3GPP TSG SA WG3 Meeting SA3#103-e S3-211706-r3

Electronic meeting, 17 – 28 May 2021

**Title: Draft LS on security protection on RRCResumeRequest message**

**Release: Release 17**

**Work Item: FS\_5GFBS**

**Source: SA3**

**To: RAN2**

**Cc: NULL**

**Contact person: Ivy Guo**

 **Ivy\_guo@apple.com**

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

**Attachments:** **None**

# 1 Overall description

SA3 is studying the R17 5GFBS (Study on 5G Security Enhancement against False Base Station), which includes key issues on protection of unicast messages, i.e. RRCResumeRequest messages.

There is one solution#17 proposing to protection RRCResumeRequest message. In this solution, when the UE initiates the RRC Resume procedure, the UE should use the whole RRCResumeRequest message, except the ResumeMAC-I/shortResumeMAC-I, as an additional input parameter to the VarResumeMac-Input part in order to calculate ResumeMAC-I/shortResumeMAC-I. The UE should send the calculated ResumeMAC-I/shortResumeMAC-I in the RRCResumeRequest message. The UE and the network negotiate/learn each other's capability/support of using the newer version of ResumeMAC-I/shortResumeMAC-I as below:

- UE's capability is part of an RRC message (i.e., AS SMComplete).

- gNB/ng-eNB's capability is part of a SI message (i.e., SIB1, refer to a closely related feature called useFullResumeID in SIB1).

Solution under consideration, needs to handle the backward incompatibility issue if the target gNBs (Rel-15/Rel-16) capability is not inline with the UE and the source gNB, the UE and the source gNB will not be aware of the capability of the target gNB. Therefore, the ResumeMAC-I/ShortResumeMAC-I verification may fail, as the Rel-15/Rel-16 target gNB will send limited parameters instead of entire RRCResumeRequest message to the source gNB, which will not be sufficient for the source gNB to calculate the ResumeMAC-I/shortResumeMAC-I for verification.

**SA3 would like to ask RAN2 the following questions:**

1. For the capability negotiation method between UE and gNB/ng-eNB as mentioned above, if there are other preferable alternatives from RAN2 perspective?
2. Is there any mechanism for the source gNB/ng-eNB to know the target gNB/ng-eNB capabilities?
3. The possibility of specifying the solution in RAN2 specification in Rel-17 timeframe, if the solution is concluded by SA3.

# 2 Actions

**To RAN2**

**ACTION:** SA3 kindly asks RAN2 to provide answers to the question above.

# 3 Dates of next TSG SA WG 3 meetings

SA3#104-e 16 - 27 August 2021 Electronic meeting