ETSI TS 133 246 V17.0.0 (2022-04)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
LTE;
3G Security;
Security of Multimedia Broadcast/Multicast Service (MBMS)
(3GPP TS 33.246 version 17.0.0 Release 17)

Reference

RTS/TSGS-0333246vh00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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**", "**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
Legal Notice 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 requirements 69

N.1 GCSE security requirements 69
N.1.1 General 69
N.1.2 GCSE Broadcast Delivery specific security requirements 69
N.2 Security solution for MB2-C interface 69
N.3 Security solution for MB2-U interface 70
Annex O (normative): Security aspects of xMB reference point between Content Provider and BM-SC 71
O.1 General 71
O.2 Protection of the xMB reference point 71
Annex P (informative): Change history 72
History 77

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".

[20] 3GPP TS 29.109: "3rd Generation Partnership Project; Technical Specification Group Core Network; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[21] IETF RFC 3629 "UTF-8, a transformation format of ISO 10646".

[22] IETF RFC 4771 "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)".

[23] 3GPP TS 23.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture".

[24] OMA DRM v2.0 Extensions for Broadcast Support, Candidate Version 1.0 – 29 May 2007" (OMA-TS-DRM_XBS-V1_0-20070529-C).

[25] IETF RFC 3376 "Internet Group Management Protocol, Version 3".

[26] IETF RFC 3810 "Multicast Listener Discovery Version 2 (MLDv2) for IPv6".

[27] 3GPP TS 25.434, "UTRAN Iub Interface Data Transport and Transport Signalling for Common Transport Channel Data Streams".

[28] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[29] 3GPP TS 26.237: "IP Multimedia Subsystem (IMS) based Packet Switch Streaming (PSS) and Multimedia Broadcast/Multicast Service (MBMS) User Service; Protocols".

[30] 3GPP TS 23.203: "Policy and charging control architecture".

[31] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[32] IETF RFC 2818: "HTTP over TLS".

[33] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[34] 3GPP TS 22.468: "Group Communication System Enablers for LTE (GCSE_LTE)".

[35] IETF RFC 3588: "Diameter Base Protocol".

[36] IETF RFC 6733: "Diameter Base Protocol".

[37] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS); Stage 3".

[38] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[39] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[40] IETF RFC 5996: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[41] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".

[42] IETF RFC 768: "User Datagram Protocol (UDP)".

[43] IETF RFC 3947 (2005): "Negotiation of NAT-Traversal in the IKE".

[44] IETF RFC 3948 "UDP Encapsulation of IPsec ESP Packets".

[45] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[46] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[47] 3GPP TS 23.179: " Functional architecture and information flows to support mission critical communication services; Stage 2".

[48] 3GPP TS 23.285: "Architecture enhancements for V2X services."

3 Definitions, abbreviations, symbols and conventions

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to TS 22.246 [5].

HDR = the general MIKEY HeaDeR.

IMPI = In the context of current specification IMSI is used in the format of IMPI as specified in GBA, cf. TS 33.220 [6].

KEMAC = A payload included in the MIKEY message, which contains a set of encrypted sub-payloads and a MAC.

Key Group= A group of MSKs that are identified by the same Key Group part of the MSK ID. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted.

MBMS download session: See TS 26.346 [13].

MBMS streaming session: See TS 26.346 [13].

MRK = MBMS Request Key: This key is to authenticate the UE to the BM-SC when performing key requests etc.

MSK = MBMS Service Key: The MBMS Service key that is securely transferred (using the key MUK) from the BM-SC towards the UE. The MSK is not used directly to protect the MBMS User Service data (see MTK).

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function MGV-F with the MSK. The key MTK is used to decrypt the received MBMS data on the ME.

MUK = MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSK's to the UE.

NOTE: When a UICC is used, the keys MSK and MUK may be stored within the UICC or the ME depending on the UICC capabilities. When a SIM card is used, the keys MSK and MUK are stored within the ME.

Salt key = a random or pseudo-random string used to protect against some off-line pre-computation attacks on the underlying security protocol.

SEQl = Lower limit of the MTK ID sequence number interval: Last accepted MTK ID sequence number interval stored within MGV-S. The original value of SEQl is delivered in the key validity data field of MSK messages.

SEQp = The MTK ID, which is received in a MIKEY packet.

SEQu = Upper limit of the MTK ID sequence number interval, which is delivered in the key validity data field of MSK messages.

(S)RTP Session: The (S)RTP and (S)RTCP traffic sent to a specific IP multicast address and port pair (one port each for (S)RTP and (S)RTCP) during the time period the session is specified to exist. An (S)RTP session is used to transport a single media type (e.g. audio, video, or text). An (S)RTP session may contain several different streams of (S)RTP packets using different SSRCs.

3.2 Abbreviations

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

B-TID	Bootstrapping Transaction Identifier
BM-SC	Broadcast-Multicast Service Centre
BSF	Bootstrapping Server Function
DCF	DRM Content Format

DRM	Digital Rights Management
EXT	Extension payload
FDT	FLUTE File Delivery Table
FLUTE	File delivery over Unidirectional Transport
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
IDi	Identity of the initiator
IDr	Identity of the responder
Ks_ext_NAF	Derived key in GBA_U
Ks_int_NAF	Derived key in GBA_U, which remains on UICC
Ks_NAF	Derived key in GBA_ME of 3G GBA or in 2G GBA
MAC	Message authentication code
MBMS	Multimedia Broadcast/Multicast Service
MGV-F	MBMS key Generation and Validation Function
MGV-S	MBMS key Generation and Validation Storage
MIKEY	Multimedia Internet Keying
MKI	Master Key identifier
MRK	MBMS Request Key
MSK	MBMS Service Key
MTK	MBMS Traffic Key
MUK	MBMS User Key
NAF	Network Application Function
OMA	Open Mobile Alliance
ROC	Roll-Over Counter
SP	Security Policy
SRTCP	Secure RTCP
SRTP	Secure RTP

3.3 Symbols

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

||	Concatenation

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 MBMS security overview

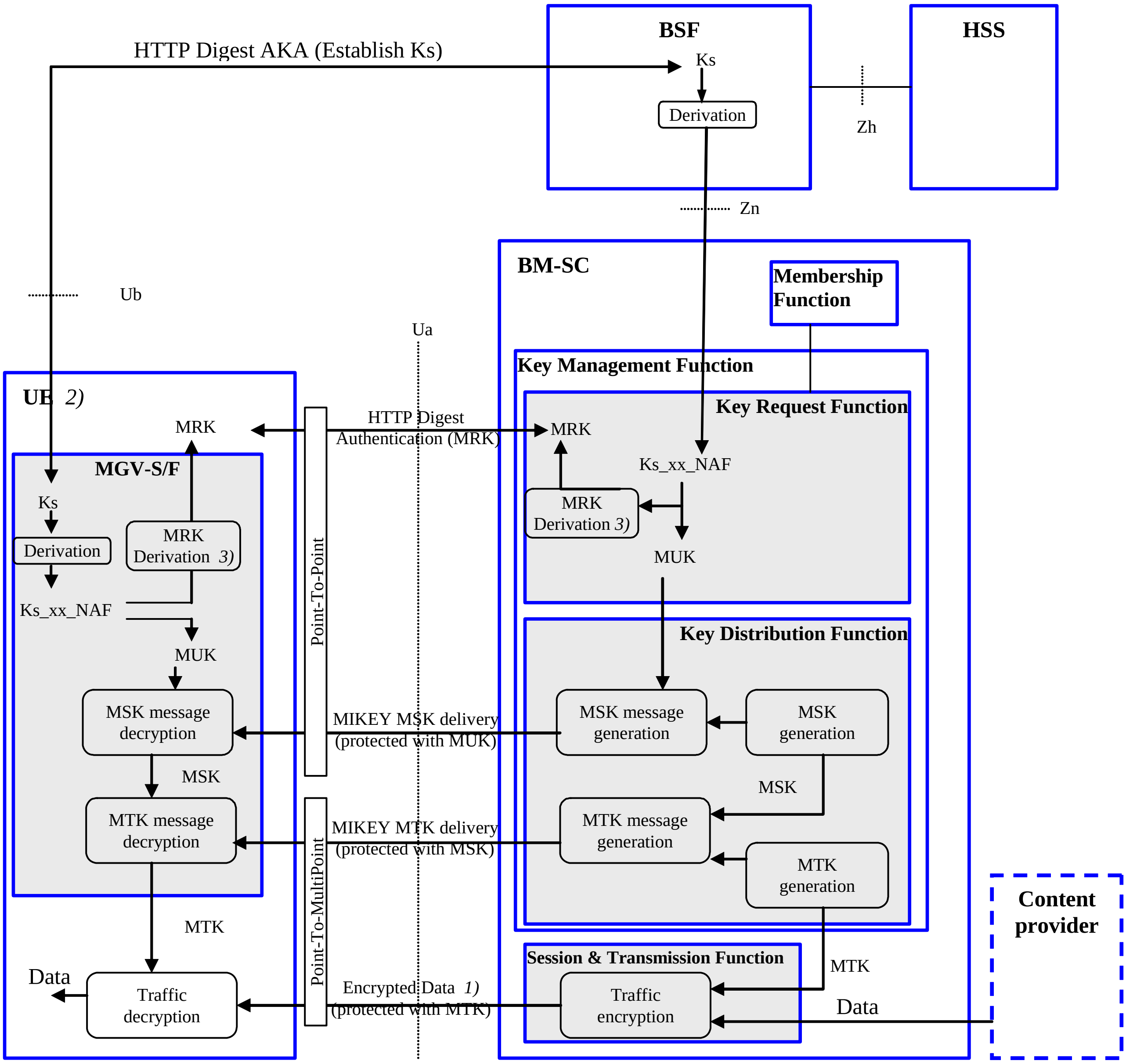
4.1 MBMS security architecture

4.1.1 General

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a MBMS User 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 MBMS User Service.

This means that MBMS security is specified to protect MBMS User Services, and it is independent on whether multicast or broadcast mode is used.

NOTE: There are two cases when multicast and broadcast mode are handled differently: usage of Membership function in authorization (see e.g. clause 4.1.1) and authorization of user related MBMS bearers (see e.g. clause 6.2.2) are only defined for multicast mode. MBMS in EPS supports only broadcast mode and functionality related to multicast mode does not apply to EPS.



Note 1) SRTP is used for streaming and modified DCF format for download

Note 2)Ks_xx_NAF stands for GBA_ME or GBA_U based NAF keys

Note 3) Not applicable for GBA_U, since MRK=Ks_ext_NAF

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS, except for the normal network bearer security, resides in either the BM-SC or the UE. The BSF is a part of GBA (TS 33.220 [6]). The UE and the BM-SC use GBA to establish shared keys that are used to protect the point-to-point communication between the UE and the BM-SC.

The 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. The BM-SC is responsible for establishing shared secrets with the UE using GBA, authenticating the UE with HTTP digest authentication mechanism, registering and de-registering UEs for MBMS User Services, generating and distributing the keys necessary for MBMS security to the UEs with MIKEY protocol and for applying the appropriate protection to data that is transmitted as part of a MBMS User Service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish MBMS bearer.

The BM-SC also verifies whether a user is authorized to register and receive keys for a MBMS User Service. For MBMS Multicast Mode this authorization is done with the help of Membership function in the BM-SC. For MBMS Broadcast Mode this authorization is done without the help of Membership function because the Membership function is only defined in the context of MBMS Multicast Mode in TS 23.246 [3].

The UE is responsible for establishing shared secrets with the BM-SC using GBA, registering to and de-registering from MBMS User Services, requesting and receiving keys for the MBMS User Service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- a UICC that contains MBMS key management functions shall implement GBA_U;
- a ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC as well as providing MBMS key management functions itself;
- a BM-SC shall support using both GBA_ME and GBA_U keys to enable both ME based and UICC based MBMS key management, respectively.

4.1.2 BM-SC sub-functions

The BM-SC has the following sub-functions related to MBMS security, see figure 4.1.

- **Key Management function:** The Key Management function includes two sub-functions: Key Request function and Key Distribution function.
- **Key Request function:** The sub-function is responsible for retrieving GBA keys from the BSF, deriving MUK and MRK from GBA keys, performing MBMS User Service Registration, Deregistration and MSK request procedures and related user authentication using MRK, providing MUK to Key Distribution function, performing authorization check. The sub-function implements the following functions and procedures:
    - Bootstrapping initiation
    - Bootstrapping re-negotiation
    - HTTP digest authentication
    - MRK derivation
    - MBMS User Service Registration procedure
    - MBMS User Service Deregistration procedure
    - MSK request procedure
- **Key Distribution function:** The sub-function is responsible for retrieving MUK from Registration function, generating and distributing MSKs and MTKs to the UE, providing MTK to Session and Transmission function. The sub-function implements the following security procedures:
    - MSK delivery procedure
    - MTK delivery procedure
    - BM-SC solicited pull procedure
- **Session and Transmission function:** The sub-function is responsible for session and transmission functions cf. TS 26.346 [13]. As part of these session and transmission functions, this function performs protection of data with MTK (encryption and/or integrity protection). The sub-function implements the following security procedures:
    - Protection of streaming data

  - Protection of download data

- **Membership function:** The Membership function is used to verify if a user is authorized to register, receive keys or to establish a MBMS bearer for MBMS Multicast Mode. The Membership function is defined only for MBMS Multicast Mode in TS 23.246 [3].

4.1.3 UE security architecture

It is assumed that the UE includes a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC. The MGV-F is implemented in a protected execution environment to prevent leakage of security sensitive information such as MBMS keys. MGV-S stores the MBMS keys and MGV-F performs the functions that should not be exposed to unprotected parts of the ME. An overview of ME based key management and UICC based key management in UE is described in figures 4.2a and 4.2b.

In particular in ME based key management it shall be ensured that the keys are not exposed to unprotected parts of the ME when they are transmitted from the UICC to the MGV-S or during the key derivations.

Figure 4.2: ME and UICC based key management in UE

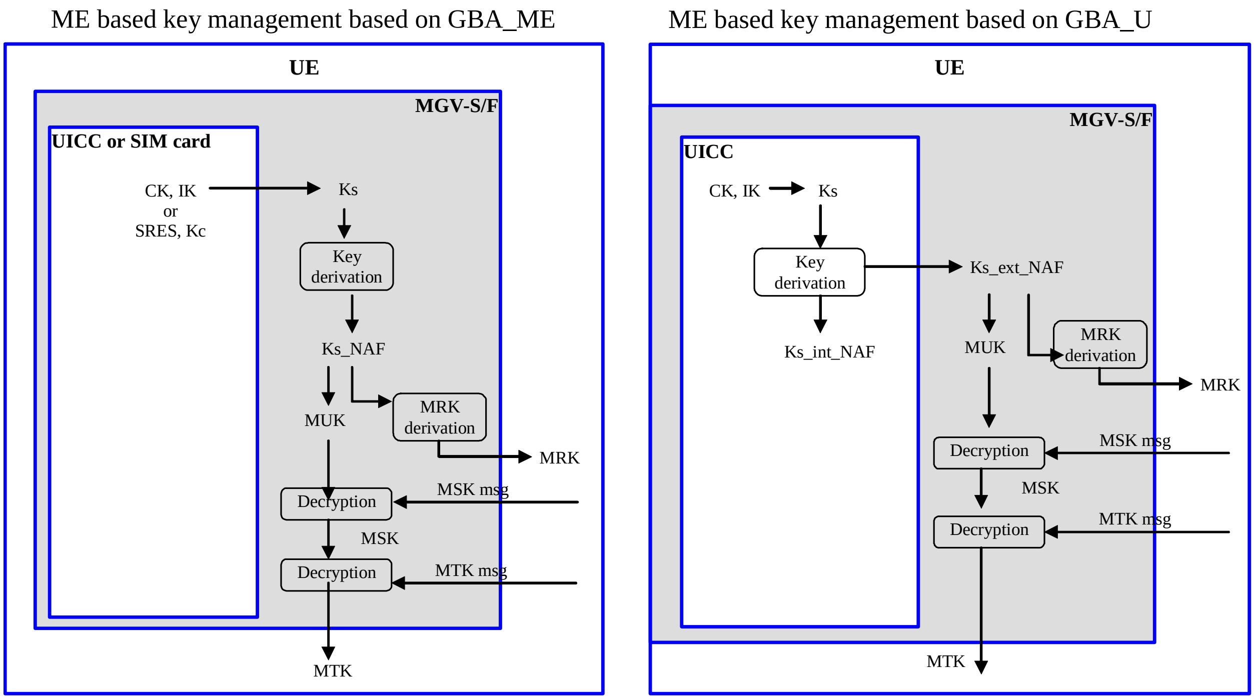


Figure 4.2a: ME based key management in UE

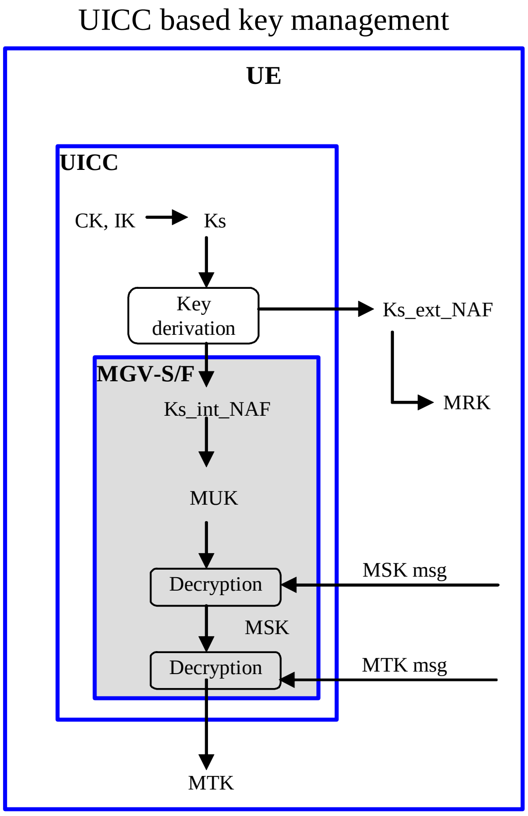


Figure 4.2b: UICC based key management in UE

4.1A Granularity of MBMS security

An MBMS User Service is composed of one or more MBMS Streaming Sessions and/or MBMS Download Sessions. An MBMS Streaming Session is composed of one or more RTP sessions, and an MBMS Download Session is composed of one or more FLUTE channels as defined in TS 26.346 [13]. MBMS streaming/download sessions may be transported over one or more MBMS Transport Services. Transport Services are defined in TS 22.246 [3]. MBMS security is used to protect RTP sessions and FLUTE channels. As such MBMS User Service protection is Transport Service independent, in particular, it is independent on whether it is carried over point-to-point bearer or MBMS bearer (in multicast mode or in broadcast mode).

4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different RTP sessions and FLUTE channels. The MSKs are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the RTP sessions and FLUTE channels as specified within clauses 6.5 and 6.6. The delivery of MSKs is secured with user specific MBMS User Key (MUK), which is received from GBA, cf. clause 6.1. MSKs and MTKs are managed at the MBMS User Service Level.

The following rules apply for MBMS key management:

The use of the same MTK within two different RTP sessions is not allowed according to RFC3711 [11] section 9.1.

It shall be possible to update the MTKs during an RTP session or FLUTE channel to enhance the security.

MSKs shall be used to protect MTKs of only one RTP session or FLUTE channel. It shall be possible to update the MSKs during an RTP session or FLUTE channel to enhance the security.

MSKs within one Key Group shall be used to protect MTKs of only one RTP session or FLUTE channel. To allow smooth transition from "current" MSK to the "next", the MGV-S shall be capable of storing two MSKs within the same Key Group as specified in clause 6.3.2.1 of TS 33.246.

Some of the rules are illustrated in figures 4.3 and 4.4.

The usage of MSKs and MTKs applied to a RTP session or FLUTE channel (i.e. usage of MSKs and MTKs for one Key group) is depicted in figure 4.3. Figure 4.4 shows an example of the usage of MSKs and MTKs for three RTP sessions. In particular it shows that MSKs and MTKs of one Key Group are used to protect exactly one RTP session.

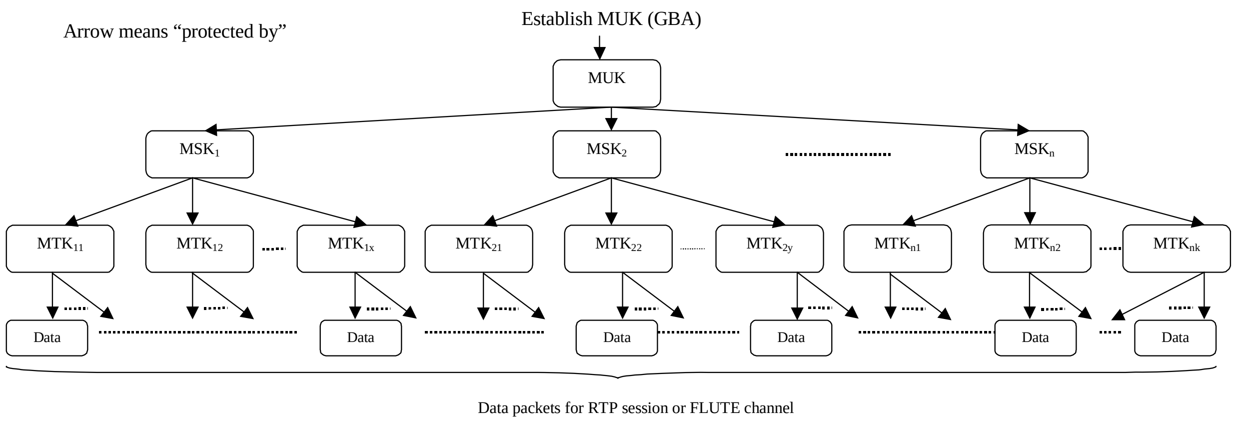


Figure 4.3: MBMS key hierarchy: usage of MSKs and MTKs within one RTP session or FLUTE channel

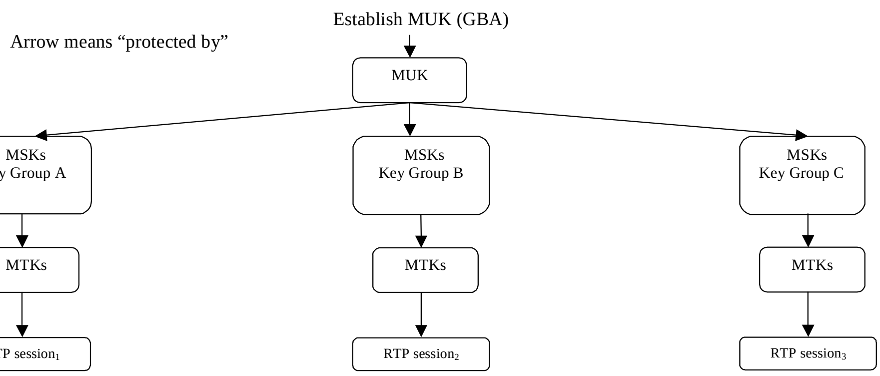


Figure 4.4: MBMS key hierarchy: usage of MSKs and MTKs for three separate RTP sessions

According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. In case two MBMS User Services share an MBMS Transport Service, they also share one or more RTP sessions or FLUTE channels carried in the Transport Service. In this case, it shall be possible for the MBMS User Services to share one or more MSKs and MTKs of the Key Groups that are used to protect the MBMS data.

An example showing how key management is used with MBMS User and Transport Services is depicted in Annex I.

As described in clause 6.6, the MTK is used as master key for SRTP (and for corresponding SRTCP) and to protect DCF in case of download. According to RFC 3711 [11] it is mandatory to support master key lengths of 128, 192 and 256 bits for SRTP. The length of the MSK does not need to exceed the length of the MTK, but should be at least as long.

5 MBMS security functions

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised such that only legitimate users are able to participate in an MBMS User Service.

When the UE uses HTTP protocol towards the BM-SC, the UE is authenticated with HTTP digest as described in clause 6.2.1. The Membership function within the BM-SC is used to verify the subscription information in MBMS Multicast Mode.

The following procedures use HTTP digest authentication:

- MBMS User Service Registration procedure (clause 6.3.2);
- MBMS User Service Deregistration procedure (clause 6.3.2);
- MSK request procedure. This can have many triggers (clause 6.3.2);
- Associated delivery procedures (specified in TS 26.346 [13]).

When the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service, it is authenticated and authorized as defined in clause 6.2.2.

5.2 Key derivation, management and distribution

Like any service, the keys that are used to protect the transmitted data in a MBMS User 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 User 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 User 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.

The following function is used by the procedures listed below:

- MRK derivation (clause 6.1);

The following procedures are involved in Key management and distribution:

- MBMS User Service Registration procedure (clause 6.3.2);
- MBMS User Service Deregistration procedure (clause 6.3.2);
- MSK request procedure (clause 6.3.2);
- MSK delivery procedure (clause 6.3.2);
- MTK delivery procedure (clause 6.3.3);
- BM-SC solicited pull procedure (clause 6.3.2).

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS User 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 User Service is actually protected by the DRM security method and hence might not require additional protection. However, MBMS protection is independent of DRM protection). If this protection is required, it will be either confidentiality and integrity or confidentiality only, or integrity only. 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.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This "double ciphering" is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.

The following traffic protection functions can be distinguished:

- Protection of streaming data (clause 6.6.2);
- Protection of download data (clause 6.6.3).

6 Security mechanisms

6.1 Using GBA for MBMS

TS 33.220 [6] GBA (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS User Service. The Ua security protocol identifier that shall be used for MBMS is defined in TS 33.220 [6].

The use of 2G GBA, as specified in Annex I of TS 33.220 [6], for MBMS may be supported as an implementation option to allow the use of SIM cards or SIMs on UICCs.

According to TS 33.220 [6], it is possible for operators to explicitly prohibit the use of SIMs for MBMS access based on policy configuration at the BSF.

If the Service Announcement indicates that protection of the MBMS User Service is applied, then the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within TS 33.220 [6]. The BM-SC will act as a NAF (Network Application Function) according to TS 33.220 [6].

Along with the GBA-keys the BSF shall send the IMPI of the user to the BM-SC. When the UE has bootstrapped, it will use a new B-TID over the Ua reference point. The IMPI is used in the BM-SC to bind the old and the new B-TID together.

The MSKs for an MBMS User Service shall be stored on either the UICC, if the UICC is capable of MBMS key management, or the ME, if the UICC is not capable of MBMS key management or a SIM card is used.

Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions.

As a result of a GBA_U run, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. In case the UICC supports MBMS then this key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK (MBMS User Key) to protect MSK (MBMS Service Key) deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK (MBMS Request Key) within the protocols as described within clause 6.2. In case the UICC does not support MBMS then the key Ks_int_NAF can not be used for ME based key management, but the key Ks_ext_NAF shall be used as MUK and the key MRK is derived from the key Ks_ext_NAF by the BM-SC and the ME as specified in Annex F of this specification.

A run of GBA_ME or 2G GBA results in the BM-SC sharing a key Ks_NAF with the ME. Both the BM-SC and the ME use the key Ks_NAF as MUK. The key MRK is derived from the key Ks_NAF by the BM-SC and the ME as specified in Annex F of this specification. The key MUK is used to protect MSK deliveries to the ME as described within clause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within clause 6.2.

The MUK and MRK are identified by the combination of B-TID and NAF-ID (without the Ua security protocol identifier) in the UE and by B-TID in the BM-SC, where B-TID and NAF-ID are defined as specified in TS 33.220 [6].

In the UE two different MUKs, i.e. the last generated and the last successfully used, are used to guarantee that the UE and the BM-SC share always one MUK. The last generated MUK is replaced immediately after when a new MUK is generated and the last successfully used MUK is updated after the successful reception of the MIKEY message, which is protected using the last generated MUK. The usage of MUKs is described within clause 6.3.

For ME based key management:

- All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC or SIM is inserted. Therefore the ME needs to store in non-volatile memory the last inserted UICC or SIM identity to be able to compare that with the used UICC or SIM identity at card insertion and power on.
- All MBMS keys (MRK, MSK and MTK) may be deleted from the ME when the ME is powered down. If the ME does not delete the MBMS keys at power down then the MBMS keys need to be stored in non-volatile

memory. The ME should store the MUKs in non-volatile memory in order to be able to authenticate the first MIKEY message of a BM-SC solicited pull procedure (see clause 6.3.2.2.4).

NOTE: If the ME deletes the MSK at power down, then the MBMS client would need to request MSK to the BM-SC and may need to run GBA to reconvene an MBMS session.

For UICC-based key management:

- When a MSK delivery procedure has to be performed and the corresponding Ks_int_NAF (GBA NAF key) is no longer available in the UICC, the UE shall re-generate a Ks_int_NAF key. If the received MSK delivery procedure refers to a Ks_int_NAF key no longer available and if the bootstrapped key Ks is associated to the same B-TID, then the ME should re-generate Ks_int_NAF with a GBA NAF derivation procedure. In case that the bootstrapped key Ks has been updated, the ME should take the new B-TID into use and run the MSK request procedure towards the BM-SC which retrieves the latest Ks_int_NAF from the BSF.

- The ME shall control the deletion of MUKs stored on the UICC. When the ME wants to free up storage in the UICC for new MUK, the ME selects the MUK no longer needed to be deleted. If a MUK is deleted then the corresponding GBA NAF Keys (i.e. GBA NAF Keys with same NAF-ID) shall be deleted; the bootstrapped key Ks shall also be deleted if Ks is present and associated to the same B-TID.

6.2 Authentication and authorisation of a user

6.2.1 Authentication and authorisation in HTTP procedures

6.2.1.1 General

This clause describes authentication of the user to the BM-SC when using HTTP digest with bootstrapped security associations.

6.2.1.2 Bootstrapping

The BM-SC shall implement,initiation of bootstrapping and bootstrapping renegotiation procedures over Ua as specified in TS 33.220 [6] and in TS 24.109 [18]. The Ua interface procedures shall use MRK.

6.2.1.3 HTTP digest authentication

When the UE initiates an HTTP procedure towards the BM-SC, HTTP digest authentication as defined in RFC 2617 [8] shall be used for mutual authentication. HTTP digest is run between BM-SC and ME. The MBMS authentication procedure is based on the general user authentication procedure over Ua interface that is specified in clause "Procedures using the bootstrapped Security Association" in TS 33.220 [6]. The BM-SC will act as a NAF according to TS 33.220 [6]. Along with the GBA-keys the BSF shall send the IMPI of the user to the BM-SC. The details of HTTP digest authentication are specified in clause 5.2 of TS 24.109 [18]

The following adaptations apply to HTTP digest:

- the B-TID as specified in TS 33.220 [6] is used as username;

- MRK (MBMS Request Key) is used as password.

All HTTP procedures within this specification including the associated delivery procedures in TS 26.346 [13] shall be integrity protected with HTTP digest as specified in this clause. In addition, the associated delivery procedures may be confidentiality protected as specified in clause 6.7 of this document.

6.2.2 Authentication and authorisation in MBMS bearer establishment

As defined in TS 23.246 [3] MBMS bearer establishment applies only to multicast mode. The authentication of the UE during MBMS bearer establishment relies on the authenticated point-to-point connection with the network, which was set up using network security described in TS 33.102 [4] or TS 43.020 [12]. 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 the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

NOTE: MBMS in EPS supports only broadcast mode and functionality described in this clause applies only to multicast mode.

6.2.3 Void

6.2.4 Void

6.3 Key management procedures

6.3.1 General

In order to protect an MBMS User Service, it is necessary to deliver both MSKs and MTKs from the BM-SC to the UE.

MSK procedures are further divided to MSK request procedures, described in clause 6.3.2.2, and MSK delivery procedure, described in clause 6.3.2.3. MSK procedures use a point-to-point bearer. MSK procedures are similar for both streaming and download services.

MBMS key management messages shall use a non-real time PDP context of QoS class "background" or "interactive" as defined by TS 23.107 [23] or PDN connection with similar QoS properties as defined TS 23.203 [30].

NOTE: In UTRAN the PS radio resources for a PDP context of QoS class "background" and "interactive" can be released and re-established on request of the network, while the IP address remains assigned to the PDP context. If the radio resources were released and the BM-SC wants to deliver an MSK (see clause 6.3.2.3) the network will page the UE. Similar functionality applies to PDN connections in E-UTRAN.

The BM-SC shall store the IP-address which was assigned for the PDP context for further key management usage. The BM-SC receives the IP address of the UE from the source IP address field of the MBMS User Service Registration message. It shall be ensured by the network that the original source UE IP address is visible to the BM-SC.

The operator may configure the BM-SC to refrain from pushing the MSK update message to the UE and let the UE request for the MSK. This may be needed in some download services where the UE fetches the MSK after receiving encrypted download object. In this case the back-off mode as described in clause 6.3.2.2.1 shall be used if present within the Service Announcement.

MTK delivery procedures use the same bearer as the MBMS User Service. MTK delivery procedures are different for streaming and download services and they are described in clause 6.3.3.

The details of the HTTP procedures and HTTP error situations are specified in Annex G. An example of detailed MSK request procedure is described in Annex H. The XML schemas of the HTTP payloads are specified in TS 26.346 [13].

6.3.2 MSK procedures

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Key Domain ID and MSK ID

where

Key Domain ID = MCC || MNC and is 3 bytes long.

NOTE 1: When MCC || MNC is used as key identifier, the UE should not try to use it in another context, e.g. the UE should not compare the received MCC || MNC to parameters in radio level.

MSK ID is 4 bytes long and with byte 0 and 1 containing the Key Group part, and byte 2 and 3 containing the Key Number part. The Key Number part is used to distinguish MSKs that have the same Key Domain ID and Key Group part. The Key Number part value zero (0x0) is reserved for special use to denote the current MSK. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted. The Key Group part value zero (0x0) is not allowed as it is reserved for future use. The MSK ID is carried in the extension payload of MIKEY extension payload.

NOTE 2: If the Key Domain ID does not uniquely identify the BM-SC, it needs to be ensured that the Key Group parts are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group value. unless multiple BM-SC deployment is used as is defined in clause 6.3.4

6.3.2.1A MBMS User Service Registration procedure

When a UE has received MBMS User Service information, which indicates that the service is protected, via User Service Discovery / Announcement procedures describing a MBMS User Service, and the user wants to receive that MBMS User Service, the UE shall register to the MBMS User Service. Registration is required to ensure that the UE receives the necessary MSK updates.

MBMS User Service Registration shall be performed by the UE irrespective of the type of MBMS Transport Service i.e. in multicast mode or broadcast mode, as soon as the user first indicates that he wants to receive the MBMS User Service. In addition, it shall be performed at subsequent power on, unless the user has previously indicated that he/she no longer wants to receive the MBMS User Service, or unless the USIM or SIM has changed.

NOTE 1: The User Service Discovery / Announcement procedures are specified in TS 26.346 [13]. It is out of the scope of the present specification how the UE receives the User Service information and how the User Service is triggered in the UE.

NOTE 2: The MBMS User Service announcements are not protected when sent over MBMS bearer.

The UE shall not release the PDP context used by the MBMS User Service Registration until an MBMS User Service De-registration has been performed. This is to ensure that the BM-SC is aware of the correct UE IP address for the purpose of performing MSK deliveries from the BM-SC as specified in clause 6.3.2.2.4 and clause 6.3.2.3.1.

If the UE detects that a PDP context, which is used for MBMS key management, is released by the network, the UE should try to re-run MBMS User Service Registration for those MBMS User Services which were using the released PDP context for MBMS key management. For performing these re-registrations the UE may establish a new PDP context or the UE may use some other existing appropriate PDP context as defined in clause 6.3.1, if available. This is to ensure that the BM-SC becomes aware of the new UE IP address for the purpose of performing MSK deliveries from the BM-SC. Any new registrations should override any existing registrations of the UE to the same MBMS User Services.

If the MBMS User Service does not require any protection (i.e. if a service protection description is not present in the Service Announcement), the UE shall not perform User Service Registration for key management purposes, which means that the UE needs no shared secret with the BM-SC and should therefore not perform a GBA-run with BSF for MBMS (e.g. if no shared secret for MBMS is available in the UE).

The UE shall receive the following information via the User Service Discovery / Announcement procedures if protection of the MBMS User Service is applied:

- One or more fully qualified domain names (FQDN) of the key management servers (i.e. the BM-SC). This is for the UE to know to which IP address to send within the MBMS User Service Registration/Deregistration and MSK request Procedures. One or more FQDNs may be indicated in the Service Announcement for load balancing purposes. The UE shall choose the FQDN at the registration phase with the same mechanism as the File Repair Server is selected in TS 26.346 [13]. The UE shall keep the same FQDN for subsequent key management procedures.

- UICC key management required: yes/ no.

- 2G GBA allowed: yes/no

  If the flag 2G GBA is not present then 2G GBA is not allowed.

- MIKEY FEC-protection, as defined in TS 26.346 [13], may be specified in the service protection description if MIKEY is FEC protected and encapsulated in FEC source packets.

- Identifiers of the MSKs needed for the User Service.

  For each MSK, the identifiers that shall be included are Key Domain ID and MSK ID. The Key Number part of each MSK ID shall be set to 0x0 to denote the current MSK. The Key Number values in the Service Announcement shall be ignored by the UE, since they may change over time and Key Group part of MSK ID is sufficient to identify the MSKs, see clause 6.3.2.1.

- Mapping information how the MSKs are used to protect the different RTP sessions or FLUTE channels.

NOTE 3: Void

NOTE 4: Void

- Back off mode parameters, as defined in TS 26.346 [13], may be specified for MSK requests, if wanted by the service provider. These parameters are then valid for all MSKs in the user service. The Back off mode is used to avoid congestion in MSK requests. In the rare cases that more than one User Service share the same MSK, but have different back off parameters, the UE is allowed to choose which ones to use. The Back off mode is optional to implement in the BM-SC and mandatory to implement in the UE. The UE shall use Back off mode if it is requested by the BM-SC in the Service Announcement.

The UE shall not register for an MBMS user service if it does not have enough storage available for any additional MSKs and MTKs required for that service. The UE should delete MSKs and MTKs that are no longer needed in order to free up storage for new MSKs and MTKs. For UICC-based key management, the ME shall control the deletion of MSKs stored on the UICC.

NOTE 4a: It is up to the ME implementation as to which keys are not needed any longer.

In case the service protection description indicates that the UICC key management is required, the UE should only try to access the MBMS User Service if the selected UICC application is capable of MBMS key management.

In case the service protection description indicates that UICC key management is not required, the use of either UICC key management or ME key management for a particular UE, depends on if the used UICC application is capable of MBMS key management or not, i.e. if the used UICC application is capable of MBMS key management, then UICC key management shall be used.

In case the service protection description indicates that UICC key management is not required and 2G GBA is not allowed, the UE should only try to access the MBMS User Service if a USIM is present in the UE as the use of SIM is not allowed for this MBMS User Service.

In case the service protection description indicates that UICC key management is not required and 2G GBA is allowed, the use of either 2G or 3G GBA for a particular UE depends on whether a UICC with a USIM is present in the UE or not as defined in TS 33.220 [6]. I.e., if a UICC with a USIM is present then 3G GBA shall be used, and if no UICC with a USIM is present then a SIM together with 2G GBA shall be used. The service protection description shall not allow 2G GBA and require UICC key management at the same time.

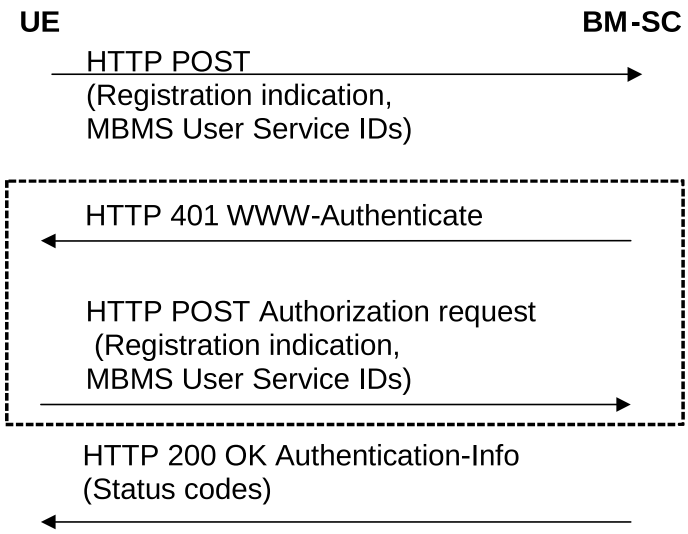


Figure 6.0A: MBMS User Service Registration procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest using bootstrapped security association as described in clause 6.2.1 of this specification.

The UE sends a registration request for the MBMS User Service using the HTTP POST message to the BM-SC Key Request function. The following information shall be included in the HTTP message.

- Indication that the UE requests to register to the MBMS User Service;
- A list of one or more MBMS User Service IDs.

The BM-SC Key Request function authenticates the UE with HTTP Digest using MRK key as described in clause 6.2.1.

If the authentication is successful, the BM-SC Key Request function shall verify whether the UE is authorized to register to the MBMS User Service(s) specified in the request. If the UE is authorized, the BM-SC Key Request function registers the UE to the MBMS User Service(s), which means that the UE is registered to receive the MSKs used in these MBMS User Service(s). The BM-SC Key Request function sends a HTTP 200 OK message with Authentication-Info header to the UE. The following information shall be included in the payload of the HTTP response message:

- A list including one status code for each MBMS User Service ID that was present in the Registration request.

The handling of multiple status codes in one response message is specified in clause 6.3.2.4.

NOTE 5: The BM-SC may not need to challenge the UE (dashed box in figure 6.0A), if the UE has used WWW Authorization request headers in the first message in figure 6.0A and BM-SC is able to authenticate the UE.

If the authentication fails, the BM-SC Key Request function resends HTTP 401 Authorization required message with the WWW-Authenticate header.

The UE checks the validity of the HTTP response message. If the message indicated failure in the HTTP status line, the UE may retry to send the request message.

The UE shall check the status codes in the payload and act accordingly. For example, the UE may retry to register to the MBMS User Service(s) that were indicated to have failed. Further error cases are described in clause G.2.4.

The BM-SC Key Distribution function initiates MSK delivery procedure(s) as specified in clause 6.3.2.3 for those MBMS User Services for which the response message indicated success. The BM-SC may decide to not initiate MSK key delivery procedures, if the combination of services is such that it only makes sense to use all of them simultaneously.

NOTE 6: The time between the MBMS User Service Registration procedure and MSK delivery procedures may vary, i.e. the UE should not expect the MSK delivery procedures to start immediately.

6.3.2.1B MBMS User Service Deregistration procedure

When the user desires to deregister from one or more MBMS User Services, the UE shall perform an MBMS User Service De-registration. This shall be done irrespective of the type of MBMS Transport Service i.e. in multicast mode or in broadcast mode.

The UE shall also perform an MBMS User Service De-registration, at UE power down, for all ongoing MBMS User Services to ensure that the BM-SC is made aware that the user is no longer contactable.

It may happen that the UE is unable to perform a MBMS User Service De-registration for all ongoing MBMS User Services e.g. due to uncontrolled power down or loss of coverage. This could lead to situations where the BM-SC wants to initiate an MSK delivery procedure (see clause 6.3.2.3) towards an unreachable UE.

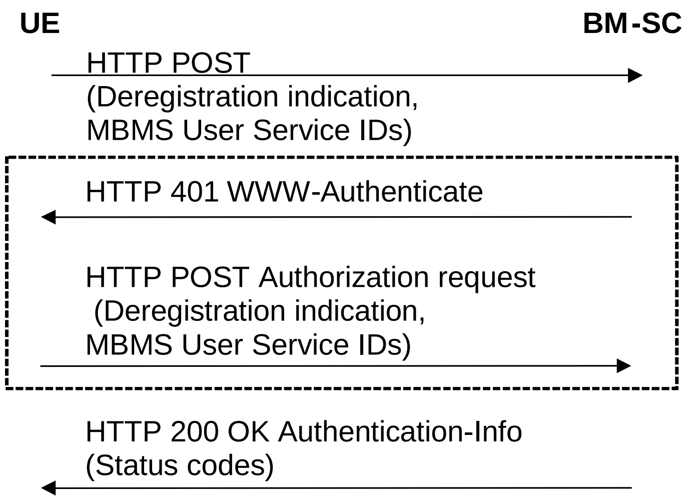


Figure 6.0B: MBMS User Service Deregistration procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest using bootstrapped security association as described in clause 6.2.1 of this specification.

The UE sends a deregistration request for the MBMS User Service using the HTTP POST message to the BM-SC Key Request function. The following information shall be included in the HTTP message.

- Indication that the UE requests to deregister from the MBMS User Service;
- A list of one or more MBMS User Service IDs.

The BM-SC Key Request function authenticates the UE with HTTP Digest using MRK key as described in clause 6.2.1.

If the authentication is successful, the BM-SC Key Request function deregisters the UE from the MBMS User Service(s), which means that the UE will no longer receive the MSKs used in these MBMS User Service(s). The BM-SC Key Request function sends a HTTP 200 OK message with Authentication-Info header to the UE. The following information shall be included in the payload of the HTTP response message:

- A list including one status code for each MBMS User Service ID that was present in the De-Registration request.

The handling of multiple status codes in one response message is specified in clause 6.3.2.4.

NOTE: The BM-SC may not need to challenge the UE (dashed box in figure 6.0B), if the UE has used WWW Authorization request headers in the first message in figure 6.0.B and BM-SC is able to authenticate the UE.

If the authentication fails then the BM-SC Key Request function resends HTTP 401 Authorization required message with the WWW-Authenticate header.

The UE checks the validity of the HTTP response message. If the message indicated failure in the HTTP status line, the UE may retry to send the request message. The UE shall check the status codes in the payload and act accordingly. Error cases are described in clause G.2.4.

The BM-SC should invalidate those MSKs from the UE, which are not used by any other MBMS User Services where the UE is registered. The BM-SC Key Distribution function performs this by running MSK delivery procedure for each MSK, where the Key Validity data is set to invalid value (see clause 6.3.2.3), i.e. SEQl is greater than SEQu.

6.3.2.2 MSK request procedures

6.3.2.2.1 Basic MSK request procedure

When a UE detects that it needs the MSK(s) for a specific MBMS User Service, the UE should try to get the MSKs that will be used to protect the data transmitted as part of this MBMS User Service. In the MSK request procedure the UE shall list the Key Domain ID - MSK ID pairs for which the UE needs the MSK(s). The UE shall always (except in the case of a BM-SC solicited pull) wait a period of time as specified by the back-off parameters in the User Service Description (if they are present) before making a request.

The basic MSK request procedure is a part of different other procedures, e.g.:

- request of MSK(s) when the UE has missed a key update procedure e.g. due to being out of coverage.

- BM-SC solicited pull procedure.

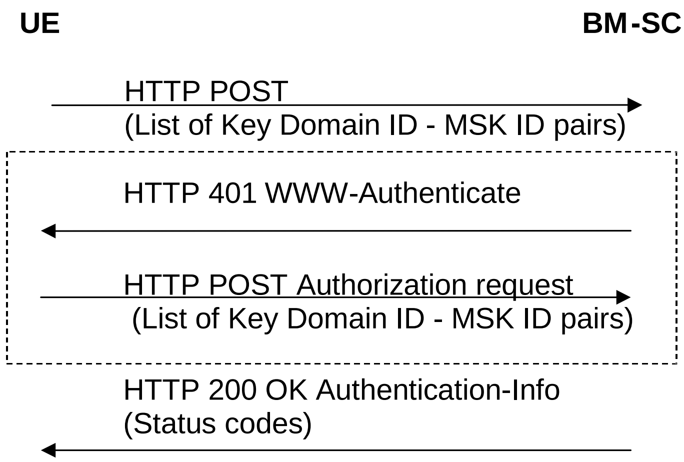


Figure 6.1: Basic MSK request procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest using bootstrapped security association as described in clause 6.2.1 of this specification.

The UE requests for one or several MSKs using the HTTP POST message. The following information is included in the HTTP message.

- key identification information: a list of one or several Key Domain ID - MSK ID pairs.

UEs may request specific MSK(s) by setting the Key Number part of the MSK ID to the requested value. When the Key Number part of the MSK ID is set to 0x0, this means the current MSK, see clause 6.3.2.1. The UE may request MSK(s) associated to more than one MBMS User Service in the same MSK request procedure.

The BM-SC Key Request function authenticates the UE with HTTP Digest using the keys received from GBA as described in clause 6.2.1.

If the authentication is successful, the BM-SC Key Request function shall verify whether the UE is registered to any MBMS User Service that uses the MSKs specified in the request. If the UE is authorized, the BM-SC Key Distribution function shall deliver requested MSKs to the UE (see clause 6.3.2.3). The BM-SC sends a HTTP 200 OK message with Authentication-Info header. The following information shall be included in the payload of the HTTP response message:

- A list including one status code for each Key Domain ID - MSK ID pair that was present in the Registration request.

The handling of multiple status codes in one response message is specified in clause 6.3.2.4.

NOTE 1: The BM-SC may not need to challenge the UE (dashed box in figure 6.1), if the UE has used WWW Authorization request headers in the first message in figure 6.1 and BM-SC is able to authenticate the UE.

If the authentication fails then the BM-SC Key Request function resends HTTP 401 Authorization required message with the WWW-Authenticate header.

The UE checks the validity of the HTTP response message. If the message indicated failure in the HTTP status line, the UE may retry to send the request message.

The UE shall check the status codes in the payload and act accordingly. For example, the UE may retry to request those MSKs that were indicated to have failed or leave the MBMS User Service.

If the HTTP procedure above resulted to success, the BM-SC Key Distribution function initiates MSK delivery procedure as specified in clause 6.3.2.3.

6.3.2.2.2 Void

6.3.2.2.3 Missed key update procedure

When the UE has missed an MSK update and it detects that it has not got the current MSK, e.g. from the received traffic, it may trigger the retrieval of the current MSK from the BM-SC. The procedure is the same as the Basic MSK request procedure in clause 6.3.2.2.1.

6.3.2.2.4 BM-SC solicited pull procedure

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC Key Distribution function solicits the UE to contact the BM-SC and request for new MSK. An example of such a situation is when the BM-SC Key Distribution function wants to trigger the UE that it needs to update the MSK.

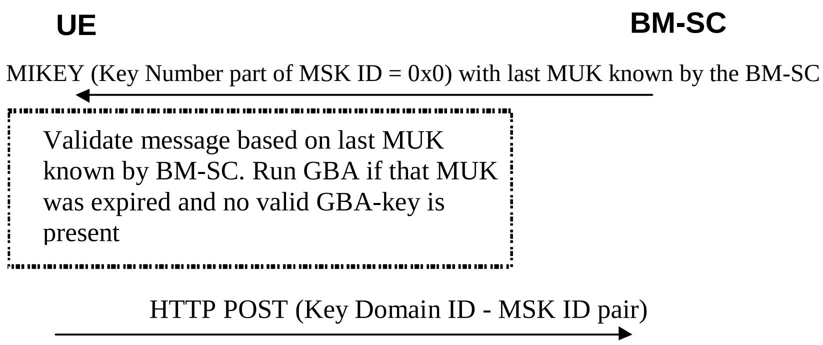


Figure 6.2b: BM-SC solicited pull

The BM-SC Key Distribution function sends a MIKEY message over UDP to the UE. The MIKEY message shall be protected by the last MUK known by the BM-SC. The Key Number part of the MSK ID in the extension payload of the MIKEY message shall be set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

If the received MUK_ID (i.e. the last MUK known by the BM-SC) does not correspond to the last MUK known by the UE, then the UE checks the solicited pull MIKEY message with the last MUK successfully used by the BM-SC.

The BM-SC shall not set the V-bit in the common header when initiating the BM-SC solicited pull procedure.

NOTE 1: A MUK may be used by the BM-SC Key Distribution function beyond the GBA key lifetime of the corresponding Ks_xx_NAF for the purpose of using the MUK within the first MIKEY message of a push solicited pull procedure.

NOTE 2: Since the integrity of the MIKEY message still needs to be assured, a KEMAC payload shall be included in the MIKEY message from the BM-SC Key Distribution function. There is however no key present in the message. Thus by setting the Encr data len field to zero, only the MAC of the message will be included.

When receiving the message, the UE shall request for the current MSK for the specified Key Group as specified in clause 6.3.2.2.1.

A situation where the use of the solicited pull procedure is needed for the BM-SC to be able to update successfully MSK's to a UE is when the BM-SC has chosen the MUK lifetime less than the GBA key lifetime of the corresponding Ks_xx_NAF, and the MUK lifetime has expired in the BM-SC. In that case the BM-SC should initiate the BM-SC solicited pull procedure and answer to the HTTP POST of Figure 6.2b with a Bootstrapping Renegotiation Request according to TS 33.220 [6].

6.3.2.3 MSK delivery procedures

6.3.2.3.1 Pushing the MSK to the UE

The BM-SC Key Distribution function controls when the MSKs used in a MBMS User Service are to be changed. The below flow describes how MSK changes are performed. This procedure can be initiated after the UE has requested for MSK(s) as described in clause 6.3.2.2.

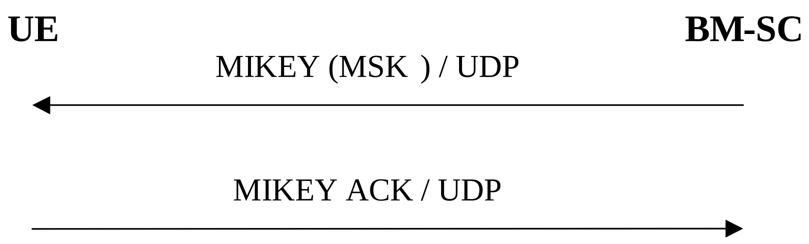


Figure 6.3: Pushing the MSKs to the UE

When the BM-SC Key Distribution function decides that it is time to update the MSK, the BM-SC Key Distribution function sends MIKEY message over UDP transporting the requested MSK to the UE.

If requested by the BM-SC Key Distribution function, the UE sends a MIKEY acknowledgement message to the BM-SC.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

When an MSK push MIKEY message is not directly preceded by an MSK key request, then it may happen that the BM-SC uses a still valid MUK that is not the last generated MUK at the UE. The UE shall handle such a MIKEY push message in a similar way as the push solicited pull MIKEY message (i.e. upon a successful integrity check the UE shall initiate an MSK request with the specified Key Group). Additionally, in this case, the UE shall not create a MIKEY acknowledgement message.

NOTE: This procedure guarantees that the UE contacts the BM-SC with the last B-TID, such that the UE now receives a MIKEY push message with the last generated MUK. The integrity of the initial pushed MIKEY message can be verified at the UE with the MUK-ID that is known as the last successfully used BM-SC MUK-ID.

6.3.2.3.2 Void

6.3.2.4 Handling of multiple status codes within one response message

The UE shall include a list of one or more MBMS User Service IDs (in MBMS User Service registration and de-registration procedures) or MSK ID-Key Domain ID -pairs (in MSK request procedure) in the payload of one HTTP request message.

When the BM-SC has processed the request message, it shall include a list of corresponding status codes in the HTTP response message, i.e. a status code for each MBMS User Service ID or MSK ID-Key Domain ID -pair. The status codes are carried in the payload of the HTTP response message and they use the values as specified in RFC 2616 [19]. A successful code, e.g. 200 OK, means that the (de-) registration or MSK request for that specific MBMS User Service ID or MSK was successful. The MBMS specific error codes are described in clause G.2.4.

There is also a status code in the status line of the HTTP response message, which has a successful value if the BM-SC was able to successfully process the corresponding request message. Otherwise the status code in the HTTP status line shall indicate the appropriate error.

NOTE 1: This means that there are two levels of status codes in the response message: the status code in the HTTP status line that is specific to the HTTP message and processed by the HTTP application and the one or more status codes in the payload that are specific to and processed by the MBMS application.

In case the response message does not include all the same status codes in the payload that were in the request message, the UE may still process the status codes that it is able to process.

The list of status codes is also used in case only one MSK or registration is requested. Figure 6.4 below illustrates an example of a UE trying to register to two MBMS User Services. The registration is successful for the first but fails for the second MBMS User service. The example procedure shows only parameters that are relevant for the functionality in question.

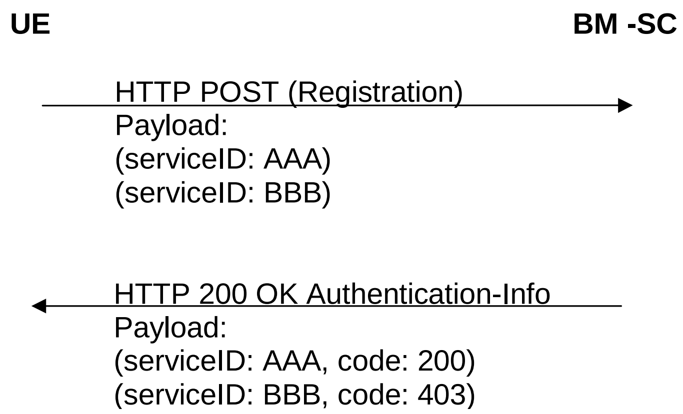


Figure 6.4: Example registration procedure

6.3.3 MTK procedures

6.3.3.1 MTK identification

Every MTK is uniquely identifiable by its Key Domain ID, MSK ID and MTK ID

where

Key Domain ID and MSK ID are as defined in clause 6.3.2.1.

MTK ID is 2 bytes long sequence number and is used to distinguish MTKs that have the same Key Domain ID and MSK ID. It is carried in the MTK ID field of MIKEY extension payload. Every time a MSK with a new MSK ID is taken into use by the BM-SC, the MTK ID of the first MTK sent by the BM-SC protected by that MSK shall be set to an initial value greater than zero chosen by the BM-SC.

NOTE 1: In most situations the practical choice for the initial MTK ID will be one, but this does not prevent the BM-SC to choose a value different for each service and greater than one.

The MTK ID that will be used in a next MTK update needs to be greater than the previously used MTK-ID.

NOTE 2: The practical choice to increment is 1 but also other increments are allowed.

NOTE 3: As the MTK ID is 2 bytes long, this allows to use 2^{16} -2 MTKs protected by one MSK if the MTK-ID is always incremented by one and the initial MTK ID starts at 1. The maximum value for MTK ID is disallowed (see clause 6.4.5.1).

6.3.3.2 MTK update procedure

The MTK is delivered to the UE using MIKEY over UDP, but the V-bit in the common header shall not be set.

The UE shall not send an error message to the BM-SC as a result of receiving an MTK message.

6.3.3.2.1 MTK delivery in download

In the download case the MIKEY message carrying the MTK shall be delivered over the same FLUTE stream as the object to be downloaded to the UE (see TS 26.346 [13]). This means that the message is specified as a separate object in the FLUTE File Delivery Table (FDT), having its own identifier. This means the MTK delivery inherits the reliability features of FLUTE. The mime-type of the object carrying the MIKEY message shall be the IANA-registered type for MIKEY.

6.3.3.2.2 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent using the same IP destination address as the RTP traffic. MIKEY messages shall be transported to UDP port number 2269 specified for MIKEY. Reliability of MTK delivery is reached by re-sending MTK messages periodically.

NOTE: Re-sending of MTK message will also allow the UE to faster switch between SRTP streams.

In order to increase the possibility that UEs receive a new MTK in time, MTK messages may be sent before the RTP traffic changes over to a new MTK.

6.3.4 Multiple BM-SC deployments

6.3.4.1 General

The requirements in the following sub-clauses apply when one and the same MBMS User Service is transmitted via multiple BM-SCs, as this case requires some coordination between the BM-SCs regarding MBMS key management.

6.3.4.2 Service announcement coordination

When one and the same MBMS User Service is transmitted via multiple BM-SCs the service shall be announced with one Service Announcement indicating common security protectection description for the involved BM-SCs.

6.3.X.3 MSK key management anchor point

The UE shall register to one BM-SC indicated in the Service Announcement and shall keep the same BM-SC for all subsequent MSK management procedures as defined in clause 6.3.2.1A.

NOTE: The MSK key management can be kept on the original BM-SC even though the UE could move under a new BM-SC. This is because the MSK key management uses the PDP/PDN connection.

6.3.4.4 MSK coordination

The BM-SCs shall use MSKs in a synchronized way. At a certain point in time the same MSK (identified by the Key Domain ID, MSK Key Group and Key Number part) shall be used in all BM-SCs per a streaming or download session. When the MSK needs to be updated, the BM-SCs shall take the new MSK (identified by the Key Number part) into use at the same time. This is to ensure that the BM-SCs are able to use the MTKs in a synchronized way. For MSK key management anchor point see clause 6.3.X.3.

6.3.4.5 MTK coordination

The BM-SCs shall use MTKs in a synchronized way. At a certain point in time the same MTK (identified by the MTK ID as defined in clause 6.3.3.1) shall be used in all BM-SCs per a streaming or download session. When the MTK needs to be updated, the BM-SCs shall take the new MTK into use at the same point in time. This is to ensure that a UE that moves under a new BM-SC, which is transmitting the same MBMS User Service as the old BM-SC, is able to decrypt the service without interruption. The BM-SCs transmitting the same MBMS User Service may transmit identical content or slightly different content, e.g. local news. Especially in the latter case it is important that the update of the MTK happens at the same point in time and is not based on the amount of content (packets or files) sent in the streaming or download session since the amount of content may vary between the BM-SCs. This is to ensure that the BM-SCs keep synchronized in their use of MTKs regardless of the amount of content sent.

6.3.4.6 MIKEY MTK timestamp coordination

MBMS uses counter-based MIKEY timestamps as specified in clause 6.4.3. The BM-SCs shall use MIKEY timestamps in MTK delivery messages in a synchronized way. At a certain point in time the same MIKEY MTK timestamp shall be used in all BM-SCs for a streaming or download session.

NOTE: There is no need to synchronize the MIKEY timestamp for MSK delivery messages as the MSK messages are sent from one BM-SC, see also clause 6.3.X.3.

When the same MBMS User Service is transmitted via multiple BM-SCs it may happen that the BM-SCs send different amount of MTK delivery messages within a streaming or download session. This will result to that the MIKEY MTK timestamps are not in synchronization between the BM-SCs, and that a UE that moves under a new BM-SC is not able to decrypt the service without interruption due to replay protection.

The BM-SCs may keep synchronization for the use of MIKEY MTK timestamps by sending the same amount of MIKEY MTK delivery messages at the same pace. However, this may not always be possible e.g. due to different amount of content transmitted by the BM-SCs. Another possibility is that the BM-SCs increase the MIKEY MTK timestamp based on NTP UTC time regardless of how many MIKEY MTK delivery messages are sent, and add the first 32 most significant bits (i.e. the integral part) of NTP UTC time to the counter-based timestamp payload field of MIKEY MTK messages. This ensures that the BM-SCs are synchronized and the UE will treat the timestamp as a counter.

6.4 MIKEY message creation and processing in the ME

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9]. The UDP port number for MIKEY is 2269 (see Port Numbers at IANA [17]).

To keep track of MSKs and MTKs, a new Extension Payload (EXT) as defined in RFC 4563 [16] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (see clauses 6.3.2 and 6.3.3).

Some MIKEY payloads contain text strings, e.g., the IDi and IDr payloads. These strings shall be encoded according to UTF-8 as defined in RFC 3629 [21].

In case MIKEY packets are FEC-protected (see TS 26.346 [13]), this is signalled within the MBMS User Service Description.

As MIKEY is used in a key transport mode, the key derivation function as defined in section 4.1.4 of RFC 3830 [9] shall be used for MIKEY internal keys and MIKEY internal salt. The preshared key used for transmission of MSK is the MUK, and the pre-shared key used for transmission of MTK is the MSK.

The size of the authentication key to be used to verify the MAC field of a MIKEY message shall be 160 bits.

6.4.2 MIKEY common header

MSKs shall be carried in MIKEY messages. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the MTK messages sent by the BM-SC over MBMS bearer. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret.

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header is not used for identification purposes but shall be present in both MSK messages and MTK messages.

NOTE: As the CSB ID field has no meaning within the context of MBMS, the BM-SC is free to assign any value to CSB ID. Assigning random values to CSB ID enhances security as CSB ID is taken into account for MIKEY key derivations (section 4.1.3 and 4.1.4 of RFC 3830 [9]).

6.4.3 Replay protection

Each MIKEY message contains the timestamp field (TS) of type 2. This means that the contents of the timestamp field is a 32-bit counter. The counter shall be increased by one for each MSK message sent from the BM-SC to the UE even in case BM-SC retransmits a previously sent MSK message. The counter shall be increased by one for each new MTK message created in the BM-SC.

NOTE: The BM-SC is allowed to retransmit a previously sent MTK message for streaming in order to provide a higher reliability of MTK delivery (cfr section 6.3.3.2.2) without having to increment the TS field for each sent MTK message. As specified in step 2 of clause 6.4.6.2, the ME will discard duplicate MTK messages based on the last received TS.

There is one counter per UE for MSK delivery, and one counter common to all UEs for MTK delivery. The counter is used for replay protection; messages with a counter less than or equal to the current counter are discarded. Less than or equal is to be taken in the meaning of RFC1982 [10]. If the less than or equal relation is undefined in the sense of RFC1982 [10], the message should be considered as being replayed and shall be discarded. The counter in the TS field shall be reset for MSK transport messages when the MUK is updated. The counter in the TS field shall be reset for MTK transport messages when the MSK is updated.

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the key that is derived in the message, a general Extension Payload (EXT) is used that conforms to the structure defined in reference RFC 4563 [16].

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see figure 6.4a. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see figure 6.4b.

See clauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MTK ID is increased every time the corresponding key is updated. It is possible that the same MTK is delivered several times over MBMS bearer, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integers.

Key Domain ID sub-payload
Key Type ID sub-payload (MSK ID)

Figure 6.4a: Extension payload used with MIKEY MSK message

Key Domain ID sub-payload
Key Type ID sub-payload (MSK ID)
Key Type ID sub-payload (MTK ID)

Figure 6. 4b: Extension payload used with MIKEY MTK message

6.4.5 MIKEY message structure

6.4.5.1 MSK message structure

The following applies for both streaming services and download services:

- The structure of the MIKEY message carrying a MSK key shall be according to Figure 6.5. (For handling of unknown MIKEY extension payloads in MGV-F, cf. clause 6.5.3.).
- The actual MSK key that is delivered is kept in the KEMAC payload. Only one MSK key shall be transported in the KEMAC payload.
- The format of the EXT payload is as described in chapter 6.4.4.
- The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent in all the MSK delivery messages. A UE and BM-SC shall support a MIKEY-RAND of 128-bit.For a specific MSK (identified by the MSK ID including the Key Number part) within an MBMS streaming or download session, the same MIKEY-RAND shall be used in MSK delivery messages for all UEs. This ensures that all UEs will use the same MIKEY-RAND for MTK message processing, cf. clause 6.5.4.
- The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID (i.e. FQDN) of the BM-SC (i.e. NAF-ID without the Ua security protocol identifier) and IDr is the ID of the UE's username (i.e. B-TID). The ID Type field of IDi and IDr payloads shall be set to value 0 (=NAI). As the content of the IDi field is not a NAI, but a FQDN of the BM-SC, the ID Type field of the IDi payload shall be ignored by the receiver and the ID data field shall be handled as a text string.

NOTE: NAF-ID without the Ua security protocol identifier (i.e. FQDN of BM-SC) is used to identify a server while a NAI identifies a user,

- The Type subfield shall be set to value 2 (=TEK) in the KEMAC payload in all MSK delivery messages.
- The KV (Key validity period) subfield shall be set to value 2 (=Interval) in the KEMAC payload in all MSK delivery messages.

- The Key Validity Data subfield is present in the KEMAC payload when MSK is transported. The field defines the validity time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the original value of SEQl to be used by the MGV-F (see clause 6.5) and the upper limit of the interval defines the SEQu. The BM-SC shall never set SEQu to its maximum possible value.

- The use of NULL algorithm in the MAC alg field is not allowed.

- The use of NULL algorithm in the Encr alg field is not allowed.

The following applies only for streaming services:

- Only one CryptoSession can be transported in the field CS ID map info for streaming.

- The #CS field shall be set to one, and CS ID map info shall be present in the MSK message.

- The CS ID map type subfield shall be set to “SRTP-ID” as defined in RFC 4563 [16].

- The SP payload shall be used only with streaming services.

- Security Policy (SP) payload shall include information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc.

- The BM-SC shall ensure that the UE has received the SP payload before the SP payload needs to be applied in the streaming service.

- The BM-SC is not allowed to change the SP payload anymore once the streaming service using that SP has started for the first time.

- The BM-SC shall include the SP payload when the MSK delivery was triggered by the UE using the MSK request procedure or the MBMS User Service Registration procedure, otherwise it is optional for the BM-SC to include the SP payload into MSK delivery messages.

- An SRTP key derivation rate of zero shall be used. The BM-SC can achieve this either by explicitly signalling a key derivation rate of zero via MIKEY SRTP policy (RFC 3830 [9]) or by omitting this parameter in MIKEY SRTP policy as the default key derivation rate of SRTP is zero.

The following applies only for download services:

- The #CS field shall be set to zero, and no CS ID map info shall be present in the MSK message.

- The CS ID map type subfield shall be set to “Empty map” as defined in RFC 4563 [16].

- The SP payload shall not be included in the MSK messages.

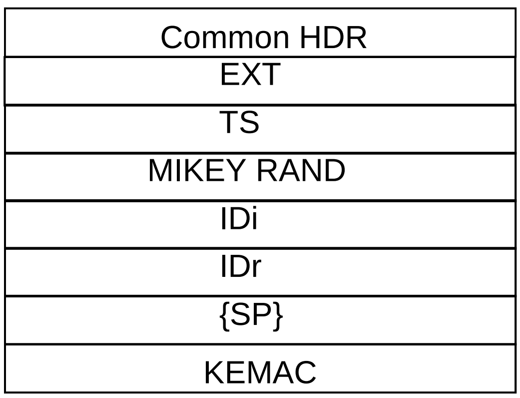


Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

6.4.5.2 MSK Verification message structure

If the BM-SC expects a response to the MSK-transport message (i.e., the V-bit in the MIKEY common header is equal to 1), the UE shall send a verification message as a response. The verification message shall be constructed according to section 3.1 of MIKEY, and shall consist of the following fields: HDR || TS || IDr || V, where IDr is the ID of the UE. The ID Type field of IDr payload shall be set to value 0 (=NAI). The CS ID map type subfield shall be set to “Empty map” as defined in RFC 4563 [16]. The #CS field shall be set to zero, and no CS ID map info shall be present in the MSK verification message. The use of the NULL algorithm in the MAC alg field is not allowed. Note that the MAC included in the verification payload, shall be computed over both the initiator's and the responder's ID as well as the timestamp in addition to be computed over the response message as defined in RFC 3830 [9].

The UE shall use the same CSB ID in the verification messages as received in the MSK delivery message.

Common HDR
TS
IDr
V

Figure 6.6: The logical structure of the MIKEY Verification message

The verification message shall not be sent as a response to MIKEY messages delivering MTK.

The ME shall send the verification message, when received as result from the MGV-F, to the BM-SC.

6.4.5.3 MTK message structure

Following requirements apply for both streaming and download services:

- The structure of the MIKEY message carrying a MTK key shall be according to Figure 6.7. (For handling of unknown MIKEY extension payloads in MGV-F, cf. clause 6.5.4)
- The actual MTK key that is delivered is kept in the KEMAC payload. Only one MTK key can be transported in the KEMAC payload.
- The EXT payload has format as described in clause 6.4.4.
- The #CS field shall be set to zero, and no CS ID map info shall be present in the MTK message.
- The CS ID type map type subfield shall be set to “Empty map” as defined in RFC 4563 [16].
- Neither shall the SP payload be included in MTK messages.
- The KV (Key validity period) subfield shall be set to NULL in the KEMAC payload when MTK is transported.
- The Key Validity Data subfield shall not be present in the KEMAC payload when MTK is transported.
- The use of NULL algorithm in the MAC alg field in the KEMAC payload is not allowed.
- The use of NULL algorithm in the Encr alg field in the KEMAC payload is not allowed.

NOTE: MIKEY-RAND is not included in MTK messages since the MIKEY-RAND sent within MSK delivery messages is used for MTK message processing, cf. clause 6.4.5.1 and 6.5.4.

Following requirement applies for streaming services only:

- The Type subfield shall be set to value 3 (=TEK + salt) in the KEMAC payload in all MTK delivery messages for streaming services.
- A 112 bit salt shall be added to the KEMAC payload in addition to the MTK.

Following requirement applies for dowload services only:

- The Type subfield shall be set to value 0 (=TGK) in the KEMAC payload in all MTK delivery messages for download services.

- No salt shall be added to the KEMAC payload.

Common HDR
EXT
TS
KEMAC

Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

6.4.6 Processing of received messages in the ME

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (EXT) is examined, and if it indicates an MSK delivery protected with MUK, the MUK ID is received by combining IDi and IDr.

2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is smaller or equal to the stored replay counter associated with the given MUK (the stored replay counter value is retrieved from MGV-S).

3. The Security Policy payload is stored temporarily in the ME if it was present.

4. The message is transported to MGV-F for further processing, cf. clause 6.5.3.

5. The MGV-F replies success or failure. In case of success the temporarily stored Security Policy payload is taken into use. Otherwise it is deleted.

6. The ME shall check if the MIKEY message indicates a BM-SC solicited pull procedure and behave as described in clause 6.3.2.2.4.

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (EXT) is examined, and if it indicates an MTK delivery protected with MSK, the MSK ID is extracted from the Extension Payload.

2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is smaller or equal to the stored replay counter associated with the given MSK (the stored replay counter value is retrieved from MGV-S).

3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.

4. The message is transported to MGV-F for further processing, cf. 6.5.4.

5. The MGV-F replies success (i.e. sending the MTK and salt if available) or failure.

6.5 Validation and key derivation functions in MGV-F

6.5.1 General

When an MSK or MTK message is received in the UE, it is processed in protected environment MGV-S.

6.5.2 Usage of MUK

When a MUK has been installed in the MGV-S, i.e. as a result of a GBA run, it is used as pre-shared secret used to verify the integrity of the MSK transport message and decrypt the MSK carried in the KEMAC payload as described in RFC 3830 [9].

6.5.3 MSK processing

When the MGV-F receives the MIKEY message, the MGV-F first determines the type of message by reading the EXT. If the EXT indicates MSK delivery (clause 6.4.4) then the text in this clause applies.

The MGV-F shall not abort processing of a MIKEY message when encountered with an extension payload with unknown type. The content of an unknown extension payload (except for the next payload, type and length fields) shall be treated as an opaque object. The MAC computation required for the KEMAC payload shall include any unknown extension payloads preceeding it.

NOTE: This is because an unknown extension payload may be specified for ME use only and it is therefore "unknown" to the MGV-F. Skipping unknown payloads during the payload parsing is a deviation from recommended receiver behavior in section 5.3 of RFC 3830 [9].

The MGV-F retrieves the MUK identified as specified in clause 6.1. If the Key Number part of the MSK ID in the EXT equals 0x0 then this indicates a solicited pull procedure (clause 6.3.2.2.4) for which the MIKEY message does not contain an MSK and for which the MUK shall be applied according to clause 6.3.2.2.4.

The integrity of the message is validated and if valid then the MSK, if present, shall be extracted from the KEMAC payload as described in section 5 of RFC 3830 [9], and the Key Validity data, shall be extracted from the message and stored (in the form of MTK ID interval).

If integrity validation is successful, then the MGV-F shall update the stored Time Stamp value associated with the corresponding MUK ID in MGV-S with the counter value in the Time Stamp payload.

If the MGV-F receives an MSK and already contains two other MSKs under the same Key Domain ID and Key Group part, then the UE shall keep the newer and delete the older of these two MSKs. The newer MSK (i.e. the MSK to be kept) of the two stored MSKs under the same Key Domain ID and Key Group part is determined by the UE from the combination of MUK ID and Time Stamp value in the following way. The MSK that was protected with the newer MUK is the newer MSK regardless of the value of the Time Stamp. In case the MUK IDs are equal, the MSK with higher Time Stamp value is the newer MSK. Updating an existing MSK (e.g. by updating the Key Validity Data) or resending an MSK means then also that the updated MSK becomes the newer MSK since the Time Stamp value is increased in these cases. In case the MUK ID values are not equal, the newer MUK is the last MUK successfully used by the BM-SC as specified in clause 6.3.2.2.4.

If the MGV-F receives an MSK, which has the same MSK ID as a stored MSK, the received MSK shall replace the stored MSK and update the Key Validity data. In case the MSK message does not include any key in KEMAC payload, then the Key Validity data shall be updated for the specified MSK except if the MSK ID is 0x0.

6.5.4 MTK processing

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the EXT. If the key inside the message is an MTK protected by MSK, MGV-F retrieves the MSK with the ID given by the Extension payload.

The MGV-F shall not abort processing of a MIKEY message when encountered with an extension payload with unknown type. The content of an unknown extension payload (except for the next payload, type and length fields) shall be treated as an opaque object. The MAC computation required for the KEMAC payload shall include any unknown extension payloads preceeding it.

NOTE: This is because an unknown extension payload may be specified for ME use only and it is therefore "unknown" to the MGV-F. Skipping unknown payloads during the payload parsing is a deviation from recommended receiver behavior in section 5.3 of RFC 3830.

It is assumed that the MBMS service specific data, MSK, MIKEY-RAND and the sequence numbers SEQl and SEQu, have been stored within a secure storage (MGV-S). MSK, MIKEY-RAND, SEQl and SEQu were transferred to the MGV-S with the execution of the MSK update procedures. The initial values of SEQl and SEQu are determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQl and SEQu. If SEQp is equal to or lower than SEQl or SEQp is greater than SEQu, then the MGV-F shall indicate a failure to the ME. Otherwise, the MGV-F shall verify the integrity of the MIKEY message according to RFC 3830 [9]. The random value to use as input to the PRF function (section 4.1.4 of RFC3830 [9]) is the MIKEY-RAND stored together with the MSK. If the verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the verification is successful, then the MGV-F shall update SEQl with SEQp value and extract the MTK from the message. The MGV-F then provides the MTK to the ME.

If MAC verification is successful, the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE 2: It is advised for the implementers of MGV-S (either on the UICC or ME) to exercise caution when implementing memory management for the MTK parameters (e.g. MTK ID field) . E.g. on the UICC, t he file EF_{MSK} containing the MSK_IDs and related timestamps is marked as a high update activity file , but that might not be sufficient to avoid potential wear-out of the non-volatile memory, if the network uses a very short MTK lifetime (e.g. 5 seconds). The approach chosen by implementers need s also to take into account the fact that users may roam and use the service in other networks than their home network. Those networks may have a different configuration.

The ME shall store the two most recent MTKs used per MBMS streaming or download session. In particular, if the ME receives an MTK and already stores two other MTKs for that MBMS streaming or download session, then the UE shall keep the newer and delete the older of the two stored MTKs before storing the received MTK. Any MTKs stored in association with a particular MBMS streaming or download session should be deleted at the end of that session.

In the case of streaming, SRTP and SRTCP require a master key and a master salt. The MTK is used as a common master key for both SRTP and SRTCP, and the salt in the KEMAC payload is used as master salt.

In case of download service, key derivation as defined in section 4.1.3 of RFC 3820 [9] shall be used to derive authentication and encryption keys from MTK in the ME using the constants for authentication and encryption keys defined in table 4.1.3 of RFC 3830 [9]. As there shall be no CS field present for download services as specified in clause 6.4.5.3, cs_id shall be set to 0x00000000 within the key derivation of section 4.1.3 of RFC 3830 [9]. The derived authentication and encryption keys shall be provided to the download protection protocol.

6.6 Protection of the transmitted traffic

6.6.1 General

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and UEs that are accessing the MBMS User Service. The protection of the data is applied by the BM-SC Session and Transmission Function. In order to determine which MTK was used to protect the data key identification information is included with the protected data. The key identification information will uniquely identify the MSK and MTK. The MTK is processed according to the methods described in clauses 6.4 and 6.5. Whenever data from an MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

NOTE: Including the key identification information with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

6.6.2 Protection of streaming data

6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in RFC 3711 [11] shall be used. The MTK is carried to the UEs from the BM-SC using RFC 3830 [9] (MIKEY) with extensions defined according to this specification. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in section 4.3 of RFC 3711 [11]. A key derivation rate as defined in clause 6.4.5 shall be used.

The correct MTK to use to decrypt the data is indicated using the MKI (Master Key identifier) field, which is included in the SRTP packets as defined in RFC 3711 [11]. The form of MKI shall be a concatenation of MSK ID and MTK ID, i.e. MKI = (MSK ID || MTK ID).

NOTE 1: The UE knows the Key Domain ID related to this MKI from the User Service Description which includes mapping between IP address and port of the traffic and the corresponding Key Domain ID and MSK ID.

The SRTP authentication tag shall be appended to the packets as defined in RFC 4771 [22].

NOTE 2: In RFC 4771 [22] it is specified that the ROC is transferred in every Rth SRTP packet. The specification furthermore defines how the constant R and the integrity transform is negotiated using MIKEY.

The parameter, constant R, shall be included in the MSK delivery messages.

NOTE 3: In RFC 4771 [22] it is specified that if the constant R is not signalled then the default value 1 is to be used. However explicit signalling of R is here required in each MSK delivery message in order to require the operator of choosing the most optimal value for the SRTP stream. The default value of R=1 causes to add a ROC to each SRTP packet implying that a MAC of 10 octets (proposed by RFC 4771 [22]) and a ROC of 4 octets will be added to each SRTP packet in both mode RCCm1 and RCCm2. Also a ROC of 4 octets will be added to each SRTP packet in mode RCCm3 (but no MAC).

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in section 6.10.1 in RFC 3830 [9].

FEC shall be applied beneath the SRTP layer as described within TS 26.346 [13]

NOTE 4: This deviates from the default FEC order as described within RFC3711 [11] clause 10. The reversed order is not signalled within the service protection description of the MBMS User Service Announcement.

6.6.2.1A Usage of SRTCP

Secure RTCP (SRTCP) provides the same security services to RTCP as SRTP does to RTP. As defined in TS 26.346 [13] only RTCP sender reports are allowed in MBMS.

As defined in RFC 3711[11] SRTCP shall be applied to RTCP control packets when SRTP is applied to RTP with the following profiling:

- Encryption of SRTCP packets is optional;
- SRTCP packets shall be integrity protected as defined in RFC 3711 [11];
- SRTCP shall share master key and master salt with the corresponding SRTP stream;
- SRTCP packets shall carry the same MKI field value as the corresponding SRTP stream;

NOTE 1: This is a consequence of sharing the same master key.

- SRTCP shall use the same encryption algorithm as corresponding SRTP session

NOTE 2: SRTCP does not need additional mechanisms, e.g. RFC 4771 [22], to synchronize the ROC as SRTCP header explicitly carries the SRTCP packet index.

6.6.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will retrieve the correct cryptographic context identified by destination transport address, destination port and SSRC (according to RFC 3711 [11] and RFC 4771 [22]), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

NOTE 1: The cryptographic context needs to be unique for each SRTP stream.

NOTE 2: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in the clause 6.3.

If the correct MTK is not present in the UE when RTP traffic arrives, the UE shall wait for the next MTK update procedure from the BM-SC as described in clause 6.3.3.2.

NOTE 3: It is implementation specific issue whether the UE spools encrypted packets or discards all packets before the UE has received the correct MTK.

The below flow shows how the protected content is delivered to the UE.

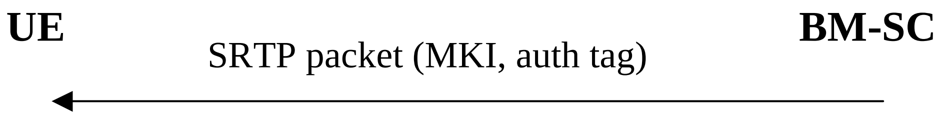


Figure 6.8: Delivery of protected streaming content to the UE

6.6.3 Protection of download data

6.6.3.1 General

Data that belongs to a download MBMS User Service is decrypted as soon as possible by the UE, if the MSK needed to provide the relevant MTK is already available on the UE.

6.6.3.2 Usage of OMA DRM DCF

NOTE: If the OMA DRM V2.0 DCF [15] specification is upgraded, these upgrades do not apply for the present document.

When it is required to protect MBMS download data, OMA DRM V2.0 DCF as defined in OMA DRM V2.0 DCF [15] shall be used. MBMS download data are therefore indicated by minor version 0x00000002 in a DCF. OMA DRM Rights Objects are not utilized. Instead, encryption and authentication keys are generated from MTK. For integrity protection, an OMADRMSignature as specified below is attached inside the optional Mutable DRM information box ('mdri') of the DCF.

The OMADRMSignature Box is an extension to OMA DRM V2.0 DCF for use by MBMS, and is defined as follows:

```
aligned(8) class OMADRMSignature extends Fullbox('odfs', version, flags) {
   Unsigned int(8) SignatureMethod;   // Signature Method
   Char            Signature[];       // Actual Signature
}

SignatureMethod Field:
NULL   0x00
HMAC-SHA1 0x01
```

The range of data for the HMAC calculation shall be according to section 5.3 of OMA DRM V2.0 DCF [15].

The correct MTK for decrypting and verifying the integrity of the download data is indicated by the KeyID in the OMABCASTKeyInfoBox 'obki' included in the ExtendedHeadersfield in the OMADRMCommonHeaders box (cf. OMA DRM XBS [24]). The use of the 'obki' box by MBMS is as follows:

- KeyIssuerPresent set to 1 if KeyIssuerURL is provided (the DCF RightsIssuerURL field is not used)
- STKMPresent set to 0 (no STKM stored in file)
- TBKPresent set to 0 (no TerminalBindingKey used)
- TBKIssuerURLPresent set to 0 (no TBKIssuerURL present)
- KeyIDType set to 0x02 (reserved by OMA BCAST for 3GPP MBMS, identifies the KeyID for MBMS usage.

KeyID is the base64 encoded concatenation (Key Domain ID || MSK ID || MTK ID).

If the MBMS download data requires protection, see 6.3.2.1A, then the FDT of the FLUTE protocol shall be integrity protectedby wrapping the FDT in a DCF of its own. The correct MTK for verifying the integrity of the FDT shall be indicated by theKeyID in the OMABCASTKeyInfoBox 'obki' included in the ExtendedHeaders field in the OMADRMCommonHeaders box.

The MBMS DCF implementation shall support the following boxes specified in OMA DRM V2.0 DCF [15]:

- Fixed DCF header;
- Mutable DRM information Box;
- OMA DRM Container Box.

6.7 Confidentiality protection of associated delivery procedures

6.7.1 General

The MBMS associated delivery procedures specified in clause 9 of TS 26.346 [13] require the UE to use HTTP protocol to transmit data associated with the MBMS user service for reception reporting and file repair purposes to a HTTP server in the network (i.e., the Reception Report server and File Repair server as defined in TS 26.346 [13]). The information transmitted by the UE using associated delivery procedures may be user privacy (e.g., MBMS service the user is listening to, location) and network privacy (e.g., network topology information) sensitive. Therefore, support for confidentiality protection in HTTP is required.

In order to protect the confidentiality of the privacy sensitive data transmitted by the UE using associated delivery procedures, the UE shall support using HTTP over TLS as specified in RFC 2818 [32]. TLS shall be used with server certificates, but the HTTP server shall not request client certificates.

The support of HTTP over TLS (i.e., HTTPS) for associated delivery procedures is optional in the network. If supported by the network, its use for an associated delivery procedure (i.e., Reception Reporting or File Repair) is determined by the UE either based on the UE preconfiguration (e.g., based on explicit configuration or on the presence of preconfigured list of trusted root certificates in the UE for the validation of HTTP servers used for associated delivery procedures or based on the reception over an integrity protected channel of an indication to the UE to use HTTP or HTTPS (e.g., User Service Description and/or FLUTE File Delivery Table contains this indication and is delivered individually as, or part of, an integrity protected MBMS Download Service). If the integrity of this indication to use HTTP or HTTPS can be verified by the UE, then this indication shall take precedence over the UE preconfiguration. If the integrity of this indication cannot be verified by the UE, then the UE preconfiguration shall take precedence). The procedures topre configure this information on the UE are outside the scope of the present specification.

6.7.2 TLS Profile

The UE shall support TLS according to the TLS profile given in TS 33.310 [31], Annex E.

The certificates shall comply with the requirements for TLS certificates in clause 6.1 of TS 33.310 [31].

When the UE decides to use TLS, the use of TLS ciphersuite without NULL encryption is mandatory.

NOTE 1: Without the use of TLS encryption, the use of TLS is not needed as authentication and integrity protection for HTTP procedures is provided using HTTP Digest, cf. clause 6.2.

Support of certificate revocation and of the related fields in certificates is optional. If supported, the certificate and CRL profiles in clauses 6.1 and 6.1a of TS 33.310 [31] should be followed.

NOTE 2: The management of Root Certificates is out of scope of the present document.

6.7.3 HTTP server authentication

The UE shall authenticate the HTTP server by use of a server certificate. The UE shall match the server name as specified in RFC 2818 [32], section 3.1.

The UE shall use a preconfigured list of trusted root certificates for TLS server certificate validation. It is recommended that a separate preconfigured list of trusted root certificates is used with associated delivery procedures. The server certificate validation shall not require manual user interaction.

6.7.4 Authentication of the UE

The HTTP server shall not request a certificate in a Server Hello Message from the UE. The HTTP server relies on the HTTP Digest for UE authentication as specified in clause 6.2.

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

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 clauses:

- unauthorized access to MBMS User Service data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS User Services;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here because in case these are transferred on a point-to-point connection (e.g. PS signalling connection), they are already secured. In case the service announcement is transferred over HTTP, it is protected by HTTP Digest as defined in the current specification and/or it may be integrity protected and optionally encrypted at the RAN level. In case the service announcements are sent over MBMS bearer, it is impractical to protect them.

B.1.1 Unauthorised access to MBMS User Service data

A1: Intruders may eavesdrop MBMS User Service data on the air-interface.

A2: Users that have not joined and activated a MBMS User Service receiving that service without being charged.

A3: Users that have joined and then left a MBMS User Service continuing to receive the MBMS User Service without being charged.

A4: Valid subscribers may derive decryption keys (MTK) 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 (MSK, MTK) 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. Deliberate manipulation of the data to disturb the communication.

B.1.4 Unauthorised access to MBMS User Services

D1: An attacker using the 3GPP network to gain "free access" of MBMS User Services and other services on another user's bill.

D2: An attacker using MBMS shared keys (MSK, MTK) 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 keys (MSK, MTK) 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 UICC-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 clauses:

- unauthorized access to data;
- threats to integrity;
- denial of service;
- a malicious UE generating MTKs for malicious use later on;
- unauthorized insertion of MBMS user data and key management data.

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 interface Gi and Gmb between the BM-SC and GGSN.

F2: Intruders may eavesdrop the 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 interfaces Gi and Gmb between the BM-SC and GGSN.

G2: The 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.

B.2.4 A malicious UE generating MTKs for malicious use later on

I1: A malicious ME querying the MTK generation function for MTK's to use them later on in an attack (e.g. in order to use the retrieved MTKs within an unauthorized data insertion attacks (See B.2.5)).

B.2.5 Unauthorised insertion of MBMS user data and key management data

J1: An ME, which deliberately inserts key management and malicious data, encrypted with valid (previously retrieved) MTK from the MTK generation function, within the MBMS User Service stream.

J2: An ME, which deliberately inserts key management and malicious data, encrypted with old (using replayed key management messages) MTK, within the MBMS User Service stream.

J3: An attacker, which deliberately inserts incorrect key management information within the MBMS User Service stream to cause Denial of Service attacks.

Annex C (normative): MBMS security requirements

C.1 Requirements on security service access

C.1.1 Requirements on secure service access

R1a: A valid USIM or SIM shall be required to access MBMS User Services.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.

C.1.2 Requirements on secure service provision

R2a: It shall be possible for the network (i.e. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.

R2b: It shall be possible to prevent the use of a particular USIM or SIM to access MBMS User Services.

NOTE: No security requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale.

C.2 Requirements on MBMS Transport Service signalling protection

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signalling on the Gmb reference point.

NOTE 1: This requirement may be fulfilled by physical or proprietary security measures if the Gmb protocol endpoints (i.e. GGSN, Gmb-Proxy and BM-SC) are located within the same security domain of the operator’s network. Otherwise the security mechanisms as specified within TS 33.210 [14] shall be applied.

R3b: Unauthorized modification, insertion, replay or deletion of all MBMS Transport Service signalling, 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.

NOTE 2: UTRAN/E-UTRAN bearer signalling integrity protection will not be provided for point to multipoint MBMS signalling and GERAN has no bearer signalling integrity protection, even for point to point signalling.

C.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.

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.

NOTE: UTRAN, E-UTRAN and GERAN bearer confidentiality protection will be not be provided for point to multipoint MBMS sessions.

C.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 shall 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 an MBMS User Service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
- users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User 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 User 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 User 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.

R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).

R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

C.5 Requirements on integrity protection of MBMS User Service data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.

NOTE 1: 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 2: 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 User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.

R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.

C.6 Requirements on confidentiality protection of MBMS User Service data

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

R7b: The MBMS User Service data may be encrypted with common encryption keys, which shall be available to all users that have joined the MBMS User Service.

R7c: It may be required to encrypt the MBMS User Service 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 protect the MBMS User Service from the BM-SC to the UE.

R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.

C.7 Requirements on content provider to BM-SC reference point

R8a: The BM-SC shall be able to authenticate and authorize a 3rd party content provider that wishes to transmit data to the BM-SC.

R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.

NOTE: This reference point will not be standardised.

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F). For details, see TS 31.102 [7].

The ME has previously performed a GBA_U bootstrapping procedure and a subsequent GBA_U NAF Derivation procedure as described in TS 33.220 [6]. The UICC stores the corresponding Ks_int_NAF and associated B-TID together with the NAF_Id without the Ua security protocol identifier, associated with this particular bootstrapping procedure.

The ME receives a MIKEY message containing an MSK update. After performing some validity checks, the ME sends the whole message to the UICC. The UICC uses the MUK ID (included in the MIKEY message, see clause 6.1) to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in clause 6.5.3).

After successful MSK Update procedure the UICC stores the Key Domain ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

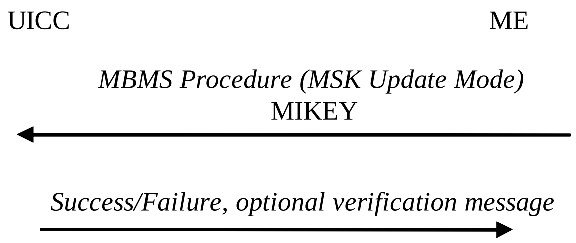


Figure D.1: MSK Update Procedure

In case the MSK update MIKEY message is acceptable (i.e. the received MSK ID corresponds to the last generated MUK in the UE, and the MSK Update procedure has been performed successfully) and the V-bit was set in the HDR, then a MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message) shall be produced. The UICC uses the same MUK ID and TS, which were received from the MSK MIKEY Message (see clause 6.1), for the MSK Verification Message Generation.

D.2 Void

D.3 MTK generation and validation

This procedure is part of the MTK generation and validation function as described in clause 6.5.4 (MTK processing). For details, see TS 31.102 [7].

The ME receives the MIKEY message (containing Header, Time stamp, Key Domain ID, MSK ID, MTK ID = SEQp, an encrypted MTK||Salt (if salt is available) and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in clause 6.5. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

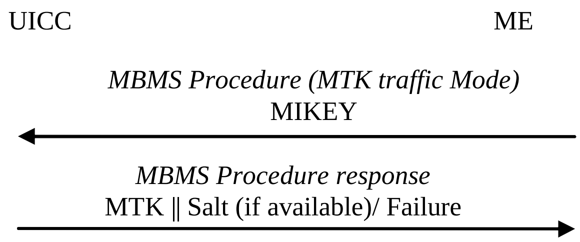


Figure D.3: MTK Generation and Validation

D.4 MSK deletion procedure

This procedure enables the ME to control the deletion of MSKs stored on the UICC as described in clause 6.3.2.1A. For details, see TS 31.102 [7].

The ME sends to the UICC the Key Domain ID and Key Group part of the MSK ID to delete. The UICC deletes all corresponding MSKs.

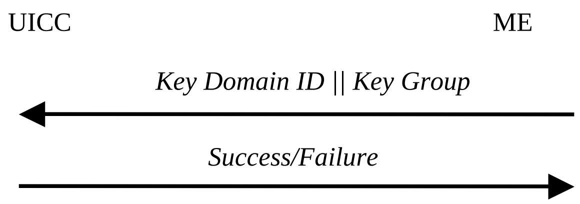
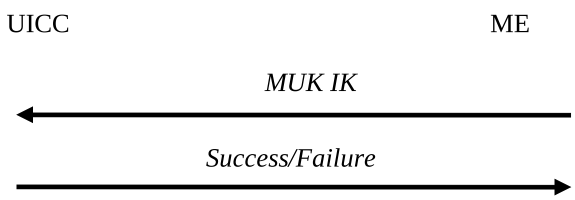


Figure D.4: MSK Deletion

D.5 MUK deletion procedure

This procedure enables the ME to control the deletion of MUKs stored on the UICC. For details, see TS 31.102 [7].

The ME sends the MUK ID to the UICC to delete. The UICC deletes the targeted MUK , the corresponding GBA NAF Key (Ks_int_NAF associated to the same NAF_ID) shall be deleted; the bootstrapped key Ks shall also be deleted if Ks is present and associated to the same B-TID.



.

Figure D.5: MUK Deletion

Annex E (Informative): MIKEY features not used in MBMS

- An MBMS capable ME/UICC and BM-SC do not need to implement the public key encryption method of MIKEY (section 3.2 of RFC 3830 [9]) and related payloads, although mentioned in RFC 3830 [9] as mandatory for implementation.

- An MBMS capable ME/UICC and BM-SC do not need to implement the Time Stamp payload types NTP-UTC and NTP of MIKEY (section 6.6 of RFC 3830 [9]) although mentioned in RFC 3830 [9] as mandatory for implementation.

- An MBMS capable ME/UICC and BM-SC do not need to implement the AES Key Wrap algorithm of MIKEY (section 4.2.3 and 6.2 of RFC 3830 [9]).

Annex F (normative): MRK key derivation for ME based MBMS key management

The MRK shall be derived from the key Ks_NAF or Ks_ext_NAF using the GBA key derivation function (see Annex B of TS 33.220 [6]) as follows (see notation style is explained in Annex B of TS 33.220 [6]):

- FC = 0x01,
- P0 = "mbms-mrk" (i.e. 0x6d 0x62 0x6d 0x73 0x2d 0x6d 0x72 0x6b), and
- L0 = length of P0 is 8 octets (i.e. 0x00 0x08).

The Key to be used in key derivation shall be:

- Ks_NAF or Ks_ext_NAF (i.e. NAF specific key) as specified in TS 33.220 [6].

In summary, the MRK shall be derived from the Ks_NAF or Ks_ext_NAF, and static string "mbms-mrk" as follows:

- MRK = KDF (Ks_NAF, "mbms-mrk") in case of GBA_ME run;
- MRK = KDF (Ks_ext_NAF, "mbms-mrk") in case of GBA_U run.

Annex G (normative): HTTP based key management messages

G.1 Introduction

Clause 6 specifies the HTTP based key management procedures between the BM-SC and the UE. It specifies that the authentication of these procedures is based on GBA and more specifically on the HTTP Digest authentication as described in clause 6.2 of the present document.

G.2 Key management procedures

This clause contains the following HTTP based procedures:

- MBMS User Service Registration;
- MBMS User Service Deregistration;
- MSK request.

G.2.1 MBMS User Service Registration

The UE shall generate a request for MBMS User Service Registration according to clause 6.3.2.1A. The UE shall send the Registration request for one or more MBMS User Services to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Registration request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [19];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net:1234);
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "register", i.e. Request-URI takes the form of "/keymanagement?requesttype= register";
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, i.e. "application/mbms-register+xml". The XML schema of the payload is specified in TS 26.346 [13];
- the HTTP payload shall contain request including a list of one or more userServiceIds of MBMS User Services to which the UE wants to register;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the request for further processing. The BM-SC Key Management function shall verify that the subscriber is authorized to register to the particular MBMS User Service.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code in the HTTP status line shall be 200;
- the HTTP header Content-Type shall be the MIME type of the payload, i.e. "application/mbms-register-response+xml ". The XML schema of the payload is specified in TS 26.346 [13];

- the HTTP payload shall contain a list including one status code for each MBMS User Service.

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

G.2.2 MBMS User Service Deregistration

The UE shall generate a request for MBMS User Service Deregistration according to clause 6.3.2.1B. The UE shall send the Deregistration request for one or more MBMS User Services to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Deregistration request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [19];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net:1234);
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "deregister", i.e. Request-URI takes the form of "keymanagement?requesttype= deregister";
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, i.e. "application/mbms-deregister+xml". The XML schema of the payload is specified in TS 26.346 [13];
- the HTTP payload shall contain the request including a list of one or more userServiceIds of MBMS User Services from which the UE wants to deregister;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the request for further processing.

Upon successful authentication verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code in the HTTP status line shall be 200;
- the HTTP header Content-Type shall be the MIME type of the payload, i.e. "application/mbms-register-response+xml". The XML schema of the payload is specified in TS 26.346 [13];
- the HTTP payload shall contain a list including one status code for each MBMS User Service.

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

G.2.3 MSK request

The UE shall generate a MSK request according to clause 6.3.2.2. The UE shall send the MSK request for one or more MSKs to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e.. MSK request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [19];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net:1234);
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "msk-request", i.e. Request-URI takes the form of "/keymanagement?requesttype= msk-request";
- the UE may add additional URI parameters to the Request-URI;

- the HTTP header Content-Type shall be the MIME type of the payload, i.e.. "application/mbms-msk+xml". The XML schema of the payload is specified in TS 26.346 [13];
- the HTTP payload shall contain a list of one or more Key Domain ID - MSK ID pair(s) of the MSKs that the UE wants to receive;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the MSK request for further processing. The BM-SC Key Management function shall verify that the subscriber is authorized to receive the particular MSKs.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code in the HTTP status line shall be 200;
- the HTTP header Content-Type shall be the MIME type of the payload, i.e.. " application/mbms-msk-response+xml". The XML schema of the payload is specified in TS 26.346 [13];
- the HTTP payload shall contain a list including one status code for each MSK.

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

An example flow of a successful MSK request procedure can be found in Annex H.

G.2.4 Error situations

The key management procedures may not be successful for multiple reasons. The error cases are indicated by using 4xx and 5xx HTTP Status Codes as defined in RFC 2616 [19]. The 4xx status code indicates that the UE seems to have erred, and the 5xx status code indicates that the BM-SC is aware that it has erred. Possible error situations during key management and their mappings to HTTP Status Codes are described in table G.2.4-1. The handling of multiple status codes within one response message is specified in clause 6.3.2.4.

NOTE: In table G.2.4-1, the "Description" column describes the error situation in BM-SC. The "BM-SC error" column describes the typical reason for the error.

Table G.2.4-1: HTTP Status Codes used for key management errors

HTTP Status Code	HTTP Error	UE should repeat the request	Description	BM-SC error
400	Bad Request	No	Request could not be understood	Request was missing, or malformed
401	Unauthorized	Yes	Request requires authentication (cf. clause 6.2)	Authentication pending, (cf. clause 6.2)
402	Payment Required	No	Reserved for future use	-
403	Forbidden	No	BM-SC understood the request, but is refusing to fulfil it	The request was valid, but subscriber is not allowed to register to this particular MBMS User Service or UE requested MSK for a MBMS User Service where it was not registered or request contained unacceptable parameters
404	Not Found	No	BM-SC has not found anything matching the Request-URI	The Request-URI was malformed and BM-SC cannot fulfil the request
405	Method not allowed	No	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.	
406 to 417	*	No	Not used by BM-SC	-
500	Internal Server Error	No	Not used by BM-SC	-
501	Not Implemented	No	BM-SC does not support the requested functionality	The server does not contain particular BM-SC service requested
502	Bad Gateway	No	Not used by BM-SC	-
503	Service Unavailable	Yes	BM-SC service is currently unavailable	BM-SC is temporarily unavailable, UE may repeat the request after delay indicated by "Retry-After" header
504	Gateway Timeout	No	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server	The BM-SC did not get response over Zn interface.
505	HTTP Version Not Supported	No	BM-SC does not support the HTTP protocol version that was used in the request line	UE should use HTTP/1.1 version with BM-SC

Annex H (informative): Signalling flows for MSK procedures

H.1 Scope of signalling flows

This annex gives examples of signalling flows for the key management procedures.

H.2 Signalling flows demonstrating a successful MSK request procedure

H.2.1 Successful MSK request procedure

The signalling flow in figure H.2.1-1 describes the message exchange between UE and BM-SC when UE wants to request MSK.

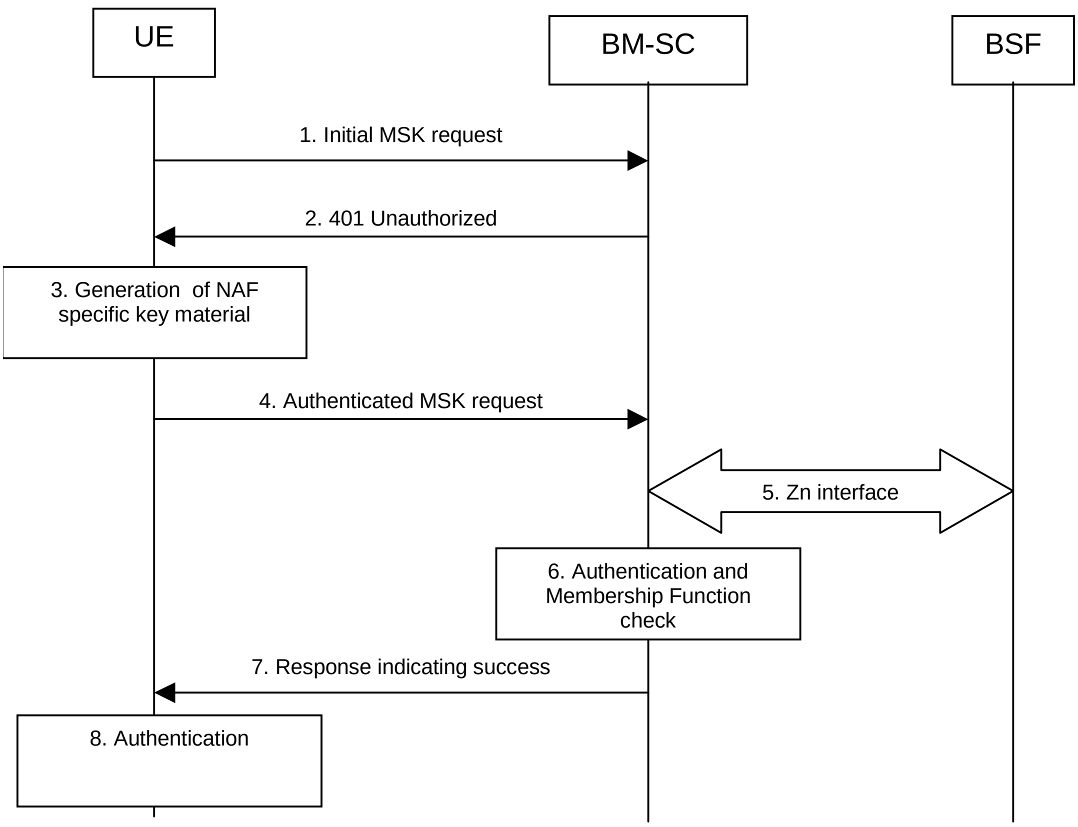


Figure H.2.1-1: Successful MSK request procedure.

1. **Initial MSK request (UE to BM-SC)** - see example in table H.2.1-1

   The UE sends an HTTP request to the BM-SC containing a MSK request.

Table H.2.1-1: MSK request (UE to BM-SC)

```
POST /keymanagement?requesttype=msk-request HTTP/1.1
Host: bmsc.home1.net:1234
Content-Type: application/mbms-msk+xml
Content-Length: (...)
User-Agent: MBMSAgent; Release-6 3gpp-gba
Date: Thu, 08 Jan 2004 10:50:35 GMT
Accept: */*
Referrer: http://bmsc.home1.net:1234/service

<MSK request BLOB>
```

Request-URI: The Request-URI (the URI that follows the method name, "POST", in the first line) indicates the resource of this POST request. The Request-URI contains the parameter "requesttype" which is set to "msk-request" to indicate to the BM-SC the desired request type, i.e. UE requests for one or several MSKs.

Host: Specifies the Internet host and port number of the BM-SC, obtained from the original URI given by referring resource.

Content-Type: Contains the media type "application/mbms-msk+xml", i.e. MSK request.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

User-Agent: Contains information about the user agent originating the request and it shall include the static string "3gpp-gba" to indicate to the application server (i.e. NAF) that the UE supports 3GPP-bootstrapping based authentication.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referrer: Allows the user agent to specify the address (URI) of the resource from which the URI for the BM-SC was obtained.

NOTE 1: This step is used to trigger the GBA-based authentication between the UE and the BM-SC.

2. **401 Unauthorized response (BM-SC to UE)** - see example in table H.2.1-2

   Upon receiving an HTTP request that contains static string "3gpp-gba" in the User-Agent header the BM-SC responds with HTTP response code 401 "Unauthorized" which contains a WWW Authenticate header. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association.

Table H.2.1-2: 401 Unauthorized response (BM-SC to UE)

```
HTTP/1.1 401 Unauthorized
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Date: Thu, 08 Jan 2004 10:50:35 GMT
WWW-Authenticate: Digest realm="3GPP-bootstrapping@bmsc.home1.net",
nonce="6629fae49393a05397450978507c4ef1", algorithm=MD5, qop="auth,auth-int",
opaque="5ccc069c403ebaf9f0171e9517f30e41"
```

Server: Contains information about the software used by the origin server (BM-SC).

Date: Represents the date and time at which the message was originated.

WWW-Authenticate: The BM-SC challenges the user. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association.

The options for the quality of protection (qop) attribute is by default "auth-int" meaning that the payload of the following HTTP requests and responses should be integrity protected.

The realm attribute contains two parts delimited by "@" sign. The first part is a constant string "3GPP-bootstrapping" instructing the UE to use a bootstrapped security association. The second part is the hostname of the server (i.e. FQDN of the BM-SC).

3. **Generation of NAF specific keys at UE**

   The UE verifies that the second part of the realm attribute does correspond to the server it is talking to.

   UE derives the NAF specific key material as specified in TS 33.220 [6]. UE further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

NOTE 2: If UE does not have a bootstrapped security association available, it will obtain one by running bootstrapping procedure over Ub interface.

4. **Authenticated MSK request (UE to BM-SC)** - see example in table H.2.1-3

   UE generates the HTTP request by calculating the Authorization header values using the bootstrapping transaction identifier B-TID it received from the BSF as the username and the MRK (base64 encoded) as the password, and sends the request to BM-SC.

Table H.2.1-3: Authenticated MSK request (UE to BM-SC)

```
POST /keymanagement?requesttype=msk-request HTTP/1.1
Host: bmsc.home1.net:1234
Content-Type: application/mbms-msk+xml
Content-Length: (...)
User-Agent: MBMSAgent; Release-6 3gpp-gba
Date: Thu, 08 Jan 2004 10:50:35 GMT
Accept: */*
Referer: http://bmsc.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@bmsc.home1.net",
nonce="a6332ffd2d234==", uri="/bmsc.home1.net/keymanagement?requesttype=msk-request", qop=auth-
int, nc=00000001, cnonce="6629fae49393a05397450978507c4ef1",
response="6629fae49393a05397450978507c4ef1", opaque="5ccc069c403ebaf9f0171e9517f30e41",
algorithm=MD5

<MSK request BLOB>
```

Authorization: This carries the response to the authentication challenge received in step 2 along with the username, the realm, the nonce, the URI, the qop, the NC, the cnonce, the response, the opaque, and the algorithm.

The qop attribute is set to "auth-int" by default.

NOTE 3: If step 1 was a POST request then this request would also be a POST request and contain the same client payload in the HTTP request as was carried in step 1.

5. **Zn: NAF specific key procedure**

   BM-SC retrieves the NAF specific key material and IMPI of the user. BM-SC further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

   For detailed signalling flows see TS 29.109 [20].

Table H.2.1-4: Bootstrapping authentication information procedure (BM-SC to BSF)

Message source and destination	Zn Information element name	Information Source in GET	Description
NAF to BSF	B-TID	Authorization	The bootstrapping transaction identifier is encoded in the username field according to the Authorization protocol.

6. **Authentication at BM-SC**

   BM-SC verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key MRK. BM-SC calculates the corresponding digest values using MRK, and compares the calculated values with the received values in the Authorization header.

   The BM-SC also verifies that the hostname (i.e. its FQDN) in the realm attribute matches its own.

If the verification succeeds, the incoming client-payload request is taken in for further processing. The BM-SC continues processing of the MSK request according to its internal policies. The BM-SC verifies that the subscriber is allowed to receive the particular MSK(s) indicated in the MSK request.

7. **Response indicating success (BM-SC to UE)** - see example in table H.2.1-5

   The BM-SC sends 200 OK response to the UE to indicate the success of the authentication and the MSK request. The BM-SC generates a HTTP response. The BM-SC can use key MRK derived from NAF key material to integrity protect and authenticate the response.

NOTE 5: The requested MSK keys are not delivered within the MSK request procedure. They are delivered with a separate MIKEY procedure, see clause 6.3.2.3.

Table H.2.1-5: Successful HTTP response (BM-SC to UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Content-Type: application/mbms-msk+xml
Content-Length: (...)
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Thu, 08 Jan 2004 10:50:35 GMT
Expires: Fri, 09 Jan 2004 10:50:36 GMT
<MSK response BLOB>
```

Authentication-Info: This carries the protection.

Expires: Gives the date/time after which the response is considered stale.

8. **Authentication at UE**

   The UE receives the response and verifies the Authentication-Info header. If the verification succeeds, the UE can regard the MSK request procedure as successful.

Annex I (informative): Example of using MSKs and MTKs in MBMS

The following table shows an example of two MBMS User Services, sports Mobile TV channel and news Mobile TV channel. Both of the MBMS User Services include an MBMS User Service Session that downloads a joke per day. The table shows how the MBMS User Services are broken down into RTP sessions (each including the data stream with related RTCP) and FLUTE channels.

The table shows how MSKs and MTKs belonging to different Key Groups are used to protect the RTP sessions and FLUTE channels. It should be noted that the MBMS download session is shared with User Services 1 and 2 so these MBMS User Services need to be able to share MSKs in Key Group C.

Furthermore the table shows how traffic could be carried over MBMS bearers, but this is not a security issue and is only shown here for completeness.

Table I.1: Example of using MSKs and MTKs in MBMS

User Service level	**User Service 1**	Sport channel with joke of the day									
	User Service 2					News channel with joke of the day					
User Service Session level	**User Service Session**	MBMS Streaming Session (Sport)				MBMS Download Session (Joke / day)		MBMS Streaming Session (News)			
	RTP session/ FLUTE channel	streaming audio (RTP session)		streaming video (RTP session)		file object download (FLUTE channel)		streaming audio (RTP session)		streaming video (RTP session)	
Key manage ment level	**Key Domain**	MCC/MNC		MCC/MNC		MCC/MNC		MCC/MNC		MCC/MNC	
	Key Group	Key Group A		Key Group B		Key Group C		Key Group D		Key Group E	
	MSK Note 1	MSK A1 (current)	MSK A2 (next)	MSK B1	MSK B2	MSK C1	MSK C2	MSK D1	MSK D2	MSK E1	MSK E2
	MTK Note 1	MTK ..	MTK ..	MTK …	MTK …	MTK …	MTK …	MTK ..	MTK …	MTK …	MTK …
Transport Service level	**Transport Service**	MBMS Bearer N		MBMS Bearer N+1		MBMS Bearer N+2		MBMS Bearer N+3		MBMS Bearer N+4	
Note 1: This row has a time dimension to illustrate that MSKs and MTKs can be updated.											

Annex J (informative): Mapping the MBMS security requirements into security functions and mechanism

J.1 Consistency check

J.1.1 Requirements on secure service access

Security requirement		Check result
R1a:	A valid USIM or SIM shall be required to access MBMS User Services.	This is provided by GBA. Ks_(ext/int)_NAF generation requires a valid USIM or SIM.
R1b:	It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.	GBA and HTTP digest authentication provide this.
R2a:	It shall be possible for the network (i.e. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.	A user is authenticated during the MBMS user service registration and MSK re-keying.
R2b:	It shall be possible to prevent the use of a particular USIM or SIM to access MBMS User Services.	GAA user security settings provide this.

J.1.2 Requirements on MBMS transport Service signalling protection

Security requirement		Check result
R3a:	It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signalling on the Gmb reference point.	NDS/IP covers this.
R3b:	Unauthorized modification, insertion, replay or deletion of all transport service signalling, 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.	Examples of the attacks could be: - Changing the source address of the content e.g. from indicating company A to company B. - Changing data indicating the type of content from type A to Type B - Changing data indicating type of protection required etc - Appending content to the end of the original content Analysis has shown that there is not any transport service signalling sent over PTM that would need protection.

J.1.3 Requirements on Privacy

Security requirement	Check result
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.	The content provider knows only the BM-SC.
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.	Such identity and control information could be: - The identities of the content providers - Information on which content providers have the most customers - The identities of the content recipients in the case of multicast services to small groups of users Information which could be used to identify specific users is not exposed on the point-to-multipoint channel. However, it may still be possible to identify whether a particular user is subscribed to a particular MBMS service. This could be done by following the physical movement of a particular subscriber and the changes between the use of point-to-point and point-to-multipoint bearers for particular MBMS services in the cells that serve the target subscriber. It is seen unnecessary to protect against this kind of an attack. The only control information exposed on the point-to-multipoint channel is the unprotected fields in the MIKEY MTK transport message. However, revealing this information does not seem to pose a significant security risk.

J.1.4 Requirements on MBMS Key Management

Security requirement	Check result
R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected..	The MSK and MTK update messages are encrypted.
R5b: The transfer of the MBMS keys between the MBMS key generator and the UE shall be integrity protected.	The MSK and MTK deliveries can 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 an MBMS User Service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.	Supported by re-keying functionality.
R5d: Only authorized users that have joined an MBMS User Service shall be able to receive MBMS keys delivered from the MBMS key generator.	MSKs are delivered only to authorized users and the delivery is protected using MUK level keys.

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).	The same CK and IK are not used in GBA and radio level. In addition, Ks_(ext/int)_NAF generation uses a one-way function.
R5f:	All keys used for the MBMS User 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	MUK is identified by the combination of B-TID and NAF-ID without the Ua security protocol identifier, and the MRK is defined by B-TID MSK is uniquely identifiable by its Key Domain ID and MSK ID MTK is uniquely identifiable by its Key Domain ID, MSK ID and MTK ID
R5g:	The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).	The BM-SC knows whether Ks_int_NAF + Ks_ext_NAF or Ks_NAF was generated.
R5h:	The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.	Freshness is checked by MGV-F.

J.1.5 Requirements on integrity protection of MBMS User Service data

Security requirement		**Check result**
R6a:	It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.	This is provided at the application layer using SRTP or OMA DRM DCF.
R6b:	The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.	This is provided at the application layer using SRTP or OMA DRM DCF.
R6c:	It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.	This can be provided by NDS/IP.

J.1.6 Requirements on confidentiality protection of MBMS User Service data

Security requirement		**Check result**
R7a:	It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.	This is provided at the application layer using SRTP or OMA DRM DCF.
R7b:	The MBMS User Service data may be encrypted with common encryption keys, which shall be available to all users that have joined the MBMS User Service	This is provided at the application layer using SRTP or OMA DRM DCF.
R7c:	It may be required to encrypt the MBMS User Service data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.	This can be provided by NDS/IP.
R7d:	It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on protect the MBMS User Service from the BM-SC to the UE.	The BM-SC decides about the security level. There is no security association negotiation between the UE and the BM-SC.
R7e:	It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.	This is provided at the application layer using SRTP or OMA DRM DCF.

J.1.7 Requirements on content provider to BM-SC reference point

Security requirement		Check result
R8a:	The BM-SC shall be able to authenticate and authorize a 3^{rd} party content provider that wishes to transmit data to the BM-SC.	The mechanism to meet the requirement is left to be implemented between the BM-SC and a 3rd party.
R8b:	It shall be possible to integrity and confidentiality protect data sent from a 3^{rd} party content provider to the BM-SC.	The mechanism to meet the requirement is left to be implemented between the BM-SC and a 3rd party.

J.2 Conclusions

Based on the above results of the consistency check between the security requirements and security functions/mechanisms the MBMS security requirements have been adequately met.

Annex K (Informative): SRTP features not used in MBMS

- An MBMS capable ME and BM-SC do not need to implement an SRTP key derivation rate different from zero.

Annex L (Normative): Multicasting MBMS user data on Iub

TS 25.434 [27] specifies the possibility to use IP multicast as defined in RFC 3376 [25] and RFC 3810 [26] for FACH data streams on Iub Interface. In order to protect the transfer of MBMS user plane data multicast between the RNC and NodeBs on the Iub interface over unprotected IP network segments, it is required to use IPsec ESP with shared secrets according to RFC 4303 [28] as profiled by TS 33.210 [14] section 5.3 with integrity protection. The use of confidentiality protection is optional.

NOTE: In case the Iub interfaces are physically protected, the above IPsec based protection is not needed and this is regarded as a closed IP based RAN.

Annex M (informative): Relation to IMS based MBMS user services

Security procedures for IMS based MBMS User Services are specified in TS 26.237 [29].

Annex N (normative): GCSE security aspects

N.0 GCSE architecture and requirements

GCSE architecture is specified in TS 23.468 [33] and based on the requirements specified in TS 22.468 [34].

NOTE 1: The MCPTT AS as specified in 3GPP TS 23.179 [47] is an instantiation of a GCS AS.

NOTE 2: The V2X AS as specified in 3GPP TS 23.285 [48] is an instantiation of a GCS AS.

N.1 GCSE security requirements

N.1.1 General

The security requirements specified in 3GPP TS 22.468 apply.

Note it is assumed that LTE access security mechanisms at the air interface are used.

Note no requirements are given on Rx and SGi, which are generic interfaces and therefore not specified in the scope of GCSE.

N.1.2 GCSE Broadcast Delivery specific security requirements

- Mutual authentication between a node in the security domain, in which the BM-SC resides, and a node in the security domain, in which the GCS AS resides, shall be performed.

NOTE 0: The present document covers only security procedures for deployments where a Diameter message on the MB2-C interface between BM-SC and GCS AS passes through at most one Diameter agent in the security domain, in which the BM-SC resides and at most one Diameter agent in the security domain, in which the GCS AS resides. Other deployments are possible, but they are not recommended for the purposes of the MB2-C interface.

- The signalling messages on MB2-C between the BM-SC and the GCS AS shall be integrity and confidentiality protected.
- The signalling messages on MB2-C between the BM-SC and the GCS AS shall be replay protected.
- The user plane messages on MB2-U between the BM-SC and the GCS AS shall be integrity protected.
- The BM-SC may apply access control on the messages initiated by the GCS AS.
- The GCS AS may apply access control on the messages initiated by the BM-SC.

NOTE 1: MBMS security may or may not be used independent of GCSE.

N.2 Security solution for MB2-C interface

The Diameter mechanisms as specified in IETF RFC 3588 [35] shall apply to MB2-C reference point unless explicitly stated otherwise.

TLS (IETF RFC 5246 [38]) shall be mandatory for implementation on MB2-C. If SCTP is supported then DTLS shall be supported (IETF RFC 6347 [39]). IKE/IPsec (IETF RFC 5996 [40]) is optional for implementation on MB2-C.

NOTE: The use of Diameter in the present specification is based on RFC 3588 [35]. Nevertheless, the security mechanism defined for MB2-C reference point rather aligns with the security mechanism in RFC 6733 [36]. The only difference to the security in RFC 6733 is that the support for DTLS is made conditional on the support of SCTP.

The security profiles for TLS and IKE/IPsec are identical to the ones defined in 3GPP TS 29.368 [37], clause 6.3.3, for the Tsp interface. The security profile of DTLS is defined in 33.310 [31], annex E.

Mutual authentication for the MB2-C interface shall be performed as defined in 3GPP TS 29.368 [37], clause 6.3.2 for the Tsp interface with MTC-IWF and SCS replaced by BM-SC and GCS AS respectively. In particular, the rules for Diameter deployments defined in TS 29.368 [37], clause 6.3.2, shall also apply to the MB2-C interface.

(D)TLS or IKE/IPsec should be used to protect MB2-C.

If the operator does not use the mechanisms described in this clause, then other adequate security measures shall be taken to ensure security on that interface. It is up to the operator, i.e. the owner of the BM-SC, to decide whether the MB2-C interface is trusted or physically protected, or whether it needs protection by a cryptographic protocol as specified above.

N.3 Security solution for MB2-U interface

The assumption is that security in the sense of end-to-end security between UE and UE or UE and GCS AS is supported at application layer. Thus, confidentiality protection of MB2-U is out of scope of 3GPP specifications.

Integrity protection is required in order to mitigate the following DoS attacks: Once ports have been assigned for transferring user data via MB2-U, i.e. by setting up the connection on MB2-C, these ports may be used by an intruder to flood the system and UEs with unwanted messages.

3GPP TS 29.468 [41], Figure 7.1-1 depicts the MB2-U protocol stack, in which user plane data, for instance an IP layer and UDP layer (IETF RFC 768 [42]) are sent over MB2-U interface.

For integrity protection of MB2-U interface, DTLS (IETF RFC 6347 [45]) should be used. IKE/IPsec/ESP (IETF RFC 4303 [46]) may be used. If NATs are present on this interface, UDP encapsulating IKE/IPsec/ESP for negotiation of NAT-Traversal (IETF RFC 3948 [44] and IETF RFCs 3947 [43]) may be used. If the operator does not use the mechanisms described in this clause, then other adequate security measures shall be taken to ensure security on that interface. It is up to the operator, i.e. the owner of the BM-SC, to decide whether the MB2-U interface is trusted or physically protected, or whether it needs protection by a cryptographic protocol as specified above.

Traffic on MB2-U is unidirectional from the GCS AS to the BM-SC, and the BM-SC does not get the user plane address of the GCS AS when the MB2-U connection is established Thereforeit shall be possible for the BM-SC to request GCS AS over MB2-C to establish a security association for the user plane. The security protocol (DTLS or IKE/Ipsec) to be used over MB2-U needs to be configured in the GCS AS, possibly dependent on BM-SC and/or target network. It shall also be possible for the BM-SC to receive a request from GCS AS for the establishment of a security association for the user plane.The target IP address and possible UDP port for this security association can be provided in the MB2-C signalling protected by MB2-C security.

Annex O (normative): Security aspects of xMB reference point between Content Provider and BM-SC

O.1 General

The xMB reference point and related stage 2 protocol procedures are defined in TS 26.346 [13]. The present Annex specifies the security aspects of the xMB reference point.

O.2 Protection of the xMB reference point

The control plane (xMB-C) shall use TLS and the user plane (xMB-U) shall use TLS for TCP-based transport and DTLS for UDP-based transport as is specified in the following:

The profile for TLS and DTLS implementation and usage shall follow the provisions given in TS 33.310 [31], Annex E. Certificate based mutual authentication using TLS or DTLS between a BM-SC and a Content Provider shall be based on certificate profiles in clauses 6.1.3a and 6.1.4a in TS 33.310 [31]. The structure of the PKI used for these certificates is out of scope of the present document, thus the provisions in these clauses on issuers of the certificates do not apply.

After the successful mutual D(TLS) authentication, the BM-SC shall perform authorization checks based on the subject field of the Content Provider certificate. For domain based authorization, the subject field shall identify the domain of the Content Provider and shall be used by the BM-SC for domain level authorization checks. The BM-SC may additionally perform user-based authorization. For an additional user-based authorization, after performing successful domain based authorization, the BM-SC shall authenticate the user using HTTP digest as specified in RFC 2617 [8] and username/password. The username shall identify the user (a human user or a machine) and shall be used by the BM-SC to perform user level authorization checks. The management of the username and password are out of the scope of the present document.

Annex P (informative): Change history

Change history									
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New	WI
2003-11	SP-22					Updated with some editorial modification and presented to the SA plenary for information	0.3.0	1.0.0	
2004-02						Updated to reflect changes agreed at SA3#32	1.0.0	1.1.0	
2004-04						Minor corrections agreed by e-mail discussion	1.1.0	1.1.1	
2004-05						Updated to reflect the decisions taken at SA3#33	1.1.1	1.2.0	
2004-06						Small editorial corrections	1.2.0	1.2.1	
2004-07						Updated to reflect the decisions taken at SA3#34 S3-040470, S3-040469, S3-040553, S3-040535, S3-040489, S3-040565, S3-04573, S3-040620 (update of S3-040582), S3-040676 (update of S3-040497 via S3-040618) and S3-040677 (update of S3-040582 via S3-040619)	1.2.1	1.3.0	
2004-09						Editorial updates after SA3#34 and some changes proposed by joint SA3/SA4 meeting	1.3.0	1.3.1	
2004-09	SP_25	SP-040624				Editorially updated for presentation to TSG SA #25 for approval	1.3.1	2.0.0	
2004-09	-	-	-	-		Updated to v6.0.0 after approval by TSG SA	2.0.0	6.0.0	
2004-12	SP_26	SP-040859	001	4		Deletion of MBMS keys stored in the ME	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	002	-		Clarification on key management	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	005	3		Clean up of MBMS TS	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	006	1		Traffic protection combinations	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	007	3		Clarifying ME and BM-SC capabilities	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	009	1		MBMS MTK Download transport	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	010	3		MBMS Transport of salt	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	011	1		SRTP index synchronisation within ME	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	012	2		Clarify the use of mandatory MIKEY features for MBMS	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	014	-		Protection of the Gmb reference point	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	015	1		Use of parallel MSKs and MTKs	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	016	3		Scope of MBMS security	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	018	4		Clarification of the format of MTK ID and MSK ID	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	020	3		MTK update procedure for streaming services	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	021	8		Clarification of MSK key management	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	022	1		Modification of delivery of MIKEY RAND field in MSK updates	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	023	2		OMA DRM DCF for protection of download services	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	028	1		Shorter MKI	6.0.0	6.1.0	
2004-12	SP_26	SP-040859	033	1		Handling of MBMS identities and definition completion/modification	6.0.0	6.1.0	
2005-03	SP_27	SP-050143	034	2		Handling of MBMS identities and definition completion/modification	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	035	1		ME based MBMS key derivation for ME based MBMS key management	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	037	1		Correct the MSK verification message handling	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	038	2		Clarify MUK key synchronisation for MSK push procedure	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	039	-		Add missing parts of CR33 (SA3#36)	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	042	-		Annex D.1: correction of the description of the GBA run	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	043	1		Alignment according to MIKEY related IETF work	6.1.0	6.2.0	

2005-03	SP_27	SP-050143	044	1		Clarification of HTTP procedures	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	045	1		Usage of security policy payload	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	047	1		Clarification of MSK and MTK procedures	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	049	2		MGV-F functionality related to MTK-ID upper limit	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	051	1		Using the term "MBMS User Service" instead of "multicast"	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	052	1		Introduction of BM-SC subfunctions	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	053	-		Removing IDi from MTK message	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	054	2		MBMS download protection details	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	055	1		Removal of Editors notes	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	056	-		Protection of MBMS Service Announcement sent over MBMS bearer	6.1.0	6.2.0	
2005-03	SP_27	SP-050143	057	-		Introduction of missing abbreviations, symbols and definitions	6.1.0	6.2.0	
2005-06	SP-28	SP-050266	058	1	C	MKI and authentication tag length in User Service Description	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	059	1	C	Clarification of Key domain ID in service announcement	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	060	1	F	Key usage clarification	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	061	1	C	Omitted MTK Update Error Message	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	062	1	D	Editorial corrections to TS 33.246	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	063	1	C	Clarifications on MBMS key management	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	064	1	F	Use of IMPI in MBMS	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	065	-	F	Clarification on CSB ID and SP payload use	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	066	-	F	MIME type adjustments according to LS S3-050192	6.2.0	6.3.0	MBMS
2005-06	SP-28	SP-050266	067	-	F	Results of mapping the MBMS security requirements into security functions and mechanisms	6.2.0	6.3.0	MBMS
2005-09	SP-29	SP-050548	0068	-	F	Clarify FEC handling	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0069	-	F	Clarification to UE handling at reception of service announcement description	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0070	-	F	Back-off parameter binding scope	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0071	-	F	IDs and encoding of MIKEY messages	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0072	-	F	Moving the EXT payload	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0073	-	F	Handling of re-sent MSK messages	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0074	-	F	Clarification of MSK ID in service announcement	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0075	-	F	More than one FQDN for key management	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050559	0076	-	F	NAF Id alignment with TS 33.220	6.3.0	6.4.0	SEC1-SC
2005-09	SP-29	SP-050548	0077	-	F	Key Domain ID in MSK request	6.3.0	6.4.0	MBMS
2005-09	SP-29	SP-050548	0078	-	F	Identifying correct MIME types, correcting various editorials and wrong references	6.3.0	6.4.0	MBMS
2005-12	SP-30	SP-050766	0079	-	F	ROC synchronization	6.4.0	6.5.0	MBMS
2005-12	SP-30	SP-050766	0080	-	F	Correction on MSK processing in case of solicited pull procedure	6.4.0	6.5.0	MBMS
2005-12	SP-30	SP-050766	0081	-	F	Handling several status codes in one response message	6.4.0	6.5.0	MBMS
2005-12	SP-30	SP-050766	0082	-	F	Definition of newer MSK	6.4.0	6.5.0	MBMS

2006-03	SP-31	SP-060048	0083	-	F	Handling unknown MIKEY payloads in MGV-F	6.5.0	6.6.0	MBMS
2006-03	SP-31	SP-060048	0084	-	F	Clarification of MTK ID reset in MSK update	6.5.0	6.6.0	MBMS
2006-06	SP-32	SP-060381	0086	-	F	SIM access to MBMS	6.6.0	7.0.0	MBMS
2006-09	SP-33	SP-060497	0087	-	F	BM-SC chooses MUK lifetime less than corresponding GBA Key lifetime	7.0.0	7.1.0	MBMS
2006-09	SP-33	SP-060490	0089	-	A	Correcting http syntax of key management procedures	7.0.0	7.1.0	MBMS
2006-09	SP-33	SP-060497	0090	-	F	Correction of incorrect description of BM-SC	7.0.0	7.1.0	MBMS
2006-09	SP-33	SP-060497	0091	-	F	Correction of possible key ID values	7.0.0	7.1.0	MBMS
2006-09	SP-33	SP-060497	0092	-	F	Removal of MIKEY internal keys	7.0.0	7.1.0	MBMS
2006-09	SP-33	SP-060491	0094	-	A	Removing TAG and MKI length from Service Announcement	7.0.0	7.1.0	MBMS
2006-09	SP-33	SP-060649	0095	1	B	Addition of a "2G GBA allowed" flag in MBMS user service announcement	7.0.0	7.1.0	MBMS
2006-12	SP-34	SP-060803	0096	-	F	Keys derived from MTK	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060803	0097	-	F	SRTP key derivation rate shall be zero	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060794	0098	1	A	Clarify the use of MBMS User Service Registration/Deregistration for protected MBMS User Services.	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060795	0101	1	A	Correction on the use of key derivation functions	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060898	0103	2	A	Correction of the MIKEY Extension payload coding	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060803	0105	1	F	AES Key Wrap not required for MBMS	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060797	0107	1	A	Correction to the Processing of received messages in the ME	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060798	0109	1	F	Specify the authentication key length of MIKEY	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060803	0111	1	F	Typical MSK and MTK key size	7.1.0	7.2.0	MBMS
2006-12	SP-34	SP-060799	0113	1	A	MTK storage rules on UEs	7.1.0	7.2.0	MBMS
2007-03	SP-35	SP-070148	0116	1	C	Allow the BM-SC to resent MTK messages without TS incrementation	7.2.0	7.3.0	MBMSE
2007-03	SP-35	SP-070148	0117	1	F	Clarification on the use of the constant R	7.2.0	7.3.0	MBMSE
2007-03	SP-35	SP-070148	0118	1	F	Clarification of MSK message structure	7.2.0	7.3.0	MBMSE
2007-03	SP-35	SP-070148	0119	1	F	Clarification of MTK message structure	7.2.0	7.3.0	MBMSE
2007-03	SP-35	SP-070142	0121	1	A	Modification to rules for MSK and MTK management on the UE	7.2.0	7.3.0	MBMS
2007-03	SP-35	SP-070143	0122	1	A	FDT protection	7.2.0	7.3.0	MBMS
2007-06	SP-36	SP-070334	0126	-	A	Mandating the support of MIKEY-RAND length of 128 bit	7.3.0	7.4.0	MBMS
2007-06	SP-36	SP-070334	0128	-	A	Adding missing requirements about PDP context and IP address handling for ptp key management	7.3.0	7.4.0	MBMS
2007-06	SP-36	SP-070334	0130	-	A	Adding a missing interworking scenario	7.3.0	7.4.0	MBMS
2007-06	SP-36	SP-070334	0132	-	A	Fixed cs_id for MIKEY PRF in case of download key derivation	7.3.0	7.4.0	MBMS
2007-06	SP-36	SP-070334	0133	1	F	Correct the SALT key generation during MSK processing	7.3.0	7.4.0	MBMS
2007-06	SP-36	SP-070334	0137	1	A	GBA NAF Key availability in the UICC	7.3.0	7.4.0	MBMS
2007-09	SP-37	SP-070579	0141	1	A	Correct the encoding of MBMS key management procedures	7.4.0	7.5.0	MBMS
2007-09	SP-37	SP-070579	0143	-	A	Correction of DRM Content Format usage	7.4.0	7.5.0	MBMS
2007-12	SP-38	SP-070791	0144	-	F	Usage of TEK and TGK in MBMS	7.5.0	7.6.0	MBMS
2008-03	SP-39	SP-080149	0147	1	F	Clarification of usage of SRTCP in MBMS	7.6.0	8.0.0	MBMS

2008-06	SP-40	SP-080266	0146	2	B	Protection of Iub when multicasting MBMS user data	8.0.0	8.1.0	MBMS
2008-06	SP-40	SP-080266	0148	1	F	Clarification of UE IP address in MBMS	8.0.0	8.1.0	MBMS
2008-06	SP-40	SP-080266	0149	1	F	IP connectivity of the UE in MBMS	8.0.0	8.1.0	MBMS
2008-12	SP-42	SP-080748	0151	1	F	Clarification of MBMS authorization	8.1.0	8.2.0	TEI8
2009-03	SP-43	SP-090139	0150	2	F	Encoding of identities as NAIs	8.2.0	8.3.0	TEI8
2009-06	SP-44	SP-090275	0152	-	F	Add reference to IMS based MBMS TS	8.3.0	8.4.0	TEI8
2009-06	SP-44	SP-090275	0153	-	F	Clarification of Service Protection Description	8.3.0	8.4.0	TEI8
2009-12	SP-46	SP-090860	0154	1		Impacts of EPS to MBMS security	8.4.0	9.0.0	MBMS_EPS
2010-12	SP-50	SP-100715	0155	--	F	Correction of references	9.0.0	10.0.0	TEI10
2012-09	-	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	11.0.0	-
2012-12	SP-58	SP-120858	0164	2	F	Fixing the lack of confidentiality protection for Associated Delivery Procedures	11.0.0	11.1.0	SEC11
2012-12	SP-58	SP-120858	0167	2	A	Support for multiple BM-SCs	11.0.0	11.1.0	SEC11
2012-12	SP-58	SP-120858	0168	1	A	MIKEY-RAND in MTK messages	11.0.0	11.1.0	TEI9
2013-06	SP-60	SP-130251	0171	2	F	Confidentiality Protection of Associated Delivery Procedure Messages	11.1.0	11.2.0	SEC11
2014-06	SP-64	SP-140313	0172	1	B	Add new normative annex on GCSE security	11.2.0	12.0.0	GCSE_LTE
			0173	1	B	Adding references needed for new GCSE security normative annex			
			0174	1	B	Requirements section for normative annex GCSE security			
			0176	1	B	MBMS Delivery requirements for normative annex GCSE security			
			0177	1	B	Solution for MB2-C interface for normative annex GCSE security			
2014-09	SP-65	SP-140589	0178	-	F	Resolving of editor’s note under N.1	12.0.0	12.1.0	GCSE_LTE
			0179	1	B	Integrity protection on MB2-U			
			0180	1	F	Solving editor's note on Diameter security mechanism			
			0181	1	B	GCSE MB2-U interface solution			
			0182	-	D	Clarification of key issue MB2 interface			
			0184	1	F	Solving editor's note on mutual authentication between GCS AS and BM-SC			
2014-12	SP-66	SP-140826	0188	1	F	Clarification to MB2-U solution	12.1.0	12.2.0	
			0187	-	D	Formatting corrections to Annex N	12.2.0	13.0.0	
2015-12	SP-70	SP-150729	0189	1	F	Annex N alignment to 23.179	13.0.0	13.1.0	MCPTT

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2016-12	SA#74	SP-160788	0190	-	F	Including V2X AS as instantiation of GCS AS	14.0.0
2017-06	SA#76	SP-170427	0191	-	B	Security aspects of xMB reference point	14.1.0
2017-09	SA#77	SP-170646	0193	1	F	User-based authorization for xMB	14.2.0
2018-06	-	-	-	-	-	Update to Rel-15 version (MCC)	**15.0.0**
2020-07	-	-	-	-	-	Update to Rel-16 version (MCC)	**16.0.0**
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	**17.0.0**

History

Document history		
V17.0.0	April 2022	Publication