3GPP TSG SA WG3 Security — S3#34 **S3-040469**

July 6 - 9, 2004

Acapulco, Mexico

Source: **Siemens, 3**

Title: **Proposed changes to Annex C of TS 33.246**

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

Introduction

This contribution contains proposed changes to the requirement section of the MBMS specification version 1.2.1, intended as a cleanup of the many Editor's Notes in the Annex C. In addition, SA3 is asked if the Editor's Note at the top of Annex C can be removed 'i.e. if there are still not-agreed requirements below, they should be removed or corrected.

Annex C (normative): Multicast security requirements

~~Editor's note: Not all the security requirements in this section have been agreed.~~

C.1 Requirements on security service access

C.1.1 Requirements on secure service access

R1a: A valid USIM shall be required to access ~~any 3G service including the~~ MBMS User Services.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.

~~Editor's note: No requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale~~

C.1.2 Requirements on secure service provision

R2a: It shall be possible for the network (e.g. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.

~~Editor's note: Authentication during service is ffs.~~

R2b: It shall be possible to prevent the use of a particular USIM to access MBMS User Services.

~~Editor's Note: It is for FFS to what extent it is required to detect and prevent fraudulent use of MBMS services.~~ NOTE: No security requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale

C.2 Requirements on MBMS signaling protection

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS signaling on the Gmb reference point.

Editor's note: When the Gmb reference point is IP-based then NDS/IP methods according to TS 33.210 may be applied to fulfill requirement R3a. The Gmb interface is ffs.

R3b: Unauthorized modification, insertion, replay or deletion of all signaling, on the RAN shall be prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE

~~Editor's note~~NOTE: UTRAN Bearer signalling integrity protection will be turned off for point to multipoint MBMS sessions and GERAN has no bearer signalling integrity protection, even for point to point signalling.

C.3 Requirements on Privacy

R4a: The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located outside the 3GPP operator's network.

~~Editor's note: This may already be covered by some national regulations.~~

R4b: MBMS identity and control information shall not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE.

NOTE~~Editor's note~~: UTRAN and GERAN Bearer confidentiality protection will be turned off for point to multipoint MBMS sessions

C.4 Requirements on MBMS Key Management

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~~ shall be integrity protected.

R5c: The UE and MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary to ensure that

- users that have joined an MBMS User Service multicast service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
- users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately
- the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.

R5d: Only authorized users that have joined an MBMS User Service shall be able to receive MBMS keys delivered from the MBMS key generator.

R5e: The MBMS keys 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).

R5f: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.

~~Editor's note: If ptm re- keying is used, the keys shall be delivered in a reliable way. Ptp re-keying is assumed to be reliable.~~

R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).

R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

C.5 Requirements on integrity protection of MBMS User Service data

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

~~Editor's note~~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~~Note~~: T~~t~~he 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 User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.

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

C.6 Requirements on confidentiality protection of MBMS User Service data

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

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

R7c: It may be required to encrypt the MBMS User Service 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 protect the MBMS User Service from the BM-SC to the UE.

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

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 provider 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.