3GPP TSG SA WG3 Security — S3#16 **S3-000708**

28-30 November, 2000

Sophia Antipolis, France

Source: **Nokia**

Title: **GERAN integrity protection**

Document for: **Decision**

Agenda Item:

The problem when adopting the UTRAN integrity algorithms for GERAN radio interface is the size of Message Authentication Code (MAC-I). If all GERAN radio interface signalling messages should be protected with the 32 bit MAC-I, performance would be degraded due to the need for segmentation for some messages.

In case segmentation is used, subsequent segments can only be transferred after acknowledgement of earlier transmitted segments. This is a concrete problem at least in case of handover, since the quality of the uplink radio channel may be quite poor resulting in a failure to transfer acknowledgements. This implies that it may be impossible to quickly transfer a segmented handover message.

This problem was already tackled in S3#15bis contribution S3z000012 by Siemens. It was proposed:

" In case the option for MAC-I lengths shorter than 32 bits is introduced, such messages must include a field that defines the length of the message authentication code (e.g., a two-bit identifier that allows for the values 8, 16, 24 and 32). "

As already mentioned by Vodafone in the discussions about this matter in S3#15bis, it is possible to save even more bits to be used for MAC-I by skipping the two-bit identifier. As it is the RRC layer which both

- appends the MAC-I and
- controls the length of the radio blocks

it is possible for the RRC layer to add as many bits of the MAC-I as fits to the message without segmentation.

Following the lines of thinking in S3z000012 we propose that

- TSG GERAN defines a list of messages for which segmentation due to integrity protection implies a severe decrease of network performance (because of time-criticality or extreme frequency or other reason)
- S3 checks for each message in the list whether security level decrease due to using shorter MAC-I can be accepted given the savings in network performance
- For messages in the S3 approved list as many bits of MAC-I are appended to the message as fits without forcing segmentation. However, minimum number of added bits of MAC-i is 8 while maximum is naturally 32.