3GPP TSG SA WG3 Security — SA3#34 **S3-040621**
6-9 July 2004
Acapulco, Mexico

Source: **MBMS Security Rapporteur**

Title: **Initial update of MBMS TS**

Document for: **Approval**

Agenda Item: **MBMS**

1 Introduction

The attachment to this document contains an initial version of the MBMS TS to reflect the changes that were agreed in the following document S3-040470, S3-040469, S3-040553, S3-040535, S3-040489, S3-040565 and S3-04573 (except the change in clause 6.5, which is included in S3-040620). A few modifications were left to the MBMS drafting group. These changes appear in clauses 4.2, 6.3.1.1, B.2.5, C.2 and C.3 are indicated with yellow highlighting.

The following contribution will also need to be included in the TS, if agreed by SA3, S3-040618 (update of S3-040479), S3-040619 (update of S3-040582) and S3-040620 (update of S3-040552).

Draft 3GPP TS 33.246 V1.3~~2~~.0~~1~~ (2004-07~~6~~)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security;
Security of Multimedia Broadcast/Multicast Service
(Release 6)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, multimedia, broadcast, security

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The security of MBMS provides different challenges compared to the security of services delivered over point-to-point services. In addition to the normal threat of eavesdropping, there is also the threat that it may not be assumed that valid subscribers have any interest in maintaining the privacy of the communications, and they may therefore conspire to circumvent the security solution (for example one subscriber may publish the decryption keys enabling non-subscribers to view broadcast content). Countering this threat requires the decryption keys to be updated frequently in a manner that may not be predicted by subscribers while making efficient use of the radio network.

1 Scope

The Technical Specification covers the security procedures of the Multimedia Broadcast/Multicast Service (MBMS) for 3GPP systems (UTRAN and GERAN). MBMS is a GPRS network bearer service over which many different applications could be carried. The actual method of protection may vary depending on the type of MBMS application.

2 References

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

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

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

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

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

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

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

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

[7] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application~~T3 specification describing MBMS application and interface procedures on UICC~~"

[8] IETF RFC 2617 "HTTP Digest Authentication"

[9] IETF: MIKEY: Multimedia Internet KEYing; http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-08.txt; Work In Progress

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

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

MFK = MBMS traffic key Freshness Key: This key is derived from MSK and is used to ensure that MTK is fresh.

MGK = MBMS traffic key Generation Key: This key is derived from MSK and is used to protect MTK.

MRK = MBMS Request Key: This key is to authenticate~~authorize~~ the UE to the BM-SC when performing key requests etc.

MSK = MBMS Service Key: The MBMS Service key that is securely transferred (using the key MUK) from the BM-SC towards the UE. For MBMS streaming the MSK is not used directly to protect the MBMS User Service data (see MTK).

~~Editors Note: How the MSK is used for download is still under study.~~

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function F_t with a key derived from MSK. The key MTK is used to decrypt the received MBMS data on the ME.

MUK = MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSK's to the UE.

~~Editors Note~~NOTE: The keys MSK and MUK may be stored within the UICC or the ME depending on the MBMS service. The function F_t may be realized on the ME or the UICC

3.2 Symbols

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

F_f	MFK generation function
F_g	MGK generation function
F_m	Keyed MAC function used to check the freshness of MTK
F_t	MTK generation function

3.3 Abbreviations

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

MBMS	Multimedia Broadcast/Multicast Service
MGV-F	MTK Generation and Validation Function

~~4 MBMS security architecture~~4 MBMS security overview

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3G network. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service. The point-to-point services in a 3G network use the AKA protocol (see TS 33.102 [4]) to both authenticate a user and agree on keys to be used between that user and the radio network. These keys are subsequently used to provide protection of traffic between the network and the UE.

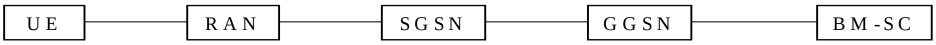


Figure 1: MBMS security architecture

Figure 1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

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

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

4.2 Key management overview

A MBMS User Service may contain one or more MSKs which may be in use at the same time and are managed at the MBMS User Service Level. The BM-SC controls the use of the MSKs towards the different Transport Services. The MSKs are not directly used towards the MBMS Transport Services but as a second level key MTK as specified within clauses 6.4 and 6.5.

NOTE: According to good security practice the use of the same MTK with two different protocols shall be avoided

For MBMS User Services it shall be possible to share one or more MSKs with other MBMS User Service, as according to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services.

NOTE: 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.

5 MBMS security functions

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised in ~~two~~ following situations ~~parts~~ when participating in an MBMS User Service. That is: ~~Firstly~~

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

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

- when the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service. ~~and secondly when the UE requests and receives MSKs for the MBMS User Service. The MBMS bearer establishment requires a point to point connection with the network on which authentication is performed using network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.~~

- when the UE requests and receives MSKs for the MBMS User Service

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

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

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

~~Editor's Note: It was agreed that the GBA method will be used for MBMS Security (GBA-U + GBA-ME + MIKEY). It was agreed that the work would continue under the assumption of there being both the UICC-based solution and ME-based solution. If a Terminal is to support MBMS, then it will need to support GBA-U.~~

~~Editor's Note: Authentication may also be needed for application layer joining and leaving. The final decision relies of work in SA4.~~

5.2 Key management and distribution

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

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

~~Editor's note: It needs to be decided if there is to be a minimum amount of traffic that is to be protected with one key, as this puts a lower limit on the frequency of key changes, e.g. one continuous transmission of data. It could also be possible for several of these minimum amounts to be transmitted with changing the key. It is ffs what this minimum amount should be and whether several of these minimum amounts can be transmitted without changing the key.~~

~~Editor's note: If all users need to request a key update simultaneously then there may need to be some method of ensuring that all the users do not request a key update at the same time. This mechanism is ffs.~~

~~Editor's note: The keys can be distributed to each user receiving the same MBMS service in point-to-point mode when the number of the users is relatively small. And the users receiving the same Multicast service within the same area can also be further combined into one to several subgroups to make it possible that the keys can be given to all users within one subgroup at a time in point-to-multipoint mode.~~

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence requires no additional protection). This protection will be either confidentiality and integrity or just confidentiality. 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.

~~Editor's note: It was agreed that the encryption should be done end-to-end between the UE and BM-SC, and not at either the Radio or the Core Network level. The actual method of protection was for further study.~~

~~Editor's note: It was noticed that when data is sent on a ptp MBMS bearer, it would be ciphered between the BM-SC and UE and also over the RAN. SA3 agreed that this "double ciphering" was unnecessary from a security point of view. This was indicated to RAN2 and GERAN2 in an LS (S3-030156) and the choice on whether to "double cipher" was left to these groups. RAN2 (S3-030328) indicated it would be easier to "double cipher" as this kept the RAN simpler, whereas GERAN2 (S3-030184) indicated that they would avoid "double ciphering".~~

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 (GE-)RAN. Although this "double ciphering" is unnecessary from a security point of view it is a (GE-)RAN decision whether to apply ciphering or not in (GE-)RAN.

6 Security mechanisms

6.1 Using GBA for MBMS

GBA[6] is used to agree keys that are needed to run an MBMS Multicast User service. MBMS imposes the following requirements on the MBMS capable UICCs and MEs:

A UICC that contains MBMS key management functions shall implement GBA_U.

An 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.

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 [6] section 5. The BM-SC will act as a NAF according to [6].

The MSKs for an MBMS User service shall be stored on either the UICC or the ME. Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions (and by requirement is GBA aware) and requires that all of the network elements, i.e. HSS, BSF and BM-SC, to be GBA_U aware. As a result of the GBA_U run in these circumstances, 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 to protect MSK deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within clause 6.2.

NOTE: A run of GBA_U on a GBA aware UICC will not allow the MSKs to be stored on the UICC, if the MBMS management functions are not present on the UICC.

In any other circumstance, a run of GBA results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK (MBMS Request Key). 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~~MBMS~~ within the protocols as described within clause 6.2.

6.2 Authentication and authorisation of a user

~~Editor's note: this section will contain the details on authentication and authorization of an MBMS user~~

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

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

6.2.1 Authentication and authorisation in application level joining

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication [~~6~~8] for 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 chapter "Procedures using the bootstrapped Security Association" in [6]. The BM-SC will act as a NAF according to [6].

The following adaptations apply to HTTP digest:

- The transaction identifier as specified in [~~8~~6] is used as username
- MRK (MBMS Request Key) is used as password.
- The joined MBMS user service is specified in client payload of HTTP Digest message.

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

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

6.2.2 Authentication and authorisation in MBMS bearer establishment

The authentication of the UE during MBMS bearer establishment relies on the authenticated point~~-~~-to-point connection with the network, which was set up using network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

6.2.3 Authentication and authorisation in MSK request

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

6.2.4 Authentication and authorisation in post delivery procedures

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

~~Editor's Note: The use of bootstrapped keys for leaving an MBMS user service, for an MSK key request and request to a download repair server is for ffs.~~

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

6.3 Key update procedures

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

6.3.1 MSK procedures

6.3.1.1 Handling of MSKs in UE

Every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID

where

Network ID = MCC || MNC and is 3 bytes long. It is carried in the ID_I payload in MIKEY message

Key Group ID is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted. It is carried in the CSB ID field of MIKEY common header.

MSK ID is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Key Service ID. It is carried in the MSK-ID field of MIKEY extension payload.

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

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

6.3.1.2 UE initiated MSK update procedure

~~Once~~ When a UE detects that it needs the MSK(s) for a specific MBMS User service~~has joined a multicast service~~, the UE should try to get the MSKs that will be used to 'protect' the data transmitted as part of this multicast service. Reasons for UE to retrieve the MSK(s) include e.g.:

- Retrieval of initial MSKs e.g. when the UE has joined the MBMS user service

Editor's note: The initial key request may~~can~~ also be part of User Service joining procedure if SA4 decides to have such procedure. In this case the MSKs will be transported after the joining procedure has completed.

- Retrieval of MSKs when the UE has missed a key update procedure e.g. due to being out of coverage

If the UE fails to get hold of the MSK or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service.

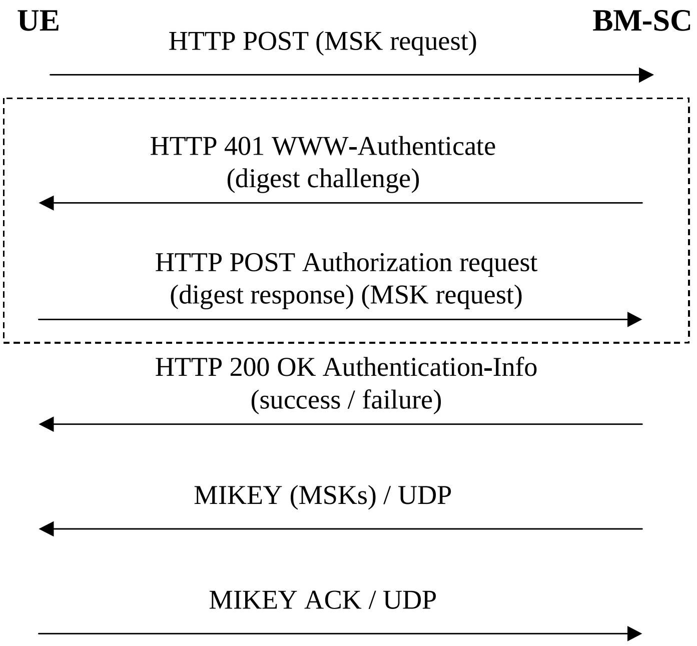

UE
BM-SC
HTTP POST (MSK request)
HTTP 401 WWW-Authenticate
(digest challenge)
HTTP POST Authorization request
(digest response) (MSK request)
HTTP 200 OK Authentication-Info
(success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP

Figure x. UE initiated MSK delivery

The UE ~~tries~~ requests for ~~to get~~ the MSKs using the ~~second message in the below flow~~HTTP POST message. The key identification information is included in the client payload of the HTTP message.~~–~~

The BM-SC may challenge the UE with HTTP response including WWW-Authenticate header and digest-challenge. Upon receiving the digest-challenge, the UE calculates the digest response and re-sends HTTP POST message including the key request and Authorization Request header including the digest response.

The BM-SC sends a response in HTTP 200 OK message with Authentication-Info header. The response in client payload includes cause code for success or reject.

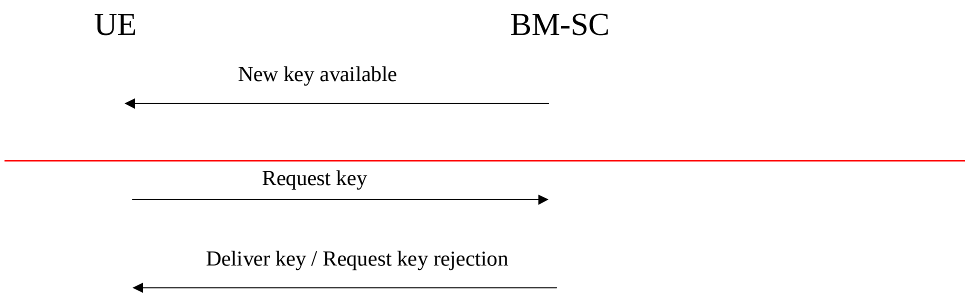
If the key request procedure above resulted to success, the BM-SC sends MIKEY messages over UDP transporting the requested MSKs to the UE.

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

6.3.1.3 BM-SC initiated MSK update procedures

6.3.1.3.1 Pushing the MSKs to the UE

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



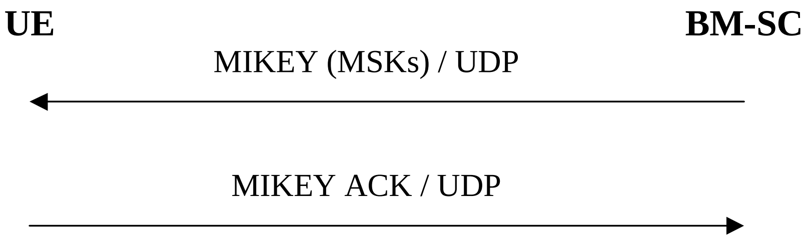


Figure x. Pushing the MSKs to the UE

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

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

6.3.1.3.2 Push solicited pull

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSKs. An example of such situation is when the BM-SC wants the UE to authenticate itself during the service or when the MUK has expired.

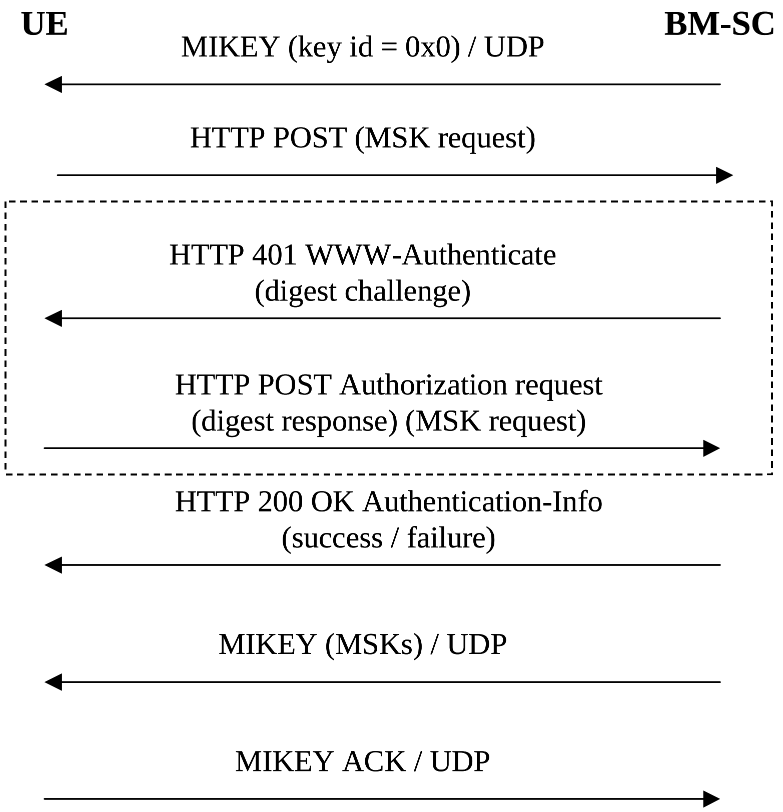

UE
BM-SC
MIKEY (key id = 0x0) / UDP
HTTP POST (MSK request)
HTTP 401 WWW-Authenticate
(digest challenge)
HTTP POST Authorization request
(digest response) (MSK request)
HTTP 200 OK Authentication-Info
(success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP

Figure x. Push solicited pull

The BM-SC sends MIKEY message over UDP to the UE. The key IDs in the extension payload of the MIKEY message set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

When the UE contacts the BM-SC, the BM-SC may trigger re-authentication of the UE or even re-run of GBA procedure to update the MUK.

The rest of the procedure is the same as in 6.3.1.

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

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

~~The second message is used to request an MSK. This is sent by the UE when it either receives the first message in the flow and does not have the new MSK, or has just joined a multicasts service and does not have an MSK for that service or has received some protected content and does not have the MSK that was used to protect the content. If the UE fails to get hold of the updated MSK or receive confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still valid older MSK, the UE shall leave the MBMS service.~~

- ~~After receiving the second message the BM-SC should send out the appropriate MSK to the UE protected by the relevant means, or reject the UE's key request with an indication of the cause. Upon successfully receiving the new MSK, the UE should store this key for later use.~~

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

6.3.2 MTK procedures

The MTK is delivered to the UE as in 6.3.2.1 but the MIKEY ACK is not used.

6.4 MTK generation and validation at the UE

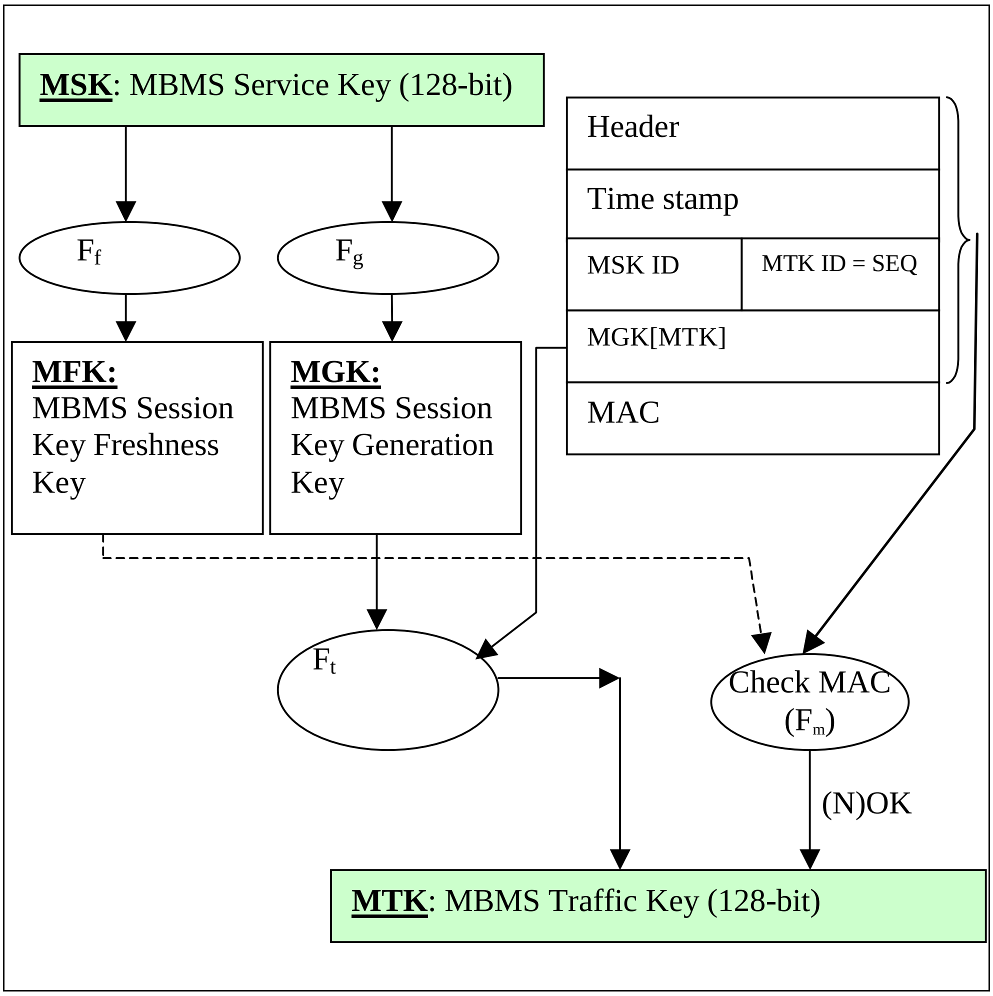

MSK: MBMS Service Key (128-bit)
Header
Time stamp
MSK ID
MTK ID = SEQ
MGK[MTK]
MAC
F_f
F_g
MFK: MBMS Session Key Freshness Key
MGK: MBMS Session Key Generation Key
F_t
Check MAC (F_m)
(N)OK
MTK: MBMS Traffic Key (128-bit)

Figure 1: MTK Validation and Generation Function

The ME will call the (*MTK Generation and Validation Function)* MGV-F that is realized as part of the ME or as part of the UICC. It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. Both MSK and SEQs were transferred to the MGV-S with the execution of the key update procedures as described in section 6.2. The initial value of SEQs is determined by the service provider.

When the ME receives the MIKEY message (including e.g.MSK ID, MTK ID = SEQp, MGK[MTK], MAC) from the ptm data stream, it shall give the MIKEY message to the MGV-F. The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh. How this shall be done is described below:

The MGV-F shall derive a key MFK (MBMS traffic key Freshness Key) from the MSK using a key derivation function F_f, and shall derive a key MGK (MBMS traffic key Generation Key) from the MSK using a key derivation function F_g.

The traffic key generation shall be performed in the following way:

The traffic key decrypt function F_t decrypts the received MGK[MTK] to obtain MTK.

The freshness check shall be performed in the following way:

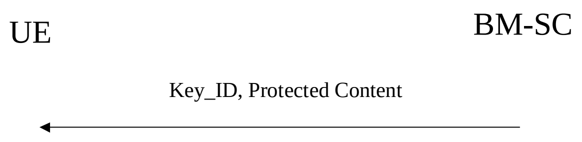
The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC using a keyed MAC function F_m with the received MIKEY message and the key MGK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message.. If the MAC defers then the MGV-F will indicate a failure to the ME. If the MAC is equal then the MGV-F shall update SEQs with SEQp value and start with the generation of MTK. The MGV-F provides the MTK to the ME.

6.5 Protection of the transmitted traffic

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and Ues that are accessing the MBMS service. The protection of the data is applied by the BM-SC. In order to determine which key was used to protect the data a Key_ID is included with the protected data. The Key_ID will uniquely identify the MSK and contain other information needed to calculate the MTK. If the UE does not have the MSK indicated by Key_ID, then it should fetch the MSK using the methods discussed in the clause 6.3. The MTK is derived according to the methods described in clause 6.4.

Note: including the Key_ID with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

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



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

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

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

Annex A (informative): Trust model

The following trust relationship between the roles that are participating in MBMS services are proposed:

The user trusts the home network operator to provide the MBMS service according to the service level agreement. .

The user trusts the network operator after mutual authentication.

The network trusts an authenticated user using integrity protection and encryption at RAN level.

The network may have trust or no trust in a content provider.

The home network and visited network trust each other when a roaming agreement is defined, in the case the user is roaming in a VPLMN.

Annex B (informative): Security threats

B.1 Threats associated with attacks on the radio interface

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

unauthorized access to multicast data;

threats to integrity;

denial of service;

unauthorized access to MBMS services;

privacy violation.

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

B.1.1 Unauthorised access to multicast data

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

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

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

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

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

B.1.2 Threats to integrity

B1: Modifications and replay of messages in a way to fool the user of the content from the actual source, e.g. replace the actual content with a fake one.

B.1.3 Denial of service attacks

C1: Jamming of radio resources. Deliberate manipulation of the data to disturb the communication.

B.1.4 Unauthorised access to MBMS services

D1: An attacker using the 3GPP network to gain “free access” of MBMS services 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.

B.1.5 Privacy violation

E1: The user identity could be exposed to the content provider, in the case the content provider is located in the 3GPP network, and then linked to the content.

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 sub-chapters:

unauthorized access to data;

threats to integrity;

denial of service;

A malicious UE generating MTKs for malicious use later on;

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.

B.2.3 Denial of service

H1: Deliberated manipulation of the data between the BM-SC <-> Content Provider to disturb the communication.

H2: Deliberated manipulation of the data between the BM-SC <-> GGSN to disturb the communication.

B.2.4 A malicious UE generating MTKs for malicious use later on.

I1: A malicious ME querying the MTK generation function for MTK's to use them later on in an attack (e.g. in order to use the retrieved MTKs within an unauthorized data insertion attacks (See B.2.5)).

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

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

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

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

Annex C (normative): Multicast security requirements

~~Editor's note: Not all the security requirements in this section have been agreed.~~

C.1 Requirements on security service access

C.1.1 Requirements on secure service access

R1a: A valid USIM shall be required to access ~~any 3G service including the~~ MBMS User Services.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.

~~Editor's note: No requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale~~

C.1.2 Requirements on secure service provision

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.

~~Editor's note: Authentication during service is ffs.~~

R2b: It shall be possible to prevent the use of a particular USIM to access MBMS User Services.

~~Editor's Note: It is for FFS to what extent it is required to detect and prevent fraudulent use of MBMS services.~~ NOTE: No security requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale

C.2 Requirements on MBMS 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.

Editor's note: When the Gmb reference point is IP-based then NDS/IP methods according to TS 33.210 may be applied to fulfill requirement R3a. The Gmb interface is ffs.

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

~~Editor's note~~NOTE: UTRAN Bearer signalling integrity protection will not be provided ~~be turned off~~ for point to multipoint MBMS signalling~~sessions~~ 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.

~~Editor's note: This may already be covered by some national regulations.~~

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~~Editor's note~~: UTRAN and GERAN Bearer confidentiality protection will be not be provided ~~turned off~~ for point to multipoint MBMS sessions

C.4 Requirements on MBMS Key Management

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

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

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

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

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

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

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

~~Editor's note: If ptm re- keying is used, the keys shall be delivered in a reliable way. Ptp re-keying is assumed to be reliable.~~

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

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

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.

~~Editor's note~~NOTE: 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~~Note~~: T~~t~~he 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.

C.6 Requirements on confidentiality protection of MBMS User Service data

R7a: It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.

R7b: The MBMS User Service data may be encrypted with~~ a~~ common encryption keys, which shall be available to all users that have joined the MBMS User Service.

R7c: It may be required to encrypt the MBMS User Service data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

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.

R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.

C.7 Requirements on content provider to BM-SC reference point

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.

R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.

NOTE: This reference point will not be standardised.

Annex <X> (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2002-09					Initial version supplied by Rapporteur		0.0.1
2002-11					Updated to include the threat and requirements discussed at SA3 #25.	0.0.1	0.0.2
2003-02					Updated to reflect changes to the requirements agreed at SA#26	0.0.2	0.0.3
2003-04					Updated to reflect changes agreed at the SA#27	0.0.3	0.10.0
2003-07					Updated to reflect the decision on TEK distribution and independence of the MBMS keys from radio level keys	0.1.0	0.1.1
2003-08					Updated to reflect agreement in SA#29 on adding confidentiality requirements, editor's note about double ciphering, and text indicating that different security mechanisms may be needed to protect different protocols/codec that may be used in MBMS and re-organisation of the requirements section.	0.1.1	0.2.0
2003-09					Updated to reflect decision at Antwerp ad-hoc.	0.2.0	0.2.1
2003-11					Updated to reflect changes to requirements and threat at SA3#30	0.2.1	0.2.2
2003-11					Updated to reflect decisions taken at SA3#31while discussing tdoc 755 and attached pseudo CR.	0.2.2	0.2.3
2003-11					Updated to reflect all the other decisions taken at SA3#31	0.2.3	0.3.0
2003-11					Updated with some editorial modification and presented to the SA plenary for information	0.3.0	1.0.0
2004-02					Updated to reflect changes agreed at SA3#32	1.0.0	1.1.0
2004-04					Minor corrections agreed by e-mail discussion	1.1.0	1.1.1
2004-05					Updated to reflect the decisions taken at SA3#33	1.1.1	1.2.0
2004-06					Small editorial corrections	1.2.0	1.2.1
2004-07					Updated to reflect the decisions taken at SA#34 S3-040470, S3-040469, S3-040553, S3-040535, S3-040489, S3-040565, S3-04573 Outstanding: Updates of S3-040497, S3-040552, S3-030582	1.2.1	1.3.0