3GPP TSG SA WG3 (Security) meeting #32 **S3-040038**
9-13 February 2004
Edinburgh, Scotland, UK

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **0.3.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [X] Core Network [X]

Title:	⌘	TS33.246 MBMS key update rejection CR
Source:	⌘	Samsung Electronics
Work item code:	⌘	MBMS
Date:	⌘	02/02/2004
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:	⌘	This CR adds the key update rejection procedure which aims to complete the high-level key update procedure.
Summary of change:	⌘	Key update rejection procedure is added.
Consequences if not approved:	⌘	The high-level MBMS key update procedure is incomplete.

Clauses affected:	⌘	6.2

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

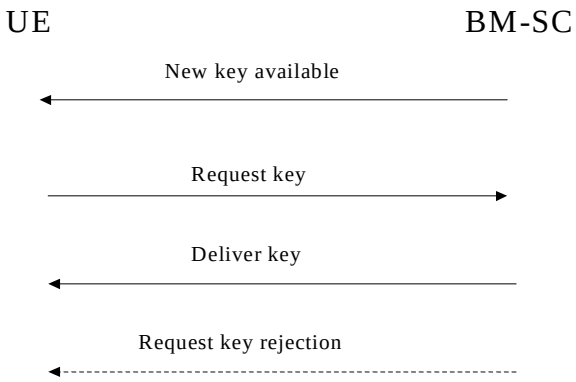
Other comments:	⌘	

*** BEGIN SET OF CHANGES ***

6.2 Key update procedure

Once a UE has joined a multicast service, the UE should try to get access to the key that will be used to protect the data transmitted as part of this multicast service. If the UE fails to get hold of the updated key or receives confirmation that no updated key is necessary or available at this time, then, unless the UE has a still-valid, older key, the UE shall leave the MBMS user service. The UE tries to get the key using the second message in the below flow.

The BM-SC controls when the keys used in a multicast service are to be changed. The below flow describes how the high-level key changes are performed.



The first message is sent out by the BM-SC to indicate that new keys are available. It is an optional message in the flow. If it is sent to all UEs, then it needs to be ensured that all the UEs do not request the new key simultaneously.

The second message is used to request a key. This is sent by the UE when it either receives the first message in the flow and does not have the new key, has just joined a multicasts service and does not have a key for that service or a UE has received some protected content which it does key that was used to protect the content. If the UE fails to get hold of the updated key or receive confirmation that no updated key is necessary or available at this time, then, unless the UE has a still valid older key, the UE shall leave the MBMS service.

After receiving the second message the BM-SC should send out the appropriate key to the UE protected by the relevant means, or reject the UE's key request with an indication of the cause. Upon successfully receiving the new key, the UE should store this key for later use.

Editor's note: MIKEY is being considered as the method for carrying keys. Possible optimisations were proposed at the ad-hoc in Antwerp (S3z030010). One identified issue was the possible need to terminate MIKEY in the UICC and/or terminal in the combined method. The use of MIKEY relates to the PTP delivery of a key

*** END SET OF CHANGES ***