**3GPP TSG-RAN WG2 Meeting #116bis Electronic DRAFT R2-220xxxx**

**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:** RAN3

**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 a giving 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 msg (i.e legacy Resume procedure). Network can identify the RRC Resume procedure is for SDT based on the used RACH by the UE which is exclusively used by the UEs initiating SDT procedure.

SDT procedure is supported with and without anchor relocation. When anchor relocation is performed, the UE context is fetched from the old anchor node (based on the RRCResumeRequest forwarded from the target gNB to the old anchor node). In this case the PDCP layer is terminated in the target gNB and path switch procedure is performed before the user data is exchanged over the air interface. 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 switch to a non-SDT procedure after NW receiving the indication of 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 sub-sequent RRC Resume procedure – in this case, a second *RRCResumeRequest* msg would be transmitted by the UE to the network regardless of whether the first *RRCResumeRequest* msg is received by the network or not.

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* msg transmitted in the second RRC Resume procedure for non-SDT data indication. Afterwards, the UE performs horizontal key derivation to obtain the keys to be used for subsequent packets exchanged with the network. when switching from the SDT procedure to second RRC Resume procedure for non-SDT data indication. In this case irrespective of whether there is path switch or not, the UE reuses the stored NCC value again for generating the new horizontally derived key. Furthermore, the UE uses this horizontally derived key for the SDT procedure for *resumeMAC-I* generation for the *RRCResumeRequest* transmitted in the second RRC Resume procedure for non-SDT data indication. In this solution, the same I-RNTI as used in the first *RRCResumeRequest* msg will 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). RAN2 would also like to point out that it is possible that the second RRCResumeRequest may be received prior to the first RRCResumeRequest (e.g. if the first RRCResumeRequest is lost over the air interface, whilst the second one is received).

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



On summary, the following are the key points to consider by SA3 for the CCCH solution:

* (A) Points related to the 2nd *RRCResumeRequest* msg:
	+ The same key in use during the SDT procedure is also re-used for calculation of R*esumeMAC-I.*
	+ C-RNTI input to the *ResumeMAC-I* is the C-RNTI assigned in the old anchor gNB and used in the first *RRCResumeRequest* message even though UE has a new C-RNTI in use during the SDT session with the new serving gNB.
	+ I-RNTI in the *ResumeRequest* message is the I-RNTI assigned by the old anchor gNB and used in the first *RRCResumeRequest* message.
	+ RAN2 assumption is that the *RRCResumeMAC-I* in the 2nd *RRCResumeRequest* msg is processed and verified by the old anchor gNB. This is under discussion with RAN3 [Ref SA3 LS]
* (B) Horizontally derived key used is used as key for the subsequent packets after the UE gets RRC\_CONNECTED in the target gNB following the second *RRCResumeRequest* message. The old anchor gNB will transmit the horizontally derived key to the serving gNB.

RAN2 would like to ask SA3 if the above is feasible from SA3 point of view to be implemented in Rel-17 SA3 specs (if any updates are needed) and to answer the following questions.

Q1: Is the autonomous horizontal key derivation at the UE as noted above acceptable to SA3?

Q2: Can the same key used for integrity protection of messages during the SDT procedure in target gNB also be used for verification of the second RRCResumeRequest in the old anchor gNB?

Q3: 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 to be implemented in Rel-17 SA3 specs (if any updates are needed) and to answer the following questions?

Q1: Is the autonomous horizontal key derivation at the UE as noted above acceptable to SA3?

Q2: Can the same key used for integrity protection of messages during the SDT procedure in target gNB also be used for verification of the second RRCResumeRequest in the old anchor gNB?

Q3: 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?

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

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