

CHANGE REQUEST

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

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:	⌘ Calculating validity for MIKEY message		
Source:	⌘ Ericsson		
Work item code:	⌘ MBMS	Date:	⌘ 26/04/2004
Category:	⌘ C	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2	(GSM Phase 2)
	A (corresponds to a correction in an earlier release)	R96	(Release 1996)
	B (addition of feature),	R97	(Release 1997)
	C (functional modification of feature)	R98	(Release 1998)
	D (editorial modification)	R99	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		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		
Consequences if not approved:	⌘		

Clauses affected:	⌘ 6.3						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
	Y	N					
	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	O&M Specifications					
Other comments:	⌘						

6.3b 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

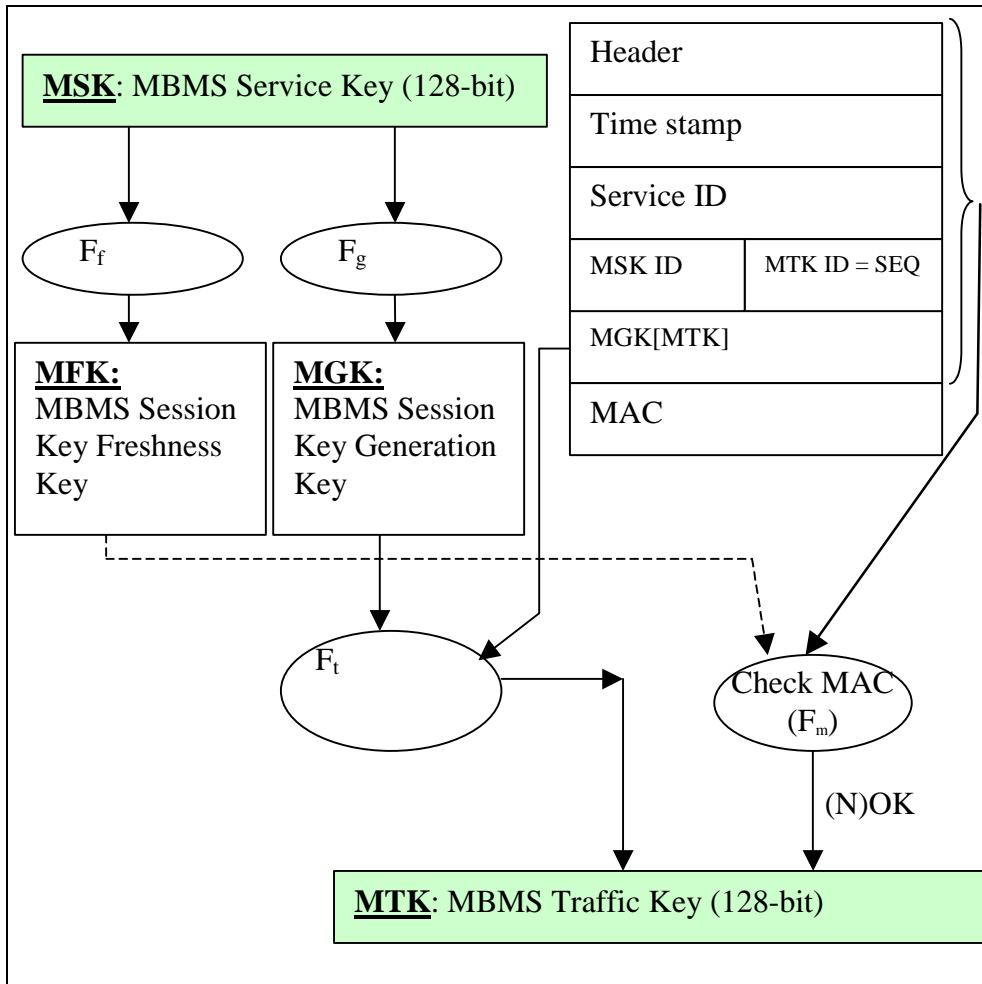


Figure 1: MTK Validation and Generation Function.

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](#) {MSK ~~Key-ID~~, [MTK ID = SEQp](#), MGK[MTK], 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 decrypt function F_t decrypts the received MGK[MTK] to obtain MTK.

The freshness check shall be performed in the following way:

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 differs 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 then 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.