3GPP TSG SA WG3 Security — SA3#33 **S3-040221**
10-14 May 2004, Beijing, China

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘	**33.246**	**CR**		⌘ **rev**	**-**	⌘ Current version: **1.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification on MSK keys and MBMS user/bearer service Make clear when User service or Bearer Service is meant	
Source:	⌘	Siemens	
Work item code:	⌘	MBMS	***Date:*** ⌘ 09/04/2004
Category:	⌘		***Release:*** ⌘ Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Avoid any misinterpretation that MSK would apply to the MBMS bearer services.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘				
		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	-			

************** First change **************

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to [5]

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 User Service data (see MTK).

Editors Note: How the MSK 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 key derived from 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

3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol>	<Explanation>

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

MBMS	Multimedia Broadcast/Multicast Service

************** next change **************

4.1 Security requirements

The following security requirements have been identified for protection of MBMS User Services in MBMS multicast mode~~traffic~~.

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

4.1.1 Requirements on security service access

4.1.1.1 Requirements on secure service access

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

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User S~~s~~ervices 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

4.1.1.2 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 S~~s~~ervices.

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 S~~s~~ervices.

Editor's Note: It is for FFS to what extent it is required to detect and prevent fraudulent use of MBMS services.

4.1.2 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: 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.

4.1.3 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.

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

4.1.4 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 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~~multicast~~ S~~s~~ervice, but then left, shall not gain further access to the MBMS User Service~~multicast service~~ without being charged appropriately

- users joining an MBMS User Service~~multicast service~~ shall not gain access to data from previous transmissions in the MBMS User Service~~multicast 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~~multicast~~ 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 S~~s~~ervice 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.

4.1.5 Requirements on integrity protection of MBMS User Service~~multicast~~ data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service ~~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 User Service ~~multicast~~ data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User S~~s~~ervice.

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.

4.1.6 Requirements on confidentiality protection of MBMS User Service ~~multicast~~ data

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

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

R7c: It may be required to encrypt the MBMS User Service~~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 to protect the ~~on~~ MBMS User Service ~~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 User Service~~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.

************** next change **************

5 MBMS security functions

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised in two parts when participating in an MBMS user service. Firstly when the UE establishes ~~a~~MBMS bearer(s) to receive an MBMS User Service~~MBMS traffic~~ and secondly when the UE request and receive MSK’s~~keys~~ for the MBMS User S~~s~~ervice. The MBMS bearer establishment requires a point to point connection with the network on which authentication is performed using the ~~normal~~ network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish ~~a~~MBMS bearer(s) (see TS 23.246 [3] for the details) corresponding to an MBMS User Service. As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. controlled by the BM-SC), there is an additional procedure to remove ~~a~~ MBMS bearer(s) related to a UE that is no longer authorised to access the MBMS User S~~s~~ervice.

Editor’s note: It was agreed to standardise a solution that allowed MBMS specific keys to be stored in either the ME or UICC in release 6. The choice of storage depends on whether the UICC has the ability to hold the keys or not. The differences between the two methods will only be visible in the UE, and the BM-SC would know which method of storing the keys in the UE will be used.

Editor’s note: The use of AKA between the BM-SC and UE was proposed. It was concluded that the issue of bootstrapping and having the BM-SC in the visited network need to be further investigated.