3GPP TSG-SA WG3 Meeting #37 **_Tdoc ⌘S3-050073_**
Sophia Antipolis, France, February 21-25, 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**038**	⌘**rev**	**-**	⌘	Current version:	**6.1.0** ⌘

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:	⌘	Clarify MUK key synchronisation for MSK push procedure			
Source:	⌘	Siemens			
Work item code:	⌘	MBMS	***Date:***	⌘	14/02/2005
Category:	⌘	**C**	***Release:***	⌘	Rel-6
		Use *<u>one</u>* *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* *<u>one</u>* *of the following releases:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change:	⌘	It may happen that the UE has already generated a new MUK/MRK pair (after a GBA run and the subsequent application NAF derivation step) but the BM-SC was never informed. From the BM-SC point of view his known MUK/MRK pair may still be valid (lifetime has not expired), hence this MUK-ID can still be used within the MSK push procedure. While the UE has already installed a new MUK-ID, the BM-SC is using an old MUK for protecting the MSK push MIKEY messages. The UE behavior for this mismatch case is not specified. A similar handling as for the push solicited pull procedure is proposed. For the push solicit pull, the BM-SC is allowed to use a MUK-ID beyond the SA-lifetime (differently than the last generated one). This MUK-ID is known to the UE as the last-successfully used.
Summary of change:	⌘	Clarify the UE behavior when receiving a normal MIKEY push message with an old (still valid) MUK-ID. The UE shall handle the MIKEY push message in a similar way as the push solicited pull message. This guarantees that the UE contacts the BM-SC with the B-TID. Subsequently the MSK is pushed again to the UE (yet with the newer MUK).
Consequences if not approved:	⌘	UE's may behave differently which may result in non-optimized MSK handling.

Clauses affected:	⌘					
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 31.102
			X	Test specifications		

	□	☒	O&M Specifications

Other comments: ⌘

===== BEGIN CHANGE =====

6.3.2.3 MSK push procedures

6.3.2.3.1 Pushing the MSKs to the UE

The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.

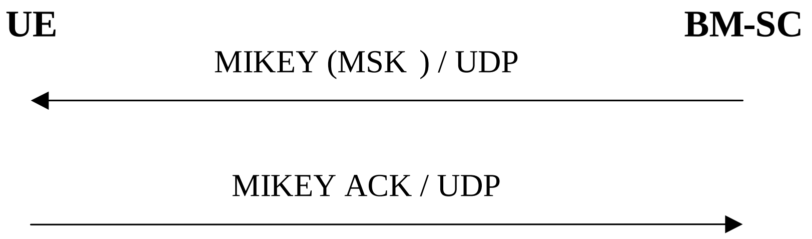

Figure 6.3: Pushing the MSKs to the UE

When the BM-SC decides that it is time to update the MSK, the BM-SC sends MIKEY message over UDP transporting the requested MSKs to the UE.

If requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

When an MSK push MIKEY message is not directly preceded by an MSK key request, then it may happen that the BM-SC uses a still valid MUK that is not the last generated MUK at the UE. The UE shall handle such a MIKEY push message in a similar way as the push solicited pull MIKEY message (i.e upon a successfull integrity check the UE shall initiate an MSK request with the specified Key Group).

NOTE: This procedure guarantees that the UE contacts the BM-SC with the last B-TID, such that the UE now receives a MIKEY push message with the last generated MUK. The integrity of the initial pushed MIKEY message can be verified at the UE with the MUK-ID that is known as the last succesfully used BM-SC MUK-ID.

6.3.2.3.2 Void

===== END CHANGE =====