3GPP TSG SA WG3 Security — S3#37 **S3-050164**

21-25 February 2005

Sophia Antipolis, France

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **050** ⌘ **rev** **2** ⌘ 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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Stop the usage of one MSK
Source:	⌘	SA3 WG
Work item code:	⌘	MBMS
Date:	⌘	22/02/2005
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:
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:	⌘	When the BMSC decides to stop using one MSK, it shall need to inform the UE about this. This can happen before the new MSK is delivered to the UE. Thus the scenarios when UE shall stop the usgae of one MSK and delete it are not fully listed in current specification.
Summary of change:	⌘	Add new clause 6.3.2.4 which lists the cases when UE shall stop the usage of one MSK. And move existing scenarios to this new clause.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	6.3.2.1, 6.3.2.4

		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 Key Domain ID MSK ID

where

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

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.~~

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

6.3.2.4 Stop the usage of one MSK

When the BMSC decides to stop using one MSK for a multicast service, it shall inform the UE about this. It may happen after BMSC pushes a new MSK to the UE, or before a new MSK is available to the UE. Thus the UE shall stop the usage of one MSK and delete it from storage in the following cases:

- If the UE receives an MSK and already contains two other MSKs under the same Key Domain ID and Key Group part of the MSK ID, then the UE shall stop the usage of the older one of these two MSKs.
- If the UE receives an MSK that sets the lower limit SEQl equal or larger than the upper limit SEQu (see clause 6.5.3), then the UE shall stop the usage of this MSK.
- If the UE receives an MTK updating with the MTK-ID larger than the upper limit SEQu (see clause 6.5.4), then the UE shall stop the usage of the MSK used for protecting this MTK updating.

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 **********