3GPP TSG SA WG3 Security — SA3#35 **S3-040703**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG-GERAN#21 **Tdoc GP-042284**
Montreal, Canada, 23rd –27th August 2004

Title: **LS on ‘Ciphering for Voice Group Call Services’.**

Response to: **LS on ‘Ciphering for Voice Group Call Services’.**

Release: **Release-6**

Source: **GERAN2**

To: **SA3**

Cc: **ETSI EP RT, T WG3**

Contact Person:
Name: Ken Isaacs
Tel. Number: +44 1794 833531
E-mail Address: kenneth.isaacs@roke.co.uk

Attachments: None

1. Overall Description:

GERAN2 would like to thank SA3 for their LSs on ‘Ciphering for Voice Group Call Services’ in Tdoc S3-030804 and ‘Key Management of group keys for Voice Group Call Services’ in Tdoc S3-040680. GERAN2 has **considered the provision of the RAND, CGI and the Global_Count** and the conclusions are summarized below:

A **RAND**

GERAN2 has already recommended in GP-041210 that a 32 bit RAND can be provided. However, SA3 has since recommended that a RAND of at least 36 bits and a 2 bit Cell Global Count should be provided (S3-040680). The main points to take into account when considering the provision of a larger RAND are:

- There are less than 40 bits available to provide additional fields in the Paging Request Type 1 message on the PCH even when the notification is segmented over two PCH blocks using extended paging
- The need to make efficient use of the NCH. In order to provide two RAND and two group call references per NCH block puts a restriction of the size of the additional information per call to be no more than 40 bits. These 40 bits have to include bits that are used to make the additional fields optional.
- Need for additional parameters in the notifications that is using the same resource as the RAND (eg 2 bit Cell Global Count)

When taking into account these restrictions, GERAN2 had determined that the size of the RAND can be a maximum of 36 bits. Whilst providing a larger RAND is feasible there would be the following consequences:

- Reduced opportunity for the use of the PCH to send notifications. The use would depend on the mandatory IEs occupying less space than their maximum size.
- On the NCH it may not be possible to include two RAND and two Group Call References per NCH block, thus resulting in greater usage of NCH blocks.

B **CGI**

GERAN2 has already recommended in GP-041210 that the CGI will be used as an input parameter to the generation of the group cipher key.

C Global_Count

GERAN2 has shown that it is possible to provide a Global_Count on the NCH, PCH and FACCH, as detailed in GP-041835. Since the resources are scarce on these channels, it is recommended that this field is kept as small as possible. It is suggested that no more than 2 bits are used for the Global_Count. GERAN2 has noted that this is inline with the proposed SA3 CR (S3-040638)

2. Actions:

To SA3 group.

ACTION: GERAN2 recommends the approval of the SA3 CR in S3-040638.

3. Date of Next TSG-GERAN Meetings:

GERAN2#21 bis	4th - 8th October 2004 MALTA
GERAN#22	8th - 12th November 2004 South Africa