**3GPP** **TSG SA WG3 Meeting 103-e S3-212257**

**Electronic meeting, 17-28 May 2021**

**Title: Reply LS on Small data transmission**

**Response to: LS S3-211426 (R2-2104401) on** **Small data transmissions**

**Release: Rel-17**

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

**Source: SA3**

**To:** **RAN2**

**Cc: SA2**

**Contact person: Alec Brusilovsky**

**Alec.Brusilovsky@interdigital.com**

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

**Attachments:** none

# 1 Overall description

SA3 would like to thank RAN2 for their LS on Small data transmission.

RAN2 asked following two questions.Q1: Can a CCCH message reusing the I-RNTI and resumeMAC-I be transmitted again in the same cell after SDT initiation, e.g. similar to legacy RRC Reject case (but without having received RRC Reject at the UE)?.

Q2: Can NCC and I-RNTI from a former cell in which an SDT procedure was initiated be reused to initiate a new SDT procedure in a new cell?.

For both cases (same cell, and different cell), SA3 would like to give following feedback.

SA3 requires that keystreams are never reused.

1. Therefore, network shall ensure separate bearer Ids for SDT and non-SDT bearers.
2. The network shall also ensure that PDCP counts are not reused for same bearer Id, KgNB pair.

SA3 asks RAN2 to confirm that the above requirements are met. The above requirements are strict and cannot be overruled.

Further, SA3 thinks it is worth doing risk assessment on availability aspect. An attacker may cause abrupt SDT session termination by capturing SDT-related RRCResumeRequest and replaying it as non-SDT-related RRCResumeRequest. There could be various ways to mitigate this attack as below. SA3 is not recommending any of them, but just listing them for sake of discussion.

1. Transfer either one of (SDT-related or non-SDT-related) RRCResumeRequest as a PDCP protected RRC message.
2. Update the calculation of resumeMAC-I to include the RRCResumeRequest message, provided that two RRCResumeRequest are distinguishable, thus providing some form of integrity protection.

SA3 asks RAN2 to discuss any potential solution and make an assessment if the complexity of such solution will commensurate with the risk. If risk is considered too low, then a note has to be recorded that 3GPP made a conscious decision for availability to accept the low risk and not provide any solution.

Further questions to RAN2: (a) Is RAN2 thinking of allowing “two and only two” RRCResumeRequests or will there be more? (b) Will there be separate “cause” values in RRCResumeRequest for SDT and non-SDT?

# 2 Actions

**To RAN2, SA2**

**ACTION:** 3GPP TSG SA WG3 would like RAN2 and SA2 to take the above feedback into account.

# 3 Dates of next TSG CT WG1 meetings

TSG SA WG3 Meeting 103-Bis-e (TBC) 05-09 July 2021

TSG SA WG3 Meeting 104-e (TBC) 16-27 August 2021