3GPP TSG SA WG3 Security — S3#25 **S3-020526**
8 - 11 October 2002, Munich, Germany

3GPP TS 33.cde V0.0.1 (2002-09)

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.

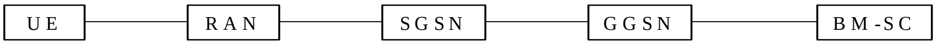

Figure 1: MBMS security architecture

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.

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> (normative): <Normative annex title>

Annex <B> (informative): <Informative annex title>

B.1 Heading levels in an annex

Annex <X> (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2001-07					*Copyright date changed to 2001; space character added before TTC in coyright notification; space character before first reference deleted.*	*1.3.2*	*1.3.3*
2002-01					*Copyright date changed to 2002.*	*1.3.3*	*1.3.4*
2002-07					*Extra Releases added to title area.*	*1.3.4*	*1.3.5*