3GPP TSG SA WG3 Security — S3#30 **S3-030517**
6 - 10 October 2003
Povoa de Varzim, Portugal

Title:	**Latest version of MBMS TS**
Source:	**MBMS Security Rappporteur**
Document for:	**Information**
Agenda Item:	
Attachments:	**Latest versions of MBMS TS**

Version 0.2.0 of the MBMS Security TS was presented at the Antwerp ad-hoc (S3z030028). This version included the changes proposed in SA3#29. Further updates to the TS were proposed at the ad-hoc. It was agreed that both sets of changes need to be confirmed by the whole of SA3 and changes proposed in the ad-hoc need to be clearly differentiated from those proposed at the SA3#29. To achieve this differentiation, version 0.2.0 has been attached to this contribution and needs to be reviewed as capturing the decisions made in SA3#29. Version 0.2.1 uses version 0.2.0 as its baseline and includes the changes proposed at the ad-hoc and editorial modifications.

The following changes are included in version 0.2.0:

- Added an Editor's note to capture the SA3 LS and the replies on double ciphering.
- Added the requirements from tdoc S3-030366 with some editorial modifications.
- Added some text to clauses 1, 4, 5.3 and 6.3 to capture the fact that many different protection methods may be needed depending on the type of application being transmitted. Re-arranged the requirements to put the ones relating to protection of content at the end, as this will enable moving the requirements more easily at a future date if necessary.

The following changes are included in version 0.2.1

- Deletion of editor’s note relating to decision about which network node generate MBMS key
- Addition of editor’s note capturing discussion of MIKEY
- Addition of editor’s note describing how SRTP could be linked to the proposed key management schemes
- Inclusion of some additional threats as proposed in S3z030007.
- Editorial modification of the security requirements numbering (not discussed at ad-hoc)

3GPP TS 33.246 V0.21.01 (2003-087)

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

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

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.

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

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

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 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).

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:

MBMS Multimedia Broadcast/Multicast Service

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. Furthermore as MBMS may be used to transport several different types of protocols/codecs e.g. a media streaming application and a file download, there may need to be different protection method specified.

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 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 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 MBMS signaling protection

R2a: 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.

4.1.3 Requirements on Privacy

R3a: 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.

4.1.4 Requirements on MBMS Key Management

R4a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R4b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

R4c: 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

R4d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

R4e: 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.

~~4.1.2~~4.1.5 Requirements on integrity protection of MBMS multicast data

R5~~3~~a: 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

R5~~3~~b: 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.

R5~~3~~c: 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~~4.1.6 Requirements on confidentiality protection of MBMS multicast data

R6~~4~~a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R64b: 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.

R64c: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

R6d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on MBMS multicast session from the BM-SC to the UE.

R6e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS multicast session when it is applied.

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.

4.1.4Requirements 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.

4.1.5Requirements 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.

4.1.6Requirements 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.

5 MBMS security functions

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 to the UE are performed 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.

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 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".

6 Security mechanisms

6.1 Authentication and authorisation of a user

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

6.3 Protection of the transmitted traffic

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

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

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.

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.

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	0.10.0
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

3GPP TS 33.246 V0.2.10 (2003-09)

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

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

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.

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

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

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 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).

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:

MBMS Multimedia Broadcast/Multicast Service

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. Furthermore as MBMS may be used to transport several different types of protocols/codecs e.g. a media streaming application and a file download, there may need to be different protection method specified.

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 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 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 MBMS signaling protection

R32a: 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 R37a. The Gmb interface is ffs.

4.1.3 Requirements on Privacy

R43a: 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.

4.1.4 Requirements on MBMS Key Management

R54a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R54b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

R54c: 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

R54d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

R54e: 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 integrity protection of MBMS multicast data

R65a: 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

R65b: 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.

R65c: 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.

4.1.6 Requirements on confidentiality protection of MBMS multicast data

R76a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R76b: 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.

R7~~6~~c: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

R7~~6~~d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on MBMS multicast session from the BM-SC to the UE.

R7~~6~~e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS multicast session when it is applied.

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.

5 MBMS security functions

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 to the UE are performed 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.

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 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".

6 Security mechanisms

6.1 Authentication and authorisation of a user

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

Editor's note: MIKEY is being considered as the method for carrying keys. Possible optimisations were proposed at the ad-hoc in Antwerp (S3z030010). One identified issue was the possible need to terminate MIKEY in the UICC and/or terminal in the combined method. The use of MIKEY relates to the PTP delivery of a key

6.3 Protection of the transmitted traffic

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

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 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	0.10.0
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