3GPP TSG SA WG3 Security — SA3#33 **S3-040386**
10-14 May 2004
Beijing, China

Source:	**MBMS Rapporteur**
Title:	**Security requirements from SA2 specification**
Document for:	**Discussion/Decision**
Agenda Item:	**MBMS**

1 Introduction

In S3-040364 SA2 asked SA3 to include the following requirements in TS 33.246.

5.1.1 Content Provider Authentication, Authorization and Charging

The BM-SC shall be able to authenticate 3rd party content providers, providing content for MBMS transmissions.

3rd party content providers may wish to initiate an MBMS transmission. In such cases, the BM-SC shall be able to authorize content providers to transmit data over MBMS bearer services depending on operator policy.

The BM-SC shall be able to verify the integrity of data received from content providers.

As the BM-SC to content provider referencepoint is not standardised in the SA2 specification, it is proposed to add requirements for the raised issues to TS 33.246 as requested along with a note to say that work on this interface is out of scope. In addition it is proposed to remove two Editor's notes relating to this issue.

2 Proposed Pseudo CR for TS 33.246

C.5 Requirements on integrity protection of MBMS multicast data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS multicast data sent to the UE on the radio interface. The use of integrity shall be optional.

Editor's note: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.

Note: the use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in

R6b: The MBMS multicast data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS service.

R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.

~~Editor's Note: It may be required to integrity protect the multimedia content on the "Content Provider - BM-SC" interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.~~

C.6 Requirements on confidentiality protection of MBMS multicast data

R7a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R7b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that have joined the MBMS service.

R7c: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

R7d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on MBMS multicast session from the BM-SC to the UE.

R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS multicast session when it is applied.

~~Editor's Note: It may be required to encrypt the multimedia content on the "Content Provider - BM-SC" interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.~~

C.7 Requirements on content provider to BM-SC reference point

R8a: The BM-SC shall be able to authenticate and authorize a 3rd party content providers that wishes to transmit data to the BM-SC.

R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.

NOTE: This reference point will not be standardised.