3GPP TSG SA WG3 Security — S3#32 **S3-040144**
9-13 February 2004
Edinburgh, UK

Source: **Siemens**

Title: **Update on Proposed terminology for MBMS keys**

Document for: **Approval**

Agenda Item: **6.20 (MBMS)**

1 Pseudo-CR text for new terminology within TS 33.246

It is proposed to change the title of clause 3 to 'Definitions and abbreviations' and to include a section 3.1 on 'Definitions'.

This update of the terminology includes

A) The addition of the definition for the Key MUK

B) The correction of MKK to MMK

C) The change of MSK to MTK

3.1 Definitions

MMK= MBMS Master Key: The MBMS service specific key that is securely transferred (using the Key MUK) from the BM-SC towards the UE. This key may be stored within the ME or the UICC depending on the MBMS service. For MBMS streaming the MMK is not used directly to protect the MBMS data (See MTK).

Editors Note: How the MMK is used for download is still under study.

MTK = MBMS Traffic Key: A Key that is obtained by the UE by calling a function fx (MMK, Key-deriv parameters) that may be realized on the ME or the UICC depending on the MBMS-service. The Key MTK is used to decrypt the received MBMS data.

Editors Note on MKK and MTK: These definitions are subject to further modification as two alternative two-tiered keying systems are still under consideration a) the SK_RAND model b) the key encryption model. For Case a) fx may be a PRF (hash function) while for case b) an encryption algorithm is needed. Key-deriv will be RAND for case a). For case b) Key-deriv will be a MTK encrypted with MMK.

MUK= MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MMK's to the UE. This key may be stored within the ME or the UICC depending on the MBMS service.