**3GPP** **TSG SA WG3 Meeting 103-e S3-212257r7**

**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 the following 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?.

SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.

During the SA3#103-e discussion SA3 could not agree on whether these issues represent “corner” or “normal” cases. SA3 failed to agree on answers to RAN2 questions.

However, for both cases (same cell and different cell), SA3 would like to provide the following feedback.

SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.

verify

# 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