**3GPP** **TSG SA WG3 Meeting 104-e S3-212428r3**

**Electronic meeting, 16-27 August 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**

**Attachments:** none

# 1 Overall description

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

SA3 discussed the incoming LS from RAN2 and would like to provide the following answers to RAN2 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)?

**SA3 answer:**

**(TBD)** There could be a scenario when an attacker may cause termination of legitimate SDT session by capturing a first SDT RRCResumeRequest and replaying it as a second non-SDT RRCResumeRequest. But the situation is same as the legacy RRC Reject case. If RAN2 does not worry about the legacy RRC Reject case, it is OK to reuse the NCC in the same cell after SDT initiation. If not, then the I-RNTI and resumeMAC-I should not be reused and legacy RRC Reject case should be enhanced.

**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 answer:**

For intra-gNB scenario, the answer is yes.

For inter-gNB scenario, it is not recommended to reuse the NCC and I-RNTI as SA3 has requirements not reusing the key. In this case, the horizontal key derivation is recommended. Horizontal key derivation can also be applied in the intra-gNB case.

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.

For both questions (same cell and different cell), 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.

# 2 Actions

**To RAN2, SA2**

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

# 3 Dates of next TSG SA3 WG3 meetings

TSG SA WG3 meeting schedule is available at the following 3GPP link:

<https://portal.3gpp.org/Home.aspx?tbid=386&SubTB=386#/>