3GPP TSG-SA WG 3 Meeting S3#34
Acapulco, Mexico, 6-9 July, 2004

Tdoc ⌘S3-040520

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.2.1** ⌘

*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:	⌘	Concatenated MSK delivery in MBMS
Source:	⌘	Nokia
Work item code:	⌘	MBMS
Date:	⌘	29/06/2004
Category:	⌘	**B**
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:	⌘	In the S3#33, it was agreed that encrypted MTK method will be used with MIKEY. Additionally, it was discussed offline a possibility to deliver concatenated 256-bit MSK and split it into separate integrity and encryption keys. This pseudo-CR presents necessary changes to provide uniform key delivery for the MSK and MTK keys. The uniform key delivery in encrypted form has the following advantages: • The MSKs and MTKs can be shared between UICC and ME based MGV-Fs so that different MBMS data streams are not required and network resources are used efficiently. (If the BM-SC wants to use higher level security for UICC based MGV-Ss then it is possible to deliver different keys to UICC and ME based MGV-Fs.) • Number of algorithms and complexity of impelementation are minimized in the UE, because MSKs and MTKs are handled in uniform way and a key generation function is not needed. • The MSK/MTK are generated in the BM-SC. It is not necessary to implement backup key generation functions, because it is easier to update key derivation function in few BM-SCs than many UEs. The update will be required if key derivation function is broken. It is also possible to use HW based pseudo random number generators in the BM-SC.
Summary of change:	⌘	This pseudo-CR adds support for the following: • Delivery of 256-bit MSK in the single MIKEY sub-key payload • Splitting 256-bit MSK into integrity and encryption keys
Consequences if not approved:	⌘	MTKs and MSKs are not handled in uniform way.

Clauses affected:	⌘	3.1, 3.2, 3.3, 6.4 and 6.5			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to [5].

~~**MFK** = MBMS traffic key Freshness Key: This key is derived from MSK and is used to ensure that MTK is fresh.~~

~~**MGK** = MBMS traffic key Generation Key: This key is derived from MSK and is used to protect MTK.~~

~~**MRK** = MBMS Request Key: This key is to authorize the UE to the BM-SC when performing key requests etc.~~

MSK = MBMS Service Key: The MBMS Service key is a concatenated key, which includes integrity and encryption keys.~~that~~ It is securely transferred (using the key MUK) from the BM-SC towards the UE. For MBMS streaming the MSK is not used directly to protect the MBMS User Service data (see MTK).

MSKi = MBMS Service Key for Integrity: A key that is used to protect integrity of MTK transfers. It is split from the securely transferred MSK.

MSKe = MBMS Service Key for Encryption: A key that is used to protect confidentiality of MTK transfers. It is split from the securely transferred MSK.

~~Editors Note: How the MSK is used for download is still under study.~~

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function F_t with a MSKe~~key derived from MSK~~. The key MTK is used to decrypt the received MBMS data on the ME.

MUKi = MBMS User Key for Integrity: The MBMS user individual key that is used by the BM-SC to protect integrity of the point to point transfer of MSK's to the UE

MUKe = MBMS User Key for Encryption: The MBMS user individual key that is used by the BM-SC to protect confidentiality of the point to point transfer of MSK's to the UE..

Editors Note: The keys MSK and MUK may be stored within the UICC or the ME depending on the MBMS service. The function F_t may be realized on the ME or the UICC

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

3.2 Symbols

For the purposes of the present document, the following symbols apply:

~~F_f~~	~~MFK generation function~~
~~F_g~~	~~MGK generation function~~
F_m	Keyed MAC function used to check the freshness of MTK
F_t	~~MTK generation~~Key decryption function

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

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

MBMS	Multimedia Broadcast/Multicast Service
MGV-F	~~MTK Generation~~ Key Decryption and Validation Function

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

6.4 MSK decryption and validation at the UE

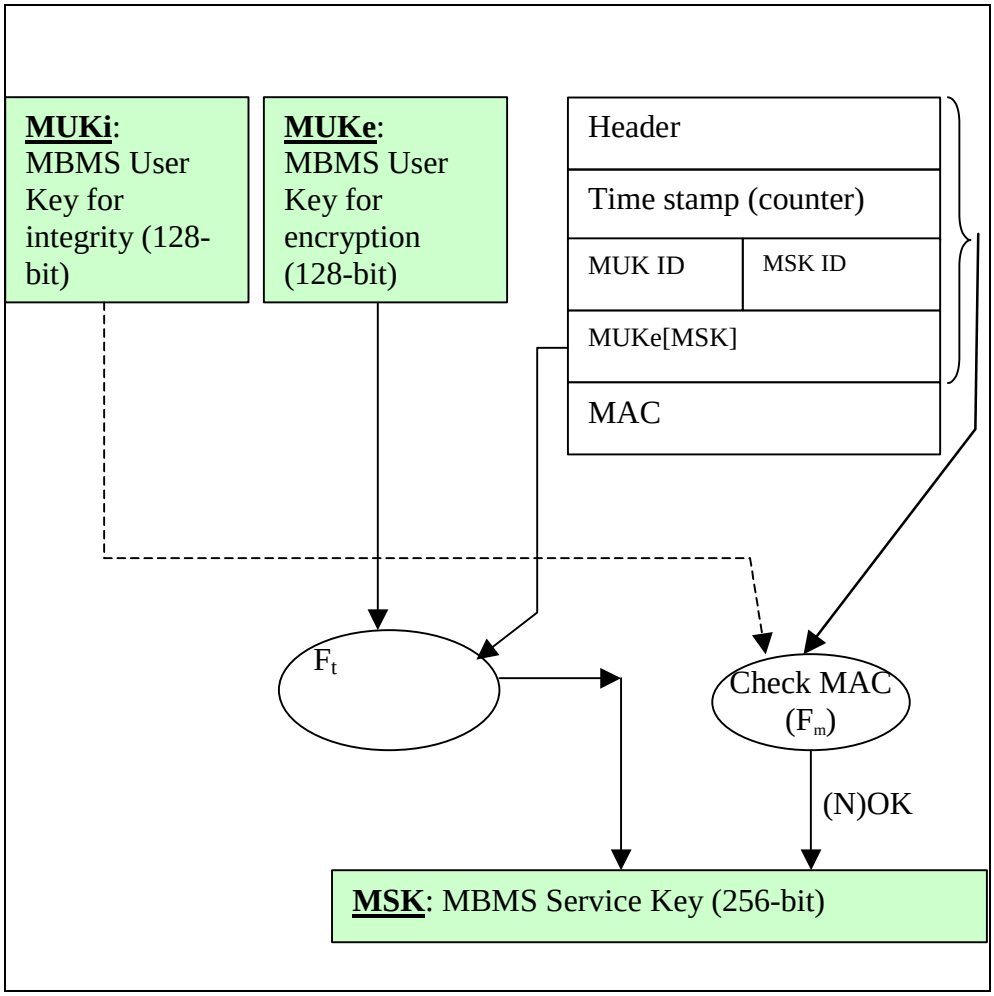


Figure 1: MSK decryption and validation at the UE.

The ME will call the MGV-F that is realized as part of the ME or as part of the UICC. It is assumed that the MBMS service specific data, MUKi, MUKe, MSKi, MSKe and the current MUK ID and MSK ID have been stored within a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. MUKs and the current key identifiers were transferred to the MGV-S with the execution of the key update procedures as described in section 6.2. The initial value of key identifiers are determined by the service provider.

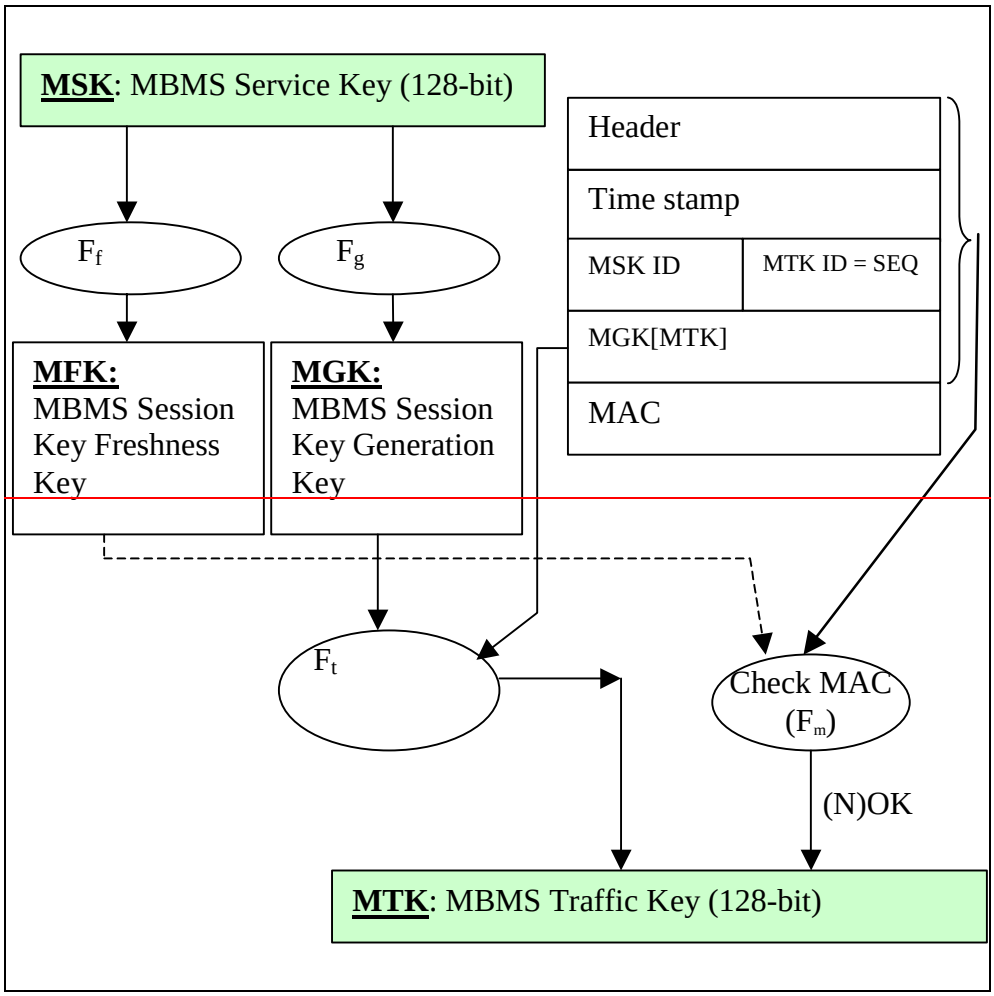
When the ME receives the MIKEY p-t-p message (including e.g. MUK ID, MSK ID, MUKe[MSKi|MSKe], MAC), it shall give the MIKEY message to the MGV-F. The MGV-F shall only decrypt and deliver the MBMS Service Keys (MSKi and MSKe) to the MGV-S if the ptp-key information is deemed to be fresh. How this shall be done is described below:

The MGV-F shall compare the received MSK ID from the MIKEY message with the current MSK ID. If the received MSK ID is equal or lower than the current MSK ID then the MGV-F shall indicate a failure to the ME. If the received MSK ID is greater than the current MSK ID then the MGV-F shall calculate the MAC using a keyed MAC function F_m with the received MIKEY message and the key MUKi as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC defers then the MGV-F will indicate a failure to the ME. If the MAC is equal then the MGV-F shall update the stored MSK ID with received MSK ID value and perform the MBMS service key generation in the following way:

The decryption function F_t decrypts the received MUKe[MSKi|MSKe] to obtain MSKi|MSKe.

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

6.5 MTK generation and validation at the UE


MSK: MBMS Service Key (128-bit)
Header
Time stamp
MSK ID
MTK ID = SEQ
MGK[MTK]
MAC
F_f
F_g
MFK:
MBMS Session Key Freshness Key
MGK:
MBMS Session Key Generation Key
F_t
Check MAC (F_m)
(N)OK
MTK: MBMS Traffic Key (128-bit)

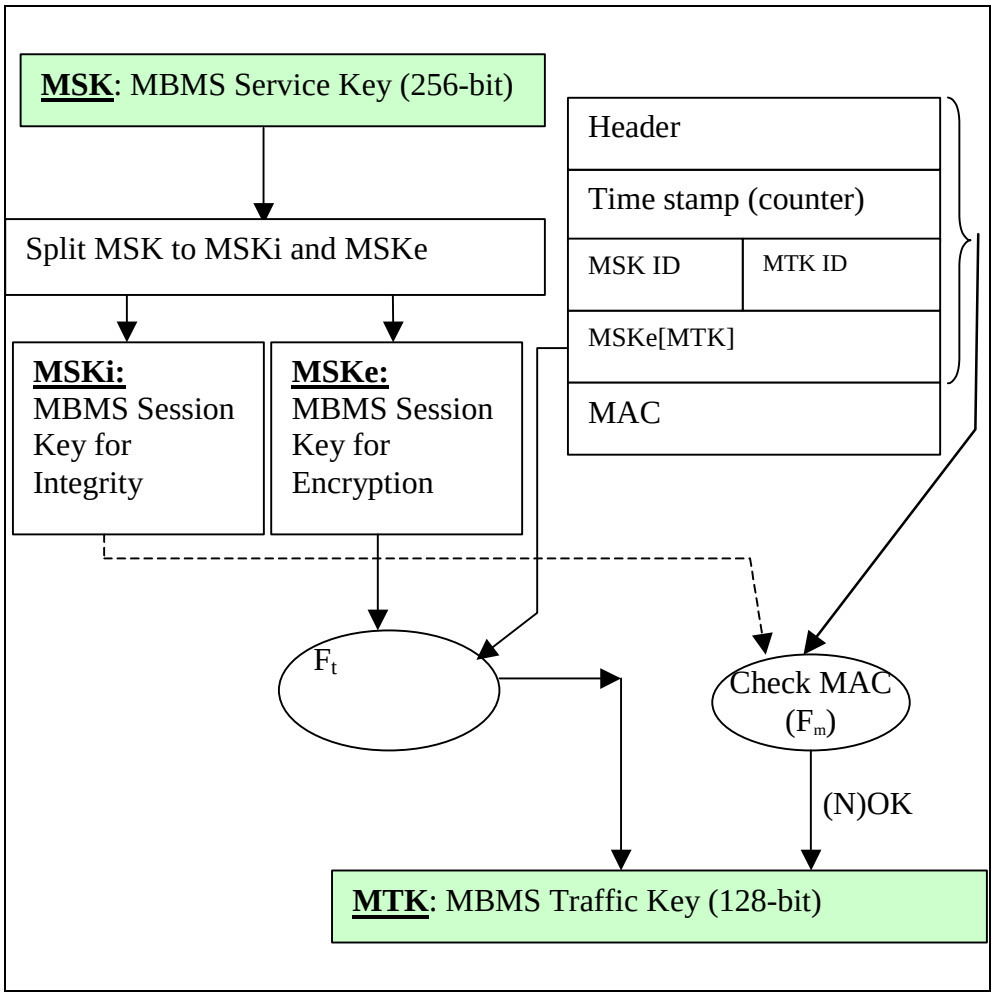


Figure 2: MTK decryption and validation at the UE ~~Validation and Generation Function~~.

~~The ME will call the (*MTK Generation and Validation Function)* MGV-F that is realized as part of the ME or as part of the UICC. It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. Both MSK and SEQs were transferred to the MGV-S with the execution of the key update procedures as described in section 6.2. The initial value of SEQs is determined by the service provider.~~

When the ME receives the MIKEY message (including e.g.MSK ID, MTK ID ~~= SEQp~~, MSKe ~~GK~~[MTK], MAC) from the ptm data stream, it shall give the MIKEY message to the MGV-F. The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh. How this shall be done is described below:

The MGV-F shall use the most significant 128 bits of 256-bit MSK as a MBMS session key for integrity (MSKi) and the rest 128 bits of MSK as a MBMS session key for encryption (MSKe) ~~derive a key MFK (MBMS traffic key Freshness Key) from the MSK using a key derivation function F_f, and shall derive a key MGK (MBMS traffic key Generation Key) from the MSK using a key derivation function F_g.~~

~~The traffic key generation shall be performed in the following way:~~

~~The traffic key decrypt function F_t decrypts the received MGK[MTK] to obtain MTK.~~

~~The freshness check shall be performed in the following way:~~

The MGV-F shall compare the received ~~SEQp, i.e.~~ MTK ID from the MIKEY message with the stored MTK ID ~~SEQs~~. If the received MTK ID ~~SEQp~~ is equal or lower than the current MTD ID ~~SEQs~~ then the MGV-F shall indicate a failure to the ME. If the received MTK ID ~~SEQp~~ is greater than the current MTK ID ~~SEQs~~ then the MGV-F shall calculate the MAC using a keyed MAC function F_m with the received MIKEY message and the MSKi ~~key MGK~~ as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. ~~.~~ If the MAC defers then the MGV-F will

indicate a failure to the ME. If the MAC is equal then the MGV-F shall update the current MTK IDSEQs with SEQp the received MTK ID and shall perform MBMS traffic key generation in the following way:value and start with the generation of MTK. The MGV-F provides the MTK to the ME.

The key decryption function F_t decrypts the received MSKe[MTK] to obtain MTK.