3GPP TSG SA WG3 Security — S3#32 **S3-040143**
9 –13 February 2004
Edinburgh, UK

Title: **Draft** Reply LS on 'Ciphering for Voice Group Call Services'
Release: 6
Work Items: Key Management of group keys for Voice Group Call Services

Source: 3GPP SA3
To: GERAN 2
Cc: ETSI EP RT, T WG 3

Contact Person:
Name: Marc Blommaert
Tel. Number: +32 14 25 3411
E-mail Address: Marc.Blommaert@siemens.com

Attachments: None

Overall description:

SA3 would like to thank GERAN2 for their reply LS on 'Ciphering for Voice Group Call Services' in Tdoc GP-040566 (S3-040117) and is pleased to hear that the work is progressing.

SA3 have discussed the GERAN2 questions and can provide following answers:

A. Is a UICC/USIM mandatory for the mobile that supports the new VGCS ciphering mechanism?
Answer: Yes. The ciphering mechanism as proposed by SA3 requires changes to the smartcard. But as the SIM-specifications are functionally frozen starting from Rel-5 on, the needed card functions can only be incorporated into the USIM.

B. How will a Release 6 MS that supports the new VGCS mechanism react with a SIM card?
Answer: VGCS ciphering will not be possible since the SIM is unable to derive the short term key from the RAND. A Rel-6 UICC will be required. The assumption is that the administrator of the group is aware of this fact such that this situation would not happen.

C. What happens if a UICC/USIM with voice group id X is inserted into a Release-5 MS and the MS is camped on to a cell where this group call is active?
Answer: Ciphering will not be possible since the Release-5 MS does not support the needed ciphering functions (i.e. the key modification function to derive the modified short term key). Again the assumption is that the administrator of the group is aware of this fact such that this situation would not happen.

D. Are the proposed changes also applicable to the VBS service?
Answer: Yes.

E. Are the proposed changes to be applied only from Release-6?
Answer: Yes

F. Is a cell based global_count in C(i) an acceptable method for providing this parameter ?
Answer: Yes.

ACTION:

3GPP SA3 kindly asks GERAN 2 to take into account the above provided answers.

Date of Next SA3 Meetings:

SA3#33	10 - 14 May 2004	Beijing
SA3#34	5 – 9 July 2004	Chicago
SA3#35	4 – 8 October 2004	tbd