Source: **SA3**

Title: **CRs to 33.246 on MBMS (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050266	33.246	058	1	Rel-6	C	MKI and authentication tag length in User Service Description	6.2.0	6.3.0	S3-050296
SP-28	SP-050266	33.246	059	1	Rel-6	C	Clarification of Key domain ID in service announcement	6.2.0	6.3.0	S3-050295
SP-28	SP-050266	33.246	060	1	Rel-6	F	Key usage clarification	6.2.0	6.3.0	S3-050298
SP-28	SP-050266	33.246	061	1	Rel-6	C	Omitted MTK Update Error Message	6.2.0	6.3.0	S3-050292
SP-28	SP-050266	33.246	062	1	Rel-6	D	Editorial corrections to TS 33.246	6.2.0	6.3.0	S3-050318
SP-28	SP-050266	33.246	063	1	Rel-6	C	Clarifications on MBMS key management	6.2.0	6.3.0	S3-050294
SP-28	SP-050266	33.246	064	1	Rel-6	F	Use of IMPI in MBMS	6.2.0	6.3.0	S3-050293
SP-28	SP-050266	33.246	065	-	Rel-6	F	Clarification on CSB ID and SP payload use	6.2.0	6.3.0	S3-050297
SP-28	SP-050266	33.246	066	-	Rel-6	F	MIME type adjustments according to LS S3-050192	6.2.0	6.3.0	S3-050290
SP-28	SP-050266	33.246	067	-	Rel-6	F	Results of mapping the MBMS security requirements into security functions and mechanisms	6.2.0	6.3.0	S3-050319

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc S3-050296

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **058** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	MKI and authentication tag length in User Service Description
Source:	⌘	SA3
Work item code:	⌘	MBMS
Date:	⌘	27/04/05
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:	⌘	Unless the MSK is pushed to the UE prior to the first SRTP packet arriving, the UE will not be able to deduce from the MKI field which MSK to request for.
Summary of change:	⌘	- Added length of authentication tag. - Added length of MKI. - Removed integrity protection on/off flag. - Removed confidentiality on/off flag.
Consequences if not approved:	⌘	It will not be possible to use a pull-only key management and may lead to that UEs request for non-existing MSKs.

Clauses affected:	⌘	6.3.2.1A

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

Other comments:	⌘	

*** START OF CHANGE ***

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 1: 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.

NOTE 2: 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~~:~~ if protection of the MBMS User Service is applied. In this case the UE shall register for the MBMS User Service. If on the other hand, the MBMS User Service does not require any protection (i.e. if service protection description is not present in the Service Announcement), the UE shall not register for key management purposes.

- 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~~

- UICC key management required: yes/ no.

~~- 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. If the MSK is applied to streaming data, then the following parameters shall be present per MSK:

  ~~o~~- SRTP authentication tag length

  NOTE 3: If there is no integrity protection applied to the data, the length of the authentication tag shall be zero.

  ~~o~~- SRTP MKI length

  NOTE 4: Using the lengths of the authentication tag and the MKI field, the UE is able to locate the beginning of the MKI field in SRTP packets even before it has received the security policy payload supplied with the delivery of the MSK. This makes it possible for the UE to request the MSK required for the packet.

- Back off mode parameters, as defined in TS 26.346 [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.

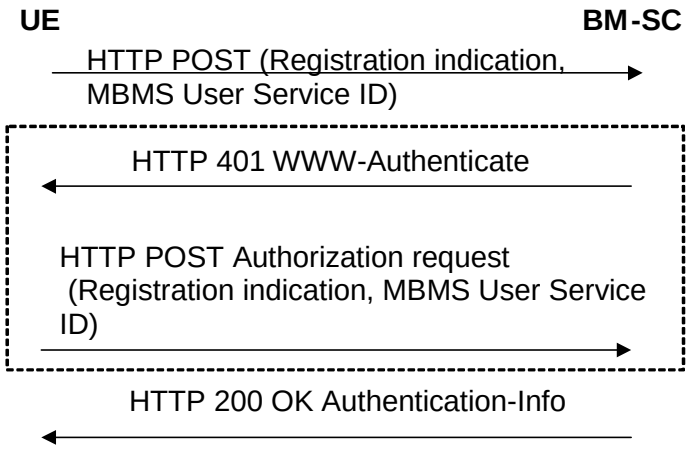


Figure 6.0A: MBMS User service registration procedure

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 6.0A), 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 clause G.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.

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc S3-050295

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **059** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Clarification of Key domain ID in service announcement
Source:	⌘	SA3
Work item code:	⌘	MBMS
Date:	⌘	27/04/05
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 are situations when a UE is connected to multiple BM-SCs that could lead to that the wrong MSK/MTK is used. This happens if two or more BM-SCs by accident use the same MSK ID.
Summary of change:	⌘	Addition of the Key Domain ID to the User Service Description. Also a note on how the UE can map a received MTK to the correct Key Domain ID is added.
Consequences if not approved:	⌘	May lead to interoperability problems.

Clauses affected:	⌘	6.3.2.1A, 6.6.2.1

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

Other comments:	⌘	

*** START OF CHANGE ***

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 1: 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.

NOTE 2: 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 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.

  For each MSK, the identifiers that shall be included are Key Domain ID and MSK ID. The Key Number part of ~~the~~ each 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 TS 26.346 [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.

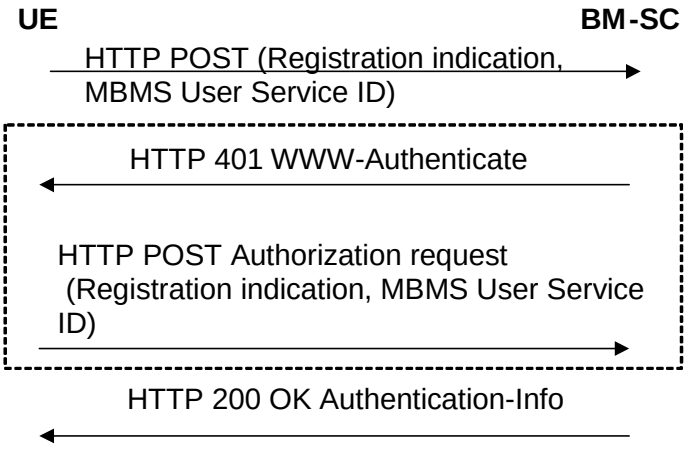


Figure 6.0A: MBMS User service registration procedure

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 6.0A), 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 clause G.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.

*** NEXT CHANGE ***

6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in RFC 3711 [11] shall be used. The MTK is carried to the UEs from the BM-SC using RFC 3830 [9] (MIKEY) with extensions defined according to this specification. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in section 4.3 of RFC 3830 [9]. The correct MTK to use to decrypt the data is indicated using the MKI (Master Key identifier) field, which is included in the SRTP packets as defined in RFC 3711 [11]. The form of MKI shall be a concatenation of MSK ID and MTK ID, i.e. MKI = (MSK ID || MTK ID).

NOTE: The UE knows the Key Domain ID related to this MKI from the User Service Description which includes mapping between IP address and port of the traffic and the corresponding Key Domain ID and MSK ID.

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in RFC 3830 [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in section 6.10.1 in RFC 3830 [9].

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc S3-050298

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **060** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Key usage clarification
Source:	⌘	Ericsson, Siemens
Work item code:	⌘	MBMS
Date:	⌘	28/04/2005
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 was unclear if MTK was applied per RTP session, per RTP stream or any combination. Also the description of the relation of MBMS User Services and usage of keys is underspecified.
Summary of change:	⌘	Granularity of MBMS security is clarified to be per RTP sessions or FLUTE channels. The usage of MSKs and MTKs with MBMS User Services is clarified. The relationship between MTK and FEC (repair) streams is specified.
Consequences if not approved:	⌘	Insecure implementation and possible interoperability problems.

Clauses affected:	⌘	3.1, 4.1A, 4.2, 6.3.2.1A, Annex (new)

Other specs Affected:	Y	N			
⌘	Y		Other core specifications	⌘	TS 26.346
		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.

Key Group= A group of MSKs that are identified by the same Key Group part of the MSK ID. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted.

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.

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 *******

4.1A Granularity of MBMS security

An MBMS User Service is composed of one or more MBMS Streaming Sessions and/or MBMS Download Sessions ~~as defined in TS 26.346 [13]~~. An MBMS Streaming Session is composed of one or more RTP sessions, and an MBMS Download Session is composed of one or more FLUTE channels as defined in TS 26.346 [13]. MBMS streaming/download sessions may be transported over one or more MBMS Transport Services. Transport Services are defined in TS 23.246 [3]. MBMS security is used to protect ~~MBMS streaming/download sessions~~ RTP sessions and FLUTE channels. As such MBMS User Service protection~~security~~ is Transport Service independent, in particular, it is independent on whether it is carried over point-to-point bearer or MBMS b~~B~~earer.

4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different RTP sessions and FLUTE channels~~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 RTP sessions and FLUTE channels~~MBMS Streaming/Download Sessions~~ as specified within clauses 6.5 and 6.6. The delivery of MSKs is secured with user specific MBMS User Key (MUK), which is received from GBA, cf. clause 6.1. 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 4.3.~~

The following rules apply for MBMS key management:

The use of the same MTK within two different RTP sessions is not allowed according to RFC3711 [11] section 9.1.

TS 26.346[13] specifies the use of a generic FEC mechanism for RTP data in which FEC source packets and FEC repair packets are respectively put into different RTP streams of the same RTP session. The RTP stream containing the FEC repair packets is protected by the MTK of the RTP session.

NOTE 1: When the RTP session contains more than one RTP stream, e.g. the FEC repair stream and FEC source stream, then a different key stream for the included RTP streams is ensured by different SSRC values as specified by RFC3711.

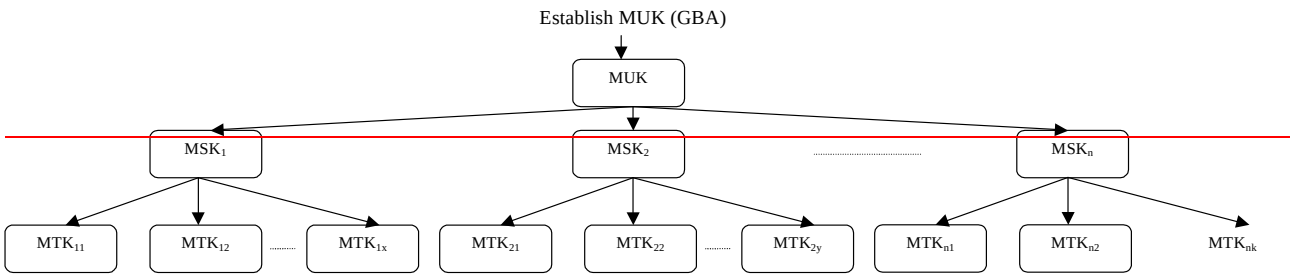
It shall be possible to update the MTKs during an RTP session or FLUTE channel to enhance the security.

MSKs shall be used to protect MTKs of only one RTP session or FLUTE channel. It shall be possible to update the MSKs during an RTP session or FLUTE channel to enhance the security.

MSKs within one Key Group shall be used to protect MTKs of only one RTP session or FLUTE channel. To allow smooth transition from "current" MSK to the "next", the MGV-S shall be capable of storing two MSKs within the same Key Group as specified in clause 6.3.2.1 of TS 33.246.

Some of the rules are illustrated in figures 4.3 and 4.4.

The usage of MSKs and MTKs applied to a RTP session or FLUTE channel (i.e. usage of MSKs and MTKs for one Key group) is depicted in figure 4.3. Figure 4.4 shows an example of the usage of MSKs and MTKs for three RTP sessions. In particular it shows that MSKs and MTKs of one Key Group are used to protect exactly one RTP session.



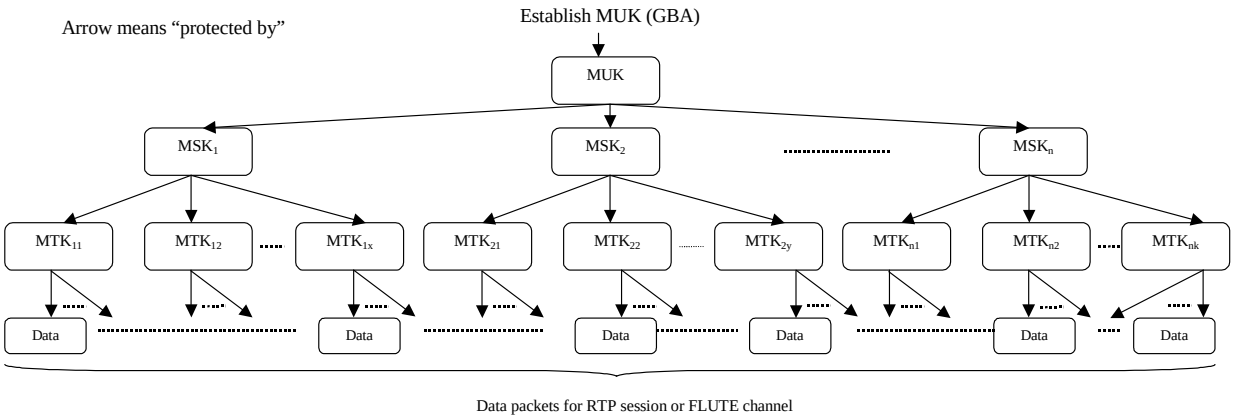


Figure 4.3: MBMS key hierarchy: usage of MSKs and MTKs within one RTP session or FLUTE channel

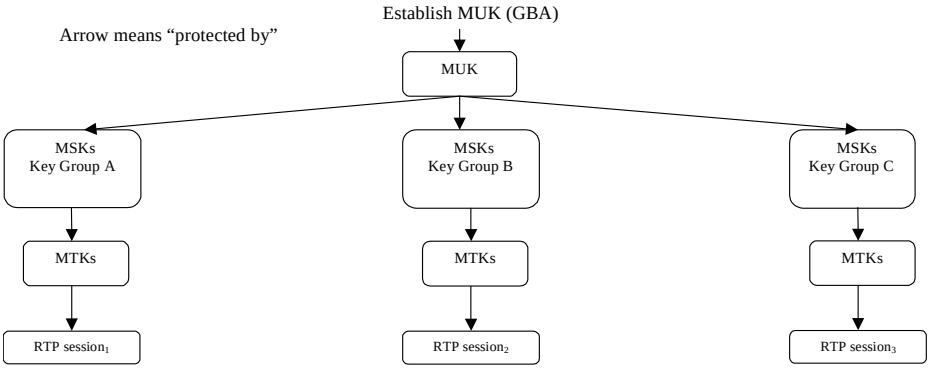


Figure 4.4: MBMS key hierarchy: usage of MSKs and MTKs for three separate RTP sessions

~~There shall be only one MSK and MTK in use with the same Key Group part of MSK ID. i.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) with the same Key Group part of MSK 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. In case two MBMS User Services share an MBMS Transport Service, they also share one or more RTP sessions or FLUTE channels carried in the Transport Service. In this case, ~~I~~it shall be possible for the MBMS User Services to share one or more MSKs and MTKs of the Key Groups that are used to protect the MBMS data~~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.~~

An example showing how key management is used with MBMS User and Transport Services is depicted in Annex x.

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

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 1: 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.

NOTE 2: 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 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~~RTP sessions or FLUTE channels.
- Back off mode parameters, as defined in TS 26.346 [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.

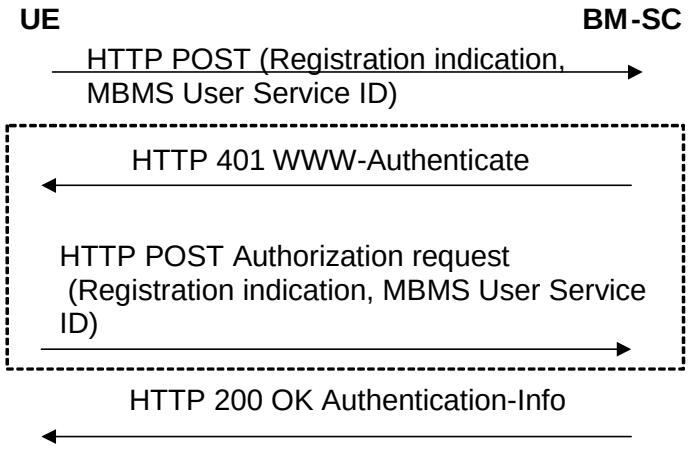


Figure 6.0A: MBMS User service registration procedure

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 6.0A), 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 clause G.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.

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

Annex x (informative): Example of using MSKs and MTKs in MBMS

The following table shows an example of two MBMS User Services, sports Mobile TV channel and news Mobile TV channel. Both of the MBMS User Services include an MBMS User Service Session that downloads a joke per day. The table shows how the MBMS User Services are broken down into RTP sessions (each including one data stream with related RTCP and FEC streams) and FLUTE channels.

The table shows how MSKs and MTKs belonging to different Key Groups are used to protect the RTP sessions and FLUTE channels. It should be noted that the MBMS download session is shared with User Services 1 and 2 so these MBMS User Services need to be able to share MSKs in Key Group C.

Furthermore the table shows how traffic could be carried over MBMS bearers, but this is not a security issue and is only shown here for completeness.

Table x.-1: Example of using MSKs and MTKs in MBMS

<table>
<tr><td rowspan="2">User Service level</td><td>User Service 1</td><td colspan="2">Sport channel with joke of the day</td><td></td></tr>
<tr><td>User Service 2</td><td></td><td colspan="2">News channel with joke of the day</td></tr>
</table>

User Service Session level	**User Service Session**	MBMS Streaming Session (Sport)				MBMS Download Session (Joke / day)		MBMS Streaming Session (News)	
	RTP session/ FLUTE channel	streaming audio (RTP session)		streaming video (RTP session)		file object download (FLUTE channel)		streaming audio (RTP session)	streaming video (RTP session)
Key management level	**Key Domain**	MCC/MNC		MCC/MNC		MCC/MNC		MCC/MNC	MCC/MNC
	Key Group	Key Group A		Key Group B		Key Group C		Key Group D	Key Group E
	MSK Note 1	MSK A1 (current)	MSK A2 (next)	MSK B1	MSK B2	MSK C1	MSK C2	MSK D1	MSK D2	MSK E1	MSK E2
	MTK Note 1	MTK ..	MTK ..	MTK …	MTK …	MTK …	MTK …	MTK ..	MTK …	MTK …	MTK …
Transport Service level	**Transport Service**	MBMS Bearer N		MBMS Bearer N+1		MBMS Bearer N+2		MBMS Bearer N+3	MBMS Bearer N+4

Note 1: This row has a time dimension.to illustrate that MSKs and MTKs can be updated.

3GPP TSG-SA WG3 Meeting #38
Geneva, Switzerland, April 26-29, 2005

Tdoc S3-050292

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **061** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Omitted MTK Update Error Message
Source:	⌘	Nokia
Work item code:	⌘	MBMS
Date:	⌘	11/04/2005
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:	⌘	At the moment, the RFC 3830 specifies that all errors SHOULD be reported to the peer(s) by an error message. The BM-SC is vulnerable to the denial of service attack, because the MTK update uses multicast and MSK_I is shared with a large number of UEs. An attacker may generate many erroneous MTK update messages with a valid message authentication code. In the result, the BM-SC may be exhausted by error messages, which were sent by genuine UEs.
Summary of change:	⌘	It is specified that it is forbidden to send an error message as a result of receiving a MTK message.
Consequences if not approved:	⌘	The BM-SC is vulnerable to denial of service attacks.

Clauses affected:	⌘	Changed: 6.3.3.2

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

⌘

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

===== **BEGIN CHANGE** =====

6.3.3.2 MTK update procedure

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

The UE shall not send an error message to the BM-SC as a result of receiving an MTK message.

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

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc ⌘ S3-050318

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **062** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Editorial corrections to TS 33.246
Source:	⌘	SA3 (Ericsson, Siemens)
Work item code:	⌘	MBMS
Date:	⌘	19/4/2005
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:	⌘	The CR introduces editorial corrections.
Summary of change:	⌘	Editorial corrections.
Consequences if not approved:	⌘	Unclear specification.

Clauses affected:	⌘	2, 4.1.1, 4.1.2, 5.1- 5.3, 6.1, 6.2.1.1, 6.2.1.3, 6.3.1, 6.3.2.1, 6.3.2.1A, 6.3.2.1B, 6.3.2.2.1, 6.3.2.2.3, 6.3.2.2.4, 6.3.2.3.1, 6.3.3.1, 6.4.4, 6.4.5.2, 6.5.2, 6.6.1, 6.6.2.1, 6.6.3.2, B.1, B.1.1, B.1.4, B.2, B.2.1, B.2.2, B.2.5, C.2, C.3, C.5, D.3, G.2, G.2.1, G.2.2, H.2.1.

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

Other comments:	⌘	

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-msec-newtype-keyid-01.txt>.

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

[18] 3GPP TS 24.109: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

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

[20] 3GPP TS 29.109: "3rd Generation Partnership Project; Technical Specification Group Core Network; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

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

4.1.1 General

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a MBMS Uuser Sservice 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 MBMS Uuser Sservice.

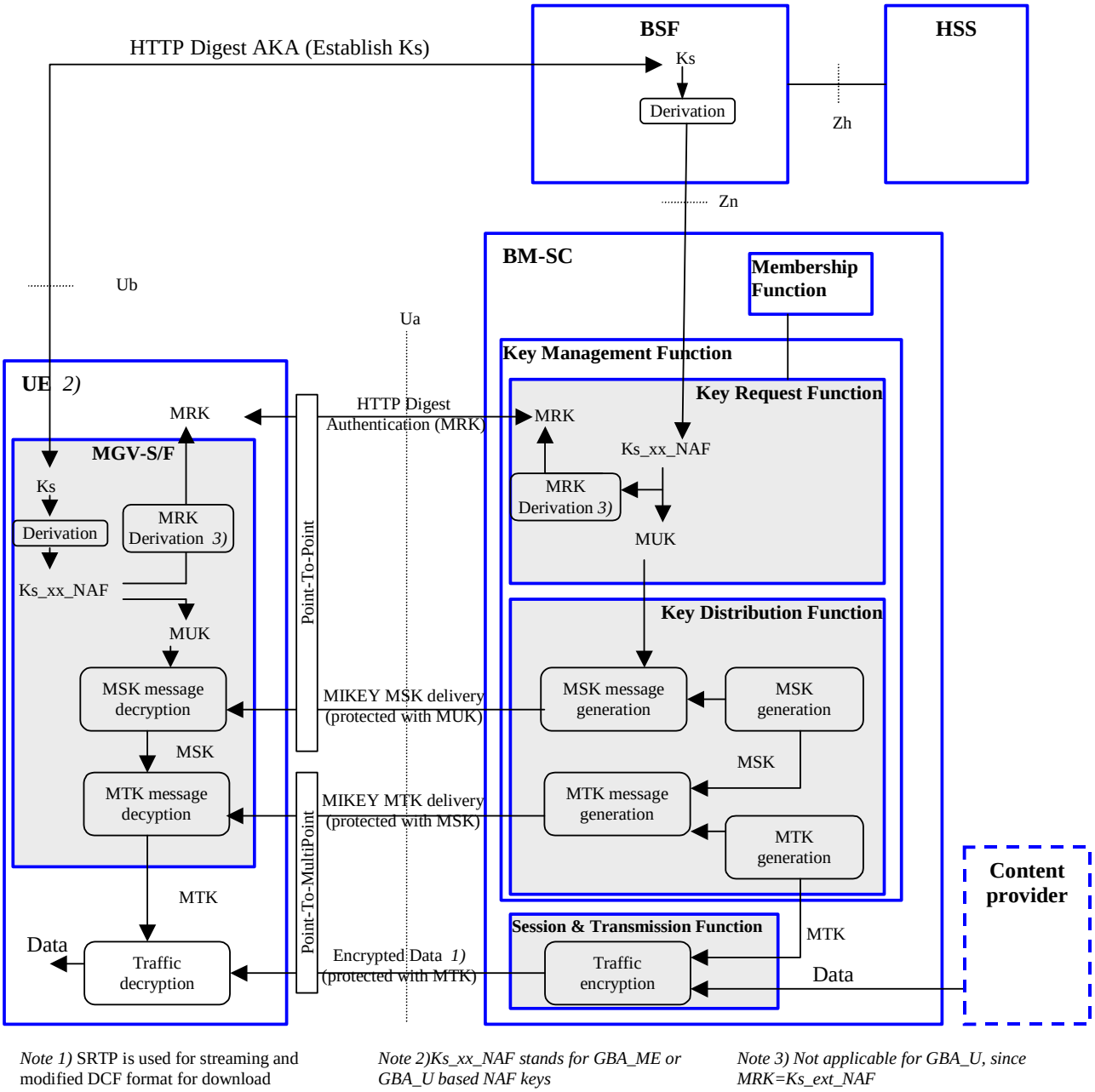


Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS, except for the normal network bearer security, resides in either the BM-SC or the UE. The BSF is a part of GBA (TS 33.220 [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 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. The 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 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 service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish 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 keys for the 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 MBMS key management functions itself;
- a BM-SC shall support using both GBA_ME and GBA_U keys to enable both ME based and UICC based MBMS key management, respectively.

4.1.2 BM-SC sub-functions

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

- **Key Management function:** The Key Management function includes two sub-functions: Key Request function and Key Delivery Distribution 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 Ddistribution function, performing subscription check from Membership function. The sub-function implements the following functions and 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 Ddistribution 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 contentdata

- **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 TS 23.246 [3].

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

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised such that only legitimate users are able to participate in an MBMS User Service.

When the UE 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 Uuser Sservice Rregistration procedure (clause 6.3.2);
- MBMS Uuser Sservice Dderegistration 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 Uuser Sservice, it is authenticated and authorized as defined in clause 6.2.2.

5.2 Key derivation, management and distribution

Like any service, the keys that are used to protect the transmitted data in a MBMS Uuser Sservice 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 User Sservice. 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 User sService.

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 function is used by the procedures listed below:

- MRK derivation (clause 6.1);

The following procedures are involved in Key management and distribution:

- ~~MRK derivation (clause 6.1);~~
- MBMS Uuser Sservice Rregistration procedure (clause 6.3.2);
- MBMS Uuser Sservice Dderegistration 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 procedure (clause 6.3.2).

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS User ~~s~~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 User S~~s~~ervice 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 traffic protection functions can be distinguished~~procedures are involved in Key management and distribution~~:

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

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

6.1 Using GBA for MBMS

TS 33.220 [6] GBA (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS U~~u~~ser S~~s~~ervice.

Before a user can access an MBMS User S~~s~~ervice, 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 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 S~~s~~ervice 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_NAF with the ME. Both the BM-SC and the ME use the key Ks_NAF as MUK. 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].

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~~ BM-SC 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 *******

6.2.1.1 General

This clause describes authentication of the user to the BM-SC when using HTTP digest with bootstrapped security associations.

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

6.2.1.3 HTTP digest authentication

When the UE initiates an HTTP procedure towards the BM-SC, 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 TS 24.109 [18]

The following adaptations apply to HTTP digest:

- the B-TID as specified in TS 33.220 [6] is used as username;
- MRK (MBMS Request Key) is used as password~~;~~.

All HTTP 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.

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

6.3.1 General

In order to protect an MBMS User S~~s~~ervice, it is necessary to 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.

The operator may configure the BM-SC ~~may also~~ to refrain from ~~sending~~ pushing 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 clause 6.3.2.2.2 shall be used if present within the Service Announcement.

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

The details of the HTTP procedures and HTTP error situations are specified in Annex G. An example of detailed MSK request procedure is described in Annex H. The XML schemas of the HTTP payloads ~~is~~ are specified in TS 26.346 [13].

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

6.3.2.1 MSK identification

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

where

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

NOTE 1: 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 2: 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.

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~~wants to receive that MBMS User Service, the UE should register to the MBMS User Service.

NOTE 1: 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.

NOTE 2: The MBMS ~~u~~User ~~s~~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 is for the UE to know to which IP address to send within the MBMS User Service ~~MSK~~ Registration/Deregistration and MSK request Procedures~~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 TS 26.346 [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.

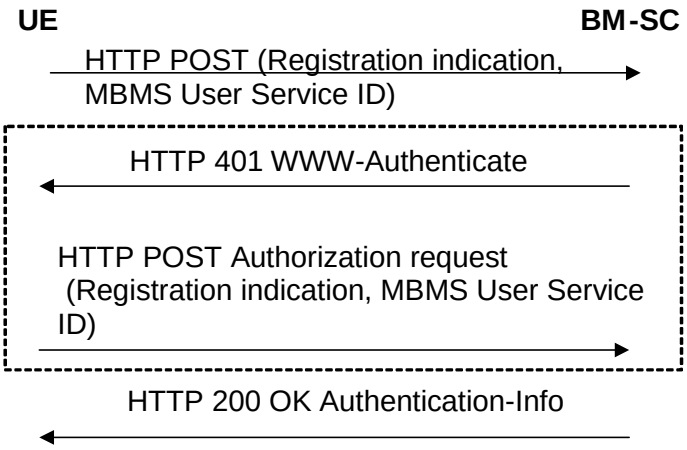


Figure 6.0A: MBMS User service registration procedure

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 6.0A), 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 clause G.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.

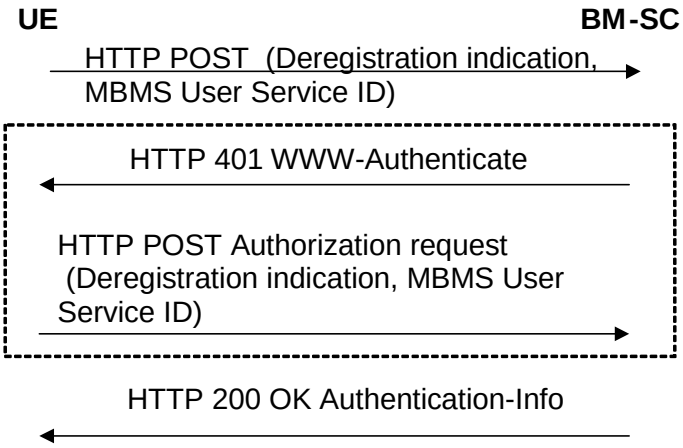


Figure 6.0B: MBMS User Sservice Dderegistration procedure

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 6.0B), if the UE has used WWW Authorization request headers in the first message in figure 6.10.B 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 clause G.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 (see clause 6.3.2.3), i.e. SEQl is greater than SEQu.

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

6.3.2.2.1 Basic MSK request procedure

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

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

- initiation of key management when the UE has joined the MBMS Uuser Sservice;
- 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 procedure.

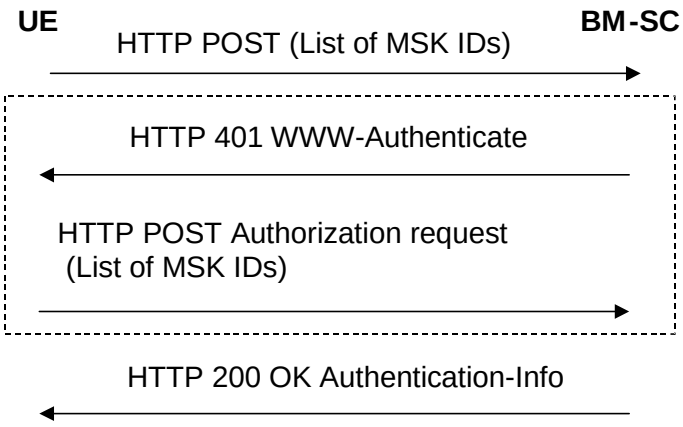


Figure 6.1: Basic MSK request procedure

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

- key identification information: a list of MSK IDs.

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.

NOTE 1: The exact syntax of the XML schema of the request parameters in the client payload and its MIME type are specified in TS 23.346 [13].

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 (see clause 6.3.2.3). The BM-SC sends a HTTP 200 OK message with Authentication-Info header.

NOTE 2: 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 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. 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 3: 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.

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

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~~ request procedure in clause 6.3.2.2.1.

6.3.2.2.4 BM-SC solicited pull procedure

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.

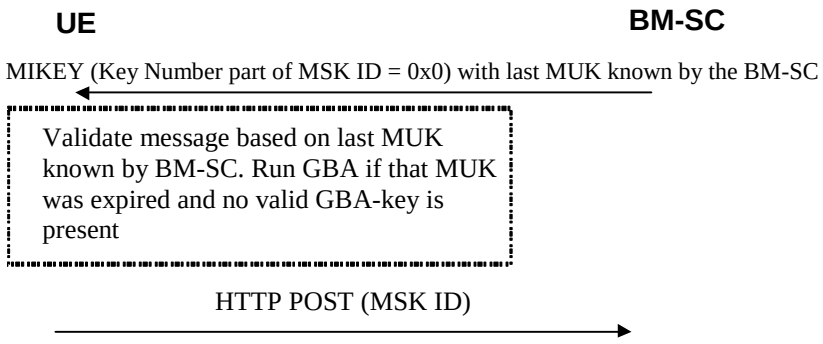


Figure 6.2b: BM-SC solicited pull

The BM-SC Key Distribution function sends a MIKEY message over UDP to the UE. The MIKEY message shall be protected by the 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.

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

6.3.2.3.1 Pushing the MSK to the UE

The BM-SC Key Distribution function controls when the MSKs used in a MBMS Uuser Sservice 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.

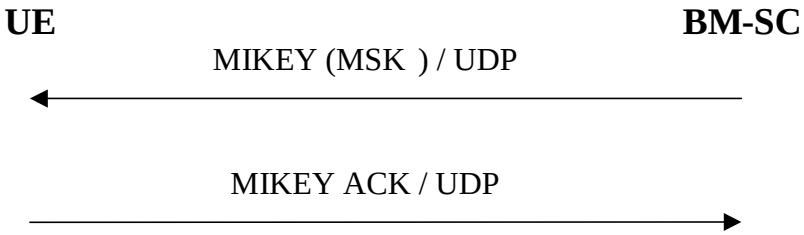


Figure 6.3: Pushing the MSKs to the UE

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 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.

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.

****** NEXT 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 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.

****** 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.

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 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.

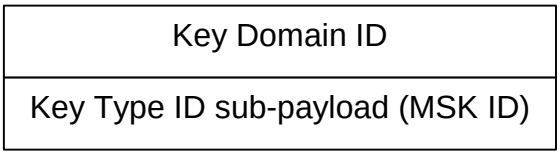


Figure 6.4a: Extension payload used with MIKEY MSK message

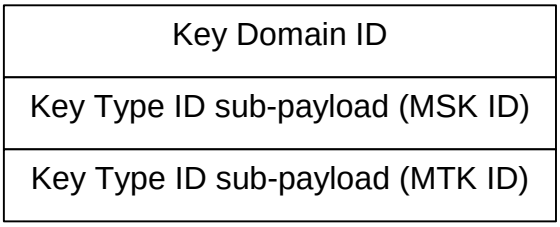


Figure 6.4b: Extension payload used with MIKEY MTK message

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

6.4.5.2 MSK Verification message structure

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.

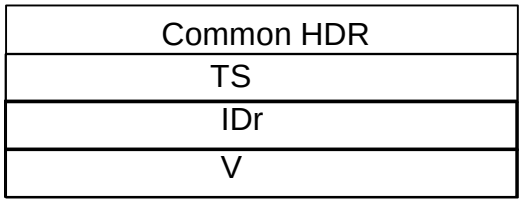


Figure 6.6: The logical structure of the MIKEY Verification message

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

The ME shall send the verification message, when received as result from the MGV-F, to the BM-SC.

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

6.5.2 Usage of MUK

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~~ MSK carried in the KEMAC payload as described in RFC 3830 [9].

****** 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 User ~~s~~Service. The protection of the data is applied by the BM-SC Session and Transmission Function. In order to determine which ~~key~~ MTK 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.

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

6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in RFC 3711 [11] shall be used. The MTK is carried to the UEs from the BM-SC using RFC 3830 [9] (MIKEY) with extensions defined according to this specification. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in section 4.3 of RFC ~~3830~~ 3711 [~~9~~11]. The correct MTK to use to decrypt the data is indicated using the MKI (Master Key identifier) field, which is included in the SRTP packets as defined in RFC 3711 [11]. The form of MKI shall be a concatenation of MSK ID and MTK ID, i.e. MKI = (MSK ID || MTK ID).

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in RFC ~~3830~~ 3711 [~~9~~11].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in section 6.10.1 in RFC 3830 [9].

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

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 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. OMA DRM Rights Objects are not utilized. Instead, encryption and authentication keys are generated from MTK. For integrity protection, an OMADRMSignature as specified below is attached inside the optional Mutable DRM information box ('mdri') of the DCF.

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

```
aligned(8) class OMADRMSignature extends Fullbox('odfssign', 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 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).

****** 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 MBMS Uuser Sservice data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS User Sservices;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here because in case these are transferred on a point-to-point connection (e.g. PS signalling connection), they are already secured. 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.

B.1.1 Unauthorised access to MBMS Uuser Sservice data

A1: Intruders may eavesdrop MBMS Uuser Sservice data on the air-interface.

A2: Users that have not joined and activated a MBMS Uuser Sservice receiving that service without being charged.

A3: Users that have joined and then left a MBMS Uuser Sservice continuing to receive the MBMS Uuser Sservice 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.1.4 Unauthorised access to MBMS User Sservices

D1: An attacker using the 3GPP network to gain "free access" of MBMS User Sservices and other services on another user's bill.

D2: An attacker using MBMS shared keys (MSK, MTK) to gain free access to content without any knowledge of the service provider.

NOTE: It cannot be assumed that keys held in a terminal are secure. No matter how the shared keys (MSK, MTK) are delivered to the terminal, we have to assume they can be derived in an attack. For example, the shared keys, while secure in the UICC, may be passed over an insecure SIM-ME interface.

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

B.2 Threats associated with attacks on other parts of the system

The threats associated with attacks on other parts of the system are split into the following categories, which are described in the following clauses:

- unauthorized access to data;
- threats to integrity;
- denial of service;
- ~~A~~a malicious UE generating MTKs for malicious use later on;
- ~~U~~unauthorized insertion of MBMS user data and key management data.

B.2.1 Unauthorised access to data

F1: It is assumed that the BM-SC and the GGSN are located in the same network. The BM-SC can though be located in a different place than the GGSN, and therefore can open up for intruders who may eavesdrop the ~~new~~ interface Gi and Gmb between the BM-SC and GGSN.

F2: Intruders may eavesdrop the ~~new~~ interface between the content provider and the BM-SC.

B.2.2 Threats to integrity

G1: It is assumed that the BM-SC and the GGSN are located in the same network. The BM-SC can though be located in a different place than the GGSN, and therefore can open up for new attacks on the ~~new~~ interfaces Gi and Gmb between the BM-SC and GGSN.

G2: The ~~new~~ interface between the content provider and the BM-SC may open up for attacks as modifications of multimedia content.

****** 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 MBMS U~~u~~ser S~~s~~ervice stream.

J2: An ME, which deliberately inserts key management and malicious data, encrypted with old (using replayed key management messages) MTK, within the MBMS U~~u~~ser S~~s~~ervice stream.

J3: An attacker, which deliberately inserts incorrect key management information within the MBMS U~~u~~ser S~~s~~ervice stream to cause Denial of Service attacks.

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

C.2 Requirements on MBMS ~~t~~Transport Service signaling protection

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signaling on the Gmb reference point.

NOTE 1: This requirement may be fulfilled by physical or proprietary security measures if the Gmb protocol endpoints (i.e. GGSN, Gmb-Proxy and BM-SC) are located within the same security domain of the operator's network. Otherwise the security mechanisms as specified within TS 33.210 [14] shall be applied.

R3b: Unauthorized modification, insertion, replay or deletion of all MBMS ~~t~~Transport ~~s~~Service signaling, on the RAN shall be prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE.

NOTE 2: UTRAN b~~B~~earer signalling integrity protection will not be provided for point to multipoint MBMS signalling and GERAN has no bearer signalling integrity protection, even for point to point signalling.

C.3 Requirements on Privacy

R4a: The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located outside the 3GPP operator's network.

R4b: MBMS identity and control information shall not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE.

NOTE: UTRAN and GERAN b~~B~~earer confidentiality protection will be not be provided for point to multipoint MBMS sessions.

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

C.5 Requirements on integrity protection of MBMS User Service data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.

NOTE 1: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.

NOTE 2: The use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in

R6b: The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.

R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.

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

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~~processing).

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.

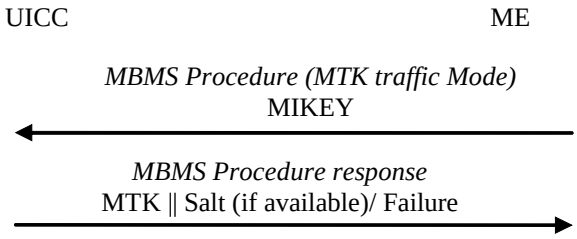


Figure D.3: MTK Generation and Validation

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

G.2 Key management procedures

This clause contains the following HTTP based procedures:

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

G.2.1 MBMS User Service Registration

The UE shall generate a request for MBMS User Service Registration according to clause 6.3.2~~*~~.1A~~*~~. 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 [19];
- 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 the 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.

G.2.2 MBMS User Service Deregistration

The UE shall generate a request for MBMS User Service Deregistration according to clause 6.3.~~*~~2.1B~~*~~. 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 [19];
- 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.

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

H.2.1 Successful MSK request procedure

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

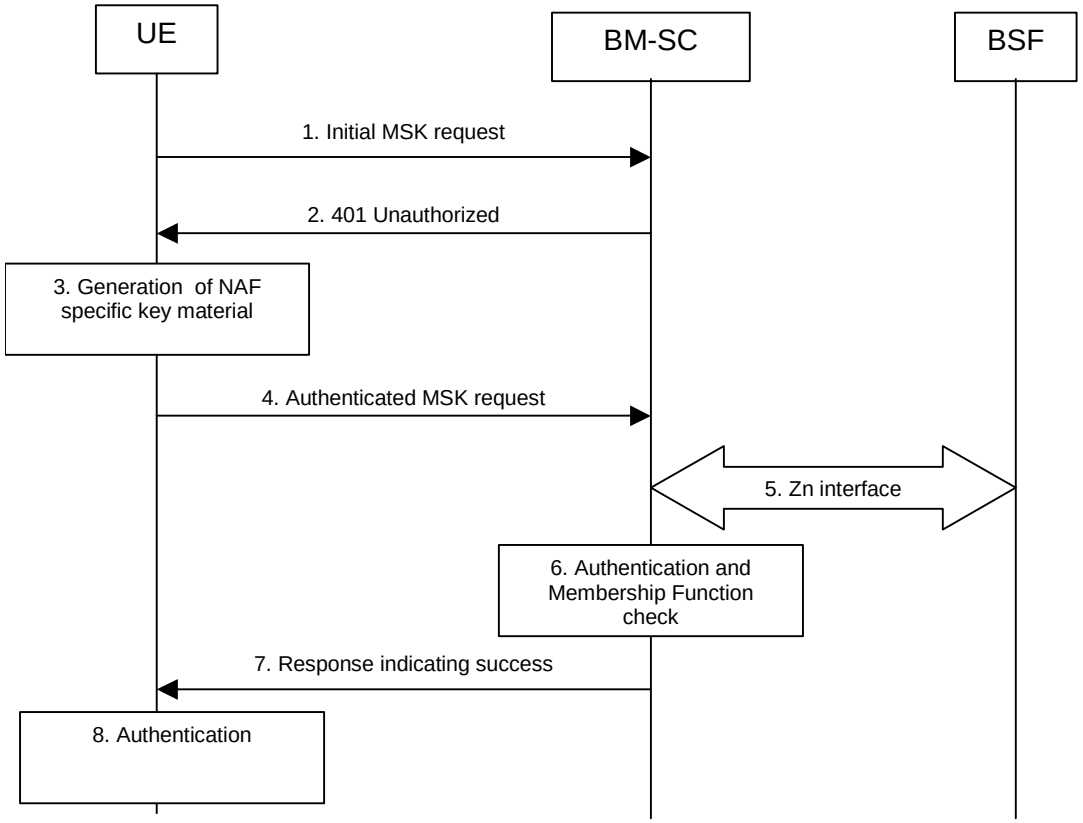


Figure H.2.1-1: Successful MSK request procedure.

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

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

Table H.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 H.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 H.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 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 H.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 H.2.1-3: Authenticated ~~enrolment~~ MSK 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 TS 29.109 [~~18~~20].

Table H.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 H.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 H.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#38 ***Tdoc S3-050294***
Geneva, Swithzerland, 26-29 May, 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **063** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Clarifications on MBMS key management
Source:	⌘	SA3 (Ericsson)
Work item code:	⌘	MBMS
Date:	⌘	19/4/2005
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 following issues are incorrect or need clarification:

- It is currently specified that MRK is identified only by the B-TID. However, the UE needs also the NAF ID.
- The NOTE in 6.3.2.1 says that Key Group parts should be unique within an operator, but it does not say why this is needed.
- Current text includes a leftover NOTE from TS version 6.1.0 that the MSK delivery may not happen immediately after MSK request. This NOTE is not needed anymore.
- Wrap around of Timestamp payload is specified in two places. The unnecessary text that also hints that MTK IDs can wrap around is removed.
- When a UE wants to deregister from an MBMS User Service, there is no need to make an authorization check. This is alignment of signal flow in annex with the text in chapter 6.3.2.1B.

Summary of change: ⌘ This CR clarifies the following issues:

- It is clarified that MRK is identified by the B-TID and NAF-ID in the UE
- It is clarified that Key Groups parts need to be unique within an operator if the Key Domain ID does not identify the BM-SCs uniquely.
- Note on time between MSK delivery after MSK request should be removed
- A duplicant statement of Timestamp wraparound that also hints that MTK IDs would wrap around is removed.
- Text on authorization check during deregistration is removed

Consequences if ⌘ Unclear specification.

not approved:	

Clauses affected:	⌘	6.1, 6.3.2.1, 6.3.2.2.1, 6.4.6.1, 6.4.6.2, G.2.2			
		Y	**N**		
Other specs Affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

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 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 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_NAF with the ME. Both the BM-SC and the ME use the key Ks_NAF as MUK. 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 and MRK are ~~is~~ identified by the combination of B-TID and NAF-ID in the UE and ~~the MRK is defined~~ by B-TID in the BM-SC, 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.

****** NEXT 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: If the Key Domain ID does not uniquely identify the BM-SC, ~~i~~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.

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

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

- initiation of key management when the UE has joined the MBMS user service;
- 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.

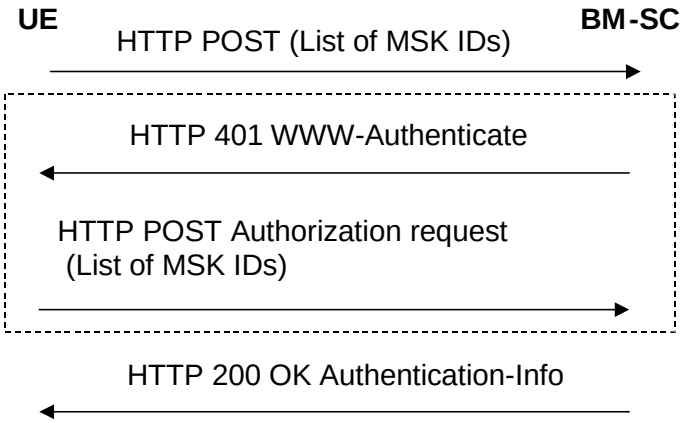


Figure 6.1: Basic MSK request procedure

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

- key identification information: a list of MSK IDs.

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.

NOTE: The exact syntax of the XML schema of the request parameters in the client payload and its MIME type are specified in TS 23.346 [13].

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 (see clause 6.3.2.3). The BM-SC 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 6.1), 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 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. 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.~~

****** 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 Timestamp payload field "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.

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 fields ``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 *******

G.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 [19];
- 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~~ authentication verification, tThe 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.

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc S3-050293

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **064** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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 **X**

Title:	⌘	Use of IMPI in MBMS
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	29/4/2005
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:	⌘	GBA TS 33.220 specifies that BSF *may* send the IMPI to the NAF. It has not been specified if IMPI is sent in case of MBMS. When the UE has run a new bootstrapping and contacts the BM-SC with a new B-TID, the BM-SC needs the IMPI to bind the old B-TID to the new B-TID (and continue the session over Ua with the UE with new GBA-keys). This CR proposes that IMPI is sent from BSF to the BM-SC when GBA-keys are received from the BSF.
Summary of change:	⌘	BSF sends IMPI to the BM-SC with the GBA-keys.
Consequences if not approved:	⌘	Update of GBA-keys in the middle of MBMS User Service is not possible. Also the Membership function may need to use the IMPI as a parameter for finding information related to a user.

Clauses affected:	⌘	3.1, 6.1, 6.2.1.3, H.2.1

	Y	N		
Other specs Affected: ⌘		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.

IMPI = In the context of current specification IMSI is used in the format of IMPI as specified in GBA, cf. TS 33.220 [6].

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.

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 *******

6.1 Using GBA for MBMS

TS 33.220 [6] (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS 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 TS 33.220 [6]. The BM-SC will act as a NAF (Network Application Function) according to TS 33.220 [6].

Along with the GBA-keys the BSF shall send the IMPI of the user to the BM-SC. When the UE has bootstrapped, it will use a new B-TID over the Ua reference point. The IMPI is used in the BM-SC to bind the old and the new B-TID together.

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_NAF with the ME. Both the BM-SC and the ME use the key Ks_NAF as MUK. 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].

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.

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

6.2.1.3 HTTP digest authentication

When the UE initiates an HTTP procedure towards the BM-SC, 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]. Along with the GBA-keys the BSF shall send the IMPI of the user to the BM-SC. The details of HTTP digest authentication are specified in clause 5.2 of TS 24.109 [18]

The following adaptations apply to HTTP digest:

- the B-TID as specified in TS 33.220 [6] is used as username;

- MRK (MBMS Request Key) is used as password;

All HTTP 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.

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

H.2.1 Successful MSK request procedure

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

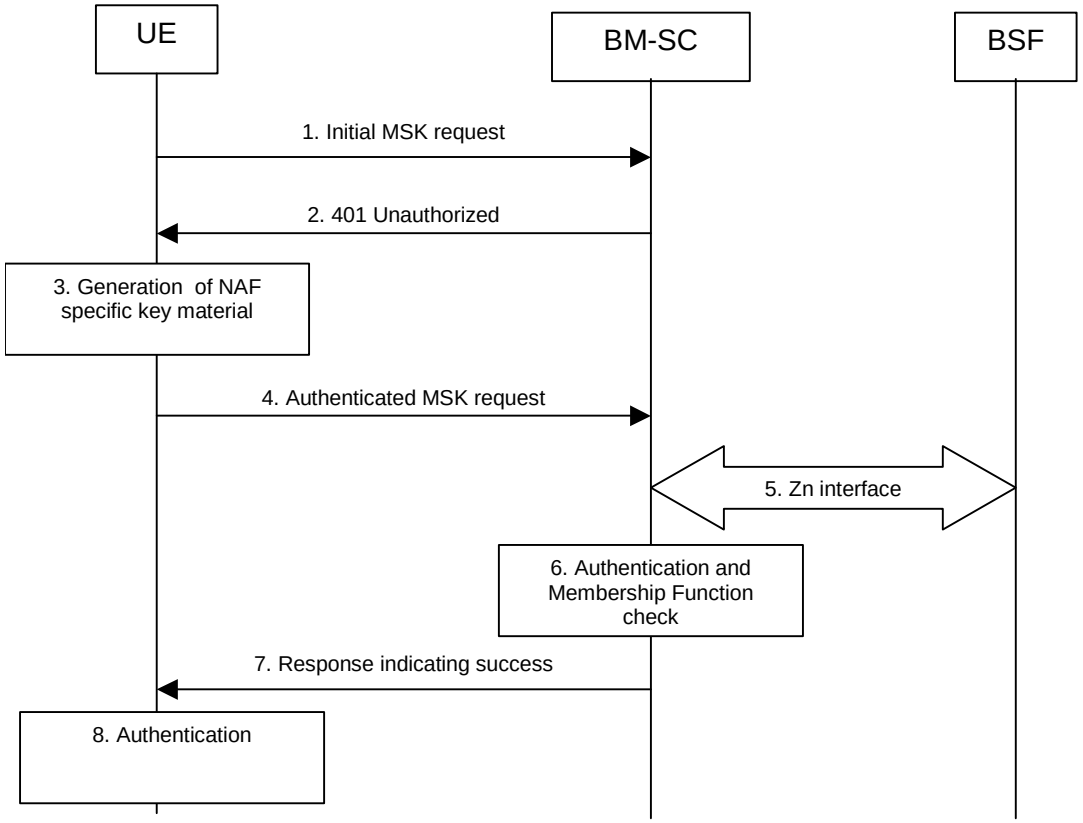


Figure H.2.1-1: Successful MSK request procedure.

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

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

Table H.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 H.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 H.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 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 H.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 H.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 and IMPI of the user. BM-SC further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

For detailed signalling flows see TS 29.109 [18].

Table H.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 H.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 H.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 SA3#38
April 26- 29, 2005, Geneva, Switzerland

Tdoc S3-050297

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **065** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

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

Title:	⌘	Clarification on CSB ID and SP payload use
Source:	⌘	SA3 (Siemens)
Work item code:	⌘	MBMS
Date:	⌘	18/4/2005
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:	⌘	Confusion about wording ‘not used’ of MIKEY header fields
Summary of change:	⌘	Clarify that SP payload is not present for download. Clarify that CSB ID shall be present, but the CSB ID is not used for identification purposes.
Consequences if not approved:	⌘	Misinterpretation possible, leading to wrong implementations.

Clauses affected:	⌘	6.4.2			
		Y	**N**		
Other specs Affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

******* BEGIN OF 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 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 for identification purposes but shall be present. The UE shall use the same CSB ID of the MSK delivery message in the ACK message.

NOTE: As the CSB ID field has no meaning within the context of MBMS, the BM-SC is free to assign any value to CSB ID. Assigning random values to CSB ID enhances security as CSB ID is taken into account for MIKEY key derivations (section 4.1.3 and 4.1.4 of RFC 3830 [9]).

In case of download services, the SP payload shall not be present ~~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].

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

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc ⌘S3-050290

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **066** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	MIME type adjustments according to LS S3-050192
Source:	⌘	SA3
Work item code:	⌘	MBMS
Date:	⌘	27/04/05
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:	⌘	In S3-050192 SA4 asks SA3 to review annex C of TS 26.346, and modify the proposed MIME types used by SA3. It was noted that the types SA3 currently proposes comes from the vendor tree, and that deviates from the naming of the other MIME types in annex C.
Summary of change:	⌘	Removal of the vendor tree naming in the MIME types for: • MSK request • Registration request • Deregistration request in the examples in annexes G and H.
Consequences if not approved:	⌘	Inconsistent naming of MIME types will be used.

Clauses affected:	⌘	G.2.1, G.2.2, G.2.3, H.2.1

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

Other comments:	⌘	

*** START OF CHANGE ***

G.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 [19];
- 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 the 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.

G.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 [19];
- 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.

G.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 [19];
- 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 H.

*** NEXT CHANGE ***

H.2 Signalling flows demonstrating a successful MSK request procedure

H.2.1 Successful MSK request procedure

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

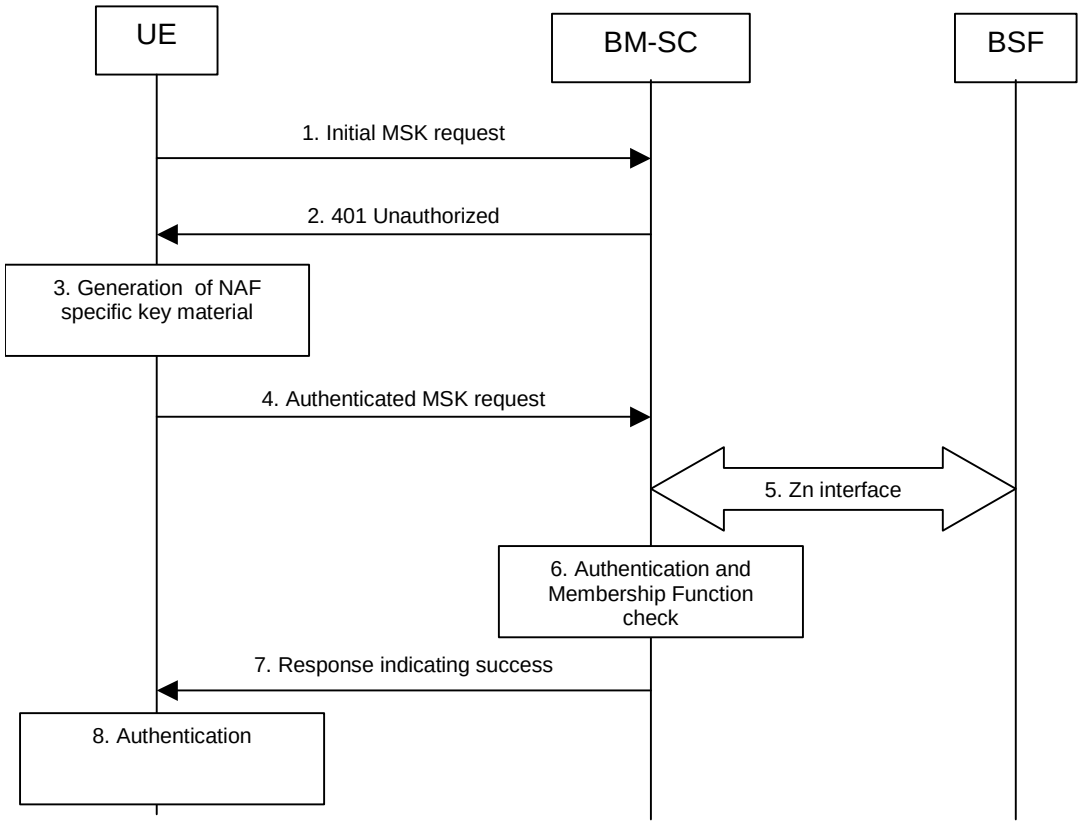


Figure H.2.1-1: Successful MSK request procedure.

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

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

Table H.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 H.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 H.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 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 H.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 H.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 TS 29.109 [18].

Table H.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 H.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 H.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 SA3#38
April 26- 29, 2005, Geneva, Switzerland

Tdoc ⌘S3-050319

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **067** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Results of mapping the MBMS security requirements into security functions and mechanisms
Source:	⌘	MCC
Work item code:	⌘	MBMS
Date:	⌘	29/4/2005
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:	⌘	According to the updated issue list to complete MBMS Security [S3-050183] from SA3#37 the consistency check has not been completed. This CR provides the results of mapping the MBMS security requirements into security functions and mechanisms.
Summary of change:	⌘	New Annex included to provide the result of the consistency check
Consequences if not approved:	⌘	Without this consistency check it is not clear that all the requirements have been met. Implementations could be affected by lack of information.

Clauses affected:	⌘	New Annex

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

Other comments: ⌘

******* BEGIN OF CHANGE *******

Annex x (informative): Mapping the MBMS security requirements into security functions and mechanism

Ax.1 Consistency check

Ax.1.1 Requirements on secure service access

Security requirement	**Check result**
R1a: A valid USIM shall be required to access MBMS User Services.	This is provided by GBA. Ks_xxx_NAF generation requires a valid USIM.
R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.	GBA and HTTP digest authentication provide this.
R2a: It shall be possible for the network (e.g. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.	A user is authenticated during the MBMS user service registration and MSK re-keying.
R2b: It shall be possible to prevent the use of a particular USIM to access MBMS User Services.	GAA user security settings provide this.

Ax.1.2 Requirements on MBMS transport Service signaling protection

Security requirement	**Check result**
R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signaling on the Gmb reference point.	NDS/IP covers this.
R3b: Unauthorized modification, insertion, replay or deletion of all transport service signaling, on the RAN shall be prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE.	Examples of the attacks could be: • Changing the source address of the content e.g. from indicating company A to company B. • Changing data indicating the type of content from type A to Type B • Changing data indicating type of protection required etc • Appending content to the end of the original content Analysis has shown that there is not any transport service signaling sent over PTM that would need protection.

Ax.1.3 Requirements on Privacy

Security requirement	**Check result**
R4a: The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located outside the 3GPP operator's network.	The content provider knows only the BM-SC.
R4b: MBMS identity and control information shall not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE.	Such identity and control information could be: • The identities of the content providers • Information on which content providers have the most customers • The identities of the content recipients in the case of multicast services to small groups of users Information which could be used to identify specific users is not exposed on the point-to-multipoint channel. However, it may still be possible to identify whether a particular user is subscribed to a particular MBMS service. This could be done by following the physical movement of a particular subscriber and the changes between the use of point-to-point and point-to-multipoint bearers for particular MBMS services in the cells that serve the target subscriber. It is seen unnecessary to protect against this kind of an attack. The only control information exposed on the point-to-multipoint channel is the unprotected fields in the MIKEY MTK transport message. However, revealing this information does not seem to pose a significant security risk.

Ax.1.4 Requirements on MBMS Key Management

Security requirement	**Check result**
R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected..	The MSK and MTK update messages are encrypted.
R5b: The transfer of the MBMS keys between the MBMS key generator and the UE shall be integrity protected.	The MSK and MTK deliveries can 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, 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	Supported by re-keying functionality.

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.	MSKs are delivered only to authorized users and the delivery is protected using MUK level keys.

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).	The same CK and IK are not used in GBA and radio level. In addition, Ks_xxx_NAF generation uses a one-way function.
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	MUK is identified by the combination of B-TID and NAF-ID and the MRK is defined by B-TID MSK is uniquely identifiable by its Key Domain ID and MSK ID MTK is uniquely identifiable by its Key Domain ID, MSK ID and MTK ID
R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).	The BM-SC knows whether Ks_int_NAF + Ks_ext_NAF or Ks_NAF was generated.
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.	Freshness is checked by MGV-F.

Ax.1.5 Requirements on integrity protection of MBMS User Service data

Security requirement	**Check result**
R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.	This is provided at the application layer using SRTP or OMA DRM DCF.
R6b: The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.	This is provided at the application layer using SRTP or OMA DRM DCF.
R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.	This can be provided by NDS/IP.

Ax.1.6 Requirements on confidentiality protection of MBMS User Service data

Security requirement	**Check result**
R7a: It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.	This is provided at the application layer using SRTP or OMA DRM DCF..
R7b: The MBMS User Service data may be encrypted with common encryption keys, which shall be available to all users that have joined the MBMS User Service	This is provided at the application layer using SRTP or OMA DRM DCF.

R7c: It may be required to encrypt the MBMS User Service data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.	This can be provided by NDS/IP.
R7d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on protect the MBMS User Service from the BM-SC to the UE.	The BM-SC decides about the security level. There is no security association negotiation between the UE and the BM-SC.
R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.	This is provided at the application layer using SRTP or OMA DRM DCF.

Ax.1.7 Requirements on content provider to BM-SC reference point

Security requirement	**Check result**
R8a: The BM-SC shall be able to authenticate and authorize a 3rd party content provider that wishes to transmit data to the BM-SC.	The mechanism to meet the requirement is left to be implemented between the BM-SC and a 3rd party.
R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.	The mechanism to meet the requirement is left to be implemented between the BM-SC and a 3rd party.

Ax.2 Conclusions

Based on the above results of the consistency check between the security requirements and security functions/mechanisms the MBMS security requirements have been adequately met.

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