include DRB data from one or more DRBs which are configured by the network for small data transmission and the UE uses new keys that are generated using the stored security context and the NCC value received in the previous RRC Release (again similar to Rel-16).

In addition to the above, it is also agreed that the SDT procedure will be terminated by an RRCRelease message that is sent at the end of the SDT procedure (i.e. UE moves back to INACTIVE/IDLE state upon receiving this RRCRelease message) and this RRCRelease message in DL is encrypted and integrity protected using the new keys as noted in agreement 4) above (same as Rel-16). This RRCRelease message contains the NCC for the security key derivation for the next Resume procedure.

In between the first UL message and the RRCRelease message subsequent UL/DL data transmissions on DRBs are supported during the SDT phase (i.e. without the UE moving to a connected state and these messages use the new keys that are generated again as noted in agreement 4) above). The UL/DL data will be integrity protected if DRB integrity protection is configured.

RAN2 has not agreed to use any other integrity protected RRC message in DL in response to the first UL message apart from the RRCRelease message that terminates the SDT procedure.

**2. Actions:**

**To TSG SA WG3 group.**

**ACTION:** RAN2 respectfully requests TSG SA WG3 to take the above overall framework for SDT into account and provide any feedback on it from security perspective

**3. Date of Next TSG-RAN WG2 Meetings:**

3GPP RAN2#113b-e 12 Apr – 20 Apr 2021 Electronic Meeting

3GPP RAN2#114-e 19 May – 27 May 2021 Electronic Meeting