3GPP TSG SA WG3 Security — S3#28 **S3-030226**
6 - 9 May 2003 Berlin, Germany

Source: **Siemens**

Title: **MBMS: Key Encryption Keys requirements**

Document for: **Discussion and Decision**

Agenda Item: **7.21**

Abstract

This contribution presents requirements on the MBMS Key Encryption Key for use between the UE and the BM-SC. It is proposed to include these into the MBMS specification.

Proposed new requirements for TS 33.246

Clause 4.1.4 in TS 33.246 on Key Management does currently not specify how the security services that shall be applied to the transfer of the MBMS keys are to be realized.

R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R5b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

Both symmetric and assymmetric methods (I.e. an MBMS key transfer from BM-SC to UE may be confidentiality protected by using the public key of the UE) can be used for this. Under the assumption that symmetric method will be selected, then following requirement seem to be valid: (Lets call the symmetric key(s) used to transport the MBMS keys: MBMS Key Encryption Key.)

Proposed new requirements:

The MBMS Key Encryption key

- shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).
- shall be MBMS-service specific.
- shall be unique per BM-SC.
- remains valid until the MBMS user leaves the MBMS-service.

A clear statement on the scope of the MBMS Key Encryption Key may be important for key derivation functions or the amount of needed key authentications.