3GPP TSG-SA3 Meeting #34
Acapulco, Mexico, 6 –9 July 2004

TD ⌘S3-040619

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:	⌘	Key management mechanism		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	09/07/2004
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:	⌘	There is currently no specified way of how key management is to be performed in MBMS. In particular, the way MSK and MTK ends up in the UE is not mentioned.
Summary of change:	⌘	This contribution clearifies how the MSK and MTK should be handeled in MBMS.The key management mechanism specified is agnostic to wheteher the delivered key is to be used for download, streaming or for protecting MTK delivery. It also explains how key derivation is to be done, and how replay protection is to be applied.
Consequences if not approved:	⌘	The key management mechanism will be not be specified.

Clauses affected:	⌘	2, 3.1, 3.2, 6.4, 6.5				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

** NEXT 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: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246 "MBMS User Services"

[6] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "T3-specification describing MBMS application and interface procedures on UICC"

[8] IETF RFC 2617 "HTTP Digest Authentication"

[9] IETF draft-ietf-msec-mikey-08.txt "Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic"

** 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 that 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).

~~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 MGV-F~~F_t~~ with ~~a key derived from~~ the MSK. The key MTK is used to decrypt the received MBMS data on the ME.

MUK = MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect 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~~

3.2 Symbols

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

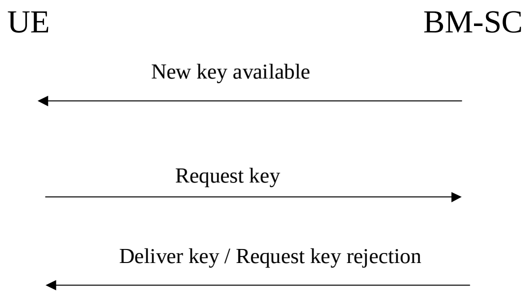
MUK_I	Integrity key derived from key MUK
MUK_C	Confidentiality key derived from key MUK
~~MUK_S~~	~~Salting key derived from key MUK~~
MSK_I	Integrity key derived from key MSK
MSK_C	Confidentiality key derived from key MSK
~~MSK_S~~	~~Salting key derived from key MSK~~
~~F_f~~	~~MFK generation function~~
~~F_g~~	~~MGK generation function~~
~~F_m~~	~~Keyed MAC function used to check the freshness of MTK~~
~~F_t~~	~~MTK generation function~~

*** NEXT CHANGE ***

6.3 Key update procedure

Once a UE has joined a multicast service, the UE should try to get the MSK that will be used to 'protect' the data transmitted as part of this multicast 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 tries to get the MSK using the second message in the below flow.

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.



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 message is used to request an MSK. 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 not have an MSK for that service or has received some protected content and does not have the MSK that was used to protect the content. If the UE fails to get hold of the updated MSK or receive 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 service.

- After receiving the second message the BM-SC should send out the appropriate MSK to the UE 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 UE should store this key for later use.

6.4~~X~~ MIKEY message processing~~ in the UE~~

~~Editor's note: MIKEY was chosen as the method for carrying keys. The use of MIKEY will be based on the proposal in S3-040258.~~

Editor's note: The need for salting keys in processing of MIKEY messages is for further study.

6.4.1 MIKEY common header

MIKEY shall be used with pre-shared keys as described in [9].

MSK:s shall be carried in MIKEY messages with a Data Type value of 0x07 in the MIKEY common header that signals that the message contains an MBMS MSK. This allows legacy MIKEY implementations to discard the message early in the processing stage. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

To keep track of MSK:s and MTK:s, a new Extension Payload is added to MIKEY (see Section 6.3.2). The Extension contains the identities of MSK:s and the MTK:s.

Once the MSK is in place in the UE, the UE can make use of the broadcast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as pre-shared secret. A Data Type value of 0x0~~7~~8 is used in the MIKEY common header to signal that the message contains an MBMS MTK.

If the BM-SC requires an ACK for a key update message this is indicated by setting the V-bit in the MIKEY common header. The UE ~~should~~shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header shall carry the Key Group ID.

~~Shared components~~

~~MBMS services can be composed of several components. For example, there could be a service composed of one video stream associated with an audio stream. Now, imagnine that there is another service that consists of only the audio stream , i.e., the same audio stream is used by both MBMS services. Then the keys used to protect the both services must of course also be the same (it is in fact the same packets being broadcast). Now, to avoid that some one who has payed for the audio-only session gets access to the video stream also, the MSK:s used to protect the audio and video stream must be different. Note that it is up to the BM-SC administrator to make sure that the MSK:s are set up in a way that prohibits unauthorized users to access the streams.~~

6.4.2 Replay protection

Each MIKEY message contains the timestamp field (TS) of type 2. This means that the contents of the timestamp field is a 32-bit counter. The counter is increased by one for each message sent from the BM-SC to the UE. Note that there is one counter per UE for MSK delivery, and one counter common to all UE:s for MTK delivery. The counter is used for replay protection; messages with a counter less than or equal to the current counter are discarded. Less than or equal is to be taken in the meaning of RFC1982. If the less than or equal relation is undefined in the sense of RFC1982, the message should be considered as being replayed. The counter in the TS field shall be reset for MSK transport messages when the MUK is updated. The counter in the TS field shall be reset for MTK transport messages when the MSK is updated.

NOTE: The counter in TS field in MTK transport messages is used to detect replay attacks while the counter in MTK ID field of EXT payload is used to detect the resendings of the same MTK keys.

6.4.3 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in MIKEY [9]. To be able to keep track of the keys, an new general Extension Payload (EXT) is defined that conforms to the structure defined in 6.15 of MIKEY[9]. The ID:s of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is contained in the message. This EXT is incorporated in the MIKEY messages (see Figure 1). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contains a MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. The ~~MSK ID and~~ MTK ID ~~are~~is increased by 1 every time the corresponding key is updated. ~~The ID:s of the involved keys are kept in the EXT, to enable the UE to look up the identityof the key which was used to protect the message, and which key is contained in the message.~~ It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F ~~(which may reside in a UICC, and hence has less computational capacity).~~

The MGV-F (see Section 6.4) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key ID:s ~~shall~~ shall be represented by unsigned integer counters, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be 2^{n} - 1 different keys in use during the same session, where n is the number of bits in the ID field.

Outer Key ID	Inner Key ID

Figure 1. The figure shows the Extension payload used with MIKEY. The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).

6.4.4 MIKEY message structure

6.4.4.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depictedin Figure 2. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent only in the initial MSK delivery message. The ~~optional~~ identity payloads of the initiator's and responder's ID:s shall be included in the MSK transport messages. ID_I is the ID of the BM-SC and ID_r is the ID of the UE. Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK Id~~s~~ and upper limit of MTK ID). The lower limit of the interval defines the SEQs in the MTK Generation and Validation Function.

Editor's note~~NOTE~~: The type (URI or NAI) of identity payloads to use ~~should be specified in stage 3~~are for further study.

Editor's Note: The contents of the Security Policy payload depends on the used security protocols. MIKEY [9] ~~already~~ has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.

~~Editor's Note: It is FFS if Identity payloads for the sender and receiver should be added to the messages. For the MSK delivery the Identity payload would carry the ID of the individual receiver, and for the MTK delivery, the identity of the service should be used~~

Common HDR	Timestamp (counter)
(RAND)	(Security Policy)
EXT	
KEMAC	

Common HDR
Timestamp (counter)
(MIKEY RAND)
ID_I
ID_R
(SP)
EXT
KEMAC

Figure 2. The logical structure of the MIKEY message used to deliver MSK.

~~6.3.6.2~~ 6.4.4.2 MSK Verification message

If the BM-SC expects a response to the MSK-transport message (i.e., the V-bit in the MIKEY common header is equal to 1), the UE shall send a verification message as a response. The verification message shall be constructed according to Section 3.1 of MIKEY, and shall consist of the following fields: HDR || TS || ID_i || ID_r || V, where ID_I is the ID of the BM-SC and ID_r is the ID of the UE. Note that the MAC included in the verification payload~~,~~ shall be computed over both the initiator's and the responder's ID:s as well as the timestamp in addition to be computed over the response message as defined in [9]. The key used in the MAC computation is the MUK_I.

Common HDR
Timestamp (counter)
ID_I
ID_R
V

Figure 3. The logical structure of the MIKEY message used to deliver MSK.

The verification message shall not be sent as a response to MIKEY messages delivering MTK.

The verification message shall be constructed by the ME, except for the MAC field, and then be given to the MGV-F that will perform the MAC computation and will return the verification message appended with the MAC to the ME. The ME shall ~~then copy the MAC received from the MGV-F into the MAC field of the verification payload, and~~ send the message to the BM-SC.

6.4.4.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 3. The actual key that is delivered is kept in the KEMAC payload. The identity payloads shall not be used in MTK~~L~~ transport messages.

~~Editor's Note: It is FFS if Identity payloads for the sender and receiver should be added to the messages. For the MSK delivery the Identity payload would carry the ID of the individual receiver, and for the MTK delivery, the identity of the service should be used~~

Common HDR
Timestamp (counter)
EXT
KEMAC

Common HDR	Timestamp (counter)
~~EXT~~	
KEMAC	

Figure 4~~3~~. The logical structure of the MIKEY message used to deliver MTK.

6.4.5 Processing of received messages in the UE

6.4.5.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ~~terminal~~ME, the processing proceeds following the steps below (basically following Section 5.3 of [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MSK delivery, the MUK ID is extracted from the Extension Payload.

2. TheTimestamp Payload is checked, and the message is discarded if the Counter is larger or equal to the current MIKEY replay counter associated with the given MUK (the Counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in sense of RFC1982 [10].

3. The Security Policy payload is stored if it was present.

4. The message is transported to MGV-F for further processing, cf 6.54.

5. The MGV-F replies success or failure.

6.4.5.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the terminal, the processing proceeds following the steps below (basically following Section 5.3 of [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MT~~S~~K delivery, the MS~~U~~K ID is extracted from the Extension Payload.

2. TheTimestamp Payload is checked, and the message is discarded if the Counter is larger or equal to the current MIKEY replay counter associated with the given M~~U~~SK (the Counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in sense of RFC1982 [10].

3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID ~~counter ~~(kept in the ~~terminal~~ME), the message must be discarded.

4. The message is transported to MGV-F for further processing, cf 6.54.

5. The MGV-F replies success (i.e. sending the MTK) or failure.

6.5. ~~4 ~~Validation and key derivation functions in MGV-F

6.5.0 General

It is assumed that the UE includes 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. The MGV-F is implemented inside MGV-S.

> Editor's note: The choice between MIKEY key derivation algorithms and other suitable key derivations has not been made as there could be algorithms already in the UE.

~~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.~~

~~It is good practice to use different keys for encryption and integrity protection. To achieve this MBMS makes use of MIKEY's cryptographical means for key derivation of a single delivered key. MIKEY shall be used to deliver a TEK (MIKEY terminology for Traffic Encryption Key), which will be split into several keys in the UE (and in the BM-SC). The key derivation is defined in Section 4.1.4 of MIKEY. Some security protocols can perform this splitting of keys themselves, and hence they are to be given only the plain MTK. Note that it is only the MTK that requires this kind of key derivation. The MSK is used as shared secret in the MIKEY protocol for the MTK delivery, and is split internally in MIKEY as described in section 4.14 of MIKEY.~~

6.54.1 MUK derivation

When a MUK has been installed in the MGV-S, ie.eg. as a result of a GBA run,~~. I~~it is used as pre-shared secret together with the MIKEY-RAND and the ~~component ID~~Key Group ID from the MIKEY message to derive encryption~~, salting~~ andintegrity keys (MUK_C~~,~~ ~~MUK_S ~~and MUK_I) as defined in Section 4.1.4 of MIKEY. MUK_I and MUK_C are used to verify the integrity of the MSK transport ~~MIKEY ~~message, and decrypt the key carried in the KEMAC payload ~~as defined in Section 4.1.4 of MIKEY~~.

6.54.2 MSK validation and derivation

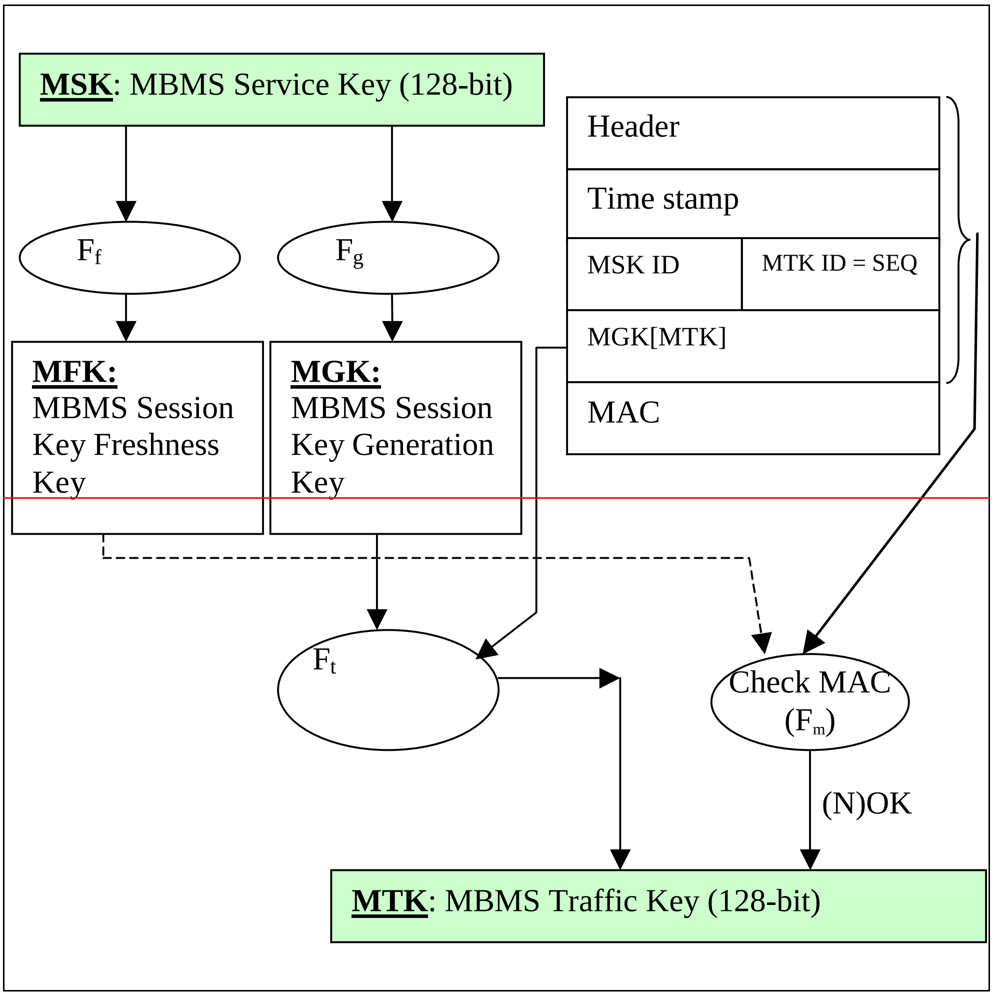
When ~~T~~the MGV-F~~ takes~~ receives the MIKEY message ~~as input. I~~it first determines the type of message by reading the ~~Key~~Data Type field in the ~~KEMAC payload~~common header. If the key in the message is an MSK, MGV-F retrieves the MUK with the ID given by the Extension payload.

The MAC in the KEMAC payload is verified using MUK_I, and the message is discarded upon failure. If the MAC verification is successful the MUK_C ~~and MUK_S ~~is used to decrypt the Key Data sub-payload, and the MSK can be installed in the key management module. The MSK is used as pre-shared secret together with the MIKEY-RAND and the ~~component ~~Key Group ID from the MIKEY message to derive (as specified in section 4.1.4 of [9]) encryption~~, salting ~~and integrity keys (MSK_I and~~,~~ MSK_C~~ and MSK_S~~) ~~to verify the integrity of the MIKEY message, and decrypt the key carried in the KEMAC payload. ~~The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval ~~is~~defines the~~-~~SEQs.

> ~~Note~~NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. ~~only ~~to update the Key Validity data.

The MGV-F shall update in MGV-S the Counter value in the Time Stamp ~~Header~~ payload ~~Counter~~ associated with the corresponding MUK ID.

~~6.4 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 1: MTK Validation and Generation Function~~

~~*MTK Generation and Validation Function)* (MGV-F) that is realized as part of the ME or as part of the UICC~~

6.54.3 MTK validation and derivation

~~The~~When the MGV-F ~~takes~~ receives the MIKEY message, ~~(including e.g. MSK ID, MTK ID = SEQp, MSK[MTK], MAC) as input. I~~it first determines the type of message by reading the ~~Key~~Data Type field in the ~~KEMAC payload~~ common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

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~~MSK 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, MGK[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. ~~The MAC in the KEMAC~~

~~payload is verified using MSK_I, and the message is discarded upon failure. If the MAC verification is successful the MSK_C and MSK_S is used to decrypt the Key Data sub-payload. 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 as defined in [9] using ~~a keyed MAC function F_m with~~ the received MIKEY message and MSK_I~~the 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 SEQs with SEQp value and start with the generation of MTK. The MGV-F provides the MTK to the ME.

The MGV-F shall update in MGV-S the Counter value in the Time Stamp ~~Header~~payload ~~Counter~~ associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in Section 4.1.3 of MIKEY [9].