3GPP TSG SA WG3 Security — S3#37 **S3-050~~089~~128**

21-25 February 2005

Sophia Antipolis, France

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **050** ⌘**rev** **1** ⌘ 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:	⌘	Samsung Electronics
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 whenever no matter this MSK is used or not, or whether a new MSK is available or not. Thus the scenarios when UE shall stop the usgae of one MSK are not fully listed in current specification. And the defination of the time when to delete one "Not usable" MSK is not security related.
Summary of change:	⌘	Add new clause 6.3.2.4 which lists the cases when UE shall stop the usage of one MSK. And state that the time when to delete one "Not usable" MSK is out of security scope.
Consequences if not approved:	⌘	Incomplete ~~list of scenarios when UE shall stop the usage of one MSK.~~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 no matter whether this MSK is currently used for MTK updating protection, or whether a new MSK is available or not. Thus the UE shall mark one MSK as “not usable” and stop its usage 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 to mark the older one of these two MSKs as “Not usable”.
- ~~If the UE receives an MSK that sets the lower limit SEQs to the maximum (see clause 6.5.3), then the UE shall mark this MSK as “Not usable”.~~
- If the UE receives an MSK that sets the lower limit SEQs equal or larger than the upper limit SEQu (see clause 6.5.3), then the UE shall mark this MSK as “Not usable”.
- If the UE receives an MTK updating with the MTK-ID reaching the upper limit SEQu (see clause 6.5.4), then the UE shall mark the MSK used for protecting this MTK updating as “Not usable”.
- ~~If the UE leaves one service or the service is over, then the UE shall mark all kept MSKs for this service as “Not usable”.~~

~~Note 1: One “Not usable” MSK shall not be used for later MTK generation, but the UE may select to keep it for previous MTKs generation, especially for download session, if service playback is supported by this UE.~~

Note 1: When marked “Not usable”, the MSK shall not be used for protecting new MTK distribution any longer. But the UE may select to keep one “Not usable” MSK if it selects to save the received encrypted MBMS service data and wants to use the older MTKs again later, if service playback is supported by this UE. This may happen especially for download sessions. The UE can keep up to **16** MSKs under the same Key Domain ID and Key Group part.

Note 2: The UE may also select to delete one MSK immediately if this MSK is marked as “Not usable”. ~~depending on UE’s capability.~~ But this is out of security scope.

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 **********