3GPP TSG SA WG3 Security — S3#30 **S3-030515**
06 - 10 October 2003
Povoa de Varzim, Portugal

Title: **Draft** LS on clarification of MBMS Service Requirements/assumptions

Work Items: Multimedia broadcast/multicast service (MBMS) AP 0309/04

Source: 3GPP SA3
To: 3GPP SA1
Cc:

Contact Person:
Name: Colin Blanchard
Tel. Number: +44 1473 605353
E-mail Address: colin.blanchard@bt.com

Attachments: none

SA3 are discussing a number of alternative proposals for providing MBMS Key Management. MBMS Key Management is required to change the Traffic Encryption Key (TEK) frequently and in an unpredictable manner to ensure that:

- It is uneconomic for subscribed users to distribute decryption keys to non-subscribed users.
- Users that have joined a multicast service, but then left, shall not gain further access to the multicast service without being charged appropriately.
- Users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately.

SA3 would appreciate guidance from SA1 on the following service issues:

1. One proposal being considered by SA3, makes use of a Broadcast Access Key (BAK) that is retained within the UICC and thus does not need to be changed so frequently as TEK and therefore can be distributed on a point to point basis using either MIKEY or SIM toolkit on say a 90 day schedule. One constraint on SA3 choice of approach may be the user expectation in the delay between service activation (subscription, service announcement, joining) and session start (i.e.

when the user must have been provided with all keys necessary for decryption of the content. SA3 have assumed that there must be some generic service performance requirements that constrain our security solution but will meet customer expectations for the service. E.g. be able to decrypt the content within 1 hour, 1 day, 7 days etc of joining etc. SA3 would appreciate some guidance from SA1 on what would be an acceptable delay if it were necessary for the user to wait for the next schedule update of a key.

2. If the BAK proposal was adopted, SA3 could also consider the providing a secure manual function to add "Provide BAK" and "delete BAK" management messages as part of the design of the MBMS Key Management scheme. This would allow the service provider to "subscribe" and "un-subscribe" a particular user at any time. Can SA1 comment on the usefulness of such a feature.

3. While it would not make best use of radio resources to request acknowledgements from all users at every key change, SA3 believe that it may be useful for technical support (help desk) purposes, to configure specific UE's to acknowledge key changes. It may also be useful to provide the ability for the service provider to query the key status of any individual UE at any time. Can SA1 comment on whether such features are required.

4. SA3 are considering the requirement for identification of key material and need to provide sufficient bits in any "key Id field" to uniquely distinguish all the services provided by an MBMS service provider and MBMS service providers with the same network. For example, 5 bits would allow 32 services. Can SA1 advice on 1) the maximum number MBMS services per MBMS provider that should be allowed for and 2) the total number of MBMS service providers that are likely to be associated with one PLMN.

Action on SA1:

To provide answers to the 4 questions above to advise SA3 on what will be the formal method of recording these e.g. CR's to the stage 1 specification TS 22.146.

Date of Next SA3 Meetings:

SA3#30	6 – 10 October 2003	Porto
SA3#31	18 – 21 November 2003	London (TBC)