3GPP TSG SA WG3 Security — S3#36
Shenzhen, China, 23-26 November 2004

S3-041131

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **024** ⌘ **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:	⌘	MBMS MSK management
Source:	⌘	Samsung Electronics
Work item code:	⌘	MBMS
Date:	⌘	15/11/2004
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:	⌘	Current UE management mechanism of the MSKs limits the BMSC operation.
Summary of change:	⌘	Add~~Change~~ the UE management mechanism of MSKs ~~to~~ as "The UE shall also delete one MSK when the corresponding MTK ID of one MTK whose delivery is protected by this MSK reaches the upper limit defined in the Key Validity Data subfield present in the KEMAC payload when this MSK is distributed. This aims to ~~To~~ stop the use of one dedicated MSK immediately~~,~~. In this case, BMSC may set the MTK ID of one MTK directly to the upper limit when the corresponding MTK is updated." And remove the associated Editor's note.
Consequences if not approved:	⌘	The MSK management mechanism is limited.

Clauses affected:	⌘	6.3.2.1

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

Other comments:	⌘	

********** START OF CHANGE **********

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID

where

Network ID = MCC || MNC and is 3 bytes long. It is carried in the IDi payload in MIKEY message

Key Group ID is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted. It is carried in the CSB ID field of MIKEY common header.

MSK ID is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Key Group ID. It is carried in the MSK-ID field of MIKEY extension payload.

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

The UE shall also delete one MSK when the corresponding MTK ID of one MTK whose delivery is protected by this MSK reaches the upper limit defined in the Key Validity Data subfield present in the KEMAC payload when this MSK is distributed. This aims to stop the use of one dedicated MSK immediately. In this case, BMSC may set the MTK ID of one MTK directly to the upper limit when the corresponding MTK is updated.

~~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 OF CHANGE **********