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

S3-040961

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**024**	⌘ **rev**	**-**	⌘ 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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

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 cannot work correctly for MBMS download service, and also limits the BMSC operation.
Summary of change:	⌘	Change the UE management mechanism of MSKs to “The UE shall 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. To stop the use of one dedicated MSK immediately, BMSC may set the MTK ID of one MTK to the upper limit when the corresponding MTK is updated”. And remove the associated Editor’s note.
Consequences if not approved:	⌘	UE cannot manage MSK correctly, especially for download service,

Clauses affected:	⌘	6.3.1.1, 6.4.4			
		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.

The UE shall 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. To stop the use of one dedicated MSK immediately, BMSC may set the MTK ID of one MTK to the upper limit when the corresponding MTK is updated. ~~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.~~

~~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.~~

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the keys, a new general Extension Payload (EXT) is defined that conforms to the structure defined in section 6.15 of RFC 3830 [9] (MIKEY). The IDs of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is delivered in the message. This EXT is incorporated in the MIKEY messages (see Figure 6.4). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. The MSK ID and MTK ID are increased ~~by 1~~ every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

********** END OF CHANGE **********