3GPP TSG SA WG3 Security — S3#32 **S3-040160**
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 with respect to contribution S3-040099 includes

A) The addition of the definition for the key MUK (as included within S3-040144)

B) The correction of MKK to MMK (here the second proposal, the same as included within S3-040144)

C) The change of MSK to MTK (as included within S3-040144)

D) Alignment of Editors Note on ME and UICC based alternatives. (this update)

E) The addition of a second alternative (proposal 1 in this document) for the 'higher level key' name: MSK. The preference goes to the first proposal. The term SK has been used for the key MTK in lot of contributions before. This could be seen as a drawback. But at the same time MSK as MBMS Service Key seems very natural and self explaining (this update).

Proposal 1:

MSK= MBMS Service Key: The MBMS Service key that is securely transferred (using the key MUK) from the BM-SC towards the UE. For MBMS streaming the MSK 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 ME by calling a function fx (MSK, Key-deriv parameters). The key MTK is used to decrypt the received MBMS data on the ME.

Editors Note on MSK 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 MSK.

MUK= MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSK's to the UE.

Editors Note: The keys MSK and MUK may be stored within the UICC or the ME depending on the MBMS service. The function fx may be realized on the ME or the UICC.

Proposal 2:

MMK= MBMS Master Key: The MBMS service specific key that is securely transferred (using the key MUK) from the BM-SC towards the UE. 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 ME by calling a function fx (MMK, Key-deriv parameters). The key MTK is used to decrypt the received MBMS data on the ME.

Editors Note on MMK 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.

Editors Note: The keys MMK and MUK may be stored within the UICC or the ME depending on the MBMS service. The function fx may be realized on the ME or the UICC.