3GPP TSG SA WG3 (Security) meeting #32 **S3-040037**

9-13 February 2004

Edinburgh, Scotland, UK

Agenda item: 6.20 MBMS

Source: Samsung Electronics

Title: BMSC handing of the previous keys

Document for: Discussion and Decision

1. Introduction

MBMS keys shall be changed regularly. And BMSC may have several selections about handling of the previous keys considering key request. SA3 is proposed to decide on this BMSC operation and capture its decision into current TS33.246.

2. Discussion

All keys used for the MBMS service shall be uniquely identifiable. And they should be changed regularly to ensure they are fresh. Thus, this leads to one question: how BMSC shall deal with the previous keys -- shall the BMSC simply abandon them, save them all or keep some latest ones? A example scenarios is following: Suppose one legal UE requests the keys after receiving all the data for quite a long time. This UE may not be able to decode them correctly because it tries but cannot obtain the corresponding keys due to network congestion, etc. However, this UE stores all the encrypted contents. And finally, this UE succeeds in asking the BMSC for keys! In this case, the BMSC may have several selections:

a) The BMSC shall only keep and give out the latest key upon UE’s request. In this case, the UE can only decrypt the content encrypted by the latest key and has to abandon the saved content encrypted by previous keys.

b) Or the BMSC shall keep all the used keys and send them out upon UE’s request. In this case, the BMSC shall have to store all these keys until the session ends, while the UE can decrypt all the content correctly.

c) Or the BMSC shall keep some latest keys and send them out upon UE’s request. In this case, the UE may decrypt the content encrypted by these keys and has to abandon the saved content encrypted by other previous keys.

3. Conclusion

Samsung proposes SA3 to make a decision on this BMSC operation and capture this decision into the specification.