3GPP TSG-SA3 Meeting #35
St Paulís Bay, Malta, October 5 ñ 8, 2004

Tdoc ⌘S3-040859

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **015** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*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 [ ] Core Network [X]

Title:	⌘	Use of parallel MSKs and MTKs
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	28/09/2004
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:	⌘	The use of parallel MSKs and MTKs is unclear.
Summary of change:	⌘	The use of parallel MSKs and MTKs is clarified: There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.This is due to the fact that MSK ID and MTK ID are sequence numbers. I.e. the UE would discard the MSK/MTK with smaller MSK ID/MTK ID. The use of the same MTK with two different transport services (or user services) should be avoided. This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic. I.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.
Consequences if not approved:	⌘	Use of MSKs and MTKs remains underspecified.

Clauses affected:	⌘	4.2

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

Other comments: ⌘

4.2 Key management overview

~~An MBMS User Service may use one or more MBMS Service Keys (MSKs), which may be in use at the same time and are managed at the MBMS User Service Level.~~ The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different Transport Services that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Transport Services, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Transport Services, as specified within subclauses 6.5 and 6.6. MSKs and MTKs are managed at the MBMS User Service Level.

There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.

~~NOTE: According to good security practice the~~ The use of the same MTK (this implies also the same MSK) with two different ~~security protocols~~ transport services (or user services) ~~shall~~ should be avoided.

NOTE: This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic. I.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

~~For MBMS User Services it shall be possible to share one or more MSKs with other MBMS User Services, since a~~According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. It shall be possible for MBMS User Services to share one or more MSKs for the shared Transport Services with other MBMS User Services.

NOTE: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.

********* NEXT CHANGE*********