**3GPP TSG-RAN WG2 Meeting #116bis Electronic** **Revised\_R2-2201920**

**Elbonia, 17 – 25 January 2022**

**Title: [DRAFT]** LS on Security for Small Data Transmission

**Response to:** -

**Release:** Release 17

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

**Source:** Nokia [TSG RAN WG2]

**To:** TSG SA WG3

**Cc:**

**Contact Person:**

#### Name: Samuli Turtinen

E-mail Address: samuli.turtinen@nokia.com

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

**Attachments:** -

**1. Overall Description:**

RAN2 is working on Small Data Transmission (SDT) feature which allows small data transmissions in INACTIVE state. As part of this work, when UL data needs to be transmitted over radio bearers configured for SDT, SDT procedure may be initiated to transmit/receive data over radio bearers configured for SDT and multiple DL and UL packets can be exchanged during the SDT session. When SDT procedure is initiated, *RRCResumeRequest* is transmitted as part of the first UL transmission by the UE along with the UL SDT data. The UE uses the stored NCC value for generating the security keys when generating this first *RRCResumeRequest* (i.e same as legacy Resume procedure).

SDT procedure is supported with and without anchor relocation. When anchor relocation is performed, the UE context is fetched from the old anchor gNB to target gNB. In this case the PDCP layer is terminated in the target gNB and path switch procedure is performed before the user data is encoded/decoded. When there is no anchor relocation, the old anchor gNB terminates the PDCP layer and path switch procedure is not performed.

While the SDT procedure is ongoing, new UL data may appear into a buffer of a radio bearer not configured for SDT. It is agreed by RAN2 that UE will initiate a procedure to indicate this non-SDT data arrival to the network. One of the solutions for such indication discussed in RAN2 is that the UE terminates the ongoing SDT procedure and triggers a new RRC Resume procedure – in this case, a second *RRCResumeRequest* would be transmitted by the UE to the network.

RAN2 further discussed the solutions for this case allowing to avoid *resumeMAC-I* reuse, as mentioned by SA3 in their previous LS in S3-213034. One option discussed is that the UE uses the key derived when initiating the SDT procedure (as clarified above), to generate *resumeMAC-I* for the second *RRCResumeRequest* transmitted in the second RRC Resume procedure for non-SDT data indication. C-RNTI input to the *resumeMAC-I* calculation is the C-RNTI issued by the anchor gNB (ie, the same approach as in legacy Resume procedure). Afterwards, the UE performs horizontal key derivation to obtain the keys to be used for subsequent messages exchanged with the network. In this solution, the same I-RNTI as used in the first *RRCResumeRequest* would be reused to send the second *RRCResumeRequest*. Thus, in case of path switch, one option that is under consideration is that the old anchor gNB will verify the UE using the key that is used in the target gNB for integrity protection of messages (i.e. KRRCint\_1 in the figure below).

An exemplary call flow for this procedure is presented below to simplify the understanding of how the procedure could look like:



RAN2 would like to ask SA3 if the above is feasible from SA3 point of view?

Furthermore, RAN2 would like to know if SA3 has any preference on the used key(s)/solution applied in the above scenario for second RRC Resume procedure for non-SDT data indication?

**2. Actions:**

**To SA3 group.**

**ACTION:** RAN2 respectfully asks SA3 if the above solution is feasible from SA3 point of view? Furthermore, RAN2 would like to know if SA3 has any preference on the used key(s)/solution applied in the above scenario for second RRC Resume procedure for non-SDT data indication?

 Further, RAN2 respectfully asks SA3 if a fast handling of the LS and related response could be possible? The next RAN2#117-e meeting would be the last meeting for functional agreements in Rel-17 work items, hence, the decision about the solution for the above issue needs to be decided by the RAN2 in the next meeting.

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

3GPP RAN2#117-e from 2022-02-21 to 2022-03-03 Electronic Meeting