

ETSI TS 133 246 V12.2.0 (2015-01)



**Universal Mobile Telecommunications System (UMTS);
LTE;
3G Security;
Security of Multimedia Broadcast/Multicast Service (MBMS)
(3GPP TS 33.246 version 12.2.0 Release 12)**



Reference

RTS/TSGS-0333246vc20

Keywords

LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	7
Introduction	7
1 Scope	8
2 References	8
3 Definitions, abbreviations, symbols and conventions	10
3.1 Definitions	10
3.2 Abbreviations	10
3.3 Symbols.....	11
3.4 Conventions.....	11
4 MBMS security overview	11
4.1 MBMS security architecture.....	11
4.1.1 General.....	11
4.1.2 BM-SC sub-functions	13
4.1.3 UE security architecture.....	14
4.1A Granularity of MBMS security.....	15
4.2 Key management overview	15
5 MBMS security functions	16
5.1 Authenticating and authorizing the user	16
5.2 Key derivation, management and distribution.....	17
5.3 Protection of the transmitted traffic.....	17
6 Security mechanisms	18
6.1 Using GBA for MBMS	18
6.2 Authentication and authorisation of a user	19
6.2.1 Authentication and authorisation in HTTP procedures.....	19
6.2.1.1 General	19
6.2.1.2 Bootstrapping.....	19
6.2.1.3 HTTP digest authentication.....	19
6.2.2 Authentication and authorisation in MBMS bearer establishment	20
6.2.3 Void	20
6.2.4 Void	20
6.3 Key management procedures	20
6.3.1 General.....	20
6.3.2 MSK procedures	20
6.3.2.1 MSK identification.....	20
6.3.2.1A MBMS User Service Registration procedure	21
6.3.2.1B MBMS User Service Deregistration procedure.....	24
6.3.2.2 MSK request procedures	25
6.3.2.2.1 Basic MSK request procedure	25
6.3.2.2.2 Void.....	26
6.3.2.2.3 Missed key update procedure	26
6.3.2.2.4 BM-SC solicited pull procedure	26
6.3.2.3 MSK delivery procedures	27
6.3.2.3.1 Pushing the MSK to the UE	27
6.3.2.3.2 Void.....	27
6.3.2.4 Handling of multiple status codes within one response message	27
6.3.3 MTK procedures	28
6.3.3.1 MTK identification.....	28
6.3.3.2 MTK update procedure	29

6.3.3.2.1	MTK delivery in download	29
6.3.3.2.2	MTK delivery in streaming	29
6.3.4	Multiple BM-SC deployments	29
6.3.4.1	General	29
6.3.4.2	Service announcement coordination	29
6.3.X.3	MSK key management anchor point	29
6.3.4.4	MSK coordination	29
6.3.4.5	MTK coordination	30
6.3.4.6	MIKEY MTK timestamp coordination	30
6.4	MIKEY message creation and processing in the ME	30
6.4.1	General	30
6.4.2	MIKEY common header	31
6.4.3	Replay protection	31
6.4.4	General extension payload	31
6.4.5	MIKEY message structure	32
6.4.5.1	MSK message structure	32
6.4.5.2	MSK Verification message structure	34
6.4.5.3	MTK message structure	34
6.4.6	Processing of received messages in the ME	35
6.4.6.1	MSK MIKEY Message Reception	35
6.4.6.2	MTK MIKEY Message Reception	35
6.5	Validation and key derivation functions in MGV-F	36
6.5.1	General	36
6.5.2	Usage of MUK	36
6.5.3	MSK processing	36
6.5.4	MTK processing	36
6.6	Protection of the transmitted traffic	37
6.6.1	General	37
6.6.2	Protection of streaming data	38
6.6.2.1	Usage of SRTP	38
6.6.2.1A	Usage of SRTCP	38
6.6.2.2	Packet processing in the UE	39
6.6.3	Protection of download data	39
6.6.3.1	General	39
6.6.3.2	Usage of OMA DRM DCF	39
6.7	Confidentiality protection of associated delivery procedures	40
6.7.1	General	40
6.7.2	TLS Profile	40
6.7.3	HTTP server authentication	41
6.7.4	Authentication of the UE	41
Annex A (informative):	Trust model	42
Annex B (informative):	Security threats	43
B.1	Threats associated with attacks on the radio interface	43
B.1.1	Unauthorised access to MBMS User Service data	43
B.1.2	Threats to integrity	43
B.1.3	Denial of service attacks	43
B.1.4	Unauthorised access to MBMS User Services	43
B.1.5	Privacy violation	44
B.2	Threats associated with attacks on other parts of the system	44
B.2.1	Unauthorised access to data	44
B.2.2	Threats to integrity	44
B.2.3	Denial of service	44
B.2.4	A malicious UE generating MTKs for malicious use later on	44
B.2.5	Unauthorised insertion of MBMS user data and key management data	45
Annex C (normative):	MBMS security requirements	46
C.1	Requirements on security service access	46
C.1.1	Requirements on secure service access	46

C.1.2	Requirements on secure service provision	46
C.2	Requirements on MBMS Transport Service signalling protection	46
C.3	Requirements on Privacy.....	46
C.4	Requirements on MBMS Key Management	47
C.5	Requirements on integrity protection of MBMS User Service data.....	47
C.6	Requirements on confidentiality protection of MBMS User Service data.....	48
C.7	Requirements on content provider to BM-SC reference point.....	48
Annex D (normative):	UICC-ME interface	49
D.1	MSK Update Procedure.....	49
D.2	Void.....	49
D.3	MTK generation and validation	49
D.4	MSK deletion procedure	50
D.5	MUK deletion procedure.....	50
Annex E (Informative):	MIKEY features not used in MBMS.....	51
Annex F (normative):	MRK key derivation for ME based MBMS key management.....	52
Annex G (normative):	HTTP based key management messages	53
G.1	Introduction	53
G.2	Key management procedures	53
G.2.1	MBMS User Service Registration	53
G.2.2	MBMS User Service Deregistration.....	54
G.2.3	MSK request.....	54
G.2.4	Error situations	55
Annex H (informative):	Signalling flows for MSK procedures	57
H.1	Scope of signalling flows	57
H.2	Signalling flows demonstrating a successful MSK request procedure.....	57
H.2.1	Successful MSK request procedure.....	57
Annex I (informative):	Example of using MSKs and MTKs in MBMS.....	61
Annex J (informative):	Mapping the MBMS security requirements into security functions and mechanism.....	62
J.1	Consistency check	62
J.1.1	Requirements on secure service access.....	62
J.1.2	Requirements on MBMS transport Service signalling protection.....	62
J.1.3	Requirements on Privacy	63
J.1.4	Requirements on MBMS Key Management.....	63
J.1.5	Requirements on integrity protection of MBMS User Service data	64
J.1.6	Requirements on confidentiality protection of MBMS User Service data.....	64
J.1.7	Requirements on content provider to BM-SC reference point.....	65
J.2	Conclusions	65
Annex K (Informative):	SRTP features not used in MBMS.....	66
Annex L (Normative):	Multicasting MBMS user data on Iub.....	67
Annex M (informative):	Relation to IMS based MBMS user services	68
Annex N (normative):	GCSE security aspects.....	69

N.0 GCSE architecture and requirements69

N.1 GCSE security requirements69

N.1.1 General69

N.1.2 GCSE Broadcast Delivery specific security requirements69

N.2 Security solution for MB2-C interface.....69

N.3 Security solution for MB2-U interface.....70

Annex O (informative): Change history71

History75

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 and confidentiality 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. The stage 1 requirements for MBMS are specified in TS 22.146 [2].

1 Scope

The Technical Specification covers the security procedures of the Multimedia Broadcast/Multicast Service (MBMS) for 3GPP systems (UTRAN, GERAN and E-UTRAN). MBMS is a 3GPP system 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 TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".
- [4] 3GPP TS 33.102: "3G Security; Security Architecture".
- [5] 3GPP TS 22.246: "MBMS User Services".
- [6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".
- [7] 3GPP TS 31.102: "Characteristics of the USIM application".
- [8] IETF RFC 2617 "HTTP Digest Authentication".
- [9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"
- [10] IETF RFC 1982 "Serial Number Arithmetic".
- [11] IETF RFC 3711 "Secure Real-time Transport Protocol".
- [12] 3GPP TS 43.020: "Security related network functions".
- [13] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".
- [14] 3GPP TS 33.210: "Network domain security; IP network layer security".
- [15] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org
- [16] IETF RFC 4563 "The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)".
- [17] Port numbers at IANA, <http://www.iana.org/assignments/port-numbers>.
- [18] 3GPP TS 24.109: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".
- [19] IETF RFC 2616 "Hypertext Transfer Protocol -- HTTP/1.1".