ETSI TS 126 348 V16.3.0 (2020-11)

TECHNICAL SPECIFICATION

LTE;
5G;
Northbound Application Programming Interface (API) for Multimedia Broadcast/Multicast Service (MBMS) at the xMB reference point
(3GPP TS 26.348 version 16.3.0 Release 16)

Reference

DTS/TSGS-0426348vg30

Keywords

5G,LTE

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

Essential patents

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

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

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.

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

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 present document defines a northbound interface between the BM-SC and the content provider. The interface is called xMB. Both external (3rd party) content providers and 3GPP defined API invokers e.g. GCS AS can use the xMB reference point to access BM-SC provided delivery services.

The xMB reference point supports different session types, such as generic file delivery e.g. for MCData, application streaming, including DASH streaming, RTP ingest and ingest for transparent delivery. The xMB reference point supports unicast delivery of content, e.g. for devices outside of the MBMS coverage area.

The xMB reference point is fully integrated into the Common API Framework for 3GPP Northbound APIs (CAPIF).

1 Scope

The present document provides interaction methods and interfaces between a BM-SC and a content provider. The purpose of the document is the definition of enablers for the usage of MBMS delivery.

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 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[3] 3GPP TS 26.234: "Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs".

[4] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2", E. Rescorla, N. Modadugu.

[7] IETF RFC 4918: "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)", L. Dusseault.

[8] IETF RFC 5795: "The Robust Header Compression (ROHC) Framework".

[9] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed".

[10] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[11] IETF Internet-Draft: "JSON Schema: A Media Type for Describing JSON Documents", draft-wright-json-schema-01, April 15, 2017.

[12] 3GPP TS 23.280, "Common functional architecture to support mission critical services; Stage 2".

[13] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[14] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 reference point; Stage 3".

[15] IETF RFC 5234 (January 2008): "Augmented BNF for Syntax Specifications: ABNF", D. Crocker and P. Overell.

[16] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

ARP	Allocation and Retention Priority
BM-SC	Broadcast-Multicast - Service Centre
DASH	Dynamic Adaptive Streaming over HTTP
DTLS	Datagram Transport Layer Security
FEC	Forward Error Correction
GBR	Guaranteed Bitrate
HLS	HTTP Live Streaming
MPD	Media Presentation Description
QCI	QOS Class Identifier
QOS	Quality of Service
QOE	Quality of Experience
ROM	Receive Only Mode
RTSP	Real-Time Streaming Protocol
RTP	Real Time Transport Protocol
RTCP	Real Time Transport Control Protocol
SACH	Service Announcement Channel
SAI	Service Area Identity
SCEF	Service Capability Exposure Function
SDP	Session Description protocol
TLS	Transport Layer Security
TV	Television
UE	User Equipment
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

4 Architecture

4.1 General

As shown in Figure 4.1-1, the reference point between Content Provider and BM-SC is called the xMB interface. Using the xMB reference point, content provider can invoke procedures supported by BM-SC(s) to setup and manage MBMS user service from BM-SC to the MBMS clients. BM-SC defines an endpoint with all supported procedures on the xMB interface, which can then be converted to SGmb procedures for the interface between BM-SC and MBMS GW (not depicted).

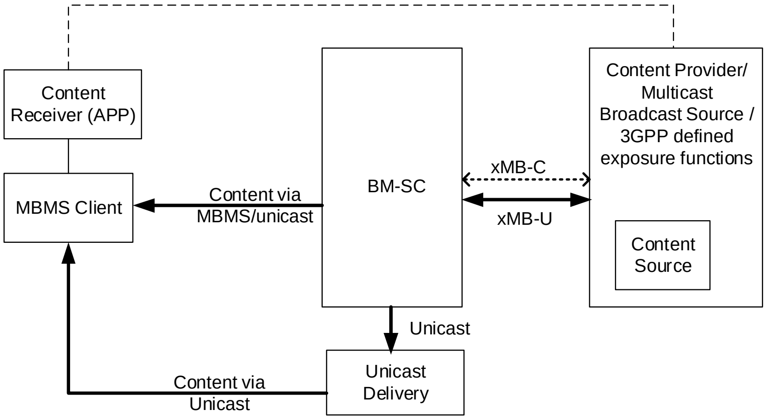


Figure 4.1-1: The xMB reference model

The BM-SC may forward the received content for unicast delivery for appropriate functions (e.g., MBMS user service fallback).

The control plane (xMB-C) and the user plane (xMB-U) may be optionally terminated by 3GPP defined enabler / exposure functions such as an SCEF, which exposes the same or a different interface to content providers. The exposed API such as by SCEF is not specified in the present document.

The content provider may optionally exchange application level information like service metadata (e.g. serviceIds or URL(s) of USD(s) or other service identifier(s)) directly with the application.

The BM-SC may support CAPIF [10]. When CAPIF is supported, then:

- the BM-SC shall support the CAPIF API provider domain functions (i.e. CAPIF-2/2e (xMB), CAPIF-3, CAPIF-4 and CAPIF-5 as specified in TS 23.222 [10]);
- the BM-SC xMB authentication and authorization functions (as defined in Clause 5.2) are replaced by CAPIF equivalent core domain functions (i.e. CAPIF-1/1e).

The CAPIF and associated API provider domain functions are specified in TS 23.222 [10].

The content provider may be a mission critical service provider ([12]), which is arranging MC Services to Mission Critical Organizations. Providing MC Services may require additional control of the resource allocation (QoS, coverage area). For this purpose, the interface can be extended with the xMB mission critical extension. The xMB mission critical extension consists in:

- additional properties within the control plane procedures (Table 5.4-6),
- specific semantic and syntax for the geographical area (Clause 5.4.7).

4.2 xMB reference point

The xMB reference point exists between the content provider and the BM-SC directly or via 3GPP defined enabler / exposure functions such as SCEF. When the BM-SC connects to content provider via a 3GPP defined enabler / exposure function, the xMB-C interface (and optionally also the xMB-U) is terminated at the 3GPP defined enabler / exposure function.

The xMB reference point provides the ability for the content provider to:

- authenticate and authorize BM-SC(s).
- create, modify and terminate a service.
- create, modify and terminate a session.
- query information.
- deliver content to the BM-SC(s)

The xMB reference point provides the ability for the BM-SC to:

- authenticate and authorize a content provider.
- notify the content provider of the status of an MBMS user service usage.
- retrieve content from the content provider.

The xMB reference point shall support security function for confidentiality protection of both control plane (xMB-C) and user plane (xMB-U).

5 Procedure

5.1 General

The xMB reference point defines procedures between a BM-SC and a content provider. The content provider may be external (i.e. 3rd party provider) or 3GPP defined API invokers.

The following procedures are available:

- Authentication and Authorization

NOTE: When CAPIF is used, the CAPIF 1 / CAPIF 1e procedures are used.

- Service Management Procedures
- Session Management Procedures

By default the BM-SC announces all the services including the different eMBMS parameters to MBMS Clients so that MBMS Clients can activate reception of the announced MBMS services. It is also possible that the Content Provider /API invoker is doing the service announcement by itself.

A set of different session types are supported, namely:

- Streaming: the BM-SC may use the MBMS Streaming delivery method for content distribution to MBMS Clients
- Files: the BM-SC may use the MBMS Download delivery method for content distribution to MBMS Clients
- Application: the BM-SC may use the MBMS Download delivery method for content distribution to MBMS Clients.

NOTE: This ession type contains DASH and HLS streaming over MBMS

- Transport-Mode: the BM-SC is transparent to the stream and passed data via MBMS bearers to UEs.

5.2 Authentication and Authorization

5.2.1 Introduction

The content provider and the BM-SC shall follow the procedures in this clause for authentication and authorization over the xMB.

When the content provider (API invoker) uses CAPIF to discover the BM-SC (xMB provider) and to interact with the BM-SC, then the xMB security procedures (as defined in this clauses) are replaced by CAPIF-1 / CAPIF-1e [10] security procedures.

Before provisioning of services at the BM-SC, the content provider has to be authenticated and authorized to perform service management functions using xMB. If the content provider wants to modify or remove the provisioned services, it can do so by using a valid access token.

The content provider may have multiple and different end-points for xMB-C and xMB-U. Each connection may have different entitlements based on the roles assigned to the requesting connecting party.

While authentication is performed based on standard (D)TLS connection and certificate exchange, authorization is performed using either the "domain-based" or "user-based" mode as described in clause 5.2.3.

In the user-based mode, fine-grained authorization shall be performed prior to any transaction to allow the BM-SC to check the access rights of the content provider user (either a human or a machine). Such authorization procedure, if successful, shall result in the creation of an "access token" that the server will return to the content provider for subsequent requests made on the xMB interface.

In the domain-based mode, additional authorization steps shall not be performed. Users within a content provider domain are not further separated.

5.2.2 Authentication Procedure

The authentication procedure is used by the content provider and the BM-SC to authenticate each other. The content provider shall be authenticated with the BM-SC when the content provider wants to provision new services or manage existing services. Similarly, the BM-SC shall be authenticated by the content provider when the BM-SC needs to send reports and notifications to the content provider. Authentication is also required for all user plane procedures.

Figure 5.2-1 shows the authentication procedure used between the content provider and the BM-SC.

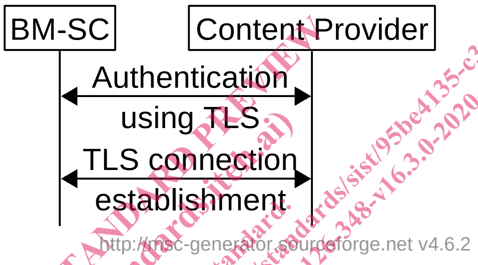

BM-SC
Content Provider
Authentication using TLS
TLS connection establishment
http://msc-generator.sourceforge.net v4.6.2

Figure 5.2-1: Authentication Procedure

1. The content provider and the BM-SC authenticate each other for performing service management and status reporting and notification respectively. During this authentication step, the content provider and BM-SC exchange their X.509 certificates using TLS as defined in TS 33.310 [5] and independently verify the validity of each other's certificate.

2. The TLS connection is established.

5.2.3 Authorization Procedure

Before using any of the MBMS xMB procedure, the Content Provider shall first use the following authorization procedure the retrieve its authorization. After successful authorization based on the content provider's representative's credentials, operations such as service and session creation within the granted permissions become possible.

In this version of the specification, the BM-SC shall support at least one of the two following modes of authorization: *domain-based* or *user-based*.

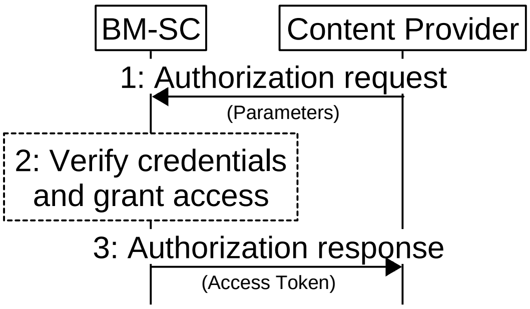
Upon a successful authentication procedure, the absence of an access token provided to the content provider in response to an authorization request is an indication that the BM-SC only supports domain-based authorization, based on the previously-established (D)TLS connection between the Content Provider server and the BM-SC. This means that the same access rights to service or session resource requests across the xMB interface will be granted at the level of the business entity represented by the sender, independent of the end-user representative of that entity or administrative domain submitting the request. This requires the network operator to have already created and provided a unique certificate for storage by the BM-SC. If the certificate of the content provider is not contained in the BM-SC, then the authorization procedure shall fail.

Presence of an access token in the authorization response is an indication that the BM-SC supports user-based authorization, i.e., fine-grained authorization at the end-user representative level, of xMB resource requests. In this case, the content provider representative shall include this access token in each subsequent resource request made on xMB.

NOTE 1: It is up to the BM-SC to decide whether it supports domain-based or user-based authorization.

NOTE 2: In Figure 5-3 and subsequent clauses on Service Management and Session Management procedures and the associated message sequence diagrams, it is assumed that user-based authorization is supported by the BM-SC.

Figure 5.2-2 shows the procedure for content provider authorization by the BM-SC.



http://msc-generator.sourceforge.net v4.6.2

Figure 5.2-2: Authorization Procedure

1) If the content provider's representative is not in possession of a valid access token, it shall connect to the BM-SC using the authenticated TLS connection and perform the authorization procedure to retrieve the access token.

2) The BM-SC checks the credentials of the content provider and upon successful verification it will generate an access token that will be returned to the content provider. The link between the access token and the entitlement is outside of the scope of the specification.

3) The content provider may then use the access token on subsequent calls to the xMB interface.

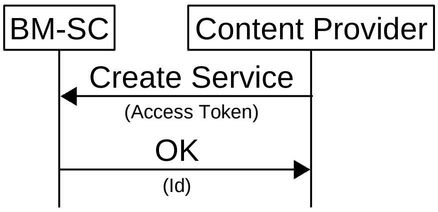
5.3 Service Management Procedures

5.3.1 Introduction

The service management procedures allow the content provider to create, modify and delete services on the BM-SC. Each service may contain multiple sequential sessions.

5.3.2 Create Service

The procedure allows a content provider to create a new the service. Service configuration and service sessions are added in subsequent procedures.



http://msc-generator.sourceforge.net v4.6.2

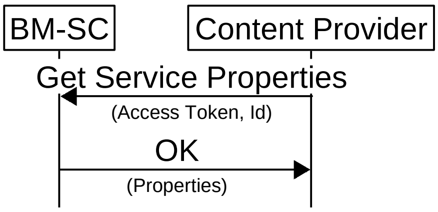
Figure 5.3-1: Service Creation

1. The service is created. The content provider provides a valid access token.

2. On successful creation, the BM-SC responds with the resource id of the service. Service properties are fetched and modified with subsequent transactions.

5.3.3 Get Service Properties

The procedure allows a content provider to fetch the current configuration of the service.



http://msc-generator.sourceforge.net v4.6.2

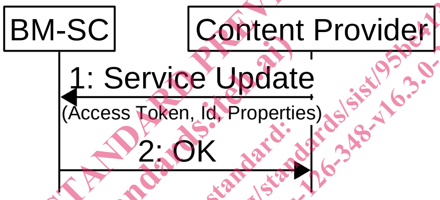
Figure 5.3-2: Get current service properties

1. The content provider sends along with the service property request, the access token and the resource id of the service.

2. The BM-SC provides the service properties in response.

5.3.4 Update Service Properties

The procedure allows a content provider to update the current configuration of the service.



http://msc-generator.sourceforge.net v4.6.2

Figure 5.3-3: Service Update

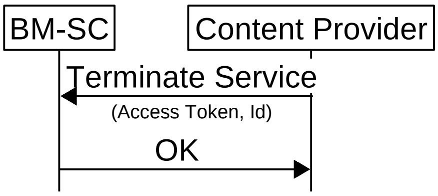
The content provider may first fetch the current service configuration using the Get Service Configuration procedure.

1. The content provider modifies the properties of the service resource. The procedure may allow modification of individual properties or all properties.

2. The content provider updates the resource identified by the id of the service.

5.3.5 Terminate a Service

The content provider may terminate a service. All sessions, including those which are being created or are already active will be deleted automatically with the termination of the service.



http://msc-generator.sourceforge.net v4.6.2

Figure 5.3-4: Service Termination

1. The content provider sends the service termination command. The access token and the resource id of the service is provided as input.

2. The BM-SC terminates the service and deletes all associated sessions, and acknowledges the reception of this request.