**3GPP** **TSG SA WG3 Meeting 106-e draft\_S3-220152-r6**

**Electronic meeting, 14-25 February 2022**

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

**Response to: LS S3-210051(R2-2201983) LS on Security for Small Data Transmission**

**Release: Rel-17**

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

**Source: SA3**

**To:** **RAN2**

**Cc: RAN3**

**Contact person: Abhijeet Kolekar**

**abhijeet.kolekar@intel.com**

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

**Attachments:** none

# 1 Overall description

SA3 thanks RAN2 for their LS on Small data transmission.

SA3 discussed the LS from RAN2 and would like to provide the following response on the exemplary call flow detailed in the RAN2 LS (S3-220051/R2-2201983):

1. Two nodes (gNBs) using a key (KRRCint\_1) to verify RRC messages (at step 12 & 13 in serving gNB and at step 18 in last serving gNB) is not acceptable from security point of view. RAN2 need to update the solution to prohibit use of same key at different entities.
2. It is not preferable (but not forbidden) for reusing the same I-RNTI according to the existing SA3 requirements for RRCResume privacy, i.e. “On transition of UE to RRC INACTIVE state requested by gNB during RRC Resume procedure or RNAU procedure, the gNB shall assign a new I-RNTI to the UE.”.
3. The key derivation between gNBs shall meet 2-hop forward security principle, i.e. the 1st node (gNB) shall not predict the 3rd node (gNB)’s key, which is similar with handover, after two handovers, the 1st gNB cannot predict the 3rd gNB since a new {NH, NCC} is received from the AMF. RAN2 need to update the solution to meet this security requirement.
4. There is SA3 work needed to develop a security solution and specify it, if RAN2 agrees for the solution similar to the one mentioned in the RAN2 LS (S3-220051/R2-2201983).

The exemplary call flow detailed in the RAN2 LS (S3-220051/R2-2201983) requires further study from security point of view, as mentioned above, to be feasible.

# 2 Actions

**To RAN2**

**ACTION:** 3GPP TSG SA WG3 asks RAN2 to take the above feedback into account and reply to SA3.

# 3 Dates of next TSG SA WG3 meetings

TSG SA WG3 Meeting 106-Bis-e 04-08 April 2022

TSG SA WG3 Meeting 107-e 27 June-01 July 2022