3GPP TSG SA WG3 Security — S3#37 **S3-050136**
21 - 25 February 2005
Sophia Antipolis, France

Title: LS on MBMS work progress
Release: Rel-6
Work Item: MBMS

Source: SA3
To: TSG CT6

Contact Person:
Name: **Jacques Seif**
Tel. Number: +33 146007228
E-mail Address: jacques.seif@axalto.com

Attachments: S3-050115, S3-050117, S3-050133

---

1. Overall Description:

3GPP TSG SA WG3 would like to inform 3GPP TSG CT WG6 about changes made to TS 33.246 (Security of Multimedia Broadcast/Multicast Service) at SA3#37.

Several change requests to TS 33.246 have been agreed by SA3 to complete SA3 MBMS work. As some of these CRs impact the MBMS functionality specified in CT6, further CT6's work is needed to finalize the Rel-6 MBMS service.

2. Actions:

To T3 group.

ACTION: 3GPP TSG SA WG3 kindly asks 3GPP TSG CT WG6 to consider the attached SA3 CRs on MBMS in order to make the appropriate changes to their specification.

3. Date of Next TSG SA WG 3 Meetings:

TSG-SA3 Meeting #38	25-29 April 2005	Geneva, Switzerland
TSG-SA3 Meeting #39	28 June - 1 July 2005	Toronto, Canada

3GPP TSG-SA WG3 Meeting #37 ***Tdoc ⌘S3-050115***
Sophia Antipolis, France, February 21-25, 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **038** ⌘ **rev** **2** ⌘ Current version: **6.1.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarify MUK key synchronisation for MSK push procedure	
Source:	⌘	SA WG3	
Work item code:	⌘	MBMS	***Date:*** ⌘ 18/02/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	It may happen that the UE has already generated a new MUK/MRK pair (after a GBA run and the subsequent application NAF derivation step) but the BM-SC was never informed. From the BM-SC point of view his known MUK/MRK pair may still be valid (lifetime has not expired), hence this MUK-ID can still be used within the MSK push procedure. While the UE has already installed a new MUK-ID, the BM-SC is using an old MUK for protecting the MSK push MIKEY messages. The UE behavior for this mismatch case is not specified. A similar handling as for the push solicited pull procedure is proposed. For the push solicit pull, the BM-SC is allowed to use a MUK-ID beyond the SA-lifetime (differently than the last generated one). This MUK-ID is known to the UE as the last-successfully used.
Summary of change:	⌘	Clarify the UE behavior when receiving a normal MIKEY push message with an old (still valid) MUK-ID. The UE shall handle the MIKEY push message in a similar way as the push solicited pull message. This guarantees that the UE contacts the BM-SC with the B-TID. Subsequently the MSK is pushed again to the UE (yet with the newer MUK). Clarify the handling of two MUKs within the UE.
Consequences if not approved:	⌘	UE's may behave differently which may result in non-optimized MSK handling.

Clauses affected:	⌘	6.1, 6.3.2.1			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	TS 31.102
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘				

===== BEGIN CHANGE =====

6.1 Using GBA for MBMS

TS 33.220 [6] (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS Multicast User service.

Before a user can access an MBMS User service, the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within clause 5 of TS 33.220 [6]. The BM-SC will act as a NAF (Network Application Function) according to TS 33.220 [6].

The MSKs for an MBMS User service shall be stored on either the UICC if the UICC is capable of MBMS key management or the ME if the UICC is not capable of MBMS key management.

Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions.

As a result of a GBA_U run, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. This key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK (MBMS User Key) to protect MSK (MBMS Service Key) deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK (MBMS Request Key) within the protocols as described within clause 6.2.

A run of GBA_ME results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK. The key MUK is used to protect MSK deliveries to the ME as described within clause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within clause 6.2.

The MUK is identified by the combination of B-TID and NAF-ID and the MRK is defined by B-TID, where B-TID and NAF-ID are defined as specified in TS 33.220 [6].

In the UE two different MUKs, i.e. the last generated and the last successfully used, are used to guarantee that the UE and the BM-SC share always one MUK. The last generated MUK is replaced immediately after when a new MUK is generated and the last successfully used MUK is updated after the successful reception of the MIKEY message, which is protected using the last generated MUK. The usage of MUKs is described within clause 6.3.

For ME based key management:

- All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC is inserted. Therefore the ME needs to store in non-volatile memory the last inserted UICC-identity to be able to compare that with the used UICC-identity at UICC insertion and power on.

- All MBMS keys (MRK, MSK and MTK) may be deleted from the ME when the ME is powered down. If the ME does not delete the MBMS keys at power down then the MBMS keys need to be stored in non-volatile memory. The ME should store the MUKs in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedure (see clause 6.3.2.2.4).

NOTE: If the ME deletes the MSK at power down, then the MBMS client would need to request MSK to the BM-SC and may need to run GBA to reconvene an MBMS session.

===== END CHANGE =====

===== BEGIN CHANGE =====

6.3.2.3 MSK push procedures

6.3.2.3.1 Pushing the MSKs to the UE

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.

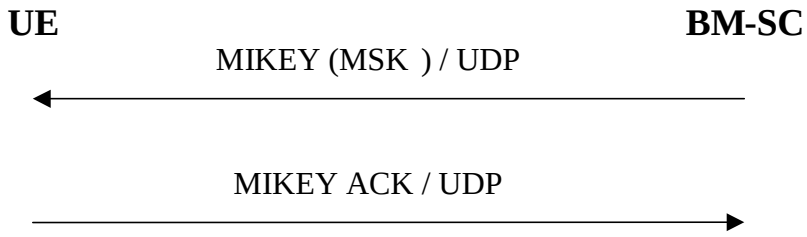


Figure 6.3: Pushing the MSKs to the UE

When the BM-SC decides that it is time to update the MSK, the BM-SC sends MIKEY message over UDP transporting the requested MSKs to the UE.

If requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

When an MSK push MIKEY message is not directly preceded by an MSK key request, then it may happen that the BM-SC uses a still valid MUK that is not the last generated MUK at the UE. The UE shall handle such a MIKEY push message in a similar way as the push solicited pull MIKEY message (i.e. upon a successfull integrity check the UE shall initiate an MSK request with the specified Key Group). Additionally, in this case, the UE shall not create a MIKEY acknowledgement message.

NOTE: This procedure guarantees that the UE contacts the BM-SC with the last B-TID, such that the UE now receives a MIKEY push message with the last generated MUK. The integrity of the initial pushed MIKEY message can be verified at the UE with the MUK-ID that is known as the last succesfully used BM-SC MUK-ID.

6.3.2.3.2 Void

===== END CHANGE =====

3GPP TSG-SA WG3 Meeting #37
Sophia Antipolis, France, February 21-25, 2005

Tdoc ⌘ S3-050117

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **037** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correct the MSK verification message handling
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	21/02/2005
Category:	⌘	**F**
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	The verification by the UICC that the inserted Time Stamp Field in the -to be signed-MIKEY packet shall match the previously handled MSK update procedure restricts the ME handling. It will cause an error if the ME would handle multiple MSK Update messages before generating the MSK verification messages. Furthermore the error handling in case the Time Stamp check would fail, is unspecified yet. From a security point of view, it has to be ensured that the ME cannot ask the UICC to sign arbitrary messages.
Summary of change:	⌘	Correct the description of MSK verification message handling for Time stamp handling. The two procedures 'MSK Update' and 'MSK verification' are combined into one procedure.
Consequences if not approved:	⌘	Parallel handling of MSK update message is not possible. More error situations for MSK updates/verification handling. A malicious ME may let the UICC sign (arbitrary) message when not needed.

Clauses affected:	⌘	6.4.5.2, Annex D

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications	⌘	TS 31.102
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

===== BEGIN CHANGE =====

6.4.5.2 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 || IDr || V, where IDr 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 as well as the timestamp in addition to be computed over the response message as defined in RFC 3830 [9]. The key used in the MAC computation is the MUK_I.

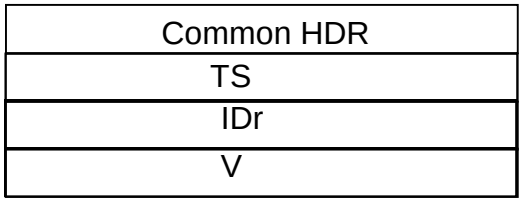


Figure 6.6: The logical structure of the MIKEY Verification message

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 send the verification message, when received as result from the MGV-F, ~~–~~to the BM-SC.

===== END CHANGE =====

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

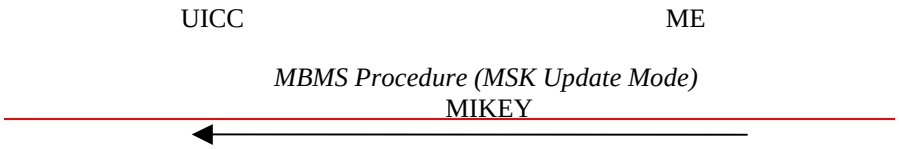
This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F).

The ME has previously performed a GBA_U bootstrapping procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF together with the NAF_Id associated with this particular bootstrapping procedure.

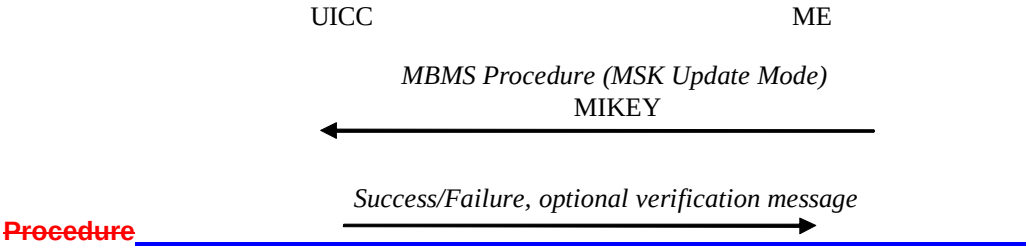
The ME receives a MIKEY message containing an MSK update ~~procedure~~. After performing some validity checks, the ME sends the whole message to the UICC. The UICC uses the MUK ID (included in the MIKEY message, see clause 6.1) to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in clause 6.5.3).

After successful MSK Update procedure the UICC stores the Key Domain ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).



~~Figure D.1: MSK Update~~



~~Procedure~~

Figure D.1: MSK Update Procedure

In case the MSK update MIKEY message is acceptable (i.e. the received MSK ID corresponds to the last generated MUK in the UE, and the MSK Update procedure has been performed successfully) and the V-bit was set in the HDR, then a MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message) shall be produced. The UICC uses the same MUK ID and TS, which were received from the MSK MIKEY Message (see clause 6.1), for the MSK Verification Message Generation.

D.2 Void

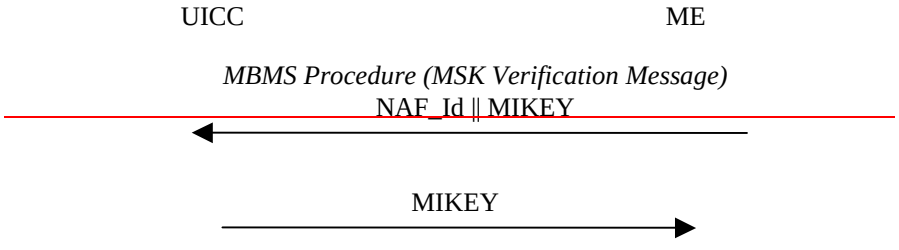
~~MSK Verification Message Generation~~

~~This procedure is part of the MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message).~~

~~The ME constructs the verification message in response to the MSK transport message when it is required by BM-SC.~~

~~The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC and the ME shall include NAF_id in this message. The UICC uses the MUK ID (see clause 6.1) to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation.~~

~~The UICC will verify that the Time Stamp MIKEY field correspond to the previous MSK Update procedure. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in clause 6.4.5.2. (MSK Verification message).~~



~~Figure D.2: MSK Verification Message~~

D.3 MTK generation and validation

This procedure is part of the MTK generation and validation function as described in clause 6.5.4 (MTK validation and derivation).

The ME receives the MIKEY message (containing Header, Time stamp, Key Domain ID, MSK ID, MTK ID = SEQp, MSK_C[MTK||Salt (if salt is available)] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in clause 6.5. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

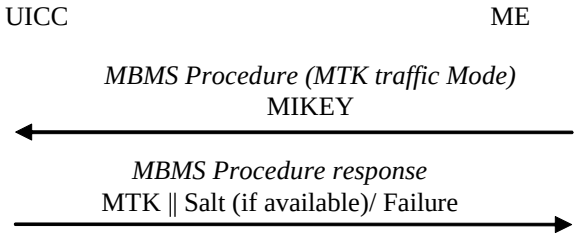


Figure D.3: MTK Generation and Validation

===== END CHANGE =====

3GPP TSG-SA WG3 Meeting S3#37
Sophia, France, 21-25 February, 2005

Tdoc ⌘S3-050133

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **047** ⌘**rev** **1** ⌘ Current version: **6.1.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘ Clarification of MSK and MTK procedures		
Source:	⌘ SA WG3		
Work item code:	⌘ MBMS	***Date:*** ⌘	24/2/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change: ⌘ It is unclear when the key management is initiated/terminated. Therefore Registration and deregistration procedures are introduced.
In addition the reliability mechanisms of MTK deliveries are underspecified.
It may happen that the UE has generated a MUK/MRK pair but the BM -SC was not informed. The UE shall store the last MUK successfully used by the BM-SC in case that the BM-SC does not use the last generated MUK for protecting the BM-SC solicited pull MIKEY message. Consequently, only one MUK can exist for the BM-SC (the last generated MUK) and two MUKs can exist for the UE: the last generated MUK and the MUK that was last successfully used by the BM-SC.

In the current description of the BM-SC solicited pull procedure the terms “last MUK” or “last used MUK” or “last known MUK” are equally used, some clarification on the usage of the MUK is required.
Current TS 33.246 allows the UE to request only the current MSK from the BM-SC. This is done by setting the Key Number part of MSK-ID to zero. However, there are likely to be situations where the UE should be able to ask for other MSK s than the current one. An example of such a situation could be where the UE has downloaded two objects that are protected with different MSKs. If the UE has missed the push key update of the first object, the UE has no means to request the corresponding MSK.
Additionally, in order to avoid that many UEs request a specific MSK at the same time and therefore cause congestion, UEs should re-use the “back-off” mechanism that is used within ‘Associated delivery procedures’ in TS 26.346. Usage of this mechanism should be optional to use but mandatory to implement. This is indicated in the Service Announcement information.

Summary of change: ⌘ The following issues are clarified:

-
- MSK procedures are clarified to include MSK request and MSK delivery procedure
- it is clarified that key management is not initiated if both confidentiality and integrity protection are indicated to be ‘off’ in the service announcement
- reliability of MTK messages in streaming is based on repetition and on

		FLUTE features in download • Clarify the usage of the MUK in the BM-SC solicited pull procedure. UEs are able to request specific MSKs from the BM-SC, i.e. Key Number is set to specific value (other than zero). • UEs should use the back-off mechanism specified in TS 26.346 to avoid that many UEs request the MSK at the same time.
Consequences if not approved:	⌘	Unclear specification and possible interoperability problems. Terms used to refer to the MUK in the BM-SC solicited pull procedure are misleading.

Clauses affected:	⌘	6.3, 6.3.1, 6.3.2, 6.3.2.1, 6.3.2.1A (new), 6.3.2.1B (new), 6.3.2.2, 6.3.2.2.1 - 6.3.2.2.4, 6.3.2.3, 6.3.2.3.1, 6.3.3.2, 6.3.3.2.1, 6.3.3.2.2, 6.4.6.1, 6.4.6.2, 6.5.1, 6.5.2, 6.5.3, 6.6.1
Other specs Affected:	⌘	Y N Y Other core specifications ⌘ TS 26.346, TS 31.102 N Test specifications N O&M Specifications
Other comments:	⌘	

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

6.3 Key ~~update~~ management procedures

Editor's Note: The contents of the http client payloads are FFS and may require input from TSG SA WG4.

6.3.1 General

In order to protect an MBMS User service, it is necessary to ~~transfer~~ deliver both MSKs and MTKs from the BM-SC to the UE.

MSK procedures are further divided to MSK request procedures, described in clause 6.3.2.2, and MSK delivery procedure, described in clause 6.3.2.3. MSK procedures use a point-to-point bearer. MSK procedures are similar for both streaming and download services. ~~Clause 6.3.2 describes the possible procedures for transferring MSKs, while clause 6.3.3 deals with the transfer of MTKs.~~

The BM-SC may also refrain from sending the MSK update message to the UE and let the UE request for the MSK. This may be needed in some download services where the UE fetches the MSK after receiving encrypted download object. In this case the back-off mode as described in 6.3.2.2.2 shall be used if present within the Service Announcement.

MTK delivery procedures use the MBMS bearer. MTK delivery procedures are different for streaming and download services and they are described in clause 6.3.3.

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

6.3.2 MSK procedures

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Key Domain ID MSK ID

where

Key Domain ID = MCC || MNC and is 3 bytes long.

MSK ID is 4 bytes long and with byte 0 and 1 containing the Key Group part, and byte 2 and 3 containing the Key Number part. The Key Number part is used to distinguish MSKs that have the same Key Domain ID and Key Group part. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted. The MSK ID is carried in the extension payload of MIKEY extension payload.

NOTE: It needs to be ensured that the Key Group parts are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group value.

If the UE receives an MSK and already contains two other MSKs under the same Key Domain ID and Key Group part, then the UE shall delete the older of these two MSKs.

~~Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.~~

6.3.2.1A MBMS User Service Registration procedure

When a UE has received MBMS User Service information via User Service Discovery / Announcement procedures describing a MBMS User Service and the user has triggered the activation of that User Service, the UE should register to the MBMS User Service.

NOTE: The User Service Discovery / Announcement procedures are specified in TS 26.346 [13]. It is out of the scope of the present specification how the UE receives the User Service information and how the User Service is triggered in the UE.

The UE shall receive the following information via the User Service Discovery / Announcement procedures:

- Fully qualified domain name of the key management server (i.e. the BM-SC). This is for the UE to know to which IP address to send the MSK request.
- Confidentiality protection: on / off.
- Integrity protection: on / off.
- UICC key management required: yes/ no.
- Identifiers of the MSKs needed for the User Service.

  The Key Number part of the MSK ID(s) shall be set to 0x0 to denote the current MSK. Specific Key Number values are not used in Service Announcement since they may change over time and Key Group part of MSK ID is sufficient to identify the MSKs, see clause 6.3.2.1.
- Mapping information how the MSKs are used to protect the different User Service Sessions.
- Back off mode parameters, as defined in [13], may be specified in association with each MSK ID if wanted by the service provider. The Back off mode is used to avoid congestion in MSK requests. The Back off mode is optional to implement in the BM-SC and mandatory to implement in the UE. The UE shall use Back off mode if it is requested by the BM-SC in the Service Announcement.

If the MBMS User Service does not require any MBMS data protection (i.e. if security description is not present in the Service Announcement or if both confidentiality and integrity protection are indicated 'off'), the UE shall not register for key management purposes.

In case the UICC key management is required, the UE should only try to access the MBMS user service if the used UICC application is capable of MBMS key management.

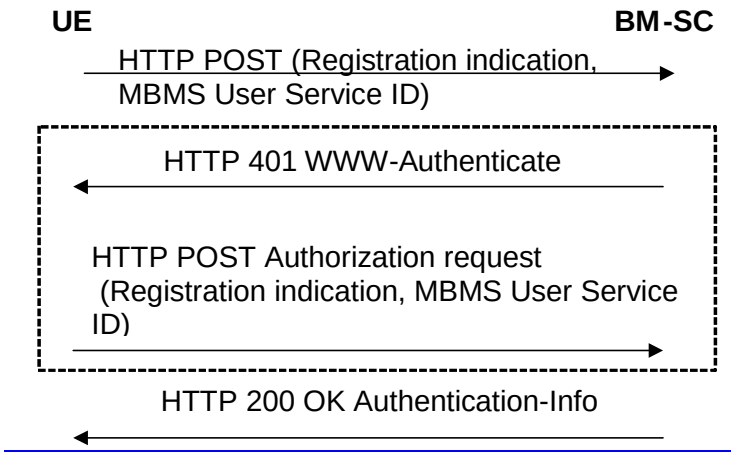


Figure 6.x: MBMS User service registration procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest using bootstrapped security association as described in clause 6.2.1 of this specification.

The UE sends a registration request for the MBMS User Service using the HTTP POST message to the BM-SC Key Request function. The following information shall be included in the HTTP message.

- Indication that the UE requests to register to the MBMS User Service;
- MBMS User Service ID.

The BM-SC Key Request function authenticates the UE with HTTP Digest using MRK key as described in clause 6.2.1.

If the authentication is successful, the BM-SC Key Request function verifies from the BM-SC Membership function whether the UE is authorized to register to the MBMS User Service specified in the request. If the UE is authorized, the BM-SC Key Request function registers the UE to the MBMS User Service, which means that the UE is registered to receive the MSKs used in this MBMS User Service. The BM-SC Key Request function sends a HTTP 200 OK message with Authentication-Info header to the UE.

NOTE: The BM-SC may not need to challenge the UE (dashed box in Figure 6.x), if the UE has used WWW Authorization request headers in the first message in Figure 6.1 and BM-SC is able to authenticate the UE.

If the authentication fails, the BM-SC Key Request function resends HTTP 401 Authorization required message with the WWW-Authenticate header.

The UE checks the validity of the HTTP response message. If the message indicated failure, the UE may retry to register to the MBMS User Service. Further error cases are described in Annex F.2.4.

If the HTTP procedure above resulted to success, the BM-SC Key Distribution function initiates MSK delivery procedure(s) as specified in clause 6.3.2.3.

NOTE: The time between the MBMS User Service Registration procedure and MSK delivery procedure may vary, i.e. the UE should not expect the MSK delivery procedures to start immediately.

6.3.2.1B MBMS User Service Deregistration procedure

When the UE desires to deregister from an MBMS User Service, it shall indicate this to the BM-SC.

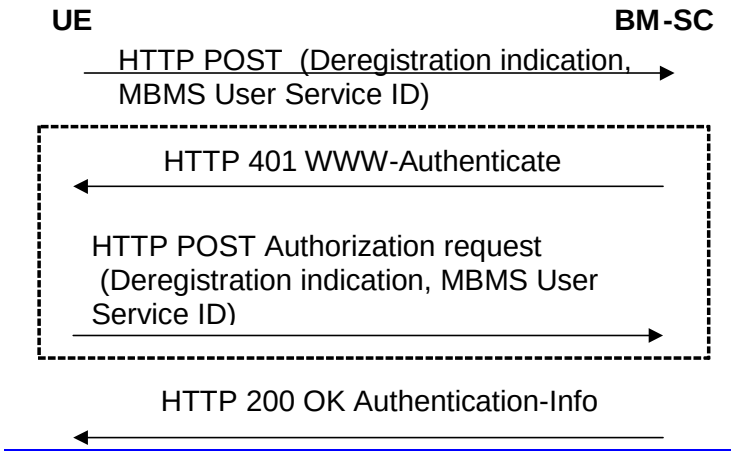


Figure 6.x1: MBMS User service deregistration procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest using bootstrapped security association as described in clause 6.2.1 of this specification.

The UE sends a deregistration request for the MBMS User Service using the HTTP POST message to the BM-SC Key Request function. The following information shall be included in the HTTP message.

- Indication that the UE requests to deregister from the MBMS User Service;
- MBMS User Service ID.

The BM-SC Key Request function authenticates the UE with HTTP Digest using MRK key as described in clause 6.2.1.

If the authentication is successful, the BM-SC Key Request function deregisters the UE from the MBMS User Service, which means that the UE will no longer receive the MSKs used in this MBMS User Service. The BM-SC Key Request function sends a HTTP 200 OK message with Authentication-Info header.

NOTE: The BM-SC may not need to challenge the UE (dashed box in Figure 6.x), if the UE has used WWW Authorization request headers in the first message in Figure 6.1 and BM-SC is able to authenticate the UE.

If the authentication fails then the BM-SC Key Request function resends HTTP 401 Authorization required message with the WWW-Authenticate header.

The UE checks the validity of the HTTP response message. Error cases are described in Annex F.2.4.

The BM-SC should invalidate those MSKs from the UE, which are not used by any other MBMS User Services where the UE is registered. The BM-SC Key Distribution function performs this by running MSK delivery procedure for each MSK, where the Key Validity data is set to invalid value (cf. clause 6.3.2.3), i.e. SEQl is greater than SEQu.

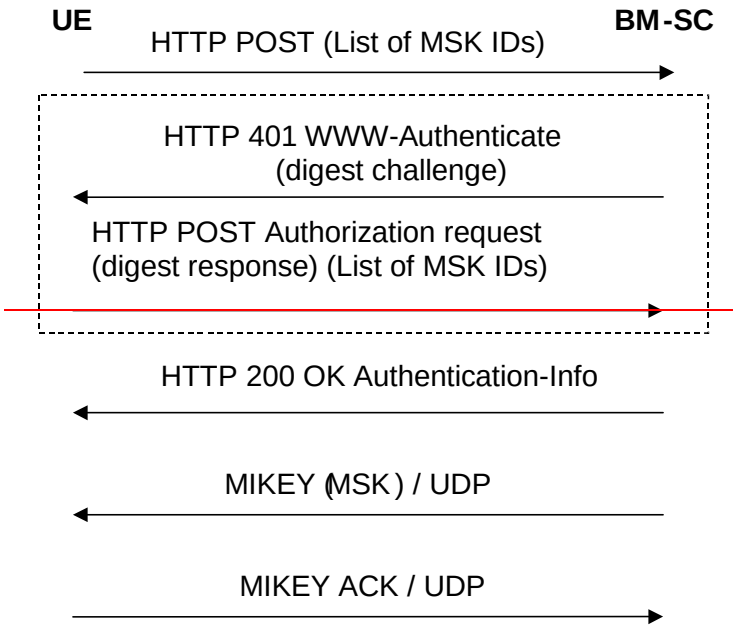
6.3.2.2 MSK ~~retrieval~~ request procedures

6.3.2.2.1 Basic MSK ~~retrieval~~ request procedure

When a UE detects that it needs the MSK(s) for a specific MBMS User service, the UE should try to get the MSKs that will be used to protect the data transmitted as part of this User Service. In the MSK request the UE shall list the MSK IDs for which the UE needs the MSK(s).

The basic MSK ~~retrieval~~ request procedure is a part of different other procedures, e.g.:

- initiation of key management when the UE has joined the MBMS user service;
- ~~retrieval~~ request of MSK(s) when the UE has missed a key update procedure e.g. due to being out of coverage.
- BM-SC solicited pull.



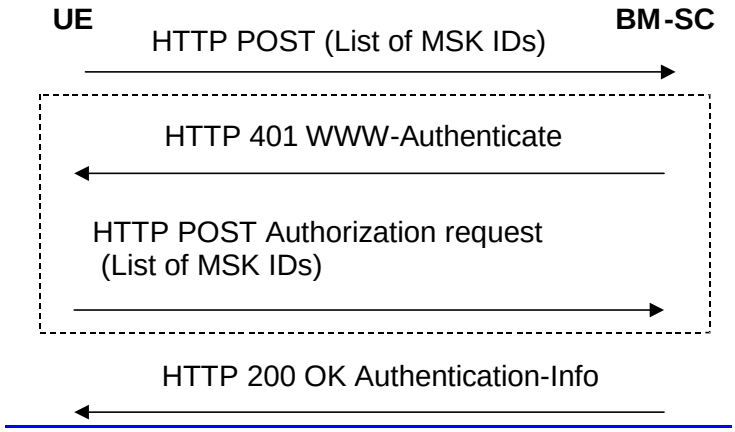


Figure 6.1: Basic MSK ~~retrieval~~ request procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest using bootstrapped security association as described in clause 6.2.1 of this specification.

The UE requests for the MSKs using ~~WITH~~ the HTTP POST message. The following information is included in the HTTP message.

- key identification information: a list of MSK IDs.

~~NOTE:~~ UEs may request specific MSKs by setting the Key Number part of the MSK ID to the requested value. When the Key Number part of the MSK ID is set to 0x0, this means the current MSK, see clause 6.3.2.1.

Editors' Note: The exact syntax of the HTTP request message, e.g. possible XML schema of the request parameters in the client payload and its MIME type are to be specified in stage 3.

The BM-SC Key Request function authenticates the UE with HTTP Digest using the keys received from GBA as described in clause 6.2.1.

If the authentication is successful, the BM-SC Key Request function verifies whether the UE is registered to any MBMS User Service that uses the MSKs specified in the request. If the UE is authorized, the BM-SC Key Distribution

function shall deliver requested MSKs to the UE (cf. clause 6.3.2.3). The BM-SC sends a HTTP 200 OK message with Authentication-Info header.

~~and verifies that the subscriber is authorized to receive the MSKs for this service.~~

NOTE: The BM-SC may not need to challenge the UE (dashed box in Figure 6.1), if the UE has used WWW Authorization request headers in the first message in Figure 6.1 and BM-SC is able to authenticate the UE.

~~If the authentication is successful then the BM-SC sends a HTTP 200 OK message with Authentication-Info header.~~ If the authentication fails then the BM-SC Key Request function resends HTTP 401 Authorization required message with the WWW-Authenticate header.

Editors' Note: The exact syntax of the HTTP response message, e.g. possible XML schema of the success or failure parameters in the client payload and its MIME type are to be specified in stage 3.

The UE checks the validity of the HTTP response message. If the message indicated failure, the UE may retry or leave the MBMS User Service.

If the HTTP procedure above resulted to success, the BM-SC Key Distribution function initiates MSK delivery procedure as specified in clause 6.3.2.3.

NOTE: The time between the MSK request procedure and MSK delivery procedure may vary, i.e. the UE should not expect the MSK delivery procedures to start immediately. ~~MIKEY message procedures over UDP transporting the requested MSKs to the UE.~~

~~If it was requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.~~

~~If the UE fails to get hold of the MSK or receives no 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~~

6.3.2.2.2 Void~~Initiation of key management~~

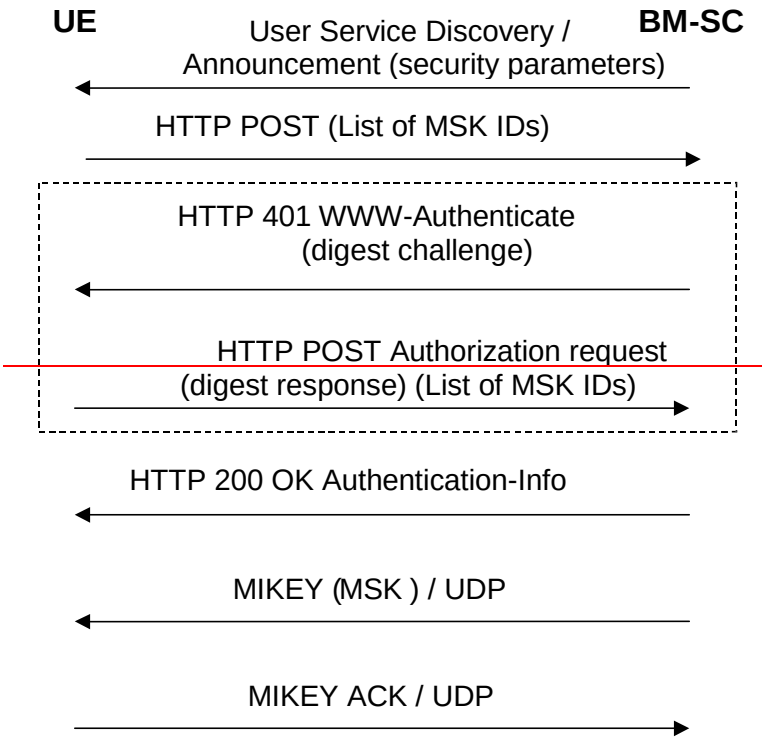
~~When a UE has received User Service information via User Service Discovery / Announcement procedures describing a MBMS User Service and the user has triggered the activation of that User Service, the UE should try to get the MSK(s) that will be used to protect the data transmitted as part of this User Service.~~

~~NOTE: The User Service Discovery / Announcement procedures are specified in TS 26.346 [13]. It is out of the scope of the present specification how the UE receives the User Service information and how the User Service is triggered in the UE.~~

~~The UE shall receive the following information via the User Service Discovery / Announcement procedures:~~

- ~~Fully qualified domain name of the key management server (i.e. the BM-SC). This for the UE to know to which IP address to send the MSK request.~~
- ~~Confidentiality protection: on / off.~~
- ~~Integrity protection: on / off.~~
- ~~UICC key management required: yes/ no.~~
- ~~Identifiers of the MSKs needed for the User Service.~~
- ~~The Key Number part of the MSK ID(s) shall be set to 0x0 to denote the current MSK. Specific Key Number values are not used since they may change over time and Key Group part of MSK ID is sufficient to identify the MSKs, see clause 6.3.2.1.~~
- ~~Mapping information how the MSKs are used to protect the different User Service Sessions.~~

~~Editors' Note: The exact syntax of the service announcement information including security parameters, e.g. possible XML schema of the parameters and its MIME type are to be specified in SA4.~~



~~**Figure 6.2a: MSK retrieval procedure**~~

~~In case the UICC key management is required, the UE should only try to access the MBMS user service if the used UICC application is capable of MBMS key management.~~

~~The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest as described in clause 6.2.1 of this specification.~~

~~The UE requests for the MSKs using with the HTTP POST message.~~

~~The rest of the procedure is the same as in clause 6.3.2.3.1.~~

6.3.2.2.3 Missed key update procedure

When the UE has missed an MSK update and it detects that it has not got the current MSK, e.g. from the received traffic, it may trigger the retrieval of the current MSK from the BM-SC. The procedure is the same as the Basic MSK Retrieval procedure in clause 6.3.2.2~~3~~.1.

6.3.2.2.4 BM-SC solicited pull

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC Key Distribution function solicits the UE to contact the BM-SC and request for new MSK. An example of such a situation is when the BM-SC Key Distribution function wants the UE to trigger a UE that it needs to update the MSK.

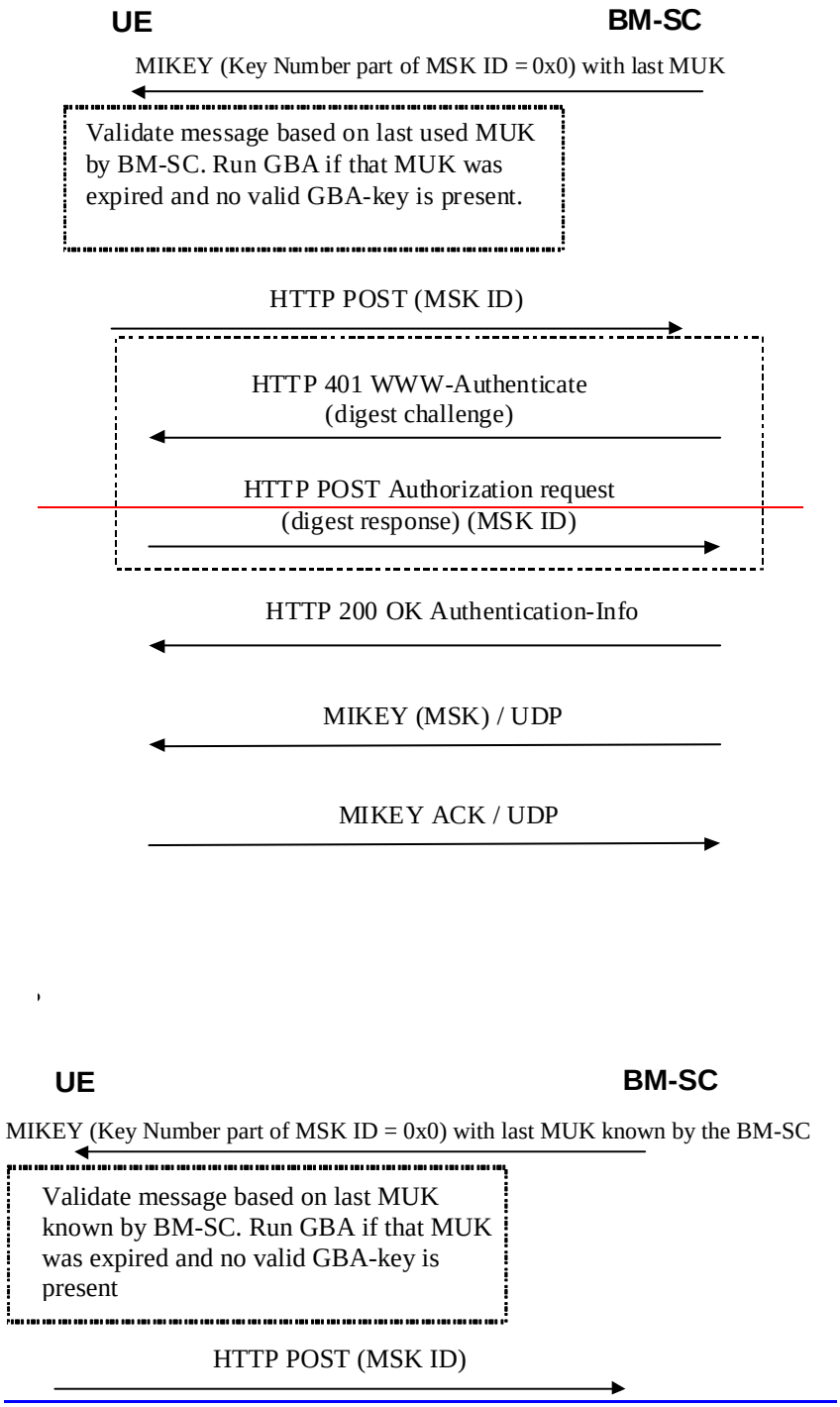


Figure 6.2b: BM-SC solicited pull

The BM-SC Key Distribution function sends a MIKEY message over UDP to the UE. The MIKEY message shall be protected by the ~~most recent~~ last MUK known by the BM-SC. The Key Number part of the MSK ID in the extension payload of the MIKEY message shall be set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

If the received MUK_ID (i.e. the last MUK known by the BM-SC) does not correspond to the last MUK known by the UE, then the UE checks the solicited pull MIKEY message with the last MUK successfully used by the BM-SC.

The BM-SC shall not set the V-bit in the common header when initiating the BM-SC solicited pull procedure.

NOTE 1: A MUK may be used by the BM-SC Key Distribution function beyond the GBA key lifetime of the corresponding Ks_xx_NAF for the purpose of using the MUK within the first MIKEY message of a push solicited pull procedure.

NOTE 2: Since the integrity of the MIKEY message still needs to be assured, a KEMAC payload shall be included in the MIKEY message from the BM-SC Key Distribution function. There is however no key present in the message. Thus by setting the Encr data len field to zero, only the MAC of the message will be included.

When receiving the message, the UE shall request for the current MSK for the specified Key Group as specified in clause 6.3.2.2.1. ~~The BM-SC may trigger re-authentication of the UE or even re-run of GBA procedure to update the MUK as is described in TS 33.220 [6].~~

~~The rest of the procedure is the same as in clause 6.3.2.3.1.~~

6.3.2.3 MSK ~~push~~ delivery procedures

6.3.2.3.1 Pushing the MSK~~s~~ to the UE

The BM-SC Key Distribution function controls when the MSKs used in a ~~multicast~~ MBMS user service are to be changed. The below flow describes how MSK changes are performed. This procedure can be initiated after the UE has requested for MSK(s) as described in clause 6.3.2.2.

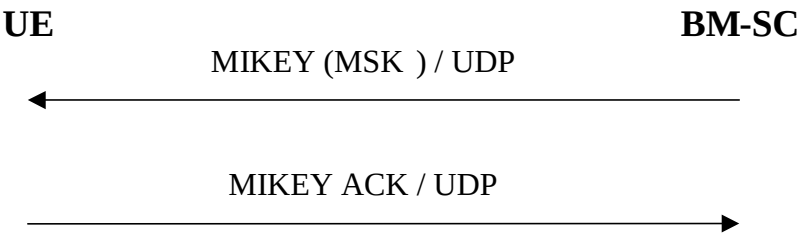


Figure 6.3: Pushing the MSKs to the UE

When the BM-SC Key Distribution function decides that it is time to update the MSK, the BM-SC Key Distribution function sends MIKEY message over UDP transporting the requested MSK~~s~~ to the UE.

If requested by the BM-SC Key Distribution function, the UE sends a MIKEY acknowledgement message to the BM-SC.

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

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

6.3.3.2 MTK update procedure

The MTK is delivered to the UE using MIKEY over UDP, ~~as in 6.3.2.3.1~~ but the ~~MIKEY ACK is not used~~V-bit in the common header shall not be set.

6.3.3.2.1 MTK delivery in download

In the download case the MIKEY message carrying the MTK shall be delivered over the same FLUTE stream as the object to be downloaded to the UE (see TS 26.346 [13]). This means that the message is specified as a separate object in the FLUTE File Delivery Table (FDT), having its own identifier. This means the MTK delivery inherits the reliability features of FLUTE. The mime-type of the object carrying the MIKEY message shall be the IANA-registered type for MIKEY.

6.3.3.2.12 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent using the same IP destination address as the RTP traffic. MIKEY messages shall be transported to UDP port number 2269 specified for MIKEY. Reliability of MTK delivery is reached

by re-sending MTK messages periodically. In order to increase the possibility that UEs receive a new MTK in time, MTK messages may be sent before the RTP traffic changes over to a new MTK.

Editor's Note: The UDP port number needs to be specified for MIKEY.

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

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (EXT) is examined, and if it indicates an MSK delivery protected with MUK, the MUK ID is received by combining IDi and IDr.
2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is smaller or equal to the stored replay counter associated with the given MUK (the stored replay counter value is retrieved from MGV-S). To avoid issues with wrap around of the ~~ID~~ Timestamp payload field~~s~~ "smaller than" should be in the sense of RFC 1982 [10].
3. The Security Policy payload is stored if it was present.
4. The message is transported to MGV-F for further processing, cf clause 6.5.2.
5. The MGV-F replies success or failure.

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (EXT) is examined, and if it indicates an MTK delivery protected with MSK, the MSK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is smaller or equal to the stored replay counter associated with the given MSK (the stored replay counter value is retrieved from MGV-S). To avoid issues with wrap around of the ~~ID~~ Timestamp payload field~~s~~ ``smaller than´´ should be in the sense of RFC 1982 [10].
3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.
4. The message is transported to MGV-F for further processing, cf 6.5.3.
5. The MGV-F replies success (i.e. sending the MTK and salt if available) or failure.

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

6.5.1 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.~~ When an MSK or MTK message is received in the UE, it is processed in protected environment 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.

6.5.2 Usage of MUK ~~derivation~~

When a MUK has been installed in the MGV-S, i.e. as a result of a GBA run, it is used as pre-shared secret used to verify the integrity of the MSK transport message and decrypt the key carried in the KEMAC payload as described in RFC 3830 [9].

6.5.3 MSK processing

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the EXT. If the key in the message is an MSK protected by MUK, MGV-F retrieves the MUK identified as specified in clause 6.1.

The integrity of the message is validated and the MSK is extracted from the KEMAC payload as described in section 5 of reference [9] if the validation is successful. The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval defines the SEQs.

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

If the MGV-F receives an MSK message, which has the same MSK ID as a stored MSK, the new MSK shall replace the old MSK. In case the message does not include any key in KEMAC payload, the Key Validity data shall be updated for the specified MSK.

If message validation is successful, then the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MUK ID.

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

6.6.1 General

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 Session and Transmission Function. In order to determine which key was used to protect the data key identification information is included with the protected data. The key identification information will uniquely identify the MSK and MTK. The MTK is processed according to the methods described in clauses 6.4 and 6.5. Whenever data from an MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

NOTE: Including the key identification information with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.