3GPP TSG SA WG3 Security — S3#33 **S3-040425**
10 - 14 May 2004
Beijing, China

Title: **Draft** Reply LS (from SA3) to T3-040329 (S3-040370) on VGCS and VBS security
Release: 6
Work Item:

Source: 3GPP TSG-SA WG3
To: 3GPP TSG-T WG3
Cc:

Contact Person:
Name: Benno Tietz
Tel. Number: +49 211 533 2168
E-mail Address: benno.tietz@vodafone.com

Attachments:

---

1. Overall Description:

SA3 thank T3 for their liaison statement (T3-040329) on 'VGCS and VBS security'.

In their LS T3 raise the following questions:

> *1- Does SA3 intend to assign one ciphering algorithm identifier per VGCS group (which is the current assumption of T3), or one per key (assuming that there are two keys for each group), or one algorithm for the VGCS?*

Answer by SA3:
The algorithm identifier is assigned per group key. To SA3's understanding the CR provided by T3 for review doesn't reflect this.

> *2- Does the SA3 work encompass VBS security in the same way as VGCS? Applying a similar mechanism to VBS could enable the operator to charge the subscriber accordingly.*

Answer by SA3:
From a security point of view the only difference between VGCS and VBS is that for VBS no encryption is provided for the uplink-channel since there is no uplink-channel in VBS. All other security functions are the same.

SA3 would like to point out that the two voice group keys V_Ki will probably be exchanged by the operator during the lifetime of a voice group (e.g. when a member leaves the voice group and the remaining members are provisioned with new group keys). USIM OTA might be an appropriate mechanism for the exchange of the group keys. The same mechanism could be applied for registering a subscriber to a VGCS/VBS group. In this context, an appropriate standardisation of these data containers is highly suitable.

SA3 thank T3 for its cooperation, the work on this topic, and welcome further T3's liaison on this matter.

2. Actions:

To T3

SA3 ask T3 to consider the above statements in their further work.

3. Date of next TSG-SA WG3 Meetings:

SA3#34	6–9 July 2004	Acapulco, Mexico
SA3#35	5–8 Oct 2004	Malta