

Title: Group Release security solution
Response to: LS to SA3 (R2-022702)on Group release security solution

Release: Rel-5
Work Item:

Source: SA3
To: RAN2
Cc:

Contact Person:
Name: Brad Owen
Tel. Number: +44 1793 73 6245
E-mail Address: bvowen@lucent.com

Attachments: None

1. Overall Description:

SA3 thanks RAN2 for their LS on possible Group release security solution in S3-020565 (R2-022702).

1. If group release functionality is introduced in RRC signalling is a security mechanism needed or not?

In the light of RAN2's concerns SA3 have re-assessed the need for a security mechanism for the group release mechanism. It was felt that there was a possible case for not providing this mechanism but that more discussion would be required. As such SA3 have under taken to have an email discussion on this subject directly after the meeting.

2. If the answer to question 1 is that it is needed, can SA3 guide RAN2 on possible ways to limit UE implementation impacts, e.g. on the possible reuse without modifications of one of the R'99 security blocks (F8 or F9).

The question of how to implement the security mechanism was also examined. SA3 recommends that the authentication function for the group release message be derived from the ciphering function f8 defined in 35.201. Depending on the outcome of the above email discussion SA3 will make any necessary changes to the security specifications with the change request(s) to be provided to our next meeting in November.

2. Actions:

To RAN2 group.

ACTION: None

3. Date of Next SA3 Meetings:

SA3 # 19th Nov. – 22th Nov. 2002 Oxford, UK