3GPP TSG SA WG3 Security — SA3#33 **S3-040286**
10-14 May 2004
Beijing, China

Source: **Siemens, Vodafone**

Title: **VGCS: Status of principles and further proceeding**

Document for: **Discussion and decision**

Agenda Item: **6.21: VGCS**

1 Introduction

The purpose of this contribution is to give an overview of the decisions that SA3 has made so far on VGCS/VBS ciphering. It is also proposed to add two more decisions to this list of agreed principles and to allow GERAN2 more time to study a solution to provide the global-count. A companion CR to this meeting also implements these agreements into TS 43.020.

2 Status of principles

Agreed principles by SA3 (including SA3#30,31,32):

A) For each voice group up to 2 group keys per group can be defined (identified by a group key number). Note: The maximum number of group keys per voice group is determined by the available number of bits in the radio access network to signal a key identifier to the UE.

B) The group keys are stored in

- the group call register (GCR) on the network side (which is co-located to an MSC),
- USIM application of the UICC on the UE side.

A SIM can not be used.

C) On call set-up the GCR selects one group key, generates a temporary key with a RAND and sends the temporary key to the BSS and the group key number and RAND to the UE. The UE then asks the UICC to generate a temporary key based on the group key number and broadcasted information (RAND).

E) The same algorithms are used for encryption of VGCS-calls as for normal GSM-speech calls (i.e. A5/0-A5/7).

Any requirement for modification of the input parameters to A5 shall be achieved using a separate Key Modification Function (KMF). How this function is realized is currently under study.

F) The use of OTA for updating VGCS group keys to the UICC is optional for the operator.

G) The cipher algorithm that shall be used per group is stored on the USIM for each group.

H) The VGCS ciphering concept also applies to VBS.

3 Proposed new SA3-agreements as indicated by S3-040255 (GP-041210)

The incoming LS from GERAN2 indicate that GERAN2 has finalized the study on CGI and RAND with following results:

1) GERAN2 recommends that a RAND of 32-bits is provided.

2) It is possible to provide the CGI as an input parameter to the generation of the cell local group cipher key.

On the global_count parameter GERAN2 has not yet finalized the study. Here it is proposed that SA3 gives GERAN2 more time to come with a result.

It is proposed that SA3 follows the GERAN2 proposal and conditionally approves those parts of the companion-CR that are not affected by the global-count discussion. The final approval of the CR at SA3#34 would then only be limited to those outstanding parts.

SAGE might want to comment on the 32-bit challenge i.e. if the 32-bit challenge is long enough. It is therefore proposed to send an LS to SAGE.

In order to progress the work in other groups and to ensure alignment with CR's of these groups, it is proposed that SA1, CN1, CN4, GERAN2 and T3 are informed of the CR parts that could be agreed by SA3.