3GPP TSG SA WG3 Security — S3#26 **S3-020604**
19 - 22 November 2002, Oxford, UK

3GPP TS 33.cde V0.0.2~~1~~ (2002-11~~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).

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.

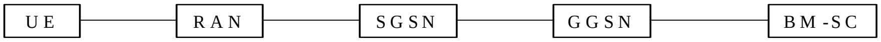

Figure 1: MBMS security architecture

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.

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 service providers (i.e. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS services.

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 and security keys

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.

Editor's note: Requirement R3a has not been agreed.

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

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

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 encryption protection of MBMS multicast data and security keys

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 has joined the MBMS service.

R4c: The encryption key(s) and the integrity key for the MBMS multicast service shall be encrypted when delivered to the users. In addition, it may be required to protect these keys with a MAC.

R4d: Only the valid users that has joined a MBMS multicast service shall be able to decrypt the encryption key(s) and the integrity key delivered from the network.

R4e: Mandate support of re-keying in the UE and BM-SC in order to ensure that users that has joined a MBMS service, but then left, shall not gain MBMS multicast service without being charged.

R4g: It may be required to encrypt the MBMS multicast data on the “BM-SC - GGSN” interface, i.e. the reference points Gi and Gmb.

R4h: User identity should not be exposed to the content provider or linked to the content, in the case the Content Provider is located in the 3GPP operator’s network.

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.

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 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.

If all users need to request a key update simultaneously then there needs to be some method of ensuring that all the users do not request a key update at the same time. This mechanism is ffs.

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.

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

Annex ~~<~~A~~>~~ (informative): ~~<Normative annex title>~~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): ~~<Informative annex title>~~Security threats

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

B.1 Threats associated with attacks on the radio interface~~Heading levels in an annex~~

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~~1~~-09~~7~~					~~Copyright date changed to 2001; space character added before TTC in coyright notification; space character before first reference deleted.~~Initial version supplied by Rapporteur	1.3.2	0.0.1~~.~~ ~~3.3~~
2002-01					~~Copyright date changed to 2002~~Updated to include the threat and requirements discussed at SA3 #25.~~.~~	0.0.1 ~~1.3.3~~	0.0.2 1.3.4
~~2002-07~~					~~Extra Releases added to title area.~~	~~1.3.4~~	~~1.3.5~~