3GPP TSG SA WG3 Security — S3#26 **S3-020644**
19 - 22 November 2002, Oxford, UK

CR-Form-v7

CHANGE REQUEST

⌘ **33.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.0.2** ⌘

*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 of re-keying requirement
Source:	⌘	H3G
Work item code:	⌘	MBMS
Date:	⌘	12/11/2002
Category:	⌘	**F**
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:	⌘	The re-keying requirement only covers a user join and leaving and then having access to further transmissions. It should also address the case of a user joining not having access to previos transmissions.
Summary of change:	⌘	To add the requirment described above.
Consequences if not approved:	⌘	Re-keying requirment not complete

Clauses affected:	⌘	4.1.1

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

Other comments: ⌘

4.1.1 Requirements on encryption protection of MBMS multicast data and security keys

R4a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R4b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that has joined the MBMS service.

R4c: The encryption key(s) and the integrity key for the MBMS multicast service shall be encrypted when delivered to the users. In addition, it may be required to protect these keys with a MAC.

R4d: Only the valid users that has joined a MBMS multicast service shall be able to decrypt the encryption key(s) and the integrity key delivered from the network.

R4e: The UE and MBMS key generator shall support re-keying to ensure ~~Mandate support of re-keying in the UE and BM-SC in order to ensure~~ that users that have~~s~~ joined a multicast~~MBMS~~ service, but then left, shall not gain further access to the~~MBMS~~ multicast service without being charged appropriately. The re-keying shall also ensure that users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately.

R4g: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi and Gmb.

R4h: User identity should not be exposed to the content provider or linked to the content, in the case the Content Provider is located in the 3GPP operator's network.

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.