3GPP TSG SA WG3 Security — S3#33
10 - 14 May 2004
Beijing, China

S3-040355
Comment to S3-040248

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

Tdoc ⌘S3-040248

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘	**TS 33.246**	**CR**	**CRNum**	⌘ **rev**		⌘	Current version:	1.1.0	⌘

*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⌘ ☒	ME ☒	Radio Access Network □	Core Network ☒

Title:	⌘	CR on MBMS key Management procedures		
Source:	⌘	AXALTO, Gemplus, OCS		
Work item code:	⌘	MBMS	***Date:*** ⌘	08/04/2004
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:	⌘	MBMS key management has not been specified
Summary of change:	⌘	UICC-based solution as MBMS key management MBMS key management based on OTA
Consequences if not approved:	⌘	

Clauses affected:	⌘	6				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	General comment: details on the interworking between BM-SC in the Visited network and the MBMS Management Server in the Home network are missing in this change request (cf S3-040246)				

Copyright Notification

********FIRST CHANGE**

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[4] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[5] 3GPP TS 22.246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Stage 1; MBMS User Services".

[6] 3GPP TS 31.115: “3rd Generation Partnership Project; Technical Specification Group Terminals; Secured packet structure for (U)SIM Toolkit applications”.

[7] 3GPP TS 31.116: “3rd Generation Partnership Project; Technical Specification Group Terminals; Remote APDU Structure for (U)SIM Toolkit applications”.

********END OF FIRST CHANGE**

********SECOND SET OF CHANGES***************************************

6 Security mechanisms

6.1 Authentication and authorisation of a user

Editor’s note: this section will contain the details of how a user joins a particular Multicast Service

6.2 Key update procedure

6.2.1 Overview

The multicast data of a specific MBMS service is protected by a MBMS Traffic Key (MTK). MTKs are derived from MBMS Service Keys (MSK), which are securely stored in the UICC.

MSK keys are never revealed in clear outside the UICC but are used with the appropriate security functions to derive the MTK (see Protection of the transmitted traffic section). MSK keys are common to all the subscribers of a particular MBMS bearer service. Hence, for security reasons, a mechanism is defined to enable frequent renewals of MSK.

MSK keys are distributed to the UICC prior to service following the administrative procedures described in the following chapter.

MBMS User Key (MUK) are used to protect MSK delivery to the UICC. MUK are different for each subscriber.

Note: MUK provision is out of the scope of this document and may likely be performed at personalization stage or by remote management.

6.2.2 Administrative procedures

The UICC is provisioned with several MBMS key sets to store MSK keys and several files containing other MBMS related data (e.g. MBMS_ID, MTK_SEQp…)

For each MBMS key set a MUK is provisioned in the UICC.

The BMSC is responsible for updating the MSK keys of the UEs that are subscribed to a particular MBMS bearer service before that the particular updated MSK is used. The mechanisms to perform these key updates are described in the following subsections distinguishing two different cases: Network initiated and UE initiated key updates.

Note: These administrative procedures do not apply exclusively to the MSK values but to any MBMS data related to a particular MBMS user service which is stored in the UICC (e.g. MBMS_ID)

6.2.2.1 Network requested key update:

When the BM-SC requests an MBMS Administrative Procedure it sends a MBMS key management request to the Remote UICC Management Entity. This request is then formatted into valid Remote APDUs for (U)SIM Toolkit applications as defined in [7]. The security mechanisms defined in -[6] are used to perform the MBMS key/file remote management to the UICC. These security mechanisms provide authentication, message integrity, replay detection, sequence integrity and message confidentiality.

Editor’s Note: Interface between BM-SC and the Remote UICC Management Entity is FFS.

The following flow shows this procedure:

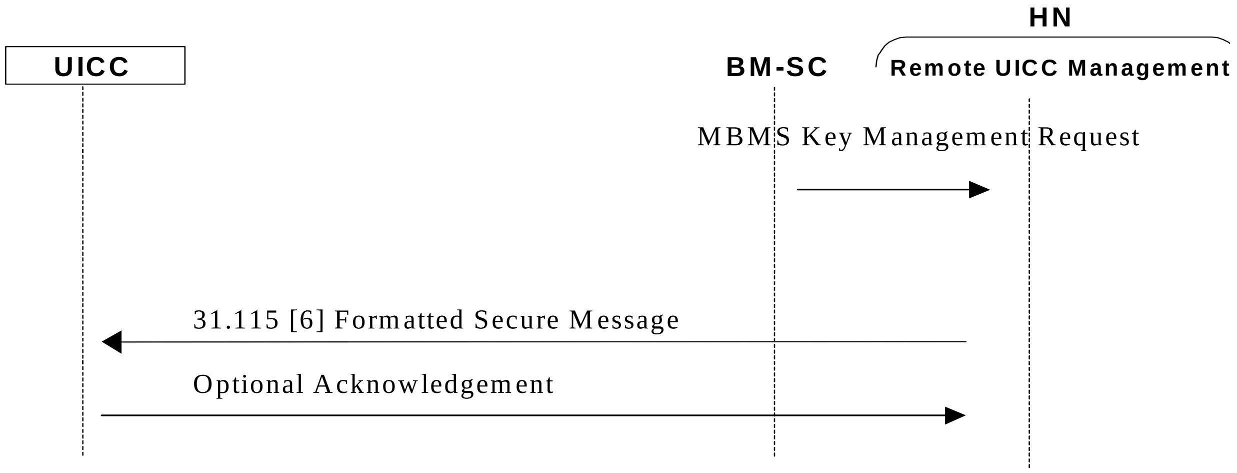

HN
UICC
BM-SC
Remote UICC Management
MBMS Key Management Request
31.115 [6] Formatted Secure Message
Optional Acknowledgement

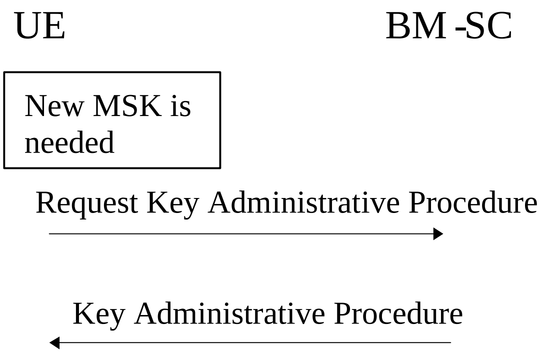
Figure 2: Key Administrative procedure to the UICC.

Note: MUK used in the roaming case may correspond to an MBMS key set in the UICC different of those used in the non-roaming case.

Note: The mechanisms to provide MUK confidentiality between the Home and Visited PLMNs is out of the scope of this specification.

6.2.2.2 UE Initiated Request

Once a UE has joined a multicast service, the ~~UE~~ME ~~should~~ may fail ~~try~~ to get the MT~~S~~K that will be used to 'protect' the data transmitted as part of this multicast service (e.g. the user's UICC has not a correct MSK corresponding to this service). The ME may notice it by inspecting the MBMS related files in the UICC. Alternatively, this can be indicated by the UICC once failing to derive the MTK corresponding to a particular service. ~~If the UE fails to get hold of the MSK or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service.~~ The UE may then try ~~tries~~ to ~~get~~ request the MSK using the ~~second~~ first message in the below flow.


UE
BM-SC
New MSK is needed
Request Key Administrative Procedure
Key Administrative Procedure

~~The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.~~

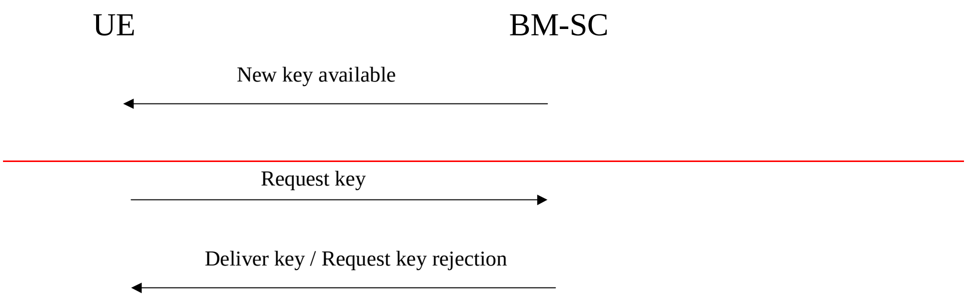


Figure 4: UE initiated Key Management Request

~~The first message is sent out by the BM-SC to indicate that new MSKs are available. It is an optional message in the flow. If it is sent to all UEs, then the BM-SC should provide the rules to the UE for subsequent request for the new MSK when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs.~~

Editor's note: A possible method for achieving the above is for the BM-SC to allocates different "request delay time" to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.

The ~~second~~ first message is sent ~~used~~ to request a MSK management procedure. This is sent by the UE when it ~~either receives the first message in the flow and does not have the new MSK, or~~ has just joined a multicasts service and ~~does~~ the UICC is not able to derive ~~not have~~ an ~~MSK~~ MTK for that service.

Editor's Note: It is FFS the list of reasons to be indicated in this request. A non-exhaustive list may be the following:
-MBMS_ID not subscribed;
-MSK_ID not available;
-MTKSequence error;

After receiving the ~~second~~ request key message, the BM-SC should send out the appropriate MSK to the ~~UE~~UICC as described in the previous case ~~protected by the relevant means~~, or reject the UE's key request with an indication of the cause. Upon successfully receiving the new MSK, the ME may retry to ask the UICC for the corresponding MTK. ~~UE should store this key for later use.~~

If the UE fails to get the key management procedure after some delay, the UE shall leave this MBMS service or retry the UE initiated request procedure.

Editor's note: If OTA is used to carry MSKs to the UICC, the following recommendations shall be followed:

- OTA should not use DES in CBC mode,
- The keys used for the ptp transporting of MSK to the UICC shall not be shared among subscribers,
- OTA shall not rely on the same keys for transporting MBMS data and other application data towards the UICC.

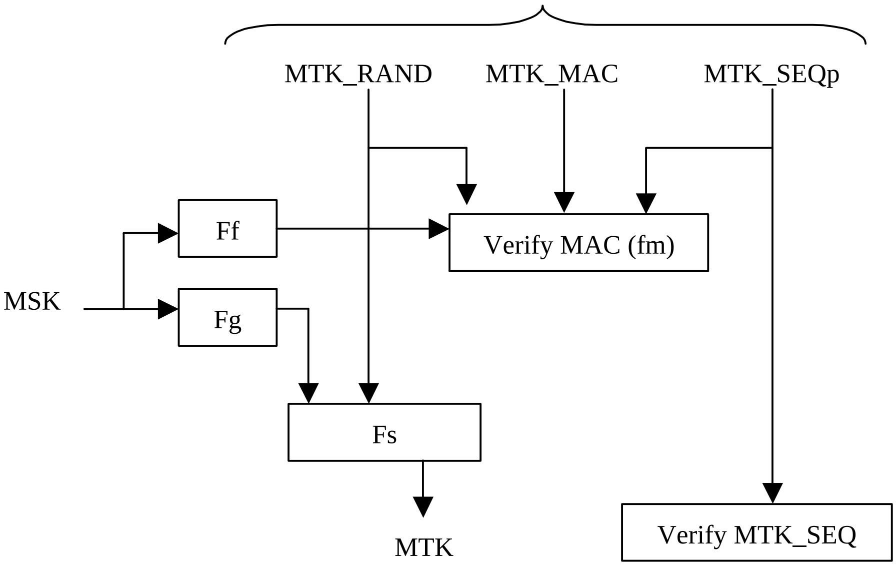
Editor's note: MIKEY is being considered as the method for carrying keys. Possible optimisations were proposed at the ad-hoc in Antwerp (S3z030010). One identified issue was the possible need to terminate MIKEY in the UICC and/or terminal in the combined method. The use of MIKEY relates to the PTP delivery of a key

********END OF SECOND SET OF CHANGES*************************************

*********SECTION MOVED to 6.4 after 6.3 “Protection of the transmitted traffic”*********

6.4~~3~~a MTK generation and validation at the UICC~~E~~

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



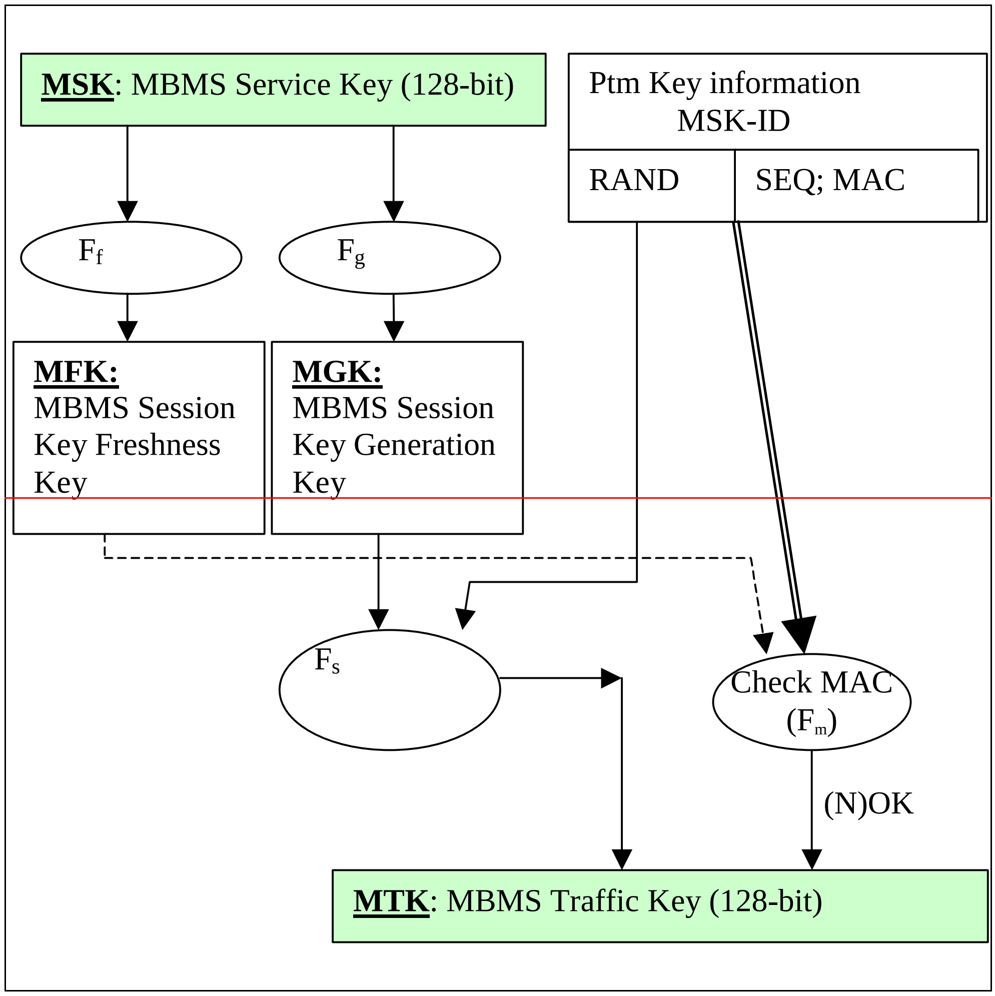

MSK: MBMS Service Key (128-bit)
Ptm Key information
MSK-ID
RAND
SEQ; MAC
Ff
Fg
MFK:
MBMS Session Key Freshness Key
MGK:
MBMS Session Key Generation Key
Fs
Check MAC
(Fm)
(N)OK
MTK: MBMS Traffic Key (128-bit)

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 MTK_SEQs, have been previously stored within ~~a secure storage (MGV-S~~the UICC~~)~~.~~ 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 MTK_SEQs were transferred to the ~~MGV-S~~UICC with the execution of the key update procedures as described in section 6.2. The initial value of MTK_SEQs is determined by the service provider.

When the ME receives {MSK_~~Key~~ID, MTK_SEQp, MTK_RAND, 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:

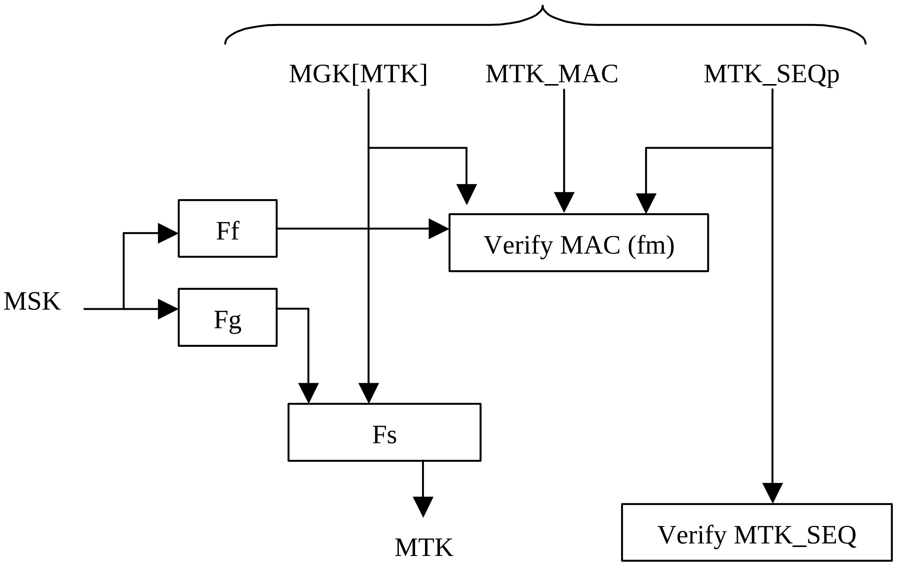
The traffic key generation function F_s uses MTK_RAND and the key MGK as input to produce MBMS Traffic key MTK.

The freshness check shall be performed in the following way:

Using a keyed MAC function f_m with the inputs MTK_SEQ, MTK_RAND and the key MGK, a MAC is calculated. This MAC is compared with the one MTK_MAC 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 MTK_SEQp from the ptm key information with the stored MTK_SEQs. If MTK_SEQp is greater than MTK_SEQs than the MGV-F shall update MTK_SEQs with MTK_SEQp value and start with the generation of MTK. If MTK_SEQp is equal or lower than MTK_SEQs then the MGV-F shall indicate a failure to the ME.

6.4~~3~~b MTK generation and validation at the UICC~~E~~

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



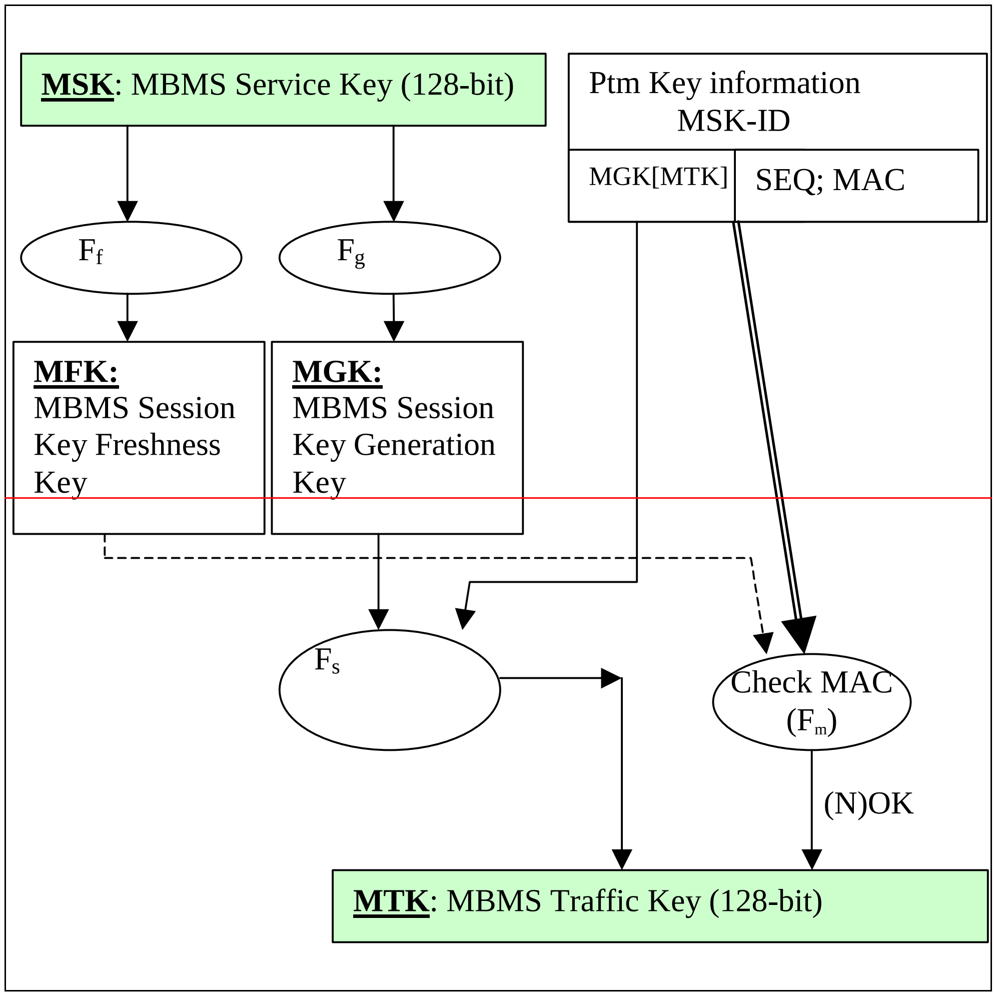

MSK: MBMS Service Key (128-bit)
Ptm Key information
MSK-ID
MGK[MTK]
SEQ; MAC
Ff
Fg
MFK:
MBMS Session Key Freshness Key
MGK:
MBMS Session Key Generation Key
Fs
Check MAC (Fm)
(N)OK
MTK: MBMS Traffic Key (128-bit)

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 MTK_SEQs, have been stored within ~~a secure storage (MGV-S~~the UICC~~)~~. ~~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 MTK_SEQs were transferred to the ~~MGV-S~~UICC with the execution of the key update procedures as described in section 6.2. The initial value of MTK_SEQs is determined by the service provider.

When the ME receives {MSK_~~K Key~~ID, MTK_SEQp, MGK[MTK], 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_s 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 inputs MTK_SEQ, ~~RAND~~MGK[MTK] and the key MGK, a MAC is calculated. This MAC is compared with the one MTK_MAC 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 MTK_SEQp from the ptm key information with the stored MTK_SEQs. If MTK_SEQp is greater than MTK_SEQs than the MGV-F shall update MTK_SEQs with MTK_SEQp value and start with the generation of MTK. If MTK_SEQp is equal or lower than MTK_SEQs then the MGV-F shall indicate a failure to the ME.

***********END of Section Move**

***********START of LAST SET OF CHANGES***

6.3~~4~~ Protection of the transmitted traffic

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and UEs that are accessing the MBMS service. The protection of the data is applied by the BM-SC. In order to determine which key was used to protect the data an ~~Key~~MTK_ID is included with the protected data. The ~~Key~~MTK_ID will uniquely identify the MSK and contain other information needed to calculate the MTK.

MTK_ID is composed of the following fields (MBMS_ID~~-~~, MSK_ID , MTK_RAND, MTK_SEQ, MTK_MAC) where:

-MBMS_ID~~-~~: Identifies the MBMS service.
-MSK_ID~~-~~: Identifies the ~~high level key (~~MSK~~)~~ to be used to derive the MTK
-MTK_RAND: Value used in the MSK Validation and Generation Function
-MTK_SEQp: Sequence Number to be used in the MSK Validation and Generation Function
-MTK_MAC: MAC value to be used in the MSK Validation and Generation Function

Editor's note: MTK_RAND may become MGK[MTK] depending on the selection for MGV-F.

If the UICC does not have the MSK indicated by MTK_ID, then the ME should fetch the MSK using the methods discussed in the clause 6.2. ~~The MTK is derived according to the methods described in clause 6.3.~~

If the ME does not have the MTK indicated by MTK_ID, then the ME should fetch MTK invoking the Retrieve MTK request as described in 6.3.1

Note: including the ~~Key~~MTK_ID with the protected data stops the UE trying to decrypt and render content for which it does not have the MS~~T~~SK.

The below flow shows how the protected content is delivered to the UE

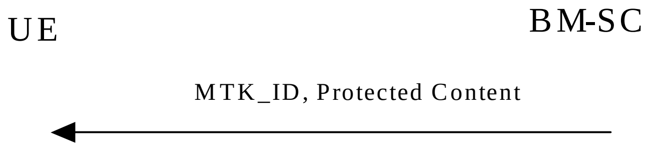
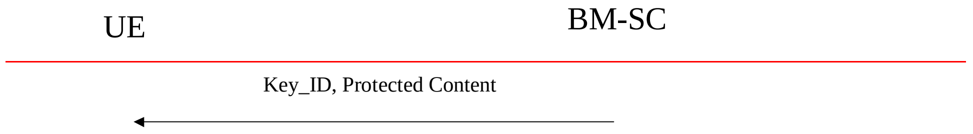


Figure 5: Protected content delivery to the UE



6.3.1 MTK request to the UICC

If the ME does not have the MTK indicated by MTK_ID, it shall ask the UICC to retrieve it using the *Retrieve MTK request* as shown in the following figure:

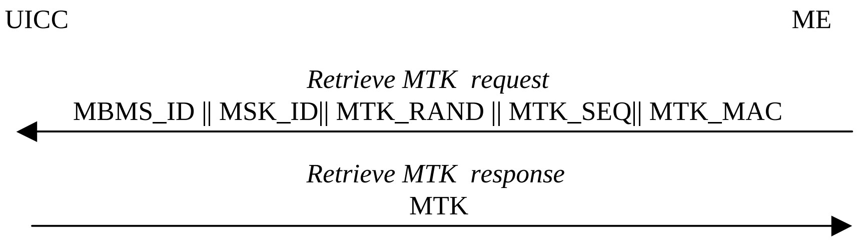


Figure 6: MTK retrieval from the UICC

Editor's note: MTK_RAND may become MGK[MTK] depending on the selection for MGV-F.

The UICC will first search the MSK corresponding to the MBMS_ID, MSK_ID pair.

If the UICC does not have the ~~high level key (~~MSK~~)~~ indicated by MSK_ID, then it shall indicate it to the ME with a corresponding status condition. The UE should then fetch ~~the high level key~~MSK ~~-~~using the methods discussed in the previous clause ~~(clause 6.2).~~

If a correct MBMS_ID, MSK_ID pair is found in the UICC, then~~,~~ the UICC calls~~computes~~ the MTK Generation and Validation Function (MGV-F) using MTK_RAND, MTK_SEQ and MTK_MAC as input values (as described in the following chapter).

As a result, the ME retrieves the corresponding MTK.

After using an MTK to decrypt protected traffic, the UE deletes any older MTK for this multicast service.

Editor's note: this section may contain several protection methods.

Editor's note: if SRTP is chosen, the master key identifier can be used to indicate the current MBMS key whichever key management method is chosen