TSGS#27(05)0143

Source: SA WG3

Title: Eighteen CRs to TS 33.246 (Rel-6)

Document for: Approval

Agenda Item: 7.3.3

The following CRs were agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-050143	33.246	034	2	Rel-6	Storing SP payload after MSK message is verified	F	6.1.0	S3-050166	MBMS
SP-050143	33.246	035	1	Rel-6	ME based MBMS key derivation for ME based MBMS key management	C	6.1.0	S3-050162	MBMS
SP-050143	33.246	037	1	Rel-6	Correct the MSK verification message handling	F	6.1.0	S3-050117	MBMS
SP-050143	33.246	038	2	Rel-6	Clarify MUK key synchronisation for MSK push procedure	C	6.1.0	S3-050115	MBMS
SP-050143	33.246	039	-	Rel-6	Add missing parts of CR33 (SA3#36)	F	6.1.0	S3-050074	MBMS
SP-050143	33.246	042	-	Rel-6	Annex D.1: correction of the description of the GBA run	F	6.1.0	S3-050078	MBMS
SP-050143	33.246	043	1	Rel-6	Alignment according to MIKEY related IETF work	C	6.1.0	S3-050114	MBMS
SP-050143	33.246	044	1	Rel-6	Clarification of HTTP procedures	C	6.1.0	S3-050130	MBMS
SP-050143	33.246	045	1	Rel-6	Usage of security policy payload	C	6.1.0	S3-050135	MBMS
SP-050143	33.246	047	1	Rel-6	Clarification of MSK and MTK procedures	C	6.1.0	S3-050133	MBMS
SP-050143	33.246	049	2	Rel-6	MGV-F functionality related to MTK-ID upper limit	C	6.1.0	S3-050163	MBMS
SP-050143	33.246	051	1	Rel-6	Using the term "MBMS User Service" instead of "multicast"	D	6.1.0	S3-050132	MBMS
SP-050143	33.246	052	1	Rel-6	Introduction of BM-SC subfunctions	C	6.1.0	S3-050134	MBMS
SP-050143	33.246	053	-	Rel-6	Removing IDi from MTK message	C	6.1.0	S3-050092	MBMS
SP-050143	33.246	054	2	Rel-6	MBMS download protection details	C	6.1.0	S3-050154	MBMS
SP-050143	33.246	055	1	Rel-6	Removal of Editors notes	F	6.1.0	S3-050116	MBMS
SP-050143	33.246	056	-	Rel-6	Protection of MBMS Service Announcement sent over MBMS bearer	C	6.1.0	S3-050124	MBMS
SP-050143	33.246	057	-	Rel-6	Introduction of missing abbreviations, symbols and defintions	D	6.1.0	S3-050137	MBMS

Tdoc ⌘*S3-0500166*

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **034** ⌘ **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⌘ ☐ ME [X] Radio Access Network ☐ Core Network ☐

Title:	⌘	Storing SP payload after MSK message is verified
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	10/01/2005
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:	⌘	It is insecure to store SP payload in ME before MSK message is verified. SP payload should be stored in ME after MSK message is verified.
Summary of change:	⌘	Changing the corresponding description in clause 6.4.6.1.
Consequences if not approved:	⌘	The procedure of MSK message reception in ME is insecure.

Clauses affected:	⌘	6.4.6.1

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

Other comments: ⌘

*** BEGIN OF 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 fields "smaller than" should be in the sense of RFC 1982 [10].
3. The Security Policy payload is stored temporarily in the ME 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. In case of success the temporarily stored Security Policy payload is taken into use. Otherwise it is deleted.

*** END OF CHANGE ***

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

Tdoc ⌘S3-050162

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **035** ⌘ **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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	ME based MBMS key derivation for ME based MBMS key management
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	14/02/2005
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:	⌘	The details how MRK and MUK are derived for ME based MBMS key management are missing
Summary of change:	⌘	The MRK is derived from Ks_NAF by using the GBA's key derivation function defined in TS 33.220. The MUK is equal to Ks_NAF.
Consequences if not approved:	⌘	It is not specified how MRK and MUK are derived for ME based MBMS key management.

Clauses affected:	⌘	6.1, 6.2, Annex F (new)

Other specs affected: ⌘	Y	N		⌘
		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. Both the BM-SC and the ME use the key Ks_NAF as MUK. ~~This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and t~~The key MRK is derived from the key Ks_NAF by the BM-SC and the ME as specified in Annex F of this specification. 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].

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.

6.2 Authentication and authorisation of a user

~~Editor's Note: The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs.~~

Editor's Note: According to S3-040212, SA4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the download repair service.

===== BEGIN NEXT CHANGE =====

Annex F (Normative): MRK key derivation for ME based MBMS key management

The MRK shall be derived from the key Ks_NAF using the GBA key derivation function (see TS 33.220 [6], Annex B) as follows (see notation style is explained in TS 33.220, Annex B):

- FC = 0x01,
- P0 = "mbms-mrk" (i.e. 0x6d 0x62 0x6d 0x73 0x2d 0x6d 0x72 0x6b), and
- L0 = length of P0 is 8 octets (i.e., 0x00 0x08).

The Key to be used in key derivation shall be:

- Ks_NAF (i.e. NAF specific key) as specified in TS 33.220 [6].

In summary, the MRK shall be derived from the Ks_NAF, and static string "mbms-mrk" as follows:

- MRK = KDF (Ks_NAF, "mbms-mrk").

===== 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:	⌘	SA WG3
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.

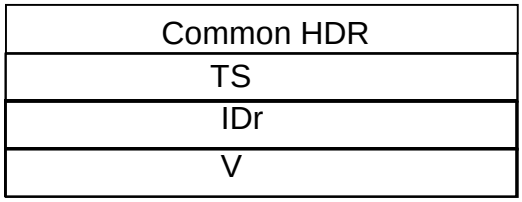


Figure 6.6: The logical structure of the MIKEY Verification message

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

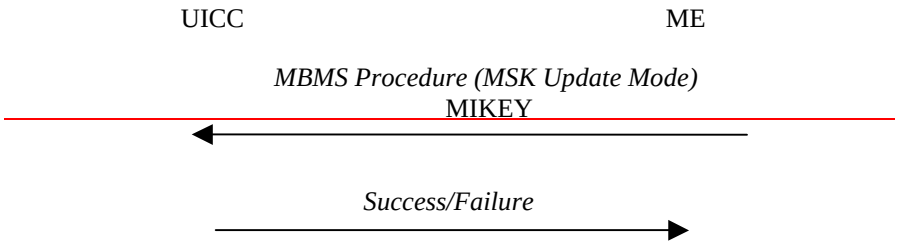
This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F).

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~~

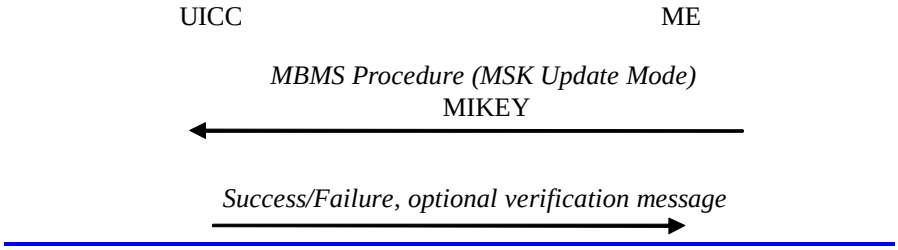


Figure D.1: MSK Update Procedure

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

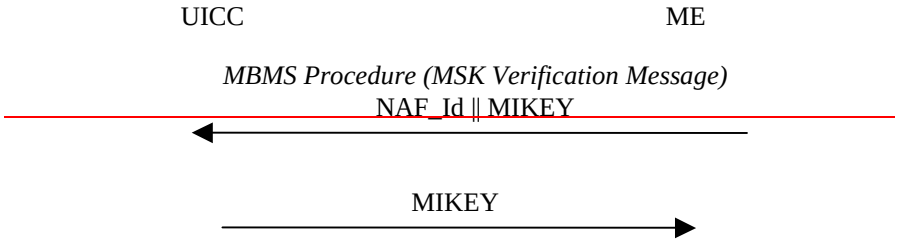
~~MSK Verification Message Generation~~

~~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.

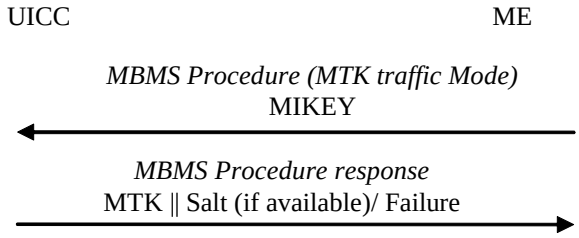


Figure D.3: MTK Generation and Validation

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

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

Tdoc ⌘S3-050115

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: X — Other core specifications ⌘ TS 31.102 Y: — N: X — Test specifications Y: — N: 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.

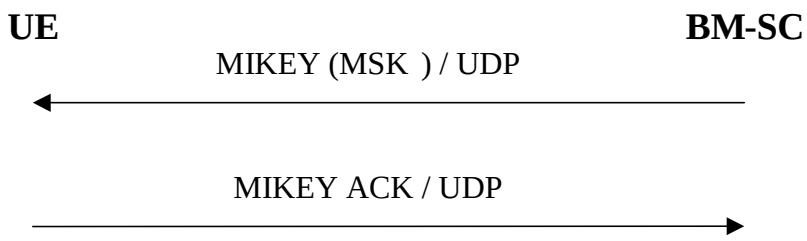


Figure 6.3: Pushing the MSKs to the UE

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 successful 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 successfully 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 ⌘S3-050074

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **039** ⌘ **rev** **-** ⌘ 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:	⌘	Add missing parts of CR33 (SA3#36)
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	14/02/2005
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 change from “Key Group Id” to “Key Group part of MSK ID” was not consistently done through the whole specification in CR 33rev1(Approved at SA3#36) Add the NOTE about Key Group Part which was agreed at SA3#36 (S3-040997), but was forgotten when several proposed CRs were redrafted into CR33
Summary of change:	⌘	Change the “Key Group ID” to “Key Group Part” in the forgotten clauses. Add forgotten NOTE.
Consequences if not approved:	⌘	Inconsistent terminology, missing NOTE

Clauses affected:	⌘	4.2, 6.3.2.1, 6.3.3.1

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

⌘

Other comments: ⌘

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

4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different MBMS Streaming/Download Sessions that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Streaming/Download Sessions, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Streaming/Download Sessions ~~,~~ as specified within clauses 6.5 and 6.6. MSKs and MTKs are managed at the MBMS User Service Level.

There shall be only one MSK and MTK in use with the same ~~in one~~ Key Group part of MSK ID~~ID~~. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) with the same ~~in a~~ Key Group part of MSK ID~~ID~~ shall not be allowed.

The use of the same MTK (this implies also the same MSK) with two different transport services (or user services) should be avoided.

NOTE 1: This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic, i.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. It shall be possible for MBMS User Services to share one or more MSKs for the shared Transport Services with other MBMS User Services.

NOTE 2: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.

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

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

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.

NOTE: When MCC || MNC is used as key identifier, the UE should not try to use it in another context, e.g. the UE should not compare the received MCC || MNC to parameters in radio level.

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.

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

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

6.3.3.1 MTK identification

Every MTK is uniquely identifiable by its Key Domain ID, MSK ID and MTK ID

where

Key Domain ID, and MSK ID are as defined in clause 6.3.2.1.

MTK ID is 2 bytes long sequence number and is used to distinguish MTKs that have the same Key Domain ID ~~Network ID, Key Group ID~~ and MSK ID. It is carried in the MTK-ID field of MIKEY extension payload. The MTK ID shall be increased every time the MTK is updated. The MTK ID shall be reset every time the MSK is updated.

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

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

Tdoc ⌘S3-050078

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **042** ⌘ **rev** **-** ⌘ 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:	⌘	Annex D.1: correction of the description of the GBA run
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	10/02/2005
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 keys MUK and MRK are derived from the GBA keys. The Ks_int_NAF key is shared by the BM-SC and the UICC and results from a GBA_U NAF Derivation procedure. The Annex D.1 indicates that "*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*." This description shall be modified to indicate that: • Ks_int_NAF results from a GBA_U Bootstrapping procedure and a subsequent NAF Derivation procedure (and not the GBA_U bootstrapping procedure only) • The UICC stores Ks_int_NAF and associated B-TID together with NAF-ID
Summary of change:	⌘	Correction of the description of the GBA run in Annex D.1 .
Consequences if not approved:	⌘	The current description of the GBA run in the MSK Update procedure is not accurate.

Clauses affected:	⌘	Annex D .1
Other specs affected:	⌘	Y: [ ] N: [X] Other core specifications Y: [ ] N: [X] Test specifications Y: [ ] N: [X] O&M Specifications
Other comments:	⌘	

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 and a subsequent GBA_U NAF Derivation procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF and associated B-TID 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 ME also includes in this request NAF_Id 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 Network ID, Key Group ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

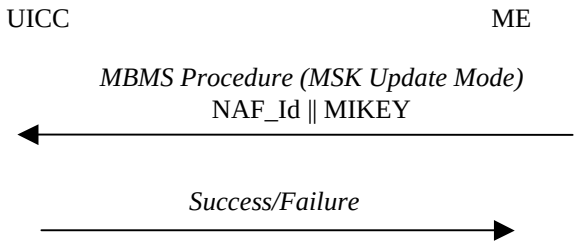


Figure D.1: MSK Update Procedure

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

Tdoc ⌘S3-050114

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **043** ⌘ **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:	⌘	Alignment according to MIKEY related IETF work
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	14/2/2005
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:	⌘	MIKEY IETF draft has been updated.
Summary of change:	⌘	Removed some editor's notes about pending IETF work and added UDP port number for MIKEY.
Consequences if not approved:	⌘	TS is not aligned with IETF draft

Clauses affected:	⌘	2, 6.3.3.2.2, 6.4.1, 6.4.4

Other specs Affected:	Y	N		
⌘		N	Other core specifications	⌘
		N	Test specifications	
		N	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: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] IETF RFC 2617 "HTTP Digest Authentication".

[9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic".

[11] IETF RFC 3711 "Secure Real-time Transport Protocol".

[12] 3GPP TS 43.020: "Security related network functions".

[13] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".

[14] 3GPP TS 33.210: "Network domain security; IP network layer security".

[15] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org

[16] IETF internet draft: "The Key ID Information Type for the General Extension Payload in MIKEY" <draft-~~carrara~~msec-newtype-keyid-0~~0~~1.txt>.

[xx] Port numbers at IANA, http://www.iana.org/assignments/port-numbers

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

6.3.3.2.~~1~~2 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent using the same IP address as the RTP traffic. MIKEY messages shall be transported to UDP port number specified for MIKEY.

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

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

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9]. The UDP port number for MIKEY is 2269 [xx]

To keep track of MSKs and MTKs, a new Extension Payload (EXT) [16] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (see clauses 6.3.2 and 6.3.3).

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the key that is derived in the message, a general Extension Payload (EXT) with Type field value x is used that conforms to the structure defined in reference [16].

Editor's Note: The type value will be replaced by value requested from IANA.

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see figure 6.4a. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see figure 6.4b.

~~Editor's Note: The Key Domain ID needs to be added to [16]. It may need an extension payload type of its own.~~

See~~.~~ clauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MTK ID is increased every time the corresponding key is updated. 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.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integers, 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.

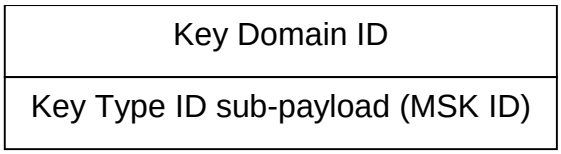


Figure 6.4a: Extension payload used with MIKEY MSK message

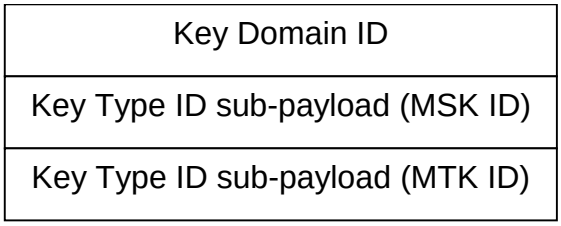


Figure 6.b: Extension payload used with MIKEY MTK message

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

Tdoc ⌘S3-050130

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **044** ⌘ **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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification of HTTP procedures
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	23/2/2005
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:	⌘	The details of HTTP procedures for MSK request have not been specified for MBMS security. In addition HTTP digest authentication has been underspecified.
Summary of change:	⌘	The details of HTTP procedures are added as annexes to 33.246. This includes details for MBMS User Service Registration, MBMS User Service Deregistration and MSK request procedures. It is proposed that the definition of HTTP payload in XML is specified in SA4 TS 26.346. HTTP digest authentication is clarified and necessary references are added to TS 24.109 for applicable parts that describe the details of HTTP digest authentication. In addition, all text regarding application level joining is removed since SA4 TS does not have such procedure.
Consequences if not approved:	⌘	HTTP procedures will remain underspecified and unclear.

Clauses affected:	⌘	2, 6.2, 6.2.1, 6.2.1.1-6.2.1.3 (new), 6.2.3, 6.2.4, 6.3, 6.3.1, 6.3.2.2.1, Annex F (new), Annex G (new)

		Y	N			
Other specs Affected:	⌘	Y		Other core specifications	⌘	TS 26.346
			N	Test specifications		
			N	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: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] IETF RFC 2617 "HTTP Digest Authentication".

[9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic".

[11] IETF RFC 3711 "Secure Real-time Transport Protocol".

[12] 3GPP TS 43.020: "Security related network functions".

[13] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".

[14] 3GPP TS 33.210: "Network domain security; IP network layer security".

[15] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org

[16] IETF internet draft: "The Key ID Information Type for the General Extension Payload in MIKEY" <draft-carrara-newtype-keyid-00.txt>.

[xx] 3GPP TS 24.109: "Bootstrapping interface Ub and network application function interface Ua".

[yy] IETF RFC 2616 " Hypertext Transfer Protocol -- HTTP/1.1".

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

6.2 Authentication and authorisation of a user

Editor's Note: The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs.

~~Editor's Note: According to S3-040212, SA4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the download repair service.~~

6.2.1 Authentication and authorisation in ~~application level joining~~HTTP procedures

6.2.1.1 General

This chapter describes authentication when using HTTP digest with bootstrapped security associations.

6.2.1.2 Bootstrapping

The BM-SC shall implement Bootstrapping procedure over Ub, Initiation of bootstrapping and Bootstrapping renegotiation procedures over Ua as specified in TS 33.220 [6] and in clause 4 and clause 5.2 of TS 24.109 [xx]. The Ua interface procedures shall use MRK.

6.2.1.3 HTTP digest authentication

When the ~~user wants to join (or leave) an MBMS user service~~UE initiates an HTTP procedure towards the BM-SC, ~~it shall use~~ HTTP digest authentication as defined in RFC 2617 [8] shall be used for mutual authentication. HTTP digest is run between BM-SC and ME. The MBMS authentication procedure is based on the general user authentication procedure over Ua interface that is specified in clause "Procedures using the bootstrapped Security Association" in TS 33.220 [6]. The BM-SC will act as a NAF according to TS 33.220 [6]. The details of HTTP digest authentication are specified in clause 5.2 of [xx].

The following adaptations apply to HTTP digest:

- the ~~transaction identifier~~B-TID as specified in TS 33.220 [6] is used as username;
- MRK (MBMS Request Key) is used as password;
- ~~the joined MBMS user service is specified in client payload of~~

All HTTP ~~Digest message~~ procedures within this specification including the associated delivery procedures in TS 26.346 [13] shall be integrity protected with HTTP digest as specified in this clause.

~~Editor's Note: The contents of the client payload are FFS and may require input from TSG SA WG4. The final decision on application level join and leave procedures relies of work in SA4.~~

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

6.2.3 Void~~Authentication and authorisation in MSK request~~

~~When the UE requests MSK(s), the UE shall be authenticated with HTTP digest as in clause 6.2.1.~~

6.2.4 Void~~Authentication and authorisation in post delivery procedures~~

~~When the UE requests post delivery procedures, the UE shall be authenticated with HTTP digest as in clause 6.2.1.~~

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

6.3 Key update 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 both MSKs and MTKs from the BM-SC to the UE. Clause 6.3.2 describes the possible procedures for transferring MSKs, while clause 6.3.3 deals with the transfer of MTKs.

The details of the HTTP procedures and HTTP error situations are specified in Annex F. An example of detailed MSK request procedure is described in Annex G. The XML schema of the HTTP payload is specified in [13].

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

6.3.2.2.1 Basic MSK retrieval 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 procedure is a part of different other procedures, e.g.:

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

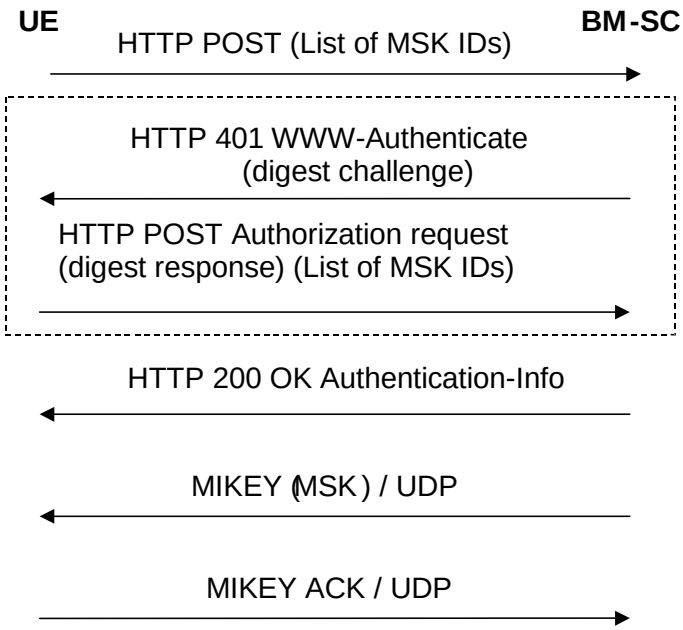


Figure 6.1: Basic MSK retrieval procedure

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 WITH the HTTP POST message. The following information is included in the HTTP message.

- key identification information: a list of MSK IDs.

NOTE: 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~~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~~ TS 26.346 [13].

The BM-SC authenticates the UE with HTTP Digest using the keys received from GBA as described in clause 6.2.1 and verifies that the subscriber is authorized to receive the MSKs for this service.

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 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 User Service.

If the HTTP procedure above resulted to success, the BM-SC initiates 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.

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

Annex F (Normative): HTTP based key management messages

F.1 Introduction

Section 6 specifies the HTTP based key management procedures between the BM-SC and the UE. It specifies that the authentication of these procedures is based on GBA and more specifically on the HTTP Digest authentication as described in clause 6.2 of the present document.

F.2 Key management procedures

This clause contains the following HTTP based procedures:

- MBMS User Service Registration;
- MBMS User Service Deregistration;
- MSK request;

F.2.1 MBMS User Service Registration

The UE shall generate a request for MBMS User Service Registration according to clause 6.3.x.x. The UE shall send the Registration request to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Registration request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [yy];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net/keymanagement)
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "register", i.e. Request-URI takes the form of " /bmsc.home1.net/keymanagement?requesttype= register"
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, e.g. "application/vnd.3gpp.mbms-register+xml ". The XML schema of payload is specified in TS 26.346 [13];
- the HTTP header Content-Length shall be the length of the Base64 encoded Register request in octets; and
- the HTTP payload shall contain the Base64 encoded Register request including the userServiceId of MBMS User Service to which the UE wants to register;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the Base64 encoded Register request for further processing. The BM-SC Key Management function shall verify from BM-SC Membership function that the subscriber is authorized to register to the particular MBMS User Service.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code shall be 200

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

F.2.2 MBMS User Service Deregistration

The UE shall generate a request for MBMS User Service Deregistration according to clause 6.3.x.x. The UE shall send the Deregistration request to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Deregistration request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [yy];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net/keymanagement)
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "deregister", i.e. Request-URI takes the form of " /bmsc.home1.net/keymanagement?requesttype= deregister"
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, e.g. "application/vnd.3gpp.mbms-deregister+xml ". The XML schema of payload is specified in TS 26.346 [13];
- the HTTP header Content-Length shall be the length of the Base64 encoded Deregister request in octets; and
- the HTTP payload shall contain the Base64 encoded Deregister request including the userServiceId of MBMS User Service from which the UE wants to deregister;

- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the Base64 encoded Deregister request for further processing.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code shall be 200

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

F.2.3 MSK request

The UE shall generate a MSK request according to clause 6.3.2.2. The UE shall send the MSK request to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, e.g. MSK request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [yy];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net/keymanagement)
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "msk-request", i.e. Request-URI takes the form of " /bmsc.home1.net/keymanagement?requesttype= msk-request"
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, e.g. "application/vnd.3gpp.mbms-msk+xml ". The XML schema of payload is specified in TS 26.346 [13];
- the HTTP header Content-Length shall be the length of the Base64 encoded MSK request in octets; and
- the HTTP payload shall contain the Base64 encoded MSK request;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the Base64 encoded MSK request for further processing. The BM-SC Key Management function shall verify from the BM-SC Membership function that the subscriber is authorized to receive the particular MSKs.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code shall be 200

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

An example flow of a successful MSK request procedure can be found in Annex G.

F.2.4 Error situations

The key management procedures may not be successful for multiple reasons. The error cases are indicated by using 4xx and 5xx HTTP Status Codes as defined in RFC 2616 [yy]. The 4xx status code indicates that the UE seems to have erred, and the 5xx status code indicates that the BM-SC is aware that it has erred. Possible error situations during key management and their mappings to HTTP Status Codes are described in table F.2.4-1.

NOTE: In table F.2.4-1, the "Description" column describes the error situation in BM-SC. The "BM-SC error" column describes the typical reason for the error.

Table F.2.4-1: HTTP Status Codes used for key management errors

HTTP Status Code	HTTP Error	UE should repeat the request	Description	BM-SC error
400	Bad Request	No	Request could not be understood	Request was missing, or malformed
401	Unauthorized	Yes	Request requires authentication (cf. clause 6.2)	Authentication pending, (cf. clause 6.2)
402	Payment Required	No	Reserved for future use	-
403	Forbidden	No	BM-SC understood the request, but is refusing to fulfil it	The request was valid, but subscriber is not allowed to register to this particular MBMS User Service or UE requested MSK for a MBMS User Service where it was not registered or request contained unacceptable parameters
404	Not Found	No	BM-SC has not found anything matching the Request-URI	The Request-URI was malformed and BM-SC cannot fulfil the request
405	Method not allowed	No	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.	
406 to 417	*	No	Not used by BM-SC	-
500	Internal Server Error	No	Not used by BM-SC	-
501	Not Implemented	No	BM-SC does not support the requested functionality	The server does not contain particular BM-SC service requested
502	Bad Gateway	No	Not used by BM-SC	-
503	Service Unavailable	Yes	BM-SC service is currently unavailable	BM-SC is temporarily unavailable, UE may repeat the request after delay indicated by "Retry-After" header
504	Gateway Timeout	No	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server	The BM-SC did not get response over Zn interface.
505	HTTP Version Not Supported	No	BM-SC does not support the HTTP protocol version that was used in the request line	UE should use HTTP/1.1 version with BM-SC

Annex G (Informative): Signalling flows for MSK procedures

G.1 Scope of signalling flows

This annex gives examples of signalling flows for the key management procedures.

G.2 Signalling flows demonstrating a successful MSK request procedure

G.2.1 Successful MSK request procedure

The signalling flow in figure G.2.1-1 describes the message exchange between UE and BM-SC when UE wants to request MSK.

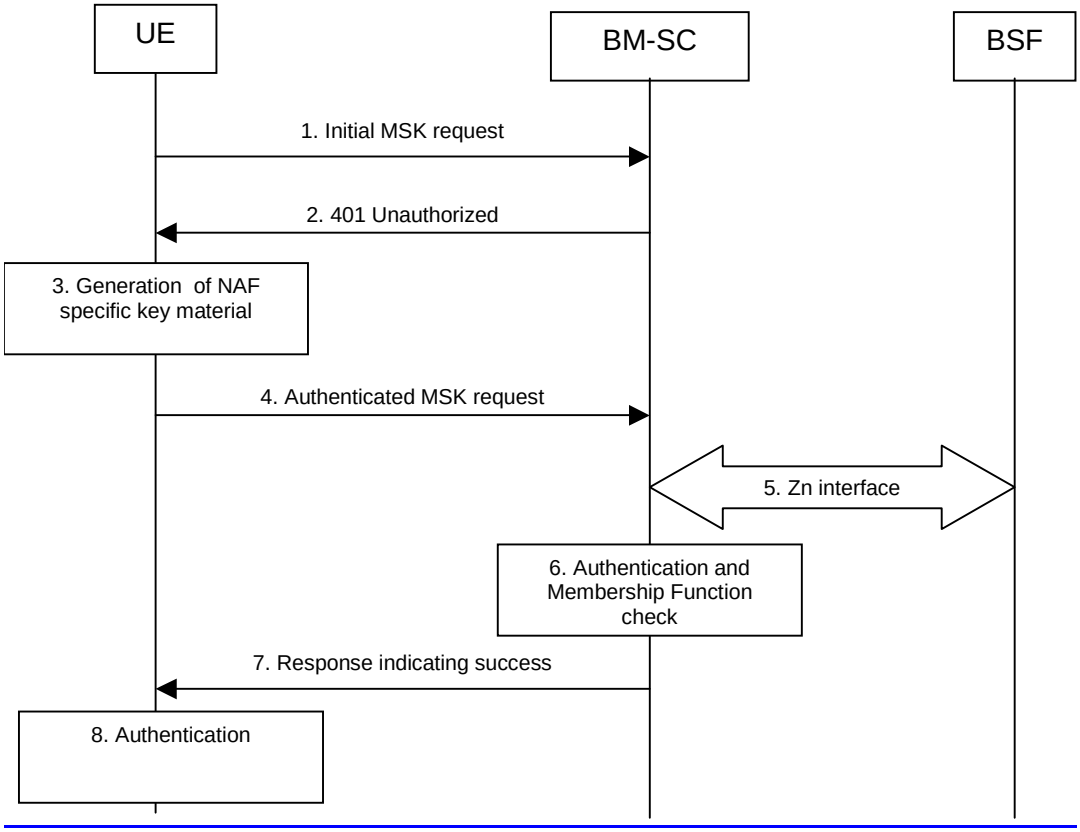


Figure G.2.1-1: Successful MSK request procedure.

1. **Initial MSK request (UE to BM-SC) - see example in table G.2.1-1**

The UE sends an HTTP request to the BM-SC containing a MSK request.

Table G.2.1-1: MSK request (UE to BM-SC)

```
POST /bmsc.home1.net/keymanagement?requesttype=msk-request HTTP/1.1
Host: bmsc.home1.net:1234
Content-Type: application/vnd.3gpp.mbms-msk+xml
Content-Length: (...)
```

```
User-Agent: MBMSAgent; Release-6 3gpp-gba
Date: Thu, 08 Jan 2004 10:50:35 GMT
Accept: */*
Referrer: http://bmsc.home1.net:1234/service

<MSK request BLOB>
```

Request-URI: The Request-URI (the URI that follows the method name, "POST", in the first line) indicates the resource of this POST request. The Request-URI contains the parameter "requesttype " which is set to "msk-request " to indicate to the BM-SC the desired request type, i.e. UE requests for one or several MSKs.

Host: Specifies the Internet host and port number of the BM-SC, obtained from the original URI given by referring resource.

Content-Type: Contains the media type " application/vnd.3gpp.mbms-msk+xml ", i.e. MSK request.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

User-Agent: Contains information about the user agent originating the request and it shall include the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referrer: Allows the user agent to specify the address (URI) of the resource from which the URI for the BM-SC was obtained.

NOTE 1: This step is used to trigger the GBA-based authentication between the UE and the BM-SC.

2. **401 Unauthorized response (BM-SC to UE) - see example in table G.2.1-2**

Upon receiving an HTTP request that contains static string "3gpp-gba" in the User-Agent header the BM-SC responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association.

Table G.2.1-2: 401 Unauthorized response (BM-SC to UE)

```
HTTP/1.1 401 Unauthorized
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Date: Thu, 08 Jan 2004 10:50:35 GMT
WWW-Authenticate: Digest realm="3GPP-bootstrapping@bmsc.home1.net",
nonce="6629fae49393a05397450978507c4ef1", algorithm=MD5, qop="auth,auth-int",
opaque="5ccc069c403ebaf9f0171e9517f30e41"
```

Server: Contains information about the software used by the origin server (BM-SC).

Date: Represents the date and time at which the message was originated.

WWW-Authenticate: The BM-SC challenges the user. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association.

The options for the quality of protection (qop) attribute is by default "auth-int" meaning that the payload of the following HTTP requests and responses should be integrity protected.

The realm attribute contains two parts delimited by "@" sign. The first part is a constant string "3GPP-bootstrapping" instructing the UE to use a bootstrapped security association. The second part is the hostname of the server (i.e. FQDN of the BM-SC).

3. **Generation of NAF specific keys at UE**

The UE verifies that the second part of the realm attribute does correspond to the server it is talking to.

UE derives the NAF specific key material as specified in 3GPP TS 33.220 [6]. UE further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

NOTE 2: If UE does not have a bootstrapped security association available, it will obtain one by running bootstrapping procedure over Ub interface.

4. **Authenticated MSK request (UE to BM-SC) - see example in table G.2.1-3**

UE generates the HTTP request by calculating the Authorization header values using the bootstrapping transaction identifier B-TID it received from the BSF as the username and the MRK (base64 encoded) as the password, and sends the request to BM-SC.

Table G.2.1-3: Authenticated enrolment request (UE to BM-SC)

```
POST /bmsc.home1.net/keymanagement?requesttype=msk-request HTTP/1.1
Host: bm.sc.home1.net:1234
Content-Type: application/vnd.3gpp.mbms-msk+xml
Content-Length: (...)
User-Agent: MBMSAgent; Release-6 3gpp-gba
Date: Thu, 08 Jan 2004 10:50:35 GMT
Accept: */*
Referer: http://bmsc.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@bmsc.home1.net",
nonce="a6332ffd2d234==", uri="/bmsc.home1.net/keymanagement?requesttype=msk-request", qop=auth-int,
nc=00000001, cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5

<MSK request BLOB>
```

Authorization: This carries the response to the authentication challenge received in step 2 along with the username, the realm, the nonce, the URI, the qop, the NC, the cnonce, the response, the opaque, and the algorithm.

The qop attribute is set to "auth-int" by default.

NOTE 3: If step 1 was a POST request then this request would also be a POST request and contain the same client payload in the HTTP request as was carried in step 1.

5. **Zn: NAF specific key procedure**

BM-SC retrieves the NAF specific key material. BM-SC further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

For detailed signalling flows see 3GPP TS 29.109 [xx].

Table G.2.1-4: Bootstrapping authentication information procedure (BM-SC to BSF)

Message source and destination	Zn Information element name	Information Source in GET	Description
NAF to BSF	B-TID	Authorization	The bootstrapping transaction identifier is encoded in the username field according to the Authorization protocol.

6. **Authentication and certificate generation at BM-SC**

BM-SC verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key MRK. BM-SC calculates the corresponding digest values using MRK, and compares the calculated values with the received values in the Authorization header.

The BM-SC also verifies that the hostname (i.e. its FQDN) in the realm attribute matches its own.

If the verification succeeds, the incoming client-payload request is taken in for further processing. The BM-SC continues processing of the MSK request according to its internal policies. The BM-SC verifies that the subscriber is allowed to receive the particular MSK(s) indicated in the MSK request by checking the BM-SC Membership function.

7. **Response indicating success (BM-SC to UE) - see example in table G.2.1-5**

The BM-SC sends 200 OK response to the UE to indicate the success of the authentication and the MSK request. The BM-SC generates a HTTP response. The BM-SC can use key MRK derived from NAF key material to integrity protect and authenticate the response.

NOTE 5: The requested MSK keys are not delivered within the MSK request procedure. They are delivered with a separate MIKEY procedure, see clause 6.3.2.3.

Table G.2.1-5: Successful HTTP response (BM-SC to UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Thu, 08 Jan 2004 10:50:35 GMT
Expires: Fri, 09 Jan 2004 10:50:36 GMT
```

Authentication-Info: This carries the protection

Expires: Gives the date/time after which the response is considered stale.

8. **Authentication at UE**

The UE receives the response and verifies the Authentication-Info header. If the verification succeeds, the UE can regard the MSK request procedure as successful.

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

Tdoc ⌘S3-050135

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **045** ⌘**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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Usage of security policy payload
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	22/2/2005
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:	⌘	Current TS specifies that CS ID map info is present in MTK messages in streaming services to carry the ROC for SRTP, but according to RFC 3830 SP (Security Policy) payload should be also present in this case. However, SP payload is not needed since it is carried in MSK level messages. It is proposed that CS ID Map info is optionally carried, but SP payload is not carried in MTK messages. Also, it is not clear in the TS when SP payload is delivered to the UE and if it is needed for download services since all required parameters are signalled outside of MIKEY. It is proposed that it is mandatory to the BM-SC to send the SP payload when the MSK delivery was triggered by the MSK request procedure and MBMS User Service Registration, otherwise the use of the SP payload in MSK messages is optional.
Summary of change:	⌘	The SP payload is not present in MTK messages although CS ID map info is present. The BM-SC may decide when to attach CS ID map info to MTK messages. It is mandatory to the BM-SC to send the SP payload when the MSK delivery was triggered by MSK request procedure, otherwise the use of SP payload in MSK messages is optional. It is clarified that SP payload is not needed for download services.
Consequences if not approved:	⌘	Unclear usage of SP payload.

Clauses affected:	⌘	6.4.2, 6.4.5.1, 6.4.5.3, 6.6.2.2
Other specs Affected:	⌘	Y N ☐ N Other core specifications ☐ N Test specifications ☐ N O&M Specifications
	⌘	
Other comments:	⌘	

6.4.2 MIKEY common header

MSKs shall be carried in MIKEY messages. 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.

Once the MSK is in place in the UE, the UE can make use of the multicast 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 the pre-shared secret.

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE 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 is not used.

In case of download services, the SP payload is not used and CS ID map type is set to value '1' as defined in [16]. In case of streaming services the CS ID map type is set to value '0' as defined in RFC 3830 [9]

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

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. 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 in all the MSK delivery messages. The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC (i.e. NAF-ID) and IDr is the ID of the UE's username (i.e.B-TID). Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The SP payload is used only with streaming services. The BM-SC shall ensure that the UE has received the SP payload before the SP payload needs to be applied in the streaming service. The BM-SC shall include the SP payload when the MSK delivery was triggered by the UE using the MSK request procedure or the MBMS User Service Registration procedure, otherwise it is optional for the BM-SC to include the SP payload into MSK delivery messages. 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 and upper limit of MTK ID). The lower limit of the interval defines the SEQs to be used by the MGV-F (see clause 6.5).

~~Editor's Note: The contents of the Security Policy payload depends on the used security protocols. RFC 3830 [9] (MIKEY) 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.~~

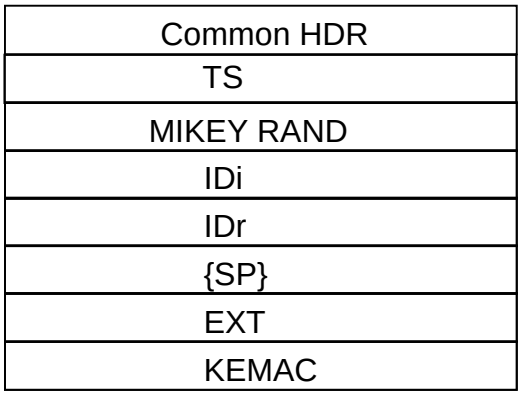


Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

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

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. If MTK is to be used for streaming protection, then a 112 bit salt shall be added to the KEMAC payload in addition to the MTK. The network identity payloads (IDi) shall be used in MTK transport messages. It is optional for the BM-SC to include the current ROC-value within the CS ID map info payload of the MIKEY common header payload in an MTK message. In this case the Policy_no_i and SSRC_i fields should be set to zero by the sender and shall be ignored by the receiver. The SP payload shall not be included in MTK messages.

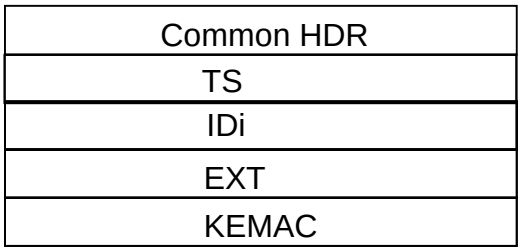


Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

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

6.6.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will retrieve the correct cryptographic context identified by destination transport address, destination port and SSRC (according to RFC 3711 [11]), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

NOTE 1: The cryptographic context needs to be unique for each SRTP stream.

NOTE 2: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in the clause 6.3.

If the correct MTK is not present in the UE when RTP traffic arrives, the UE shall wait for the next MTK update procedure from the BM-SC as described in clause 6.3.3.2.

NOTE 3: It is implementation specific issue whether the UE spools encrypted packets or discards all packets before the UE has received the correct MTK.

If the SRTP module has lost synchronisation on the ROC (Roll-over counter) of the SRTP stream, it shall wait for the next MTK update message received within the ptm stream. ~~The BM-SC shall deliver the current ROC-value within the CS ID map info payload of the MIKEY common header payload.~~

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

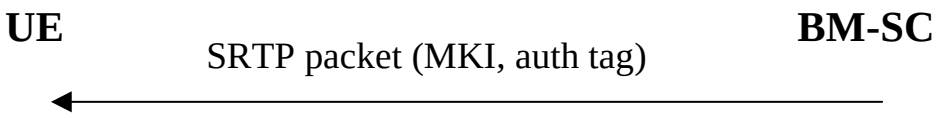


Figure 6.8: Delivery of protected streaming content to the UE

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			
		Y **N**			
Other specs Affected:	⌘	**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.

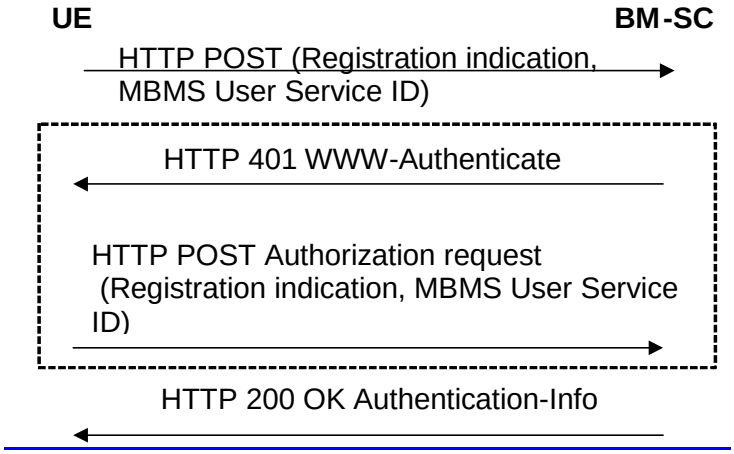


Figure 6.x: MBMS User service registration procedure

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.

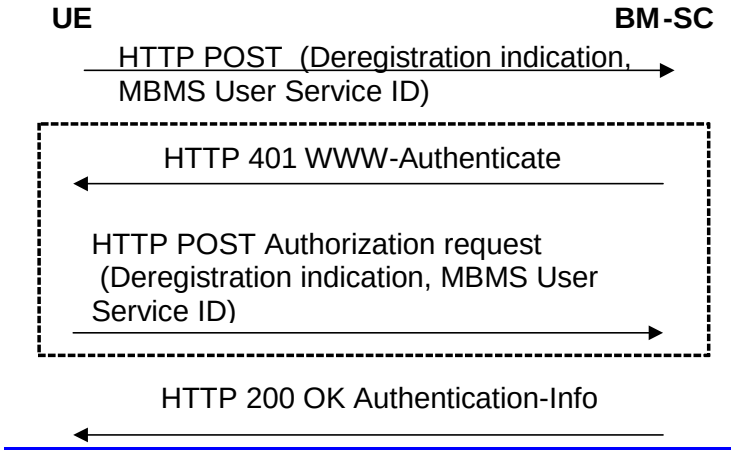


Figure 6.x1: MBMS User service deregistration procedure

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.

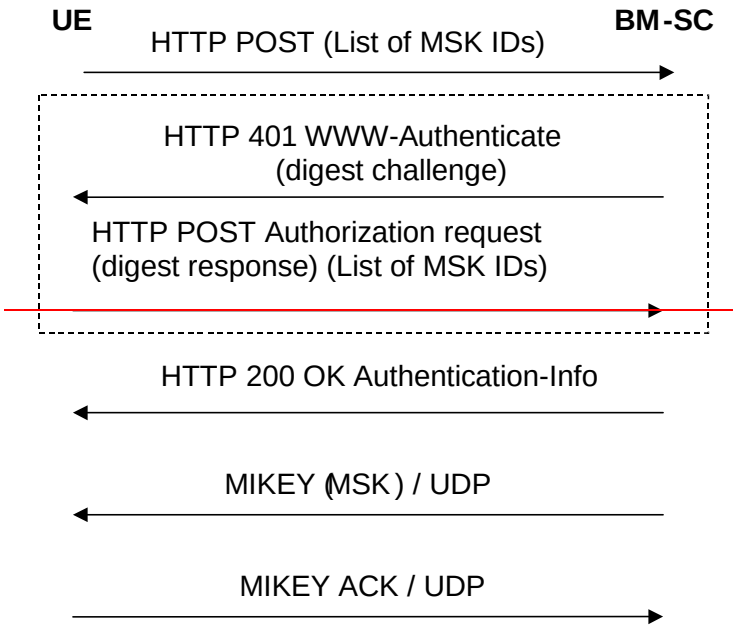
6.3.2.2 MSK ~~retrieval~~ request procedures

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.



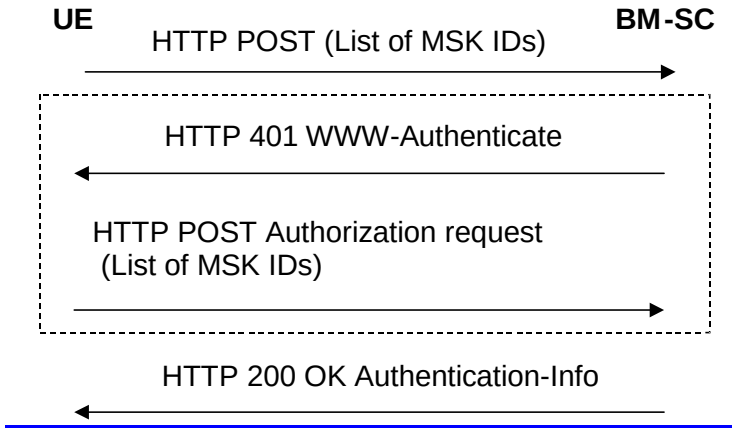


Figure 6.1: Basic MSK ~~retrieval~~ request procedure

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~~

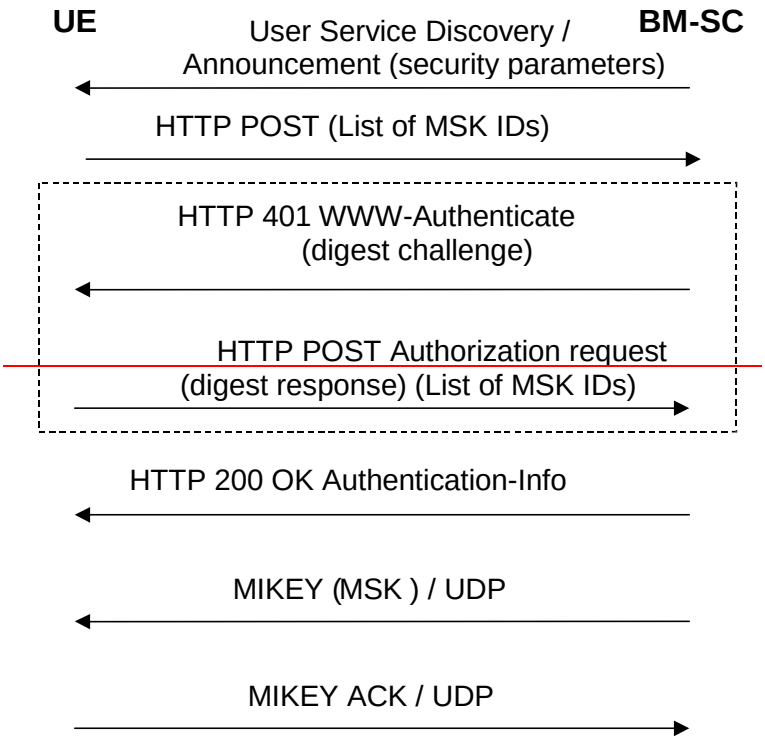
~~When a UE has received User Service information via User Service Discovery / Announcement procedures describing a MBMS User Service and the user has triggered the activation of that User Service, the UE should try to get the MSK(s) that will be used to protect the data transmitted as part of this User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

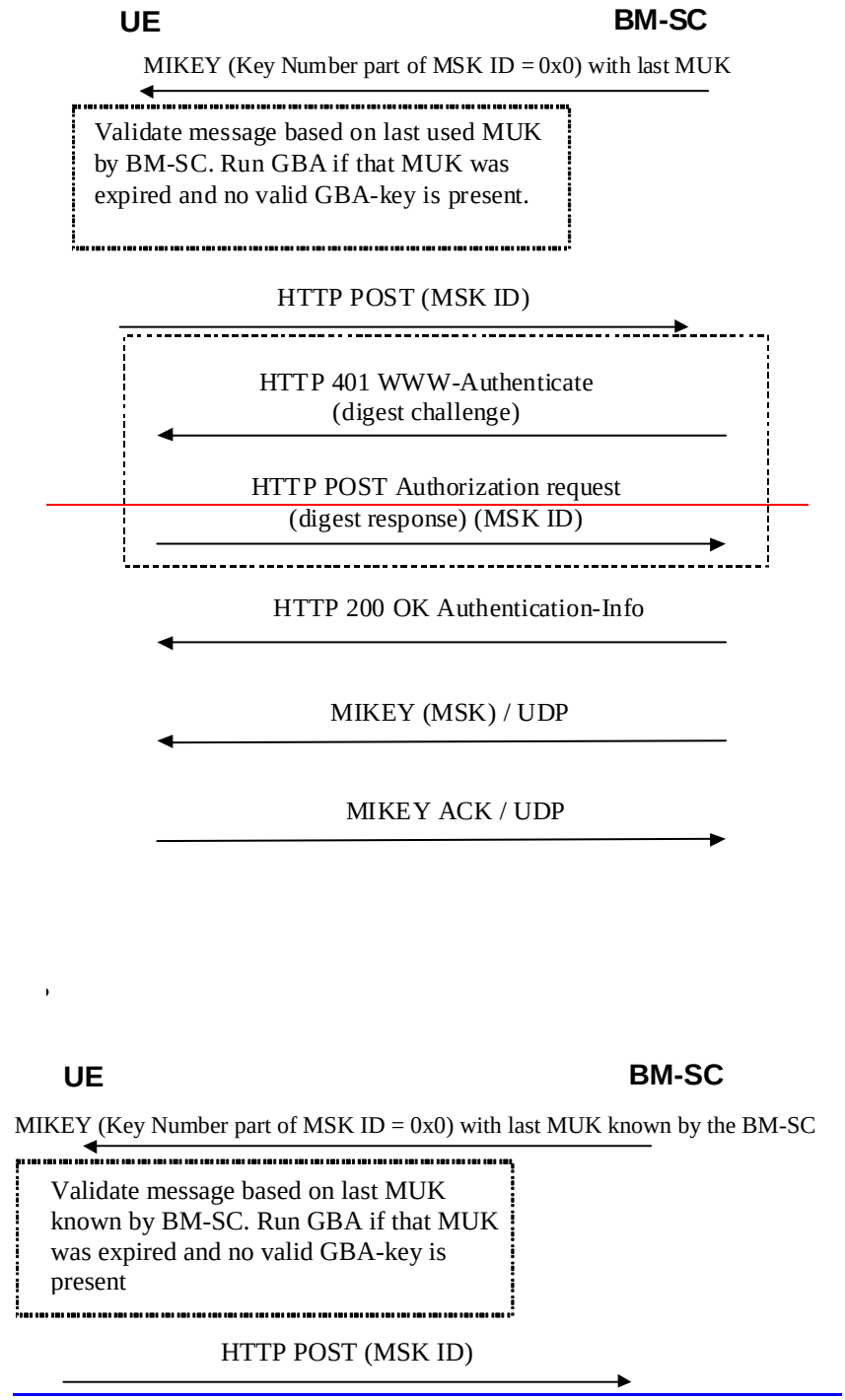


Figure 6.2b: BM-SC solicited pull

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.

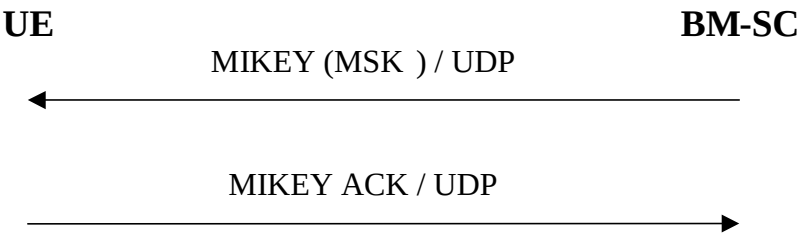


Figure 6.3: Pushing the MSKs to the UE

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.

3GPP TSG SA WG3 Security — S3#37 **S3-050163**

21-25 February 2005

Sophia Antipolis, France

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **049** ⌘**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 [X]

Title:	⌘	MGV-F functionality related to MTK-ID upper limit
Source:	⌘	SA3 WG
Work item code:	⌘	MBMS
Date:	⌘	25/02/2005
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:	⌘	There is no statement of the MGV-F functionality which is related to the MTK-ID upper limit.
Summary of change:	⌘	Add the defination of SEQl, SEQp and SEQu, and remove the re-definition.. Add the MGV-F functionality which is related to MTK-ID upper limit.
Consequences if not approved:	⌘	Arbitrary implementation of the MTK-ID upper limit related MGV-F functionality may lead to MGV-F wrong operation.

Clauses affected:	⌘	3.1, 6.4.5.1, 6.5.3, 6.5.4

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

Other comments:	⌘	

********** START OF CHANGE **********

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to TS 22.246 [5].

MBMS download session: See TS 26.346 [13].

MBMS streaming session: See TS 26.346 [13].

MRK = MBMS Request Key: This key is to authenticate 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. The MSK is not used directly to protect the MBMS User Service data (see MTK).

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function MGV-F with 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.

NOTE: The keys MSK and MUK may be stored within the UICC or the ME depending on the UICC capabilities.

SEQl = Lower limit of the MTK ID sequence number interval: Last accepted MTK ID sequence number interval stored within MGV-S. The original value of SEQl is delivered in the key validity data field of MSK messages.

SEQp = The MTK ID, which is received in a MIKEY packet.

SEQu = Upper limit of the MTK ID sequence number interval, which is delivered in the key validity data field of MSK messages.

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

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. 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 in all the MSK delivery messages. The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC (i.e. NAF-ID) and IDr is the ID of the UE's username (i.e.B-TID). 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 and upper limit of MTK ID). The lower limit of the interval defines the original value of ~~SEQs~~ SEQl to be used by the MGV-F (see clause 6.5), and the upper limit of the interval defines the SEQu. The BM-SC shall never set SEQu to its maximum possible value.

Editor's Note: The contents of the Security Policy payload depends on the used security protocols. RFC 3830 [9] (MIKEY) 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.

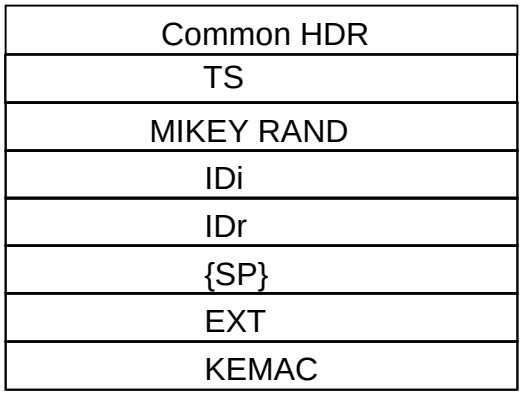


Figure 6.5: The logical structure of the MIKEY message used to deliver MSK.
For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

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

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 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 **********

6.5.4 MTK processing

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the EXT. If the key inside the message is an MTK protected by MSK, 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 numbers ~~SEQs~~SEQl and SEQu, have been stored within a secure storage (MGV-S). ~~Both~~ MSK, SEQl and ~~SEQs~~ SEQu were transferred to the MGV-S with the execution of the MSK update procedures. The initial values of ~~SEQs~~ SEQl and SEQu ~~is~~ are determined by the service provider.

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 MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored ~~SEQs~~SEQl and SEQu. If SEQp is equal or lower than ~~SEQs~~ SEQl, or SEQp is greater than SEQu, then the MGV-F shall indicate a failure to the ME. ~~If SEQp is greater than SEQs~~ Otherwise, ~~then~~ the MGV-F shall verify the integrity of the MIKEY message according to RFC 3830 [9]. If the verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the verification is successful, then the MGV-F shall update ~~SEQs~~ SEQl with SEQp value and extract the MTK from the message. The MGV-F then provides the MTK to the ME.

If MAC verification is successful, the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

In the case of streaming, SRTP requires a master key and a master salt. The MTK is used as master key, and the salt in the KEMAC payload is used as master salt.

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 RFC 3830 [9] (MIKEY).

In case of download service, MIKEY key derivation as defined in section 4.1.3 of MIKEY [9] shall be used to derive MTK authentication and encryption keys from MTK in the ME. These keys shall be provided to the download protection protocol.

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

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

Tdoc ⌘S3-050132

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **051** ⌘ **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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Using the term "MBMS User Service" instead of "multicast"
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	14/2/2005
Category:	⌘	**D**
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:	⌘	SA3 TS 33.246 describes how the MBMS user services described in SA4 TS are protected. The terminology of the specifications should be consistent.
Summary of change:	⌘	MBMS multicast service is corrected to MBMS user service
Consequences if not approved:	⌘	Terminology will be inconsistent.

Clauses affected:	⌘	4.1, 6.1, 6.3.2.3.1, 6.4.2, 6.4.4, B.1, B.1.1, B.2.5, C, C.4,			
Other specs Affected:	⌘	Y	N		⌘
			N	Other core specifications	
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

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

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a ~~multicast~~MBMS user service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a ~~multicast~~MBMS user service.

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

The Broadcast Multicast – Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. It is responsible for generating and distributing the keys necessary for multicast security to the UEs and for applying the appropriate protection to data that is transmitted as part of a multicast service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish multicast bearer.

The UE is responsible for receiving or fetching keys for the multicast service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- a UICC that contains MBMS key management functions shall implement GBA_U;
- a ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC as well as providing key management functions itself;
- a BM-SC shall support using GBA_U keys to enable UICC key management.

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

5.2 Key management and distribution

Like any service, the keys that are used to protect the transmitted data in a ~~Multicast~~ MBMS user service should be regularly changed to ensure that they are fresh. This ensures that only legitimate users can get access to the data in the MBMS service. In particular frequent re-keying acts as a deterrent for an attacker to pass the MBMS keys to others users to allow those other users to access the data in an MBMS service.

The BM-SC is responsible for the generation and distribution of the MBMS keys to the UE. A UE has the ability to request a key when it does not have the relevant key to decrypt the data. This request may also be initiated by a message from the BM-SC to indicate that a new key is available.

******* NEXT 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 U~~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].

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.

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

6.4.2 MIKEY common header

MSKs shall be carried in MIKEY messages. 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.

Once the MSK is in place in the UE, the UE can make use of the ~~multicast~~ MTK messages sent by the BM-SC over MBMS bearer. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret.

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE 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 is not used.

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the key that is derived in the message, a general Extension Payload (EXT) with Type field value x is used that conforms to the structure defined in reference [16].

Editor's Note: The type value will be replaced by value requested from IANA.

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see figure 6.4a. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see figure 6.4b.

Editor's Note: The Key Domain ID needs to be added to [16]. It may need an extension payload type of its own.

See. clauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MTK ID is increased every time the corresponding key is updated. It is possible that the same MTK is delivered several times ~~in multicast~~ over MBMS bearer, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integers, 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.

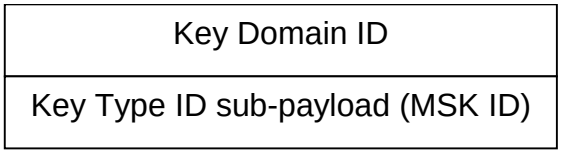


Figure 6.4a: Extension payload used with MIKEY MSK message

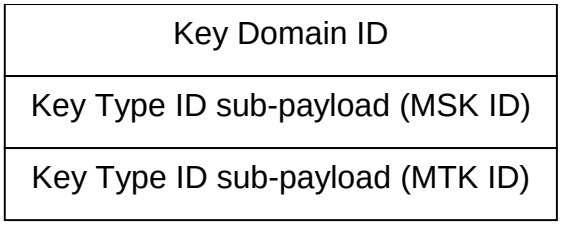


Figure 6.b: Extension payload used with MIKEY MTK message

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

B.1 Threats associated with attacks on the radio interface

The threats associated with attacks on the radio interface are split into the following categories, which are described in the following clauses:

- unauthorized access to ~~multicast~~ MBMS user service data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS services;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here, as these will most likely be transferred on a point-to-point connection (e.g. PS signaling connection), which is already secured today (integrity protected and optionally encrypted RAN level).

B.1.1 Unauthorised access to ~~multicast~~ MBMS user service data

A1: Intruders may eavesdrop MBMS ~~multicast~~ user service data on the air-interface.

A2: Users that have not joined and activated a MBMS ~~multicast~~ user service receiving that service without being charged.

A3: Users that have joined and then left a MBMS ~~multicast~~ user service continuing to receive the MBMS ~~multicast~~ user service without being charged.

A4: Valid subscribers may derive decryption keys (MTK) and distribute them to unauthorized parties.

NOTE: It is assumed that the legitimate end user has a motivation to defeat the system and distribute the shared keys (MSK, MTK) that are a necessary feature of any broadcast security scheme.

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

B.2.5 Unauthorised insertion of MBMS user data and key management data

J1: An ME, which deliberately inserts key management and malicious data, encrypted with valid (previously retrieved) MTK from the MTK generation function, within the ~~multicast~~ MBMS user service stream.

J2: An ME, which deliberately inserts key management and malicious data, encrypted with old (using replayed key management messages) MTK, within the ~~multicast~~ MBMS user service stream.

J3: An attacker, which deliberately inserts incorrect key management information within the ~~multicast~~ MBMS user service stream to cause Denial of Service attacks.

Annex C (normative): ~~Multicast~~ MBMS security requirements

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

C.4 Requirements on MBMS Key Management

R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R5b: The transfer of the MBMS keys between the MBMS key generator and the UE shall be integrity protected.

R5c: The UE and MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary to ensure that:

- users that have joined an MBMS User Service ~~multicast service~~, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
- users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately
- the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.

R5d: Only authorized users that have joined an MBMS User Service shall be able to receive MBMS keys delivered from the MBMS key generator.

R5e: The MBMS keys shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).

R5f: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.

R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).

R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

******* END OF CHANGES *******

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

Tdoc ⌘S3-050134

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **052** ⌘ **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:	⌘	Introduction of BM-SC subfunctions
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	23/2/2005
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:	⌘	The current specification lacks a proper security architecture overview and description of security sub-functions as defined in SA4 TS 26.346.
Summary of change:	⌘	New text is added to describe the MBMS security sub-functions. The Security architecture is clarified.
Consequences if not approved:	⌘	The specification will not be aligned with SA4 TS 26.346.

Clauses affected:	⌘	4.1.1 (New), 4.1.2 (New), 4.1.3 (New), 4.2, 5.1, 5.2, 5.3

Other specs Affected:	Y	N			
⌘	Y		Other core specifications	⌘	TS 26.346
		N	Test specifications		
		N	O&M Specifications		

Other comments: ⌘

4 MBMS security overview

4.1 MBMS security architecture

4.1.1 General

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service.

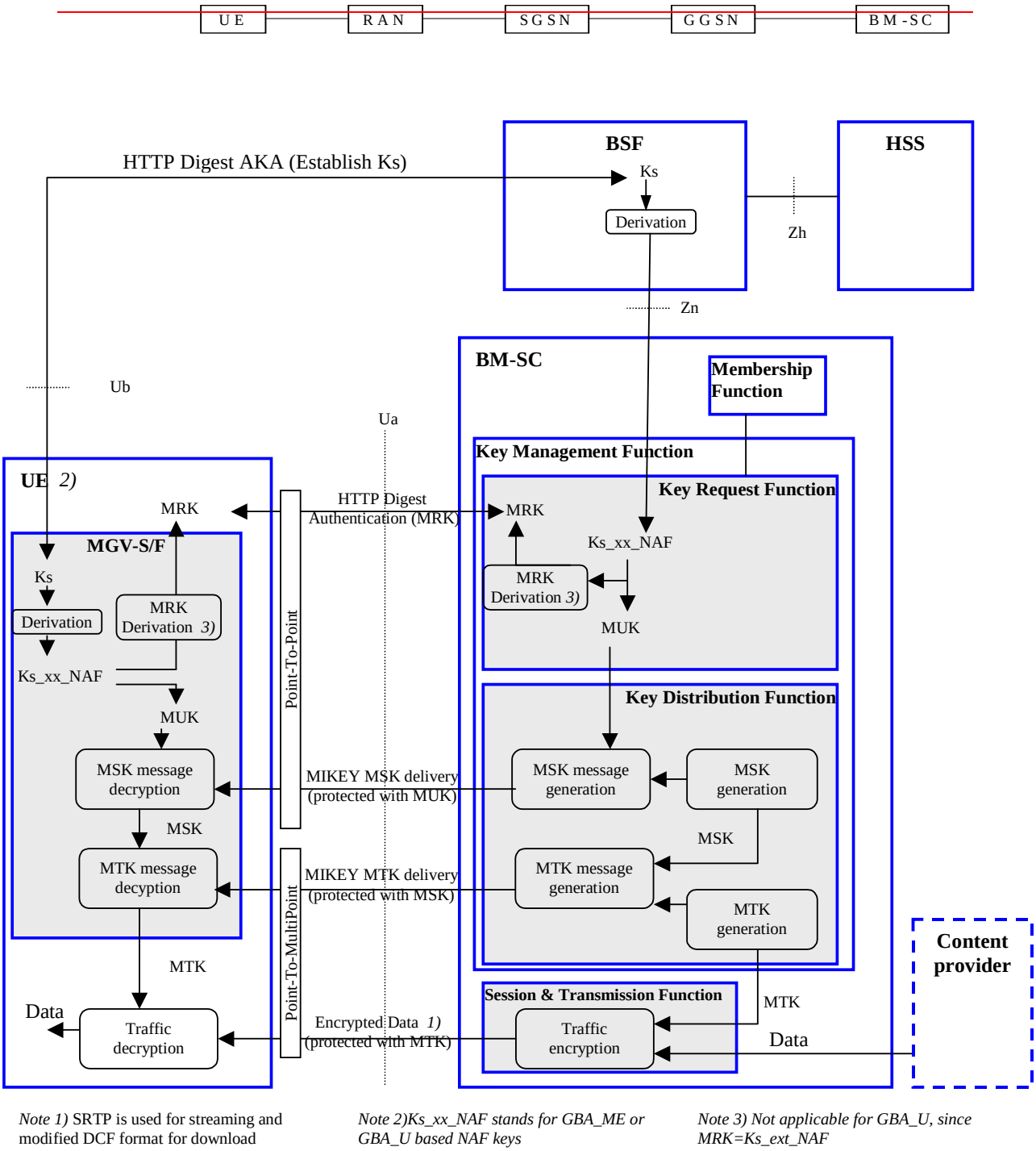


Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS , ~~(beyond~~except for the normal network bearer security~~)~~ resides in either the BM-SC or the UE. The BSF is a part of GBA [6]. The UE and the BM-SC use GBA to establish shared keys that are used to protect the point-to-point communication between the UE and the BM-SC.

The ~~Broadcast Multicast Service Centre (~~BM-SC~~)~~ is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. ~~It~~ BM-SC is responsible for establishing shared secrets with the UE using GBA, authenticating the UE with HTTP digest authentication mechanism, registering and de-registering UEs for MBMS User Services, generating and distributing the keys necessary for ~~multicast~~ MBMS security to the UEs with MIKEY protocol and for applying the

appropriate protection to data that is transmitted as part of a MBMS user ~~multicast~~ service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish ~~multicast~~ MBMS bearer.

The UE is responsible for establishing shared secrets with the BM-SC using GBA, registering to, and de-registering from, MBMS User Services, requesting and receiving ~~or fetching~~ keys for the ~~multicast~~ MBMS user service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- a UICC that contains MBMS key management functions shall implement GBA_U;
- a ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC as well as providing key management functions itself;
- a BM-SC shall support using GBA_U keys to enable UICC key management.

4.1.2 BM-SC sub-functions

The BM-SC has the following sub-functions related to MBMS security, cf. Figure 4.1.

- **Key Management function**: The Key Management function includes two sub-functions: Key Request function and Key Delivery function.
- **Key Request function**: The sub-function is responsible for retrieving GBA keys from the BSF, deriving MUK and MRK from GBA keys, performing MBMS User Service Registration, Deregistration and MSK request procedures and related user authentication using MRK, providing MUK to Key distribution function, performing subscription check from Membership function. The sub-function implements the following procedures:
  - Bootstrapping initiation
  - Bootstrapping re-negotiation
  - HTTP digest authentication
  - MRK derivation
  - MBMS User Service Registration procedure
  - MBMS User Service Deregistration procedure
  - MSK request procedure
- **Key distribution function**: The sub-function is responsible for retrieving MUK from Registration function, generating and distributing MSKs and MTKs to the UE, providing MTK to Session and Transmission function. The sub-function implements the following security procedures:
  - MSK delivery procedure
  - MTK delivery procedure
  - BM-SC solicited pull procedure
- **Session and Transmission function**: The sub-function is responsible for session and transmission functions cf. TS 26.346 [13]. As part of these session and transmission functions, this function performs protection of data with MTK (encryption and/or integrity protection). The sub-function implements the following security procedures:
  - Protection of streaming data
  - Protection of download content
- **Membership function**: The Membership function is used to verify if a user is authorized to register, receive keys or to establish a MBMS bearer. The Membership function is defined in [3].

4.1.3 UE security architecture

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. The MGV-F is implemented in a protected execution environment to prevent leakage of security sensitive information such as MBMS keys. MGV-S stores the MBMS keys and MGV-F performs the functions that should not be exposed to unprotected parts of the ME. An overview of ME based key management and UICC based key management in UE is described in Figure 4.y.

In particular in ME based key management it shall be ensured that the keys are not exposed to unprotected parts of the ME when they are transmitted from the UICC to the MGV-S or during the key derivations.

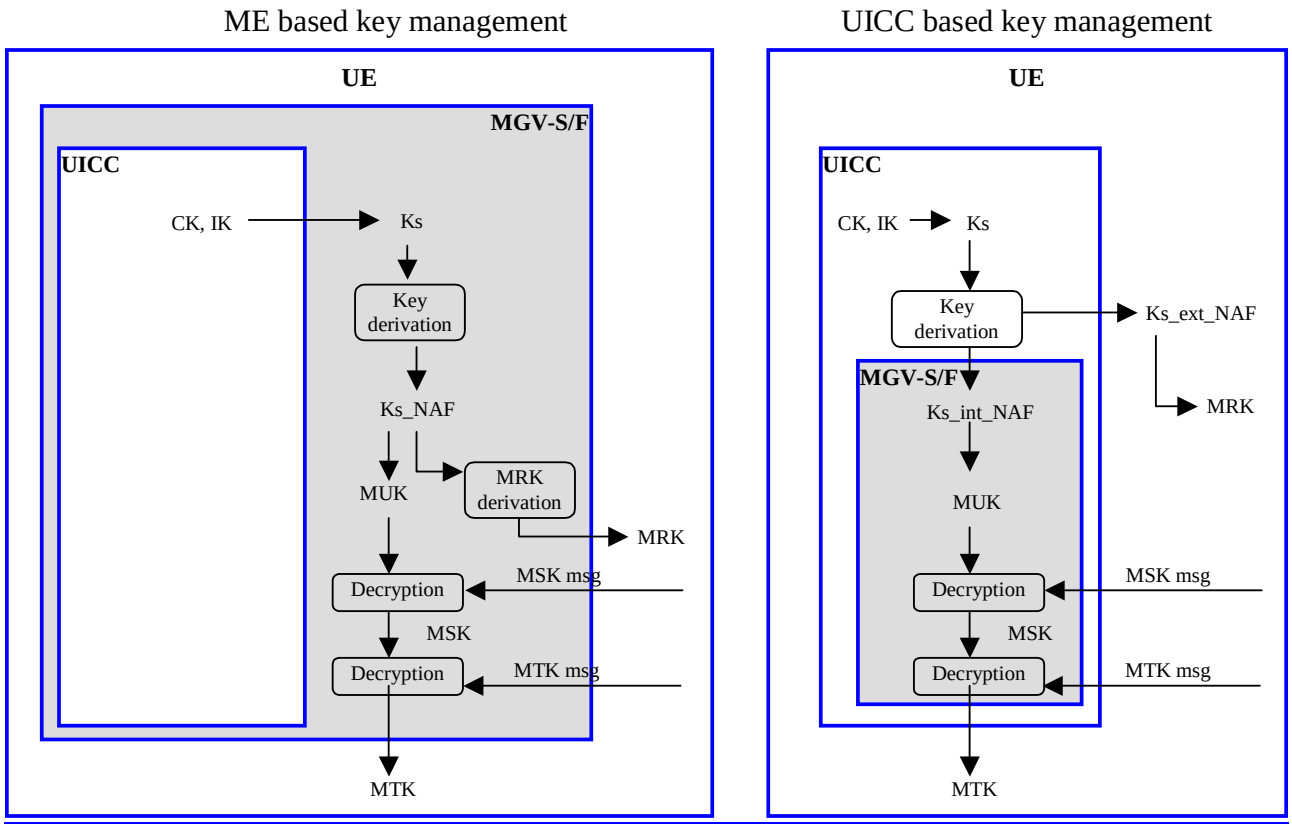


Figure 4.y: ME and UICC based key management in UE

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

4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different MBMS Streaming/Download Sessions that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Streaming/Download Sessions, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Streaming/Download Sessions~~.~~ as specified within clauses 6.5 and 6.6. MSKs and MTKs are managed at the MBMS User Service Level. The usage of MSKs and MTKs for one Key group is depicted in figure 4.x.

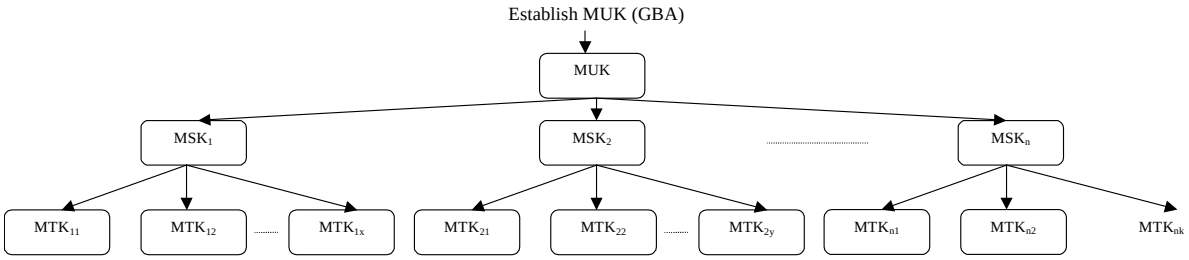


Figure 4.x: MBMS key hierarchy

There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.

The use of the same MTK (this implies also the same MSK) with two different transport services (or user services) should be avoided.

NOTE 1: This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic, i.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. It shall be possible for MBMS User Services to share one or more MSKs for the shared Transport Services with other MBMS User Services.

NOTE 2: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.

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

5 MBMS security functions

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised ~~in the following situations~~ such that only legitimate users ~~when~~ are able to participate~~ing~~ in an MBMS User Service. ~~That is:~~

~~- when the UE performs User Service joining (or leaving) on the application level;~~

~~Editor's Note: The final decision on application level join procedures relies of work in SA4.~~

~~- when the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service;~~

~~-~~ ~~w~~When the UE ~~requests and receives MSKs for the MBMS User Service~~uses HTTP protocol towards the BM-SC, the UE is authenticated with HTTP digest as described in clause 6.2.1. The Membership function within the BM-SC is used to verify the subscription information~~;~~

The following procedures use HTTP digest authentication:

- MBMS User Service Registration procedure (clause 6.3.2)
- MBMS User Service Deregistration procedure (clause 6.3.2)
- MSK request procedure. This can have many triggers (clause 6.3.2)
- Associated delivery procedures (specified in TS 26.346 [13])

When the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service, it is authenticated as defined in clause 6.2.2;

~~- when the UE performs post delivery procedures (e.g. point to point repair service).~~

~~Editor's Note: The final decision on post delivery procedures relies of work in SA4.~~

~~NOTE: The list above does not reflect the order of authentications.~~

5.2 Key derivation, management and distribution

Like any service, the keys that are used to protect the transmitted data in a Multicast service should be regularly changed to ensure that they are fresh. This ensures that only legitimate users can get access to the data in the MBMS service. In particular frequent re-keying acts as a deterrent for an attacker to pass the MBMS keys to others users to allow those other users to access the data in an MBMS service.

The BM-SC is responsible for the generation and distribution of the MBMS keys to the UE. A UE has the ability to request a key when it does not have the relevant key to decrypt the data. This request may also be initiated by a message from the BM-SC to indicate that a new key is available.

The following procedures are involved in Key management and distribution:

- MRK derivation (clause 6.1)
- MBMS User Service Registration procedure (clause 6.3.2)
- MBMS User Service Deregistration procedure (clause 6.3.2)
- MSK request procedure (clause 6.3.2)
- MSK delivery procedure (clause 6.3.2)
- MTK delivery procedure (clause 6.3.3)
- BM-SC solicited pull (clause 6.3.2)

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence might not require additional protection. However, MBMS protection is independent of DRM protection). If this protection is required, it will be either confidentiality and integrity or confidentiality only, or integrity only. The protection is applied end-to-end between the BM-SC and the UEs and will be based on a symmetric key shared between the BM-SC and the UEs that are currently accessing the service. The actual method of protection specified may vary depending on the type of data being transmitted, e.g. media streaming application or file download.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This "double ciphering" is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.

The following procedures are involved in Key management and distribution:

- Protection of streaming data (clause 6.6.2)
- Protection of download content (clause 6.6.3)

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

Tdoc ⌘S3-050092

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **053** ⌘ **rev** **-** ⌘ 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:	⌘	Removing IDi from MTK message
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	14/2/2005
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:	⌘	The usage of ID payloads in MIKEY messages was agreed in S3-041097 and implemented in S3-041127. However, S3-041127 did not remove the IDi payload from MIKEY MTK message although this was agreed in S3-041097. This CR aligns the TS 33.246 to the agreed decisions made.
Summary of change:	⌘	The IDi payload is removed from MTK message.
Consequences if not approved:	⌘	The IDi payload is carried unnecessarily in MTK message.

Clauses affected:	⌘	6.4.5.3

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

Other comments: ⌘

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

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. The EXT payload has format as described in clause 6.4.4. If MTK is to be used for streaming protection, then a 112 bit salt shall be added to the KEMAC payload in addition to the MTK. ~~The network identity payloads (IDi) shall be used in MTK transport messages.~~

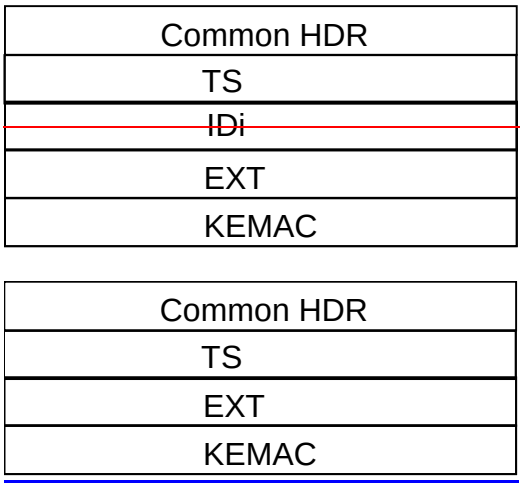


Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

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

S3-050154

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **054** ⌘ **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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	MBMS download protection details
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:	⌘	Align with the proposal from OMA BAC DLDRM in response to suggestion from OMA where a specific version of their specification is cited (V2.0)
Summary of change:	⌘	The name of MBMSSignature Box is changed because of the generic nature of this feature. The definition of the special value 1 of the flags field in the CommonHeaders box is unnecessary as the structure of the value of the RightsIssuerURL field is enough information to prevent misunderstanding of a MBMS DCF in a general OMA DRM context, or vice versa. Deletion of the editor's note in 6.6.3 Addition of note in 6.6.3.2 to clarify specific version of OMA specification to be used. List of the OMA DCF boxes that the MBMS DCF implementation shall support is added. The word "content" is replaced with "data" since MBMS by definition is not content protection in the DRM sense.
Consequences if not approved:	⌘	Incomplete specification

Clauses affected:	⌘	6.6.3, 6.6.3.2
Other specs affected:	⌘	Y / N ☐ / N Other core specifications ☐ / N Test specifications ☐ / N O&M Specifications
Other comments:	⌘	

6.6.3 Protection of download datacontent

~~Editor's Note: The details of MBMS download protection are subject to the response from OMA BAC DLDRM. SA3 has asked OMA BAC DLDRM whether it is possible to include the extensions and deviations needed for using the DCF format for MBMS download protection to OMA DRM v2.0 DCF specification. If the answer is positive, some material in this section will be removed and the OMA specification referenced instead.~~

6.6.3.1 General

Data that belongs to a download MBMS User Service is decrypted as soon as possible by the UE, if the MSK needed to provide the relevant MTK is already available on the UE.

6.6.3.2 Usage of OMA DRM DCF

NOTE: If the OMA DRM V2.0 DCF [15] specification is upgraded, these upgrades do not apply for the present document.

When it is required to protect MBMS download ~~content~~data, OMA DRM V2.0 DCF as defined in reference [15] shall be used. In particular, minor version 0x00000003 of OMA DRM V2.0 DCF specifies how DCF is used to protect MBMS download data. MBMS download data are therefore indicated by minor version 0x00000003 in a DCF. ~~MBMS download contents are indicated by the 3GPP_MBMS_DCF flag in the Common Headers Box of a DCF.~~ OMA DRM Rights Objects are not utilized. Instead, encryption and authentication keys are generated from MTK. For integrity protection, an OMADRM~~MBMS~~Signature as specified below is attached inside the optional Mutable DRM information box ('mdri') ~~in the FreeSpaceBox~~ of the DCF.

The ~~MBMS~~OMADRMSignature Box is an extension to OMA DRM V2.0 DCF for use by MBMS, and is defined as follows:

```
aligned(8) class OMADRM~~MBMS~~Signature extends Fullbox('odfs~~sign~~', version, flags)
{
   Unsigned int(8) SignatureMethod;   // Signature Method
   Char            Signature[];       // Actual Signature
}

SignatureMethod Field:
NULL   0x00
HMAC-SHA1 0x01
```

The range of data for the HMAC calculation shall be according to section 5.3 of reference [15].

The correct MTK for decrypting and verifying the integrity of the download ~~content~~ data is indicated by the key_id in the RightsIssuerURL field as follows:

mbms-key://<key_id>

where key_id is defined as the base64 encoded concatenation (Key Domain ID || MSK_ID || MTK ID).

In case the FDT of the FLUTE protocol needs to be protected, the FDT may also be wrapped in a different DCF. Confidentiality and/or integrity protection of FDT can be provided this way.

The MBMS DCF implementation shall support the following boxes specified in OMA DRM V2.0 DCF [15]:

- Fixed DCF header;
- Mutable DRM information Box;
- OMA DRM Container Box.

Editors' note: The optionality of FDT protection is still under study (i.e. whether it should be mandated).

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

Tdoc ⌘S3-050116

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **055** ⌘ **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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Removal of Editors notes
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	21/2/2005
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:	⌘	Some CRs from SA3#36 are incompletely implemented
Summary of change:	⌘	MIKEY key derivations were agreed to be used in S3-040858 (CR008rev1), but the CR did not remove the editor's note on the issue from clause 6.5.1: *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*. S3-041125 (CR010R3) introduced the usage of salt in MTK messages, but the CR missed to remove the related editor's note in clause 6.4.
Consequences if not approved:	⌘	Unnecessary Editors' notes in the specification

Clauses affected:	⌘	6.4, 6.5.1

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

Other comments:	⌘	

6.4 MIKEY message creation and processing in the ME

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

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9].

To keep track of MSKs and MTKs, a new Extension Payload (EXT) [16] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (see clauses 6.3.2 and 6.3.3).

****** Next Change ******

6.5 Validation and key derivation functions in MGV-F

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.

~~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.~~

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

Tdoc ⌘S3-050124

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **056** ⌘ **rev** **-** ⌘ 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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Protection of MBMS Service Announcement sent over MBMS bearer
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	22/02/2005
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 is considered not practical to protect service announcements in case they are sent over MBMS Bearer.
Summary of change:	⌘	The service announcements are not protected.
Consequences if not approved:	⌘	It is not specified whether MBMS service announcements are protected.

Clauses affected:	⌘	6.3.2.2.2 (see note below), B.1

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

Other comments: ⌘ **NOTE: The change in 6.3.2.2.2 should be made in new clause 6.3.2.1A after implementation of CR047R1 if both CRs are approved by TSG SA.**

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

6.3.2.2.2 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.

NOTE1: 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.

NOTE2: The user service announcements are not protected when sent over MBMS bearer.

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.

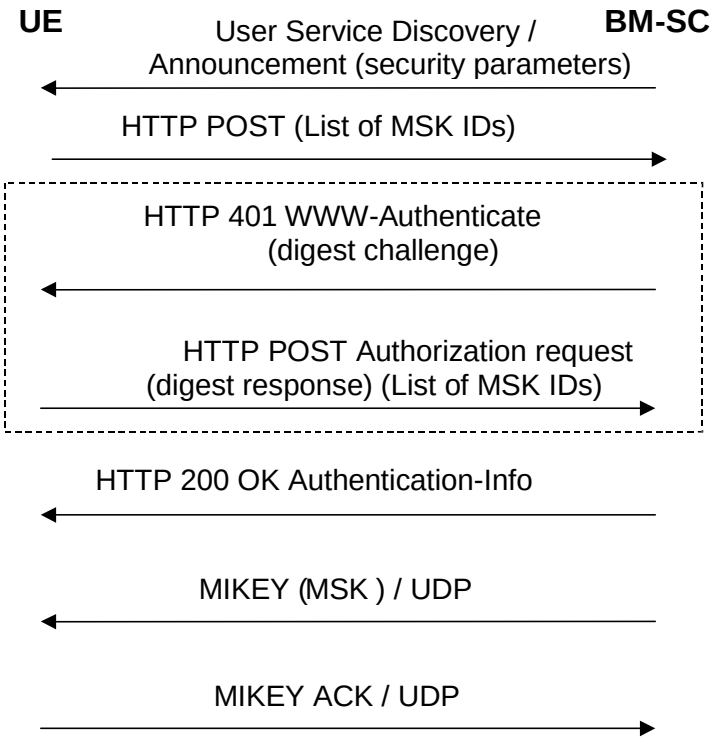


Figure 6.2a: MSK retrieval procedure

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.

===== **NEXT CHANGE** =====

Annex B (informative): Security threats

B.1 Threats associated with attacks on the radio interface

The threats associated with attacks on the radio interface are split into the following categories, which are described in the following clauses:

- unauthorized access to multicast data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS services;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here~~,~~ because in case~~as~~ these are~~will most likely be~~ transferred on a point-to-point connection (e.g. PS signaling connection) they are~~, which is~~ already secured~~ today~~. In case the service announcement is transferred over HTTP, it is protected by HTTP Digest as defined in the current specification and/or it may be ~~(~~integrity protected and optionally encrypted at the RAN level~~)~~. In case the service announcements are sent over MBMS bearer, it is impractical to protect them.

===== **END CHANGE** =====

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

Tdoc ⌘ S3-050137

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** CR **057** ⌘ rev **-** ⌘ 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⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Introduction of missing abbreviations, symbols and defintions
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	24/02/2005
Category:	⌘	**D**
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:	⌘	Some abbreviations, terminology, and symbols used in TS 33.246 are not defined.
Summary of change:	⌘	Missing abbreviations, symbols and defintions are introduced
Consequences if not approved:	⌘	Ambiguity in the specification

Clauses affected:	⌘	3.1, 3.2, 3.x(new)

Other specs Affected:	Y	N		
⌘		**N**	Other core specifications	⌘
		N	Test specifications	
		N	O&M Specifications	

Other comments: ⌘

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to TS 22.246 [5].

HDR = the general MIKEY HeaDeR

KEMAC = A payload included in the MIKEY message, which contains a set of encrypted sub-payloads and a MAC

MBMS download session: See TS 26.346 [13].

MBMS streaming session: See TS 26.346 [13].

MRK = MBMS Request Key: This key is to authenticate 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. The MSK is not used directly to protect the MBMS User Service data (see MTK).

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function MGV-F with 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.

NOTE: The keys MSK and MUK may be stored within the UICC or the ME depending on the UICC capabilities.

Salt key = a random or pseudo-random string used to protect against some off-line pre-computation attacks on the underlying security protocol

3.2 Abbreviations

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

B-TID	Bootstrapping Transaction Identifier
BM-SC	Broadcast-Multicast Service Centre
BSF	Bootstrapping Server Function
DCF	DRM Content Format
DRM	Digital Rights Management
EXT	Extension payload
FDT	FLUTE File Delivery Table
FLUTE	File delivery over Unidirectional Transport
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
IDi	Identity of the initiator
IDr	Identity of the responder
Ks_ext_NAF	Derived key in GBA_U
Ks_int_NAF	Derived key in GBA_U, which remains on UICC
Ks_NAF	Derived key in GBA_ME
MAC	Message authentication code
MBMS	Multimedia Broadcast/Multicast Service
MGV-F	MBMS key Generation and Validation Function
MGV-S	MBMS key Generation and Validation Storage
MIKEY	Multimedia Internet Keying
MKI	Master Key identifier
MRK	MBMS Request Key
MSK	MBMS Service Key
MSK_C	Confidentiality key derived from key MSK
MSK_I	Integrity key derived from key MSK
MTK	MBMS Traffic Key
MUK	MBMS User Key
MUK_C	Confidentiality key derived from key MUK
MUK_I	Integrity key derived from key MUK
NAF	Network Application Function
OMA	Open Mobile Alliance
ROC	Roll-over counter

SP Security Policy
SRTP Secure RTP

3.x Symbols

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

|| Concatenation