3GPP TSG SA WG3 Security — S3#31 **S3-030710**
18 - 21 November 2003
Munich, Germany

3GPP TSG SA WG3 Security — S3#30 **S3-030522**
06 - 10 October 2003
Povoa de Varzim, Portugal

Agenda item: 7.20

Source: Samsung

Title: Differentiation of MBMS traffic protection mechanisms

Document for: Discussion and Decision

1. Introduction

Based on the operator's decision, different traffic data protection mechanisms may be adopted for different MBMS services. UEs should know this information in advance for later data decryption. It is proposed that this detail protection mechanism information shall be indicated to the UEs in the service announcement.

2. Discussion

Users services that use MBMS bearer are currently being standardized within the work item "MBMS Teleservice", which was approved during previous SA#21 plenary meeting. Also, the MBMS bearer is suggested to be available to support services other than the MBMS Teleservice. Based on operator's choice, different traffic data protection mechanisms may be adopted for these different services. For example, MBMS traffic data can be protected by the DRM security method or protected by the MBMS ciphering, as indicated within SA3 currently. And it is indicated within current TS that "it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence requires no additional protection."

Since the UE has to know the exact traffic protection mechanism for data decryption, it is quite obvious that this traffic protection mechanism indication for one specific service should be given to the joined UEs before this service starts. And it is better to broadcast this information to all UEs in the service announcement, because this shall give the users the selection whether to even activate this service or not.

3. Conclusion

It is proposed that SA3 can confirm the above consideration and agree on the following text proposal:

5.2 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence requires no additional protection). This protection will probably be either confidentiality and integrity or just confidentiality. The detail traffic data protection mechanism for one specific service shall be indicated to the UEs in the service announcement.

It was agreed that the MBMS encryption should be done end-to-end between the UE and BM-SC, and not at either the Radio or the Core Network level. The actual method of protection was for further study.