3GPP TSG SA WG3 Security — SA3#35 **S3-040755**

October 5-8, 2004

St Paul's Bay, Malta

Source: **Samsung**

Title: **UE handling of MSKs received**

Document for: **Discussion / Decision**

Agenda item: **MBMS**

1. INTRODUCTION

As defined in current TS33.246 MBMS security, for UE handling of the MSKs received, “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.” This mechanism seems to be not quite suitable, especially for MBMS download service. This contribution proposes some change to this UE handling of MSKs received.

2. DISCUSSION

“An MBMS User Service may contain one or more MSKs which may be in use at the same time and are managed at the MBMS User Service Level”, and “every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID.” “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.” This means that the BMSC shall be able to use at most 2 different MSKs for each Network ID and Key Group ID combination. If the BMSC assigns multiple MSKs at the same time for one user service, say 3 MSKs, the BMSC has to use different Network ID and/or Key Group ID to identify these 3 MSKs. In this case, 2 bits for MSK ID is enough and the use of 2-bytes-long MSK ID seems to be a kind of waste.

Also, this MSK management mechanism is not suitable for the MBMS download service, where it is assumed that the MSKs can be delivered after the content is received. So one MSK should be kept until it is used/expired other than simply updated by the one that owns the same Network ID, Key Group ID but a new MSK ID.

Actually UE can know whether one MSK should be kept or not by the use of its Key Validity Time. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. This field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). So if the MTK ID of the MTK associated with one MSK reaches its upper limit, the UE can delete this MSK.

3. PROPOSAL

It is proposed to adopt these changes and approve the associated CR.

3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘Att1_S3-040755

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**004**	⌘**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:	⌘	UE handling of MSKs received		
Source:	⌘	Samsung Electronics		
Work item code:	⌘	MBMS	***Date:*** ⌘	19/08/2004
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:

2	*(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)*

Reason for change:	⌘	As defined in current TS33.246 MBMS security, for UE handling of the MSKs, "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." This mechanism does not take the full use of 2-bytes-long MSK ID and is not feasible for MBMS download service.
Summary of change:	⌘	Change the UE handling of MSKs into "The UE shall delete one MSK once its corresponding MTK ID reaches the upper limit as defined in the Key Validity Data subfield present in the KEMAC payload when this MSK is distributed." and remove the Editor's note.
Consequences if not approved:	⌘	Current mechanism does not take the full use of 2-bytes-long MSK ID and is not feasible for MBMS download service.

Clauses affected:	⌘	6.3.1.1				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

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

6.3.1.1 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 ID_I 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 Service ID. It is carried in the MSK-ID field of MIKEY extension payload.

The UE shall delete one MSK once its corresponding MTK ID reaches the upper limit as defined in the Key Validity Data subfield present in the KEMAC payload when this MSK is distributed. .~~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.~~