**3GPP TSG-SA3 Meeting MBMS Ad Hoc**
**Antwerp, Belgium, September 2003**

***Tdoc ⌘S3z030007***

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ⌘ | **33.246** | **CR** | | ⌘ **rev** | | ⌘ Current version: | **0.1.1** ⌘ |

*For* ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

| | | | | |
|---|---|---|---|---|
| ***Proposed change affects:*** | UICC apps⌘ ☒ | ME ☒ | Radio Access Network □ | Core Network ☒ |

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | MBMS Security Architecture | | |
| ***Source:*** | ⌘ | BT Group, Gemplus, Giesecke and Devrient, Lucent Technologies, Qualcomm Europe, SchlumbergerSema | | |
| ***Work item code:*** | ⌘ | MBMS | ***Date:*** ⌘ | 01/09/2003 |
| ***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:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | Description of key management for MBMS |
| ***Summary of change:*** | ⌘ | Add Introduction. Add reference to 3GPP2 standard in Section 2. Add appropriate defintions and abbreviations in Section 3. Update MBMS functional architecture in Section 4. Replace reference to (undefined) 'TEK' in section 5. Add description of key management in Section 6. Note further threats in Annex B, sections B.1.1 and B.1.4. |
| ***Consequences if not approved:*** | ⌘ | |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ | |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

**3GPP TSG SA WG3 Security — S3#29** **S3-030358**
**15 - 18 July 2003, San Francisco, USA**

# 3GPP TS 33.246 V0.1.1~~0~~ (2003-07~~4~~)

*Technical Specification*

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

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

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.

*Select keywords from list provided in specs database.*

Keywords

<keyword[, keyword]>

***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 4

Introduction 4

1 Scope 5~~65~~

2 References 5~~65~~

3 Definitions, symbols and abbreviations 5~~65~~
3.1 Definitions 5~~65~~
3.2 Symbols 6~~75~~
3.3 Abbreviations 6~~75~~

4 MBMS security architecture 7~~86~~
4.1 Security requirements 7~~86~~
4.1.1 Requirements on security service access 7~~86~~
4.1.1.1 Requirements on secure service access 7~~86~~
4.1.1.2 Requirements on secure service provision 7~~86~~
4.1.2 Requirements on integrity protection of MBMS multicast data 7~~86~~
4.1.3 Requirements on confidentiality protection of MBMS multicast data 8~~97~~
4.1.4 Requirements on MBMS Key Management 8~~97~~
4.1.5 Requirements on Privacy 8~~97~~
4.1.6 Requirements on MBMS signaling protection 8~~97~~

5 MBMS security functions 10~~118~~
5.1 Authenticating and authorizing the user 10~~118~~
5.2 Key management and distribution 10~~118~~
5.3 Protection of the transmitted traffic 10~~128~~

6 Security mechanisms 11~~128~~
6.1 Authentication and authorisation of a user 11~~128~~
6.2 Key management 11~~128~~
6.3 Protection of the transmitted traffic 15~~168~~

**Annex A (informative):Trust model 16~~179~~**

**Annex B (informative): Security threats 16~~179~~**

B.1 Threats associated with attacks on the radio interface 16~~179~~
B.1.1 Unauthorised access to multicast data 16~~179~~
B.1.2 Threats to integrity 16~~179~~
B.1.3 Denial of service attacks 17~~1810~~
B.1.4 Unauthorised access to MBMS services 17~~1810~~
B.1.5 Privacy violation 17~~1810~~

B.2 Threats associated with attacks on other parts of the system 17~~1810~~
B.2.1 Unauthorised access to data 17~~1810~~
B.2.2 Threats to integrity 17~~1810~~
B.2.3 Denial of service 17~~1810~~

**Annex <X> (informative): Change history 18~~1911~~**

# 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

*This clause is optional. If it exists, it is always the second unnumbered clause.*

Operators providing MBMS services face threats stemming from a different trust model than that of existing services: 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.) Combined with the fact that content decryption takes place in Mobile Equipment which is assumed to be insecure, MBMS demands a unique security solution and frequently updated decryption keys which may not be predicted by subscribers, while making efficient use of the radio network.

Assuming the primary threat is subscribed users distributing decryption keys to non-subscribed users, the solution is for the decryption key to change frequently and in an unpredictable manner. The challenge is achieving this while minimizing the transmission overhead required for key distribution. The solution described herein is to take a two-tiered approach, distributing a Broadcast Access Key (BAK) to each user individually, and for many short-term decryption keys SK to be derived using the BAK and public information sent with the broadcast. The BAK is stored in the UICC. This approach allows the short-term keys SK to be changed as frequently as desired, without incurring significant costs in radio resources or key management, while BAK is changed depending on business requirements stemming from the subscription periods for the services.

# 1 ~~1~~ Scope

The Technical Specification covers the security procedures of the Multimedia Broadcast/Multicast Service (MBMS) for 3GPP systems (UTRAN and GERAN).

# 2 ~~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 TR 23.846: " Multimedia Broadcast/Multicast Service; Architecture and Functional Description".

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

[5] *3GPP2 S.P0083 Version 0.5*, Broadcast-Multicast Security Framework,.

# 3 ~~3~~ Definitions, symbols and abbreviations

*Delete from the above heading those words which are not applicable.*

*Subclause numbering depends on applicability and should be renumbered accordingly.*

## 3.1 ~~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.

~~**example:** text used to clarify abstract rules by applying them literally (place saver to retain format).~~

**Broadcast Access Key:** A 128-bit key that provides access to the content of a particular multicast service/session for a certain amount of time (for example, one day, week or month). Each encrypted multicast service should have a different BAK value. Each BAK should have the associated BAK_ID, BAK_Expire:

**Broadcast Access Key Identifier:** A sequence number that identifies which value of BAK is currently being used to generate SK values for a particular multicast service. For a particular BAK, the corresponding value of BAK_ID is the same for all users.

**Broadcast Access Key Expire:** Indicates when the BAK will expire. This may be indicated by the time when the BAKwill expire, or by the Delta time left until the BAK expires, in which case it is calculated when a new BAK is received. Therefore, there may be multiple BAK_Expire values associated with the same BAK. The UE is expected to request a new BAK value before the BAK_Expire time expires.

**Broadcast Access Key Distributor:** (functional entity): Obtains authorization and TK from SM and encrypts BAK for delivery to UICCs.

**Broadcast Access Key Generator:** (functional entity): Generates BAK, determines BAK_ID and BAK_Expire, and delivers them to the BAKD and SKM. BAKs should be generated in a secure manner and appear random.

**Content Encryptor:** (functional entity): Encrypts content, and sends the encrypted content to the UE via the cellular system.

**Content Provider**: A third party content provider.

**Registration Key:** provisioned in the UICC and SM prior to joining a multicast service. Each SM should have a unique 128-bit RK for each UICC.

**Short-term Key:** The CE to encrypt the multicast data using the 128-bit short-term key (SK). The UE decrypts the multicast data using SK. The SK is calculated in the SKM and the UICC. The SK is derived from SK_RAND and BAK.

**Short-term Key Random Number**: used to calculate a unique SK

**Short-term Key Manager**: (functional entity): Generates SK using BAK and SK_RAND and passes SK, SK_RAND and BAK_ID to the CE.

**Subscription Manager:** (functional entity): performs accounting, authentication and authorization for MBMS. The SM also calculates the TK, based on the RK, used to hide the BAK. The SM may be the subscriber's home AAA (H-AAA) or be an independent entity.

**Temporary Key:** A 128-bit key used by the BAKD to encrypt BAK when provisioning BAK in the UICC. The TK is obtained from the SM.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

| | |
|---|---|
| BAK | Broadcast Access Key |
| BAK_ID | BAK Identifier |
| BAK_Expire: | Indicates when the BAK will expire. |
| BAKD | BAK Distributor (functional entity) |
| BAKG | BAK Generator (functional entity) |
| CE | Content encryption (functional entity) |
| CP | Content provider |
| MBMS | Multimedia Broadcast/Multicast Service |
| RK | Registration Key |
| SK | Short-term Key |
| SK_RAND | SK Random Number use to calculate a unique SK |
| SKM | SK Manager (functional entity) |
| SM | Subscription Manager (functional entity) |
| TK | Temporary Key |

# 4 4 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 network. These keys are subsequently used to provide integrity protection of signalling traffic and optional confidentiality protection of both signalling and user data between the RNC and the UE.

MBMS could possibly use the AKA procedure to authenticate the user. It requires its own key management/distribution process, as the same key(s) needs to be sent to a group of users. The key distribution method could rely on the point-to-point confidentiality to protect the transfer of MBMS keys. The protection of the data may also require a special mechanism.

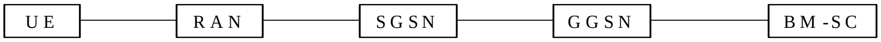

**Figure 1: MBMS security architecture**

Figure 1 gives an overview of the network elements involved in MBMS from a security perspective. 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.

## 4.1 Security requirements

The following security requirements have been identified for MBMS.

Editor's note: Not all the security requirements in this section have been agreed. Most of the requirements are for the multicast service only.

### 4.1.1 Requirements on security service access

#### 4.1.1.1 ~~4.1.1.1~~ Requirements on secure service access

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

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

#### 4.1.1.2 ~~4.1.1.2~~ 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 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 services.

Editor's Note: It is for FFS to what extent it is required to detect and prevent fraudulent use of MBMS services.

### 4.1.2 Requirements on integrity protection of MBMS multicast data

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS multicast data sent to the UE on the radio interface. The use of integrity shall be optional.

Editor's 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: 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

R3b: The MBMS multicast data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS service.

R3c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.

Editor's Note: It may be required to integrity protect the multimedia content on the "Content Provider - BM-SC" interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.

### 4.1.3 Requirements on confidentiality protection of MBMS multicast data

R4a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R4b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that have joined the MBMS service.

R4c: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

Editor's Note: It may be required to encrypt the multimedia content on the "Content Provider - BM-SC" interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.

### 4.1.4 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 be integrity protected.

R5c: The UE and MBMS key generator shall support re-keying to ensure that users that have joined a multicast service, but then left, shall not gain further access to the multicast service without being charged appropriately. The re-keying shall also ensure that users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately

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

R5e: The MBMS key encryption key 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).~~

Editor's Note: The MBMS key generator function is still to be allocated to a network node.

### 4.1.5 Requirements on Privacy

R6a: 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.

### 4.1.6 Requirements on MBMS signaling protection

R7a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS 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 R7a. The Gmb interface is ffs.

## 4.2 Security Functional Architecture

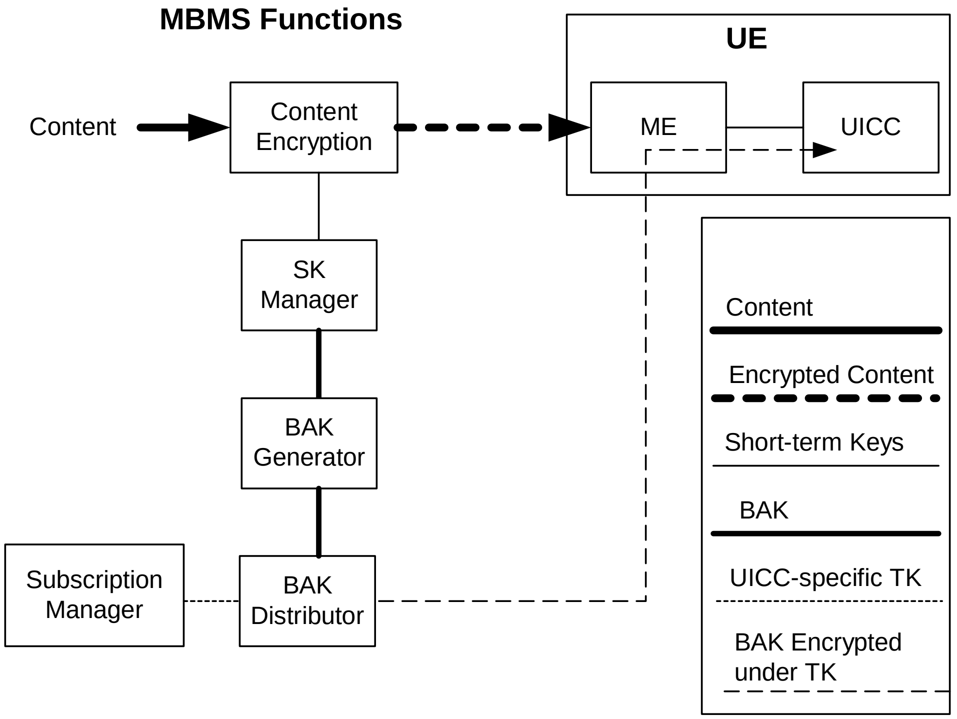

Figure 4.2 Functional Architecture

Figure 4.2 shows the functional entities that may be involved in MBMS. Those entities represent functions essential to support secure MBMS. They could be incorporated in one or more physical entities in the network. It should not be assumed that these functional entities correspond to separate architectural entities, so not all interfaces will require standardization. The allocation of the security functions to network entities is outside the scope of this document.

### 4.2.1 Summary of Functional Entities

**CONTENT PATH**

Content Source (CS)**: Generates the un-encrypted content.**

**Content Encryptor (CE)**: Encrypts the content using the SK provided by the SKM. Encryption may take place at the Content Source or in the serving cellular system.

**KEY/AUTHORIZATION PATH**

**Subscription Manager (SM)**: May provide the functions of Authentication, Authorization and Accounting (AAA). The SM shares a Registration Key RK with the UICC: This key RK may be the key K used for AKA, a derivative, or some other key provisioned specifically for MBMS. The SM calculates the TK, based on the user specific RK.

**BAK Generator (BAKG):** Generates the Broadcast Access Key (BAK) as required, and distributes BAK and to BAKD and SKM.

**BAK Distributor (BAKD):** Controls the distribution of the Broadcast Access Key (BAK).

**SK Manager (SKM):** Controls the updating and distribution of the Short-term Key (SK).

**User Equipment (UE)** For the purposes of this document, the UE is considered as two separate entities, the UICC and ME.

**UICC**: The UICC shares a key RK with the SM. The UICC performs all key management related to MBMS.

**ME**: Mobile Equipment. Includes equipment for receiving the broadcast. The ME performs decryption of encrypted content using SK obtained from the UICC.

# 5 ~~5~~ MBMS security functions

## 5.1 ~~5.1~~ Authenticating and authorizing the user

The user and the network could mutually authenticate each other using the AKA protocol that is used for standard point-to-point communication. Once authenticated, there should be an authorisation to determine whether a particular user is allowed to access that particular multicast service or not, e.g. some multicast services may be only available to some users.

Editor's note: The use of AKA between the BM-SC and UE was proposed. It was concluded that the issue of bootstrapping and having the BM-SC in the visited network need to be further investigated.

## 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 is even more necessary in a Multicast service, as the need to changed keys can also be driven by a new user joining the service (to stop them being able to decrypt data sent before they joined the service) or a user leaving the service (to stop them being able to decrypt traffic sent after they left the service).

It was agreed that ~~TEK~~ generation and distribution of content encryption keys ~~to the UE~~ are managed by the BM-SC.

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 probably be either confidentiality and integrity or just confidentiality.

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.

# 6 ~~6~~ Security mechanisms

## 6.1 ~~6.1~~ Authentication and authorisation of a user

~~6.2~~Editor’s note: this section will contain the details of how a user joins a particular Multicast Service

## 6.2 Key management

~~Editor’s note: this section will contain the details of how the keys are updated in a Multicast Service~~Figure 6.2 shows the basic communications involved in the key distribution for MBMS encryption. Many details are omitted in this diagram for the sake of clarity. The Figure is described below.

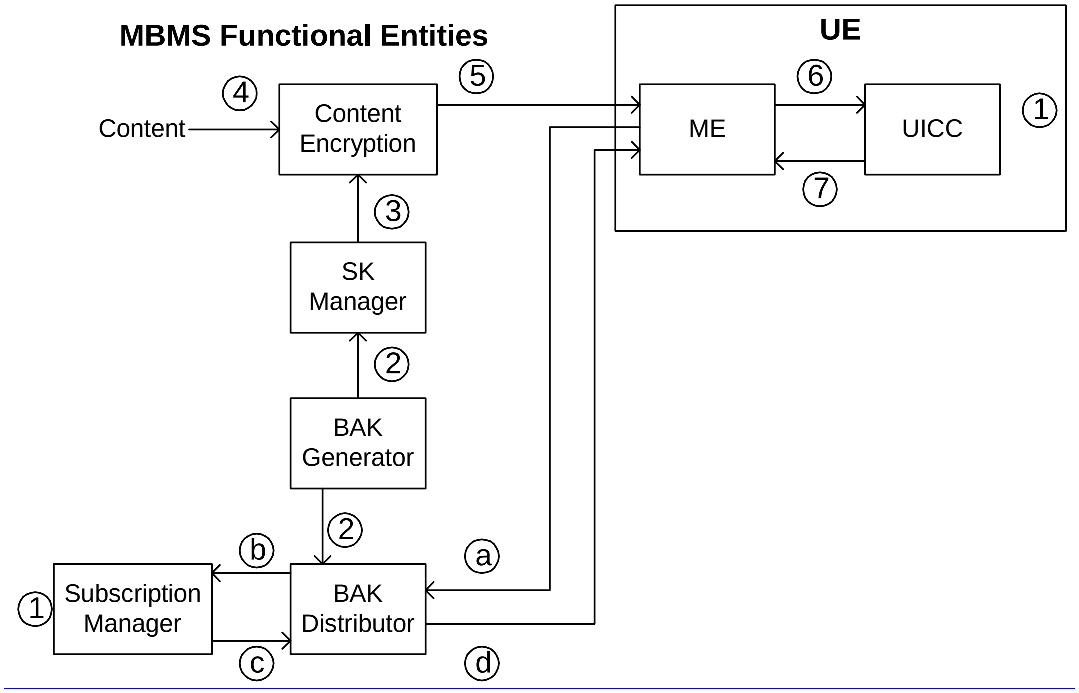

Figure 6.2 Logical Architecture showing functional entities involved in MBMS security.

#### 6.2.1.1 BAK Generation

The following steps (1-2) are performed prior to the transmission of encrypted content to the UE:

1. The UICC and SM are provisioned with a Registration Key RK that will be the basis of authentication and key exchange with respect to MBMS.

2. The BAKG generates a value for BAK, and associates the value with an identifier BAK_ID and an expiry time (BAK_Expire). The value of BAK, along with the corresponding values of BAK_ID and BAK_Expire are passed to the SKM and BAKD.

### 6.2.1.2 Normal Procedure With Unchanged BAK

The following steps (3-7) occur under normal circumstances, when BAK is unchanged from the previous decryption operation in the UE.

3. The SKM creates SK from the current BAK and a random value SK_RAND. The SKM passes SK, SK_RAND, BAK_ID and BAK_Expire to the CE.

4. The CS sends unencrypted content to the CE.

5. The CE encrypts the content using SK and sends the encrypted content to the UE via the serving system. The CE also includes SK_RAND and BAK_ID with the encrypted content stream.

6. The ME receives the encrypted content, and takes action as follows:

    a. If BAK_ID and SK_RAND are unchanged from the last received content, the ME decrypts the content using the value of SK currently assigned to that content stream and passes the result to the user application;

    b. If BAK_ID or SK_RAND have changed, the ME requests a new SK from the UICC, including the broadcast service identifier, BAK_ID and SK_RAND.

7. The UICC generates SK from BAK and SK_RAND and returns SK to the ME, which decrypts the content and passes the result to the user application.

### 6.2.1.3 Procedure With Changed or Unavailable BAK

Steps (a-d) in Figure 6.2 are performed to request a new BAK. Section 6.2.2 discusses possible methods by which the UE determines that a new BAK is needed.

a. The ME sends a BAK request to the BAKD, including the BAK_ID of the BAK requested. The BAK request may include authentication information based on RK, which can be used by the SM to determine that the request came from a legitimate subscriber. Section 4.4.1 discusses the need for authentication of BAK requests.

b. In order to send BAK to the UICC, the BAK must be encrypted to protect it against reception by other than the intended recipient. The BAKD requests a temporary key (TK) generated by the SM.

c. The SM generates TK from a random value TK_RAND and RK. TK_RAND may be generated by the BAKD, or by the SM. TK_RAND may also be used as a challenge in the authentication process described in step a. The SM sends TK and TK_RAND to the BAKD.

d. The BAKD encrypts the value of BAK with TK, and sends the encrypted BAK, along with TK_RAND and BAK_LIFE to the UICC via the ME. The UICC first forms TK from TK_RAND and RK, and then decrypts the encrypted BAK with TK to form BAK. The value of BAK and its associated BAK_LIFE are stored in the UICC. The UICC should be able to store at least two values of BAK so that a new BAK can be obtained and stored in anticipation of the expiration of the BAK lifetime.

## 6.2.2 BAK Management

A user can repeat the BAK update process with multiple content streams. Thereafter (from a security perspective) the UE has the potential to be managing the decryption keys for multiple content streams simultaneously. In order to determine which BAK corresponds to which content stream, a MBMS identifier MBMS_ID should be stored with the BAK.

This document does not specify how an UE determines that it needs to update BAK. We assume that a means will be provided for the UE to determine that its BAK is about to expire or has expired, triggering action to perform a BAK update. Several methods are possible for accomplishing this. The specific method used is not important for the present subject.

**BAK_ID**. The UICC can determine if a BAK is associated with a particular content stream by referring to the corresponding MBMS_ID. However, there will be times when the UICC needs to store two BAK values associated with a particular MBMS_ID. The reason is that the BAK must be updated in the UICC prior to the BAK actually being used to encrypt/generate SK values (see Section 4.4.3). Consequently, both the old BAK and the new BAK will reside in the UICC simultaneously. The UICC must have some means to determine which BAK is valid. The recommended method is to allocate a BAK identifier BAK_ID to each BAK, in addition to the MBMS_ID. the BAK is identified by the MBMS_ID and BAK_ID. The CE will include the BAK_ID with the encrypted content in the broadcast data. The UICC can now distinguish if the old BAK is still being used or if the new BAK has begun to be used.

A value for BAK_Expire will be provided along with the BAK, so the UE can update expired keys.

**BAK lifetime.** The BAKG decides how often BAK is changed. The following issues should be considered in deciding how often BAK is to be changed.

- Frequent BAK changes will provide more security.

- Frequent BAK changes will also provide greater flexibility in subscription control. We show this by example. Once a user has BAK, they can access the content for the lifetime of that BAK. Suppose the BAK is changed at the beginning of every month. If a user’s subscription runs out halfway through the lifetime of a BAK, the user will still be able to generate SK (and thus view the content) until the BAK expires. So by changing BAK only every month, the SM can only charge subscriptions from the beginning of the month to the end of the month. A user can’t subscribe from the middle of one month to the middle of the next. However, if BAK changed every day, then the user could subscribe from the beginning of any day during the month.

- Increasing the frequency of BAK changes should be evaluated against a possible increase in the number of times the mobile station has to retrieve new BAK values.

## 6.2.3 Authenticating BAK Requests

An adversary cannot obtain BAK by performing a BAK request while impersonating a subscribed user. Only the subscribed user will be able to derive TK from RAND_TK, and thus extract BAK. For this reason, the BAKD does not need to authenticate BAK requests in order to protect BAK.

If, however, other control functions or accounting data are included with the BAK request, then it is necessary to prove the authenticity of the data source. It may also be desirable to authenticate requests to prevent malicious generation of excess network traffic. *The procedures for authenticating the request are for further study.*

Note that even though authentication of BAK requests may not be needed, there is still a need for authorization of the request. Such authorization must be specific to the broadcast service to which the requested BAK applies.

### 6.2.4 Storage of BAK

It is essential to the security model used herein that the UICC does not reveal BAK. If a single UICC reveals BAK, then all security is compromised until the BAKG changes BAK.

The UICC shall store BAK and related data about BAK, such as BAK_ID and expiration time, if any. The BAK is identified by the MBMS_ID (of the corresponding MBMS content stream) and BAK_ID.

The ME may store the BAK-related data, to save requesting this information from the UICC.

### 6.2.5 Updating BAK before use

It may prove beneficial to provision UICC with BAK shortly before BAK begins being used to derive SK values. Otherwise, once the CE starts sending packets with SK derived from the new BAK, the user would experience a delay as the UE performs a BAK update. If many users are tuned in, then there will be a burst of traffic as all the UEs perform a BAK update.

To avoid such problems, the BAKD should allow an UE to obtain the new BAK shortly before the BAK changes. Different UE may have different schedules for performing BAK updates, to prevent too many UEs performing a BAK update at once.

For security reasons, BAK should be distributed as close as possible to the time of use.

## 6.3 MBMS Security Algorithms

### 6.3.1 Encryption of Content

The specification of encryption algorithms is for further study.

### 6.3.2 Encryption of BAK

The specification of encryption of BAK (under key TK) is for further study.

### 6.3.3 Management of TK

#### 6.3.3.1 TK_RAND

TK_RAND shall be 64 bits in length.

TK_RAND shall be generated in a manner that minimizes the probability that the same TK_RAND is used to create a TK for different BAK encryptions destined to the same terminal. The probability should be the same as for random selection of TK_RAND.

#### 6.3.3.2 TK Generation

TK shall be 128 bits in length.

TK shall be generated from TK_RAND and RK using a secure one-way function chosen to minimize the likelihood that an adversary can obtain TK with knowledge of TK_RAND alone, and to minimize the likelihood that an adversary can obtain RK with knowledge of TK_RAND and TK. A standardized SHA-1 based function will be used for this purpose.

### 6.3.4 SK

#### 6.3.4.1 SK_RAND

SK_RAND shall be 32 bits in length.

SK_RAND shall be generated in a manner that minimizes the probability that the same SK_RAND is used to create an SK for different content encryptions destined to the same terminal. The probability should be the same as for random selection of SK_RAND.

SK_RAND shall be generated in a manner that minimizes the probability that an adversary can guess the next value of SK_RAND with knowledge of previous values. This requirement makes it more difficult for a modified ME shell to compute future SK values and distribute the values to other MEs.

#### 6.3.4.2 SK Generation

SK shall be 128 bits in length.

SK shall be generated from SK_RAND and BAK using a secure one-way function chosen to minimize the likelihood that an adversary can obtain SK with knowledge of SK_RAND alone, and to minimize the likelihood that an adversary can obtain BAK with knowledge of SK_RAND and SK.

## ~~6.3~~6.4 Protection of the transmitted traffic

Editor’s note: this section will contain the details of how traffic is protected

# 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 home operator trusts the user to be accountable for his actions.~~

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

This annex contains some security threats that have been identified for MBMS.

# 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 encryption keys and distribute them to unauthorized parties

## 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. Deliberated 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 encryption keys to gain free access to content without any knowledge of the service provider

### 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.

### 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.

# 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~~1~~.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 |
| | | | | | | | |