3GPP TSG-SA-WG3 Meeting #33
10th – 14th May 2004, Beijing, China

Tdoc ⌘S3-040392

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.246 CR CRNum** ⌘ **rev** ⌘ Current version: 1.1.1 ⌘

*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 [ ]

Title:	⌘	Calculating validity for MIKEY message
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	13/05/2004
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:	⌘	MGV-F can be updated to support MIKEY.
Summary of change:	⌘	Updating the MGV-F to support MIKEY. Section 6.3a is removed. The order of MAC calculation and SEQ checking is reversed to optimize the performance. The service ID is removed from the figure since it is indicated in the CSB-ID of MIKEY header (This is alignment with S3-040258).
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.3

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

6.3a MTK generation and validation at the UE

Editor's note: Either this clause or 6.3b will be removed once it is agreed how to generate MTK.

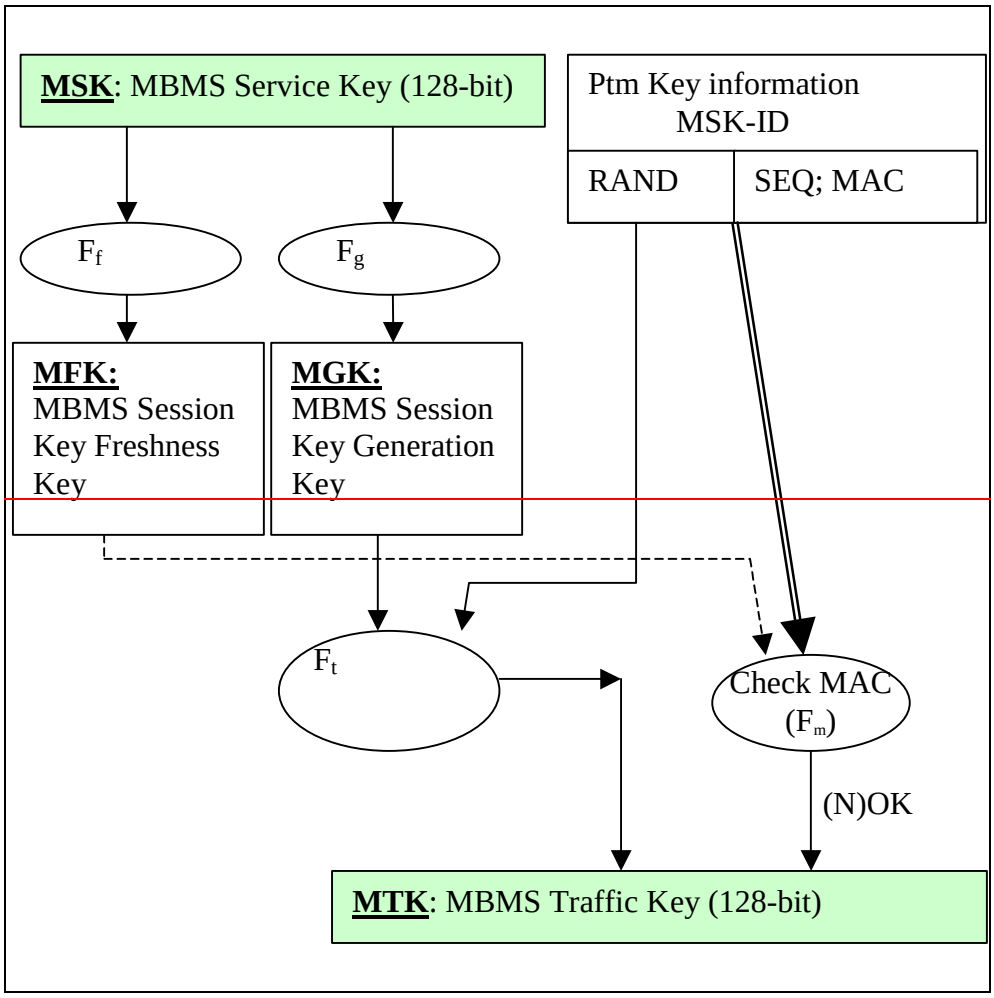


Figure 1: MTK Validation and Generation Function.

Editor's note: It is ffs whether the inputs to the function Fs can be optimized.

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 {MSK Key ID, SEQp, RAND, MAC} from the ptm data stream, it shall give that information to the MGV-F. The MGV-F shall only 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 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:

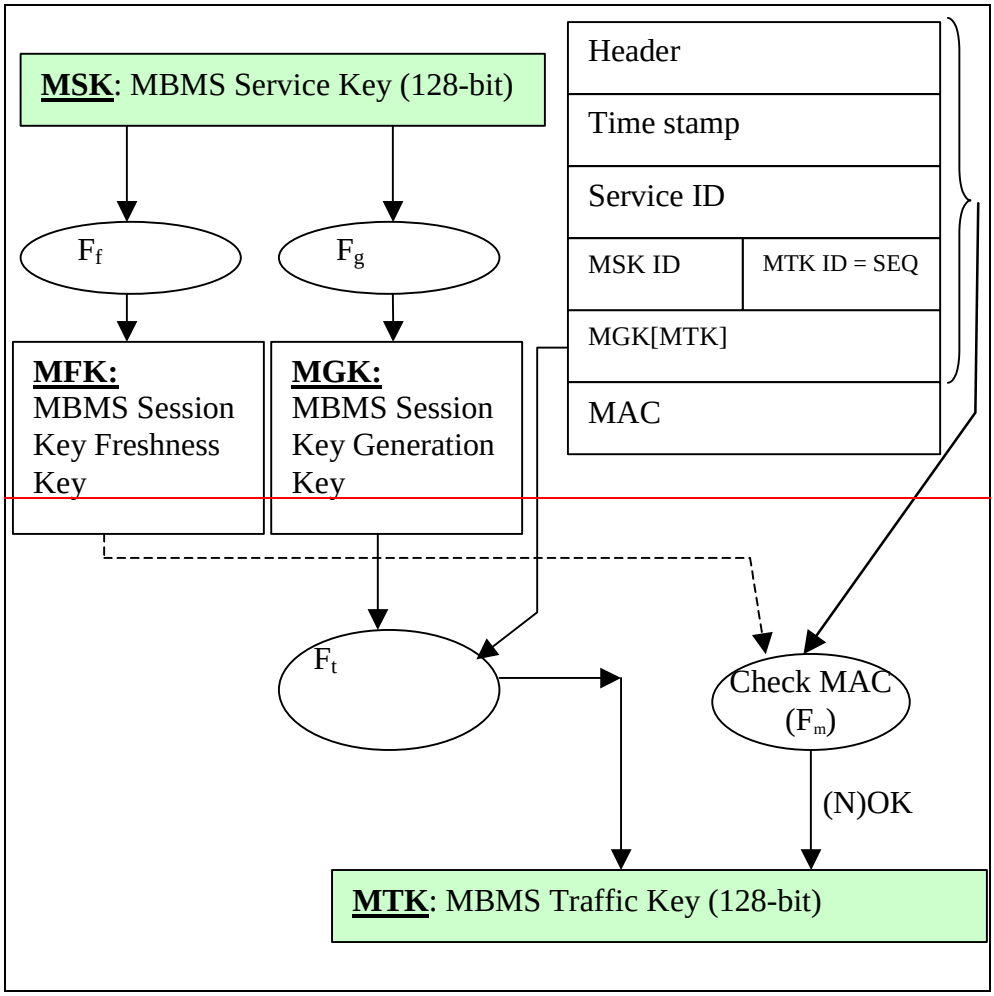
The traffic key generation function F_t uses RAND and the key MGK as input to produce MBMS Traffic key MTK.

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

~~Using a keyed MAC function F_m with the inputs SEQ, RAND and the key MGK, a MAC is calculated. This MAC is compared with the one received from the ptm key information. 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 compare the received SEQp from the ptm key information with the stored SEQs. If SEQp is greater than SEQs than the MGV-F shall update SEQs with SEQp value and start with the generation of MTK. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME.~~

6.3~~b~~ MTK generation and validation at the UE

~~Editor's note: Either this clause or 6.3a will be removed once it is agreed how to generate MTK~~



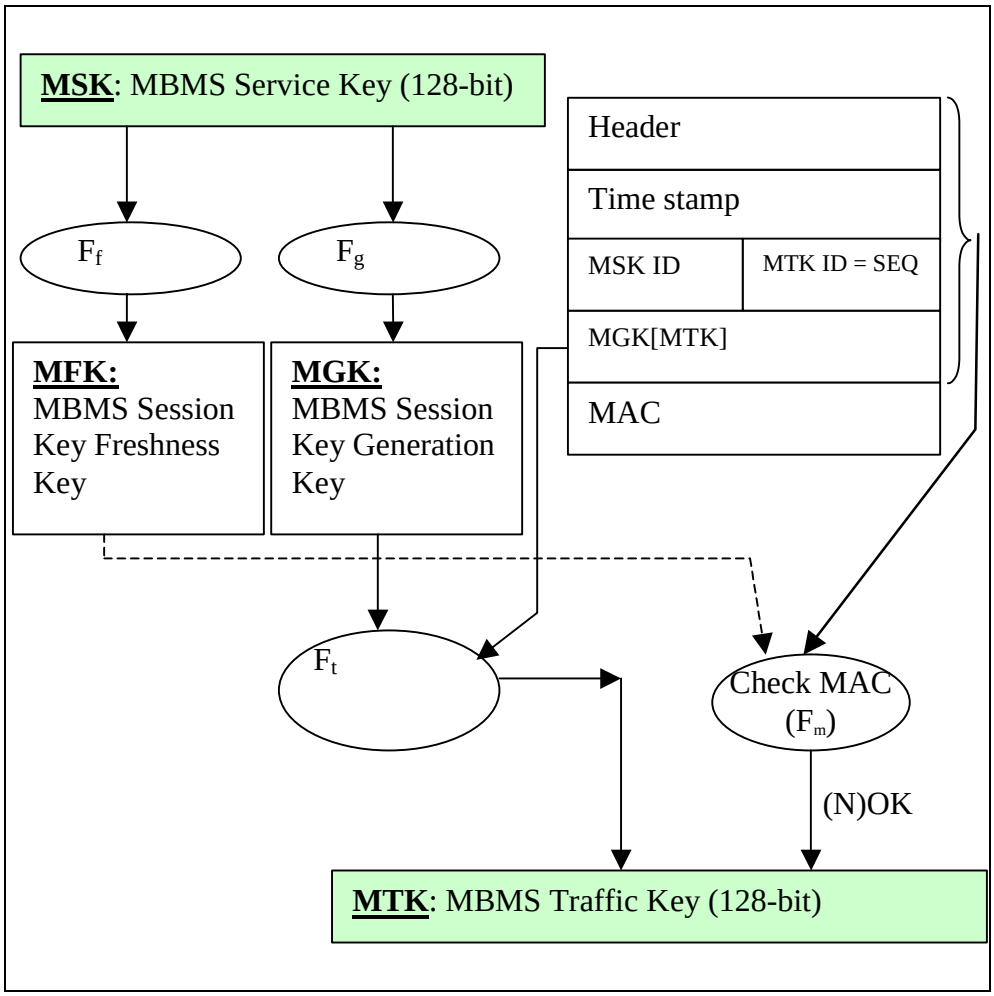


Figure 2: MTK Validation and Generation Function.

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 ~~Key~~-ID, MTK ID = SEQp, MGK[MTK], MAC} from the ptm data stream, it shall give ~~that information~~the MIKEY message to the MGV-F. The MGV-F shall only calculate and deliver the MBMS Traffic Key~~s~~ (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 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 SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC ~~U~~using a keyed MAC function F_m with the received MIKEY message ~~as inputs SEQ, RAND~~ and the key MGK as input~~, a MAC is calculated. The MIKEY message includes the MGK[MTK] and MTK ID~~

~~as the SEQp~~. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. ~~one received from the ptm key information.~~ 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 compare the received SEQp, i.e. MTK ID from the ptm key information from the MIKEY message with the stored SEQs. If SEQp is greater than SEQs than the MGV-F shall~~ the MGV-F shall update SEQs with SEQp value and start with the generation of MTK. ~~If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME.~~

The MGV-F provides the MTK to the ME.