**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:**

**Contact Person:**

#### Name: Samuli Turtinen

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

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](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. When SDT procedure is initiated, *RRCResumeRequest* is transmitted as part of the first UL transmission by the UE along with the UL small data. The UE uses the stored NCC value for generating the security keys when generating this RRCResumeRequest (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). 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 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 *RRCResumeRequest* 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 messages 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 pathswitch 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 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 horizontally derived key and will transmit the same horizontally derived key to the target gNB to be used for the ongoing SDT session in the target gNB (e.g. for integrity protection of the DL RRCResume/RRCRelease message in the target gNB).

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 to be implemented in Rel-17 SA3 specs 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 horizontally derived key be used for verification of the second RRCResumeRequest in the old anchor gNB and also for integrity protection of DL RRCRelease/RRCResume message in the target 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 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 horizontally derived key be used for verification of the second RRCResumeRequest in the old anchor gNB and also for integrity protection of DL RRCRelease/RRCResume message in the target 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