Technical Specification Group Services and System Aspects **TSGS#22(03)0586**

Meeting #22, Hawaii, USA, 15-18 December 2003

Presentation of Specification to TSG or WG

Presentation to:	**TSG SA Meeting #22**
Document for presentation:	**TS 33.246, Version 1.0.0**
Presented for:	**Information**

Abstract of document:

The specification covers the security of the Multimedia Broadcast/Multicast Service (MBMS). The aim is to enable the secure transfer of some data to multiple users simultaneously. As multicast presents specific security concerns, the specification contains the threats to a multicast service and the security requirements that are derived from these threats. The specification then describes some security mechanisms to tackle those threats. These are a key management scheme that allows a Broadcast/Multicast Service Centre to securely distribute MBMS specific keys to known mobiles and a method of protecting (using the distributed keys) the data that is transmitted to the UE, such that only the intended recipients can decrypt the data.

Changes since last presentation to TSG Meeting:

There are no changes, as the document has not been presented previously.

Outstanding Issues:

The stage 1 and stage 2 parts of the specification are stable. It has been agreed that the MBMS specific keys can be held on the UICC or the ME in release 6. The choice of storage depends purely on the whether the UICC supports the ability to hold the keys. This decision is not yet reflected in the specification. This will require fairly simple additions to the text. Possible harmonisations with OMA DRM are also being considered.

The following outstanding issues are to be solved:

- The exact way that the GBA can be used to provide shared keys (when necessary) between the UE and BM-SC in order that MBMS specific keys can be securely delivered to the terminal.
- The secure point-to-point delivery and request of keys specific to a multicast service. This includes how the parameters are carried between the BM-SC and UE and how they are protected during transit. There have been proposals in SA3 and a decision needs to be taken on the best one.
- The keys that are actually used to protect the traffic are delivered in a point-to-multipoint to all the UEs that are receiving the data. The algorithm to do this and the way in which the algorithm is used has yet to be selected. It also needs to be specified how the parameters are carried from the BM-SC to the UE. There have been proposals in SA3 and a decision needs to be taken on the best one.

- The actual method that is used to protect the data in transit between the BM-SC and the UE.

Contentious Issues:

None

3GPP TS 33.246 V1.0.0 (2003-12)

Technical Specification

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

Keywords
Security, MBMS

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

This 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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[4] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[5] 3GPP TS 22.246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Stage 1; MBMS User Services".

3 Abbreviations

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

MBMS Multimedia Broadcast/Multicast Service

4 MBMS security architecture and requirements

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.

4.1 Security requirements

The following security requirements have been identified for MBMS multicast traffic.

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

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.

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.

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

R3a: 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 R3a. The Gmb interface is ffs.

R3b: Unauthorized modification, insertion, replay or deletion of all 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: UTRAN Bearer signalling integrity protection will be turned off for point to multipoint MBMS sessions and GERAN has no bearer signalling integrity protection, even for point to point signalling.

4.1.3 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.

Editor's note: UTRAN Bearer confidentiality protection will be turned off for point to multipoint MBMS sessions

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 the operator to perform re-keying as frequently as it believes necessary 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;
- users joining a multicast service shall not gain access to data from previous transmissions in the multicast 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 multicast 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 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: A UICC, realizing the function of providing session keys for decrypting the streaming data at the UE, shall only give session keys back to the UE if the input values used for obtaining the session keys were fresh (have not been replayed) and came from a trusted source.

4.1.5 Requirements on integrity protection of MBMS multicast data

R6a: 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

R6b: 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.

R6c: 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

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

R7b: 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.

R7c: It may be required to encrypt the MBMS multicast 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 MBMS multicast session from the BM-SC to the UE.

R7e: 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

A UE is authenticated and authorised in two parts when participating in an MBMS service. Firstly when the UE establishes a bearer to receive MBMS traffic and secondly when the UE request and receive keys for the MBMS service. The bearer establishment authentication is performed using the normal 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 a bearer (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the network (i.e. controlled by the BM-SC), there is an additional procedure to remove a MBMS bearer related to a UE that is no longer authorised to access the MBMS service.

Editor's note: It was agreed to standardise a solution that allowed MBMS specific keys to be stored in either the ME or UICC in release 6. The choice of storage depends on whether the UICC has the ability to hold the keys or not. The differences between the two methods will only be visible in the UE, and the BM-SC would know which method of storing the keys in the UE will be used.

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 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".

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 update procedure

Once a UE has joined a multicast service, the UE should try to get the high level key that will be used to 'protect' the data transmitted as part of this multicast service. If the UE fails to get hold of this key or receives confirmation that no updated key is necessary or available at this time, then, unless the UE has a still-valid, older key, the UE shall leave the MBMS user service. The UE tries to get the high level key using the second message in the below flow.

The BM-SC controls when the high level keys used in a multicast service are to be changed. The flow in figure 2 describes how the high-level key changes are performed.

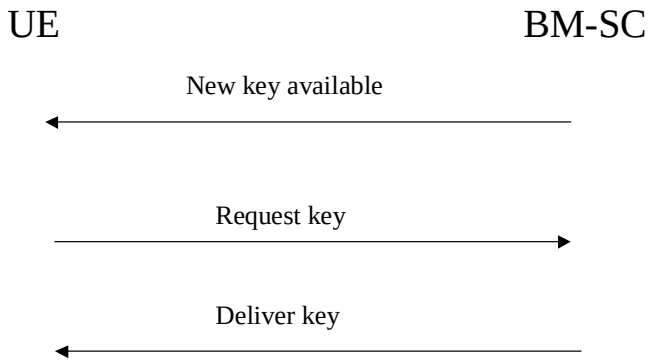

Figure 2: high-level key changes

The first message is sent out by the BM-SC to indicate that new keys are available. It is an optional message in the flow. If it is sent to all UEs, then it needs to be ensured that all the UEs do not request the new key simultaneously.

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

After receiving the second message the BM-SC should send out the appropriate key to the UE protected by the relevant means. Upon successfully receiving the new key, the UE should store this key for later use.

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.

6.2 Protection of the transmitted traffic

The data transmitted to the UEs is protected by a symmetric key that is shared by the BM-SC and UEs that are accesing 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 high-level key and contain other information needed to calculate the low-level keys. If the UE does not have the high level key indicated by Key_ID, then it should fetch the high level key using the methods discussed in the previous clause.

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 correct key.

The flow in figure 3 shows how the protected content is delivered to the UE.

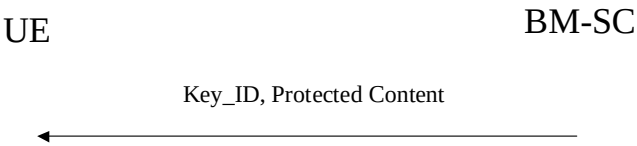

Figure 3: Protected content delivery to the UE

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

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.

NOTE: It is assumed that the legitimate end user has a motivation to defeat the system and distribute the shared keys 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. 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.

NOTE: It cannot be assumed that keys held in a terminal are secure. No matter how the shared encryption keys 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.

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 C (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					Minor Editorial update	0.3.0	0.3.1
2003-12	SP-22	SP-030586	-	-	Presentation to TSG SA#22 for Information	0.3.1	1.0.0