3GPP TSG-SA WG3 Meeting #37
Sophia Antipolis, France, February 21-25, 2005

Tdoc ⌘S3-050074

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**039**	⌘**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:	⌘	Add missing parts of CR33 (SA3#36)		
Source:	⌘	Siemens		
Work item code:	⌘	MBMS	***Date:*** ⌘	14/02/2005
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:

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:	⌘	The change from “Key Group Id” to “Key Group part of MSK ID” was not consistently done through the whole specification in CR 33rev1(Approved at SA3#36) Add the NOTE about Key Group Part which was agreed at SA3#36 (S3-040997), but was forgotten when several proposed CRs were redrafted into CR33
Summary of change:	⌘	Change the “Key Group ID” to “Key Group Part” in the forgotten clauses. Add forgotten NOTE.
Consequences if not approved:	⌘	Inconsistent terminology, missing NOTE

Clauses affected:	⌘	4.2, 6.3.2.1, 6.3.3.1

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

Other comments:	⌘	

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

4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different MBMS Streaming/Download Sessions that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Streaming/Download Sessions, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Streaming/Download Sessions ~~,~~ as specified within clauses 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 with the same ~~in one~~ Key Group part of MSK ID~~ID~~. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) with the same ~~in a~~ Key Group part of MSK ID~~ID~~ shall not be allowed.

The use of the same MTK (this implies also the same MSK) with two different transport services (or user services) should be avoided.

NOTE 1: 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.

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 2: 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.

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

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

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Key Domain ID MSK ID

where

Key Domain ID = MCC || MNC and is 3 bytes long.

NOTE: When MCC || MNC is used as key identifier, the UE should not try to use it in another context. E.g. UE should not compare the received MCC || MNC to parameters in radio level.

MSK ID is 4 bytes long and with byte 0 and 1 containing the Key Group part, and byte 2 and 3 containing the Key Number part. The Key Number part is used to distinguish MSKs that have the same Key Domain ID and Key Group part. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted. The MSK ID is carried in the extension payload of MIKEY extension payload.

NOTE: It needs to be ensured that the Key Group parts are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group value.

If the UE receives an MSK and already contains two other MSKs under the same Key Domain ID and Key Group part, then the UE shall delete the older of these two MSKs.

Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.

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

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

6.3.3.1 MTK identification

Every MTK is uniquely identifiable by its Key Domain ID, MSK ID and MTK ID

where

Key Domain ID, and MSK ID are as defined in clause 6.3.2.1.

MTK ID is 2 bytes long sequence number and is used to distinguish MTKs that have the same Key Domain ID ~~Network ID, Key Group ID~~ and MSK ID. It is carried in the MTK-ID field of MIKEY extension payload. The MTK ID shall be increased every time the MTK is updated. The MTK ID shall be reset every time the MSK is updated.

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