3GPP TSG SA WG3 Security — S3#30 **S3-030513**
06 - 10 October 2003, Povoa de Varzim, Portugal

CR-Form-v7

CHANGE REQUEST

⌘ **33.246 CR CRNum** ⌘ **rev** **-** ⌘ Current version: **0.2.0** ⌘

*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:	⌘	TS33.246 MBMS Security Requirements CR (non controversial)
Source:	⌘	BT Group
Work item code:	⌘	
Date:	⌘	26/09/2003
Category:	⌘	C
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: ⌘ As a result of AP 29/11, this CR adds the identified security requirements that were not considered to be controversial.

Summary of change: ⌘

1. Added requirement that solutions that requires UE to be customised to a particular customer prior to the point of sale should be avoided

2. Explicit requirement added to ensure that Unauthorized modification, insertion, replay or deletion of all signaling, on the RAN is prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE (Bearer integrity protection will be turned off for point to multipoint MBMS sessions)

3. Explicit requirement added to ensure MBMS provider identity and control information should not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE. (Bearer confidentiality protection will be turned off for point to multipoint MBMS sessions)

4. Additional rationale for changing keys added "The UE and MBMS key generator shall change the decryption key frequently and in an unpredictable manner to ensure that it is uneconomic for subscribed users to distribute decryption keys to non-subscribed users"

5. Requirement on key identification added

Consequences if not approved:	⌘	Subsequent specification of security mechanisms may be less effective and efficient.

Clauses affected:	⌘	4.1				
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	
				Test specifications		
				O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** BEGIN SET OF CHANGES ***

4.1 Security requirements

The following security requirements have been identified for MBMS.

Editor’s note: Not all the security requirements in this section have been agreed. Most of the requirements are for the multicast service only.

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 service.

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

R1c: 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 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 services.

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

R2a: 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 R7a. The Gmb interface is ffs.

R2b 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

Editors note: Bearer integrity protection will be turned off for point to multipoint MBMS sessions

4.1.3 Requirements on Privacy

R3a: 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.

R3b 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.

Editors note: Bearer confidentiality protection will be turned off for point to multipoint MBMS sessions

4.1.4 Requirements on MBMS Key Management

R4a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R4b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

R4c: The UE and MBMS key generator shall ~~support re-keyin~~change the ~~g~~decryption key frequently and in an unpredictable ~~to~~manner to ensure that

- ~~users~~Users that have joined a multicast service, but then left, shall not gain further access to the multicast service without being charged appropriately. ~~The re-keying shall also ensure that~~
- ~~users~~Users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately
- It is uneconomic for subscribed users to distribute decryption keys to non-subscribed users.

Note 1 it is assumed that the legitimate end user has a motivation to defeat the system and distribute the shared keys that are a necessary feature of any broadcast security scheme.

Note 2 It cannot be assumed all terminals to be secure and, no matter how the shared encryption keys are delivered to the terminal, we have to assume they can be derived in an attack. For example, the shared keys while, secure in the UICC may be passed over an insecure SIM-ME interface.

R4d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

R4e: 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).

Editor’s Note: The MBMS key generator function is still to be allocated to a network node.

R4f: All keys used for the MBMS 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.

R4g: If ptm re- keying is used this shall be repeated a number of times around the scheduled re- keying time.

Editors note: This requirement is for Ptm re-keying. Ptp re-keying is assumed to be reliable

*** END SET OF CHANGES ***