ETSI TS 129 116 V14.0.0 (2017-04)

TECHNICAL SPECIFICATION

LTE;
Representational state transfer over xMB reference point between content provider and BM-SC
(3GPP TS 29.116 version 14.0.0 Release 14)

Reference

DTS/TSGC-0329116ve00

Keywords

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Foreword

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

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

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**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.

1 Scope

The present document describes the REST-based protocol for the xMB reference point between the Content Provider and the BM-SC. The xMB reference point and related stage 2 protocol procedures are defined in 3GPP TS 23.246 [2] and in 3GPP TS 26.346 [3].

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 23.246: "Multimedia Broadcast/Multicast Service (MBMS) Architecture and Functional Description".

[3] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and Codecs".

[4] IETF RFC 5246 (August 2008): "The Transport Layer Security (TLS) Protocol", T. Dierks, E. Rescorla.

[5] IETF RFC 6749 (October 2012): "The OAuth 2.0 Authorization Framework", D. Hardt, Ed.

[6] IETF RFC 7231 (June 2014): "Hypertext transfer protocol (HTTP/1.1): Semantics and Content", R. Fielding and J. Reschke, Ed.

[7] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[8] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication"

[9] IETF RFC 4918, "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)".

[10] 3GPP TS 26.234, "Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs".

[11] IETF RFC 3711, "The Secure Real-time Transport Protocol (SRTP)".

[12] IETF RFC 4347, "Datagram Transport Layer Security".

[13] IETF RFC 2818, "HTTP over TLS".

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

[15] IETF RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

[16] IETF RFC 6749, "The OAuth 2.0 Authorization Framework".

[17] IETF RFC 7235, "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[18] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[19] IETF RFC 3926: "FLUTE - File Delivery over Unidirectional Transport".

[20] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[21] 3GPP TS 26.347: "MBMS URLs and APIs".

3 Definitions, symbols 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].

Content Provider: Entity/Entities which supplies/supply content in the form of streaming media or non-real-time (NRT) files to be delivered to UEs over the 3GPP network, via MBMS Bearer and/or unicast bearer services. Also referred to in this document as the Multicast Broadcast Source. The Content Provider may reside either inside or outside the operator's network.

Service: One of the resource types exposed by the RESTful xMB API and operated on by a Content Provider using HTTP methods. It corresponds to a Content Provider’s service offering for delivery over the MBMS network to UEs. Each service instance created over the xMB API maps to an MBMS User Service as specified by 3GPP TS 26.346 [3]. The delivery of the contents of a created service is performed during one or more sessions associated with that service.

Session: One of the resource types exposed by the RESTful xMB API and operated on by a Content Provider using HTTP methods. It represents one or more time intervals during which the MBMS Bearer is active for the transmission of service contents from the BM-SC to the UE. Each session instance, besides the activity times, may contain various properties pertaining to transport, media and application level information (session type, session state, data rate, permitted delay, user plane ingestion mode, targeted delivery area, reporting parameters, identification of content components delivered during the session, etc.).

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].

API	Application Programming Interface
BM-SC	Broadcast Multicast Service Center
CDN	Content Delivery Network
CP	Content Provider
DASH	Dynamic Adaptive Streaming over HTTP
FER	Forward Error Correction
FLUTE	File Delivery over Unidirectional Transport
HTTP	HyperText Transfer Protocol
IS	Initialization Segment
JSON	JavaScript Object Notation
MPD	Media Presentation Description
MSA	MBMS Service Area
REST	Representational State Transfer
SACH	Service Announcement Channel
SAF	Service Announcement Function
SLA	Service Level Agreement
TLS	Transport Layer Security
TMGI	Temporarily Mobile Group Identity
TSI	Transport Session Identifier
URI	Universal Resource Identifier
WebDAV	Web Distributed Authoring and Versioning

4 xMB reference point

4.1 Overview

4.2 Reference model

The xMB reference point resides between the BM-SC and the Content Provider as depicted in Figure 4.2.1. Control- and user-plane procedures are operated over the xMB-C and xMB-U reference points, respectively. The overall xMB reference model is depicted in subclause 5.4A of 3GPP TS 26.346 [3].

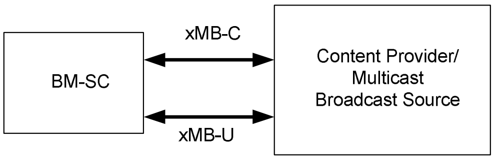

Figure 4.2.1 xMB reference point

4.3 Functional elements

4.3.1 BM-SC

The complete functionality of the BM-SC is defined in 3GPP TS 26.346 [3]. In the context of the xMB reference point, the BM-SC represents the peer endpoint to the Content Provider in supporting all procedures on the xMB interface.

4.3.2 Content Provider / Multicast Broadcast Source

The functional role of the Content Provider is defined in subclause 4.4.1a of 3GPP TS 26.346 [3]. Using the xMB reference point, a Content Provider/Multicast Broadcast Source may provide media, as well as service descriptions and control data, to the BM-SC to set up and manage MBMS User Service(s) from the BM-SC to MBMS clients (the latter is not depicted in Figure 4.2.1).

4.4 Procedures over xMB reference point

4.4.1 Introduction

All procedures that operate across the xMB reference point, as specified in subclause 5.4A of 3GPP TS 26.346 [3], are summarized in the following subclauses.

4.4.2 Authentication Procedures

Authentication procedures shall be performed via TLS as specified by 3GPP TS 33.210 [7] and IETF RFC 5246 [4]. The Content Provider shall act as the TLS client and the BM-SC as the TLS server when the Content Provider wants to provision new services or manage existing services. Similarly, the BM-SC shall act as the client when the BM-SC wishes to send reports and notifications to the Content Provider. All of the following procedures require the authentication procedure to be completed successfully.

4.4.3 Authorization Procedures

The authorization procedure shall be done using OAuth as specified by IETF RFC 5246 [4]. The TLS client shall act as the OAuth client and BM-SC shall act as the server. All following procedures shall use the Access Token provided by the BM-SC during authorization. Any unauthorized procedure in the following shall be responded with a corresponding error code.

Editor's Note: BM-SC Authorization is FFS pending feedback from SA3 and SA4.

4.4.4 Service Management Procedures

4.4.4.1 Create Service

This procedure is used by the Content Provider to create a service at the BM-SC. The Content Provider shall use HTTP POST for this purpose. A successfully created service is associated with a resource identifier which is used by the Content Provider to discover, update and delete the service.

4.4.4.2 Get Service Properties

This procedure is used by the Content Provider to obtain the service properties from the BM-SC. The Content Provider shall use HTTP GET for this purpose.

4.4.4.3 Update Service Properties

This procedure is used by the Content Provider for updating the service properties at the BM-SC. The Content Provider shall use HTTP PUT or HTTP PATCH, corresponding to complete or partial update of service properties, respectively, for this purpose.

4.4.4.4 Delete Service

This procedure is used by the Content Provider to terminate the service at the BM-SC. The Content Provider shall use HTTP DELETE for this purpose.

4.4.4.5 Service Notifications

This procedure is used by the BM-SC to send service related notifications to the Content Provider.

4.4.5 Session Management Procedures

4.4.5.1 Create Session

This procedure is used by the Content Provider to create a session for a previously created service at the BM-SC. The Content Provider shall use HTTP POST for this purpose. A successfully created session is associated with a resource identifier which is used by the Content Provider to discover, update and delete the session.

4.4.5.2 Get Session Properties

This procedure is used by the Content Provider to obtain the session properties of a service from the BM-SC. The Content Provider shall use HTTP GET for this purpose.

4.4.5.3 Update Session Properties

This procedure is used by the Content Provider for updating the session properties of a session at the BM-SC. The Content Provider shall use HTTP PUT or HTTP PATCH, corresponding to complete or partial update of session properties, respectively, for this purpose.

4.4.5.4 Delete Session

This procedure is used by the Content Provider to terminate a session of a service at the BM-SC. The Content Provider shall use HTTP DELETE for this purpose.

5 xMB API

5.1 Overview

The xMB API is a RESTful API that allows Content Providers to provision broadcast services over 3GPP networks and to ingest their content for distribution using eMBMS. The xMB API defines a set of resources and the related procedures for the creation and management of broadcast services and sessions in section 5.2. The corresponding JSON schema for the representation of the resources and operations defined by the xMB API is provided in its complete form in Annex B.

5.1.1 Supported Methods

The xMB API follows the RESTful design principles. All operations SHALL be performed using HTTP 1.1 (IETF RFC 7231 [6]) over TLS (IETF RFC 5246 [14]).

The following table gives a summary of the supported HTTP methods and their applicability on a per resource basis

Table 5.1.1-1

HTTP Method	CRUD	Resource	PATH
POST	Create	Service	/xmb/v1.0/services
		Session	/xmb/v1.0/services/{service-res-id}/sessions
GET	Read	Service	/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
		Session	/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
		Report	/xmb/v1.0/reports?query or /xmb/v1.0/reports/{report-res-id}
		Notification	/xmb/v1.0/notifications?query or /xmb/v1.0/notifications/{notification-res-id}
PUT	Replace	Service	/xmb/v1.0/services/{service-res-id}
		Session	/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
PATCH	Modify	Service	/xmb/v1.0/services/{service-res-id}
		Session	/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
DELETE	Delete	Service	/xmb/v1.0/services/{service-res-id}
		Session	/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}

5.1.2 Error Handling

The xMB API shall use the HTTP status codes to indicate any errors that might occur in the processing of operations on xMB resources. Unless defined otherwise, the HTTP status codes shall be interpreted as specified in IETF RFC 7231 [6]. API operations that are not successfully handled shall not leave the resource at an undefined state. The response should provide sufficient information for a human operator to understand and locate the error.

API operations that do not follow the security procedures defined in section 7 shall be rejected without any impact on the resources.

Errors may also happen during the content ingestion and shall be notified to the Content Provider in a timely manner depending on the severity of the error.

5.1.3 xMB Entry Point Discovery

The Content Provider may be provided with the URL that serves as the entry point for the xMB-C interface, it may discover it through the SCEF, or it may automatically build it as follows:

http://mbmsbs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org/xmb/v1.0/

5.2 Resources

5.2.1 Services

The Content Provider shall configure services at the BM-SC using the REST API methods over two resources managed at the BM-SC.

Table 5.2.1-1 summarizes different resources for provisioning and managing services at the BM-SC.

Table 5.2.1-1: Resources for managing services at BM-SC

Resource Name	Resource Type	Description
service	Instance resource	Represents a single service resource. The Content Provider can provision or modify a single service at the BM-SC by invoking REST API requests to this service resource at the BM-SC.
services	Collection Resource	Represents a collection of service resources.

5.2.1.1 Properties

Each service resource described in Table 5.2.1-1 has the set of properties described in Table 5.2.1.1-1. The Content Provider shall modify one or more of the properties of the service resource using the API operations described in subclause 5.2.1.2.

Table 5.2.1.1-1 summarizes different service properties of a service resource.

Table 5.2.1.1-1: Properties of service resource

Property Token	JSON Value Type	Defaults			Property Description
		Child Paramete r	Units	Values	
service-id	string		None	N/A	Identifies the MBMS User Service as defined in Clause 11.2.1.1 of 3GPP TS 26.346 [3]
service-class	string		None	(operator defined default)	The service class that service belongs to. (see *serviceClass* element in Clause 11.2.1.2 of 3GPP TS 26.346 [3]).

service-languages	array		None	Empty list	List of language of the service content. (see *serviceLanguage* element in Clause 11.2.1.1 of 3GPP TS 26.346 [3]).
service-names	array		None	Empty list	List of Service Names. (see *name* element in Clause 11.2.1.1 of 3GPP TS 26.346 [3])
service-announcement-mode	string		None	SACH	Enumeration of Service Announcement Mode. Additional service announcement modes may be added in future. - "SACH": BM-SC performs the Service Announcement for the current service using the SACH channel (cf. Annext L.2, L3 of 3GPP TS 26.346 [3]). - "CP": BM-SC provides the necessary service access information used by the Content Provider to create the service announcement information.
consumption-reporting-configuration	object	Enabled	Boolean	False	The Content Provider wishes to collect consumption reports for the service. Enabled: Flag to indicate enabling of consumption-reporting Reporting interval: The interval for which the BM-SC has to aggregate the statistics for Sample percentage: Percentage of users to collect reports from
		Reporting interval	Integer	3600 (in seconds)	
		Sample percentage	Integer	10 (in %)	
push-notification-url	string		None	“”	The Content Provider provides Notification URL over which it will receive notifications "pushed" by the BM-SC. The Notification procedure is described in Clause 5.4A.3. of 3GPP TS 26.346 [3]

push-notification-configuration	string		None	All	If the Content Provider enables push delivery of notifications, then the Content Provider may provide notification filters This parameter contains a comma separated list of Classes it wishes to receive among the following options: **Critical**, **Warning**, **Information**, **Service**, **Session**, or **All** to get all types of notification. The notification message shall be sent immediately to the Content Provider upon becoming available

The service instance resource with the properties defined above can be shown using the following JSON schema:

```
"service": {
        "type": "object",
        "description": "Service Description",
        "properties": {
                        "service-id": {
                                "type": "string",
                                "description": "Refer to Table 5.2.1.1-1 for detailed description"
                         },
                        "service-class": {
                                 "description": "Service class",
                                 "type": "string"
                         },
                        "service-languages": {
                                "type": "array",
                                "description": "List of service languages",
                                 "items" : {
                                        type" : "string"
                                }
                         },
                        "service-names": {
                                "type": "array",
                                "description": "List of service names",
                                 "items" : {
                                        "type" : "string"
                                }
```

```
                },
                "service-announcement-mode": {
                        "description": "Refer to Table 5.2.1.1-1 for detailed description",
                        "type": "string"
                },
                "consumption-reporting-configuration": {
                        "type": "object",
                        "description": "Refer to Table 5.2.1.1-1 for detailed description",
                         "properties": {
                                    "reporting-interval": {
                                            "type": "number",
                                            "description": "The interval for which the BM-SC has to aggregate the
                                            statistics for"
                                    },
                                    "sample-percentage": {
                                            "type": "number",
                                            "description": "Percentage of users to collect reports from"
                                    },
                                    "start-time": {
                                            "type": "string",
                                            "description": "Start time of consumption report collection"
                                    },
                                    "end-time": {
                                            "type": "string",
                                            "description": "End time of consumption report collection"
                                    }
                        }
                },
            "push-notification-url" : {
            "type" : "string",
            "description" : "The Content Provider supplied Notification URL over which it will receive
notifications “pushed” by the BM-SC. The Notification procedure is described in Clause 5.4A.4.6."
           },
           "push-notification-configuration" : {
            "type" : "string",
        "description" : "If the Content Provider enables push delivery of notifications, then the Content Provider may provide notification filters. This parameter contains a comma separated list of Classes it wishes to receive among the following options: Critical, Warning, Information, Service, Session, or All to get all types of notification. The notification message shall be sent immediately to the Content Provider upon becoming available."
      }
    }
  },
```

5.2.1.2 API Operations

5.2.1.2.1 Introduction

Services can be created, updated, or deleted at the BM-SC by the Content Provider, or the properties of a previously created service at the BM-SC may be obtained by the Content Provider, by invoking HTTP methods on the "service" instance resource or the “services” collection resource. In all HTTP requests, the message body shall contain an Access Token as authorization parameter for the associated method.

5.2.1.2.2 Service Creation

POST /xmb/v1.0/services

To create a service, the Content Provider shall use the HTTP POST method on the "services" collection resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services".
- the Host field is set to the address of the BM-SC

The content body of the POST request shall be empty. Upon receipt of the HTTP POST request from the Content Provider to create a service, the BM-SC will check whether the Content Provider is authenticated and authorized to create services as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.1.2.2-1. If the authorization is successful, the BM-SC create a service with default service property values as described in subclause 5.2.1.1. Upon successful creation of a service, the BM-SC shall respond to the Content Provider with a 201 message indicating that the service is successfully created along with the service resource identifier of the service resource. The service resource identifier is the identifier that uniquely identifies the service. When the Content Provider receives the service resource identifier, it shall use this identifier in subsequent requests to the BM-SC to refer to this service. Alternatively, if the creation of service failed, the BM-SC shall send a 403 message.

The possible response messages from the BM-SC, depending on whether the POST request is successful or unsuccessful, are shown in Table 5.2.1.2.2-1.

Table 5.2.1.2.2-1: Response status code, message, and contents for service creation

Status Code	Message	Contents
201 Created	Service created successfully	The BM-SC shall send the service resource identifier of the created service.
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.1.2.3 Service Modification

5.2.1.2.3.1 Partial Modification of Service Properties

PATCH /xmb/v1.0/services/{service-res-id}

Assuming that a service has been created using the service creation method described in subclause 5.2.1.2.2, partial updating of its properties can be performed by the Content Provider using the HTTP PATCH method on the "service" instance resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services/{service-res-id}"
- the Host field is set to the address of the BM-SC
- the Content-Type header field is set to "application/json"
- the body of the message is encoded in JSON format

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

The content body of the service modification request shall contain updated partial representation of the service resource. The representation of the service is based on the JSON schema of the service resource as described in subclause 5.2.1.1. Further, one or more properties of the service listed in Table 5.2.1.1-1, with the exception of the properties service-id and pull-notification-url, can be updated. The value of the properties service-id and pull-notification-url cannot be modified.

Upon receipt of the HTTP PATCH request from the Content Provider to update a service, the BM-SC will check whether the Content Provider is authenticated and authorized to update services as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message. If the authorization is successful, the BM-SC update the requested service. Upon successful updating of the requested service, the BM-SC shall respond to the Content Provider with a 200 OK message indicating that the service is successfully updated along with the service resource identifier of the service. If the service was not found, the BM-SC shall send a 404 Not Found message. If the service cannot be updated, the BM-SC shall send a 403 Forbidden message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the PATCH request is successful or unsuccessful, are shown in Table 5.2.1.2.3.1-1.

Table 5.2.1.2.3.1-1: Response status code, message, and contents for service modification using HTTP PATCH

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier of the service that is modified
204 No Content	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.1.2.3.2 Full Modification of Service Properties

PUT /xmb/v1.0/services/{service-res-id}

Assuming that a service has been created using the service creation method described in sub clause 5.2.1.2.2, full modification of its properties can be performed by the Content Provider using the HTTP PUT method on the "service" instance resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services/{service-res-id}".
- the Host field is set to the address of the BM-SC

- the Content-Type header field is set to "application/json"
- the body of the message is encoded in JSON format

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

The content body of the service update request shall contain updated representation of the service resource. The representation of the service is based on the JSON schema of the service resource as described in subclause 5.2.1.1. Further, when HTTP PUT method is used for updating the service, the Content Provider shall specify the updated values of all the service properties, with the exception of the properties service-id and pull-notification-url, in the updated representation. The value of the properties service-id and pull-notification-url cannot be modified.

Upon receipt of the HTTP PUT request from the Content Provider to update a service, the BM-SC will check whether the Content Provider is authenticated and authorized to update services as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.1.2.3.2-1. If the authorization is successful, the BM-SC update the requested service. While updating the service representation, the BM-SC shall overwrite the values of all properties of the service being updated with the values provided in the update request. Upon successful update of the requested service, the BM-SC shall respond to the Content Provider with a 200 OK success message indicating that the service is successfully updated along with the service resource identifier of the service. If the service was not found, the BM-SC shall send a 404 Not Found message. If the service cannot be updated, the BM-SC shall send a 403 Forbidden message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the PUT request is successful or unsuccessful, are shown in Table 5.2.1.2.3.2-1.

Table 5.2.1.2.3.2-1: Response status code, message, and contents for service modification using HTTP PUT

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier of the service that is modified
204 No Content	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.1.2.4 Service Deletion

DELETE /xmb/v1.0/services/{service-res-id}

To delete a service, the Content Provider shall use the HTTP DELETE method on the "service" instance resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services/{service-res-id}"
- the Host field is set to the address of the BM-SC
- the Content-Type header field is set to "application/json"
- the body of the message is encoded in JSON format

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

Upon receipt of the HTTP DELETE request from the Content Provider to delete a service, the BM-SC will check whether the Content Provider is authenticated and authorized to delete services as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.1.2.4-1. If the authorization is successful, the BM-SC delete the requested service. Upon successful deletion of requested service, the BM-SC shall respond to the Content Provider with a 200 OK success message indicating that the service is successfully deleted along with the service resource identifier of the service that is deleted. If the service was not found, the BM-SC shall send a 404 Not Found message. If the service cannot be deleted, the BM-SC shall send 403 Forbidden message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the DELETE request is successful or unsuccessful, are shown in Table 5.2.1.2.4-1.

Table 5.2.1.2.4-1: Response status code, message, and contents for service deletion

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier of the service that is deleted
204 No Content	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.1.2.5 Service Retrieval

Services can be read when the Content Provider wishes to know the latest representation of the service resource at the BM-SC.

Retrieval of a specific Service

GET /xmb/v1.0/services/{service-res-id}

The retrieval of a service shall be performed by the Content Provider using the HTTP GET method on the "service" instance resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services/{service-res-id}"
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

Upon receipt of the HTTP GET request from the Content Provider, the BM-SC will check whether the Content Provider is authenticated and authorized to read services as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in table 5.2.1.2.5-1. If the authorization is successful, the BM-SC shall respond to the Content Provider with a 200 OK message along with the service information. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field is set to "application/json"
- the body of the message is encoded in JSON format

The content body of this response message shall be the representation of the requested service based on the JSON schema of service resource as described in sub-clause 5.2.1.1. The properties "service-id", "service-class", and "service-announcement-mode" shall be included in the response to the Content Provider. All other properties of the service instance are optional to be returned to the Content Provider.

Alternatively, if the service was not found, the BM-SC shall send a 404 Not Found message. If the request cannot be fulfilled, the BM-SC shall send a 403 Forbidden message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.1.2.5-1.

Table 5.2.1.2.5-1: Response status code, message, and contents for service modification using HTTP GET

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service representation of the service resource to the Content Provider
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

Retrieval of all Services

GET /xmb/v1.0/services

The retrieval of all services shall be performed by the Content Provider using the HTTP GET method on the "services" instance resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services"
- the Host field is set to the address of the BM-SC

Upon receipt of the HTTP GET request from the Content Provider, the BM-SC will check whether the Content Provider is authenticated and authorized to read services as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in table 5.2.1.2.5-2. If the authorization is successful, the BM-SC shall respond to the Content Provider with a 200 OK message along with information of all services configured at the BM-SC. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the representation of the list of all services configured at the BM-SC where each service representation is based on the JSON schema of service resource as described in sub-clause 5.2.1.1. The properties "service-id", "service-class", and "service-announcement-mode" shall be included for each service representation in the response to the Content Provider. All other properties of the service instance are optional to be returned to the Content Provider.

Alternatively, if there are no services configured at the BM-SC, the BM-SC shall send message content in the 200 OK message indicating to the Content Provider that there are no services configured at the BM-SC. If the request cannot be fulfilled, the BM-SC shall send a 403 Forbidden message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.1.2.5-2.

Table 5.2.1.2.5-2: Response status code, message, and contents for service modification using HTTP GET

Status Code	Message	Contents
200 OK	The request has succeeded	If there are services configured at the BM-SC, the BM-SC shall send the representations of all the configured services to the Content Provider. If there are no services configured at the BM-SC, the BM-SC shall send message content in this message that there are no services configured at the BM-SC
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.2 Sessions

The Content Provider shall configure sessions at the BM-SC using the REST API methods over two resources managed at the BM-SC.

Table 5.2.2-1 summarizes different resources for provisioning and managing sessions at the BM-SC.

Table 5.2.2-1: Resources for managing sessions at BM-SC

Resource Name	Resource Type	Description
Session	Instance resource	Represents a single session resource. The Content Provider can provision or modify a single session at the BM-SC by invoking REST API requests to this session resource at the BM-SC.
Sessions	Collection Resource	Represents a collection of session resources.

Since sessions are configured for each service, the session instance resource or the sessions collection resource are referenced through a particular service.

5.2.2.1 Properties

Each session resource described in Table 5.2.2-1 has the set of properties described in Table 5.2.2.1-1. The Content Provider shall modify one or more of the properties of the session resource using the API operations described in sub-clause 5.2.2.2

Table 5.2.2.1-1 summarizes different properties of a session resource.

Table 5.2.2.1-1: Properties of session resource

Property Token	JSON Value Type	Defaults		Parameter Description
session-start	number	UTC Date timestamp (with second precision)	Session creation date + 1h	Start time when the MBMS Bearer become active.

session-stop	number	UTC Date timestamp (with second precision)	Session start date + 1h	End time at which the MBMS bearer becomes inactive.
max-ingest-bitrate	number	kbps	0	The requested bitrate excludes FEC overhead and transport overhead. The BM-SC calculates the MBMS Bearer bitrate from it, considering overhead like FEC and other transport overheads. The session bitrate is always larger or equal to the payload bitrate
max-delay	number	ms	-1	Specifies the maximum delay the MBMS System should add, i.e. from the time a packet is received by the BM-SC to the time when the packet is received by the MBMS client.
session-state	string	None	Idle	The BM-SC may automatically change the state of the session. Possible states: "Session Idle", "Session Announced", "Session Active".
service-announcement-starttime	number	UTC Date timestamp (with second precision)	None	When present, this time at which the BM-SC shall start service announcement. If absent, the BM-SC may automatically start service announcement when it has all the data needed to perform such service announcement.
geographical-area	<array> string	None	Empty list	Geographical area, at which the service is to be provided, either through unicast or through MBMS bearers. The BM-SC derives the MBMS service area and the SAI list for the availability information from geographical area as provided by the Content Provider. The Geographical Area contains list of string. The content of each string item is left to the business agreement between the Content Provider and the Operator.
qoe-reporting-configuration	object			The Content Provider wishes to collect QoE reports for the session. The Content Provider can supply a list of QoE metric configurations where each metric configuration shall have: Metric name: Name of QoE metric Metric type: Type of metric Reporting interval: The interval for which the BM-SC has to aggregate the statistics for Sample percentage: Percentage of users to collect reports from Start time: Start time of report collection End time: End time of report collection

				If this configuration is included, the QoE reporting configuration shall be applied only for this session. If this configuration is present, the Content Provider requests overriding of service level configuration for this session with this configuration. Note: SA4 should define the list of parameters for qoe-reporting-configuration. SA4 shall also indicate if service level qoe-reporting configuration can be applied.
session-type	string	None	Files	The Session Type represents the method used by the Content Provider in providing content to the BM-SC (via xMB-U). The BM-SC is select the appropriate delivery method from the session type. Valid values: "Streaming", "Files", "Application", "Transport-Mode" When the Session Type is set to "Streaming", the BM-SC expects a Streaming type input (RTP), and the format is compliant to MBMS streaming (as defined in 3GPP TS 26.346 [3]). When the Session Type is set to "Files", the BM-SC expects generic files as input. The files can be provided either by on-request pull interactions or continuous push ingest. When the Session Type is set to "Application", then the ingest method depends on the application service description. When the Application Service Description corresponds to DASH, the BM-SC expects an MPD and optionally one or more Initialization Segments. The content is assumed to be 3GP-DASH compliant (as defined by 3GPP TS 26.247 [18]). The BM-SC may either pull the Media Segments from the Content Provider or the Content Provider will continuously push Media Segments to the BM-SC. When the Session Type is set to "Transport-Mode", the BM-SC provides transport of data/TV content in a transparent manner. The Content Provider may provide some properties for the distribution. The Session Type shall be extensible for further session types.
session-announcement-mode	string	– None –	Other	Represents the session announcement mode. The session announcement mode is either "Content Provider" or "MBMS, with the following behavior: "Content Provider": The BMSC generates the session parameters and provides those to the Content Provider. "MBMS User Service": In this case, the session announcement is done by the MBMS system through the SACH. (see Annex L.2, L.3 of 3GPP TS 26.346 [3]). Additional modes may be added in future releases.

				Only applicable if the Session Type is set to "Transport-Mode"
userplane-session-description-parameters	object			The session description parameters for the xMB-U user plane provide the information on where and how the to access the session at the Content Provider, and may comprise one or both of the following types: *Type*: the type of the session, typically for proper interpretation of the Location element, for example the Internet Media Type of the document, or the URL in an HTTP URL. *Access URL*: A URL that enables the access to and possibly control of the ingest session. The URL may, for example, be an RTSP URL or a URL to an SDP that describes a multicast stream, or an HTTP URL to retrieve an already-packaged MPEG-2 TS stream, etc. Note that the BM-SC may get input on session properties from the Content Provider, e.g. bitrate, depending on the ingest session. Only applicable if the session type is set to "Transport-Mode".
userplane-delivery-mode-configuration	string	– None –	Forward-only	This mode configures how the session needs to be delivered to the application, i.e. it basically establishes the delivery mode. Mode Enumeration: Specifies the delivery mode. Forward-only: The BM-SC receives complete IP Multicast packets for to be forwarded. The Content Provider will create the IP multicast packets. Proxy: The BM-SC proxies the incoming UDP payloads to the outgoing UDP payloads. The BM-SC will create the IP multicast packets. Only applicable if the Session Type is set to "Transport-Mode".
delivery-session-description-parameters	string			If the Service Announcement Mode is set to Other, then at least the following information is provided by the BM-SC: TMGI of the MBMS Bearer Note that additional parameters may be provided, based on the configuration options of the delivery method for transport only. Only applicable if the Session Type is set to "Transport-Mode".
sdp-url	string	– None –	“”	A URL to the SDP that describes the streaming session between the Content Provider and the BM-SC, which will be used for ingesting the streaming session via xMB-U. The SDP shall include the RTSP links for every media session as part of the “a=control” attribute to

				enable RTSP control of the session. The SDP shall also contain the required bitrate for each of the media sessions. The content shall conform to the constraints of this specification. Only applicable if the Session Type is set to "Streaming".
time-shifting	number	second	0	Indicates if and for how long time shifting access to the content (using unicast) may be provided for this session. If not set (so defaulted to 0), there shall be no time shifting access. Only applicable if the Session Type is set to "Streaming".
application-service	string	MIME type	application/dash+xml	MIMEtype of the Application Service Only applicable if the Session Type is set to "Application".
ingest-mode	string	None	"Push" when Session Type is set to "Application" "Pull" when Session Type is set to "Files"	The ingest mode enumerates how resources are ingested into the BM-SC via xMB-U. When the Session Type is set to "Application": Pull: The BM-SC pulls the resources as described by the application entry point document. Push: The Content Provider pushes resources. The BM-SC needs to provide a push URL. In case of DASH, resources are Media Segments: Pull: The BM-SC pulls the Media Segments as described by the segment availability start time from a DASH MPD. Push: The Content Provider pushes Media Segments, so that the Media Segment is available on the BM-SC according to segment availability start time. The BM-SC needs to provide a push URL. When the Session Type is set to "Files": Push: The Content Provider shall push the file to the BM-SC that will immediately process and deliver as soon as it is ready. The BM-SC may be configured to ignore all files that are pushed before session active time, or stage them. In case of Push mode, the BM-SC shall provide back to the Content Provider the URL the Content Provider shall use to push the files. Pull: In this case, the Content Provider provides the resource location from which the BM-SC will fetch the file. The Content Provider may tell the BM-SC when to start fetching the file

application-entrypoint-url	string	None	“”	The application entry point refers to an MPD when Application Service Description pertains to DASH. When the Ingest Mode is set to Push, then the MPD URL refers to a DASH MPD which should be fetched, optionally conditioned, and inserted into Service Announcement. When the Ingest Mode is set to Pull, then the BM-SC starts fetching the segments using unicast. Note that if not set to a valid URL, the session will not be started.
push-url	string	None	“”	When the Session Type is set to "Application": A resource locator for ingesting Media Segments using HTTP via xMB-U. The Content Provider may create additional sub-resources using WebDAV procedures. This is a read-only property managed by the BM-SC and only present when Ingest Mode is set to Push This property is mandatory if the Session type is set to "Application" and Ingest Mode is set to Push. When the Session Type is set to Files: A resource locator for ingesting content using HTTP via xMB-U. This is a read-only property managed by the BM-SC and only present when Ingest Mode is set to Push.
unicast-delivery	boolean	None	False	Indicator whether the content is also available for unicast retrieval. Only applicable if the Session Type is set to "Application".
Components	array	None	Empty list	List of Components of the application, which are recommended to be made available on MBMS Bearers. In case of DASH, each component is identified by a representation identifier. Only applicable if the Session Type is set to "Application".
file-list	array			List of files to be sent. In the Push mode, the file list is not used since the BM-SC will monitor its push folder and send the files it receives on a first-come first-served basis. In Pull mode, the file list contains the following information per file entry: file URL: the URL to the file the BM-SC will use to fetch the content

				file display URL: The URL to the file as seen by the UE file earliest fetch time: The BM-SC shall fetch the file no sooner than this UTC timestamp. If absent, then the file shall be present on the Content Provider server and the BM-SC may fetch it when it wants. file size (optional): The Content Provider may provide the precise or a file size estimate as input. The BM-SC may update the file size once it has started to fetch the file. file status: Enumeration stating the state of the file. Possible values are pending, fetched, prepared, transmitting, sent. Target reception completion time (on the MBMS Client): hint on the due date, when the file should be completely received by the UE. The BM-SC should schedule and order the transmission etc accordingly. Keep Update Interval: The BM-SC checks the file resources with the given interval for changes. File repeat / Duration: The number of times the file shall be sent on the session (a value of 1 means the file shall be sent only once). This counter shall be decreased each time the file has been transmitted. When equals to zero, no more file repeat is scheduled. The BM-SC may send FEC instead of source information.
file-delivery-manifest-url	string	None	“”	Alternative to the file list. The resource may additionally describe scheduling information for the file. Only applicable if the Session Type is set to Files.
display-base-url	string	None	“”	When ingest mode is set to Push, the Base URL is seen by the UE.

The session instance resource with the properties defined above for each session can be shown using the following JSON schema:

```
"Session": {
        "type": "object",
        "description": "Session Description",
        "properties": {
                "session-start": {
                        "description": "Wall-clock time at which the MBMS Bearer becomes active",
                        "type": "number"
                },
                "session-stop": {
```

```
        "description": "Wall-clock at which the MBMS bearer becomes inactive",
        "type": "number"
    },
     "max-ingest-bitrate": {
        "description": "Refer to Table 5.2.2.1-1 for detailed description",
         "type": "number",
        "format": "float"
    },
    "max-delay": {
        "description": "Refer to Table 5.2.2.1-1 for detailed description",
        "type":  "number",
        "format": "float"
    },
    "session-state": {
        "description": "Refer to Table 5.2.2.1-1 for detailed description",
        "type": "string"
    },
    "service-announcement-starttime": {
        "description": "Refer to Table 5.2.2.1-1 for detailed description",
        "type": "number"
    },
    "geographical-area": {
        "description": "Refer to Table 5.2.2.1-1 for detailed description",
        "type": "array",
        "items" : {
            "type" : "string"
        }
    },
    "qoe-reporting-configuration": {
        "type": "array",
        "description": "Refer to Table 5.2.2.1-1 for detailed description",
        "items" : {
           "type" : "object",
          "description": "QoE metric configuration",
          "properties": {
            "metric-name": {
                "type": "string",
                "description": "Name of QoE metric"
            },
            "metric-type": {
                "type": "string",
                "description": "Type of metric"
            },
            "reporting-interval": {
                "type": "number",
                "description": "The interval for which the BM-SC has to aggregate the statistics for"
            },
            "sample-percentage": {
                "type": "number",
                "description": "Percentage of users to collect reports from"
            },
            "start-time": {
                "type": "string",
                "description": "Start time of consumption report collection"
            },
            "end-time": {
                "type": "string",
                "description": "End time of consumption report collection"
            }
        }
    }
},
"session-type": {
    "description": "Refer to Table 5.2.2.1-1 for detailed description",
    "type": "string",
    "enum" : ["Streaming", "Files ", "Application", "Transport-Mode"]
},
"transport-mode-session": {
    "description": "Describes a transport mode session",
        "type": "object",
        "properties": {
            "session-announcement-mode": {
                "description": "The session announcement mode is either Other or MBMS",
                "type": "string",
                "enum" : ["Other”, “MBMS"]
            },
            "userplane-session-description-parameters": {
                "description": "Refer to Table 5.2.2.1-1 for detailed description",
                "type": "object",
                “properties": {
                      "sessionDescriptionType": {
                            “type": "string",
                            "description": "Refer to Table 5.2.2.1-1 for detailed
                          description”
                      },
                      "sessionDescriptionAccessURL": {
                            "type": "string",
                            "description": "Refer to Table 5.2.2.1-1 for detailed
                          description”
                      }
                }
            },
            "userplane-delivery-mode-configuration": {
                "description": "Refer to Table 5.2.2.1-1 for detailed description ",
                "type": "string",
                "enum" : ["Forward-only", "Proxy"]
            },
            "delivery-session-description-parameters": {
                "description": "Refer to Table 5.2.2.1-1 for detailed description”,
                "type": "string"
            }
        }
    },
    "streaming-session": {
        "description": "Describes a streaming session ",
                "type": "object",
                "properties": {
                        "sdp-url": {
                                "description": "Refer to Table 5.2.2.1-1 for detailed description”,
                                "type": "string"
                        },
                        "time-shifting": {
                                "description": "Refer to Table 5.2.2.1-1 for detailed description”,
                                 "type": "number"
                        }
                }
        },
        "application-session": {
                "description": "Describes a application session ",
                "type": "object",
                "properties": {
                        "application-service": {
                                "description": "Mime-type of the Application Service",
                                "type": "string"
                        },
                        "ingest-mode": {
                                "description": "The ingest mode enumerates how resources are ingested into the
                                BM-SC",
                                "type": "string",
                                "enum": ["Pull”, "Push”]
                        },
                        "application-entry-point-url": {
                                "description": "Refer to Table 5.2.2.1-1 for detailed description”,
                                "type": "string"
                        },
                        "push-url": {
                                "description": "Refer to Table 5.2.2.1-1 for detailed description",
                                "type": "string"
                        },
                        "unicast-delivery": {
```

```
                    "description": "Indicator whether the content is also available for unicast
                    retrieval",
                    "type": "boolean"
                },
                "components": {
                    "description": "Refer to Table 5.2.2.1-1 for detailed description",
                    "type": "array",
                    "items" : {
                          "type" : "string"
                    }
                }
            }
        },
        "file-session": {
            "description": "Describes a file session ",
            "type": "object",
            "properties": {
                "ingest-mode": {
                    "description": "The ingest mode enumerates how resources are ingested into the
                    BM-SC",
                    "type": "string",
                    "enum" : ["Pull”, "Push”]
                },
                "file-list": {
                    "type": "array",
                    “description": "Refer to Table 5.2.2.1-1 for detailed description",
                    "items" : {
                        "type" : "object",
                        "properties": {
                            "file-url": {
                                "type": "string",
                                "description": "the URL to the file"
                            },
                            "file-earliest-fetch-time" : {
                                "type": "string",
                                "description": "Refer to Table 5.2.2.1-1 for detailed description",

                                "format": "date-time"

                            },

                            "file-size": {

                                "type": "integer",

                                "format": "int32",

                                "description": " Refer to Table 5.2.2.1-1 for detailed description"

                            },

                            "file-status" : {

                                "type": "string",

                                "description": " Refer to Table 5.2.2.1-1 for detailed description",

                                "enum": ["pending", "fetched", "prepared", "transmitting", "sent"]

                            },

                            "target-reception-completion-time" : {

                                "type": "string",

                                "description": "Refer to Table 5.2.2.1-1 for detailed description",

                                "format": "date-time"

                            },

                            "keep-update-interval": {

                                "type": "string",

                                "description": "Refer to Table 5.2.2.1-1 for detailed description"

                            },

                            "file-repeat-duration": {

                                "type": "integer",

                                "format": "int32",

                                "description": "Refer to Table 5.2.2.1-1 for detailed description"

                            }

                        }

                    }

                },

                "file-delivery-manifest-url": {
```

```
                              "description": "Refer to Table 5.2.2.1-1 for detailed description",
                              “type": "string"
                         },
                         "display-base-url": {
                              "type": "string",
                              "description": "Refer to Table 5.2.2.1-1 for detailed description"
                         }
                    }
               }
            }
    }
```

5.2.2.2 API Operations

5.2.2.2.1 Introduction

Sessions can be created, updated, or deleted at the BM-SC by the Content Provider, or the properties of a previously created session at the BM-SC, may be obtained by the Content Provider by invoking HTTP methods on the “session” instance resource or the “sessions” collection resource. In all HTTP requests, the message body shall contain an Access Token as authorization parameter for the associated method.

5.2.2.2.2 Session Creation

POST /xmb/v1.0/services/{service-res-id}/sessions

To create a session, the Content Provider shall use the HTTP POST method on the "sessions" collection resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/services/{service-res-id}/sessions.
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service for which the session creation is sought.

The content body of the session creation request shall be empty.

Upon receipt of the HTTP POST request from the Content Provider to create a session, the BM-SC will check whether Content Provider is authenticated and authorized to create sessions as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message. If authorization is successful, the BM-SC shall check to see if the service already exists with the given service resource identifier. If the service with given service resource identifier exists at the BM-SC, the BM-SC shall create the requested session for that service with default session property values described in clause 5.2.2.1. Upon successful creation of requested session, the BM-SC shall respond to the Content Provider with a 201 success message indicating that the session is successfully created along with the session resource identifier of the created session. The session resource identifier is the identifier that uniquely identifies the session within that service. When the Content Provider receives the session resource identifier, it shall use this identifier in subsequent requests to the BM-SC to refer to this session. If the creation of session failed, the BM-SC shall send a 403 message. If the service was not found for which the session creation is sought, the BM-SC shall send a 404 message.

The possible response messages from the BM-SC, depending on whether the POST request is successful or unsuccessful, are shown in Table 5.2.2.2.2-1.

Table 5.2.2.2.2-1: Response status code, message, and contents for session creation

Status Code	Message	Contents
201 Created	Session created successfully	The BM-SC shall send the session resource identifier of the created session and the service resource identifier.
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable		

5.2.2.2.3 Session Modification

Sessions created using the session creation methods described in subclause 5.2.2.2.2 can be updated when the Content Provider wishes to modify the session properties.

5.2.2.2.3.1 Partial Modification of Session Properties

PATCH /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}

Assuming that a session has been created using the session creation method described in sub-clause 5.2.2.2.2, partial updating of its properties can be performed by the Content Provider by using the HTTP PATCH method on the “session” instance resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
- the Host field is set to the address of the BM-SC
- the Content-Type header field is set to "application/json"
- the body of the message is encoded in JSON format

The {service-res-id} in the request URI is the service resource identifier of the service whose session is being modified.

The {session-res-id} in the request URI is the session resource identifier of the session that is being modified.

The content body of the session update request shall contain updated partial representation of the session resource. The representation of the session is based on the JSON schema of session resource as described in sub-clause 5.2.2.1. Further, one or more properties of the session listed in table 5.2.2.1-1 with the exception of properties "session-state", "qoe-report-url", "delivery-session-description-parameters", "push-url" can be updated. The session properties "session-state", "qoe-report-url", "delivery-session-description-parameters", and "push-url" cannot be modified.

Upon receipt of the HTTP PATCH request from the Content Provider to update a session, the BM-SC will check whether the Content Provider is authenticated and authorized to update sessions as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in table 5.2.2.2.3.1-1. If the authorization is successful, the BM-SC checks to see if the service already exists with the given service resource identifier, and a session already exists with the given session resource identifier. If both of them exist, BM-SC update the session as requested for that service. Upon successful update of the requested session, the BM-SC shall respond to the Content Provider with a 200 success message indicating that the session is successfully updated along with the session resource identifier. As alternative to the 200 OK message, BM-SC may send a 204 No Content success message without any message content to the Content Provider. If the session cannot be updated, the BM-SC shall send a 403 message. If the session is not found or if the service was not found for which the session creation is sought, the BM-SC shall send a 404 message.

The possible response messages from the BM-SC, depending on whether the PATCH request is successful or unsuccessful, are shown in Table 5.2.2.2.3.1-1.

Table 5.2.2.2.3.1-1: Response status code, message, and contents for session modification using HTTP PATCH

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the session resource identifier of the session that is modified and the service resource identifier of the corresponding service
204 No Content	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.2.2.3.2 Full Modification of Session Properties

PUT /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}

Assuming that a session has been created using the session creation method described in subclause 5.2.2.2.2, full update of its properties can be performed by the Content Provider using the HTTP PUT method on the "session" instance resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
- the Host field is set to the address of the BM-SC
- the Content-Type header field is set to "application/json"
- the body of the message is encoded in JSON format

The {service-res-id} in the request URI is the service resource identifier of the service whose session is being modified.

The {session-res-id} in the request URI is the session resource identifier of the session that is being modified.

The content body of the session update request shall contain updated representation of the session resource. The representation of the session is based on the JSON schema of session resource as described in subclause 5.2.2.1. Further, when HTTP PUT method is used for updating the service, the Content Provider shall specify the updated values of all the session properties with the exception of the properties "session-state", "qoe-report-url", "delivery-session-description-parameters", and "push-url" in the updated representation. The session properties "session-state", "qoe-report-url", "delivery-session-description-parameters", and "push-url" cannot be modified.

Upon receipt of the HTTP PUT request from the Content Provider to update a session, the BM-SC will check whether the Content Provider is authenticated and authorized to update sessions as described in clause 7. If the authorization is unsuccessful, the BM-SC shall send a 401 message as described in table 5.2.2.2.3.2-1. If the authorization is successful, the BM-SC checks to see if the service already exists with the given service resource identifier, and a session already exists with the given session resource identifier. If both of them exist, BM-SC update the session as requested for that service. While updating session representation, the BM-SC shall overwrite the values of all properties of the session being updated with the values from provided in the update request. Upon successful update of the requested session, the BM-SC shall respond to the Content Provider with a 200 success message indicating that the session is successfully updated along with the session resource identifier. As an alternative to 200 OK success message, BM-SC may send a 204 No Content success message without any message content to the Content Provider. If the session cannot be updated, the BM-SC shall send a 403 message. If the session is not found or if the service was not found for which the session creation is sought, the BM-SC shall send a 404 message.

The possible response messages from the BM-SC, depending on whether the PUT request is successful or unsuccessful, are shown in Table 5.2.2.2.3.2-1.

Table 5.2.2.2.3.2-1: Response status code, message, and contents for session modification using HTTP PUT

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the session resource identifier of the session that is modified and the service resource identifier of the corresponding service
204 No Content	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.2.2.4 Session Deletion DELETE /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}

To delete a session, the Content Provider shall use the HTTP DELETE method on the "session" instance resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service whose session is being deleted.

The {session-res-id} in the request URI is the session resource identifier of the session that is being deleted.

Upon receipt of the HTTP DELETE request from the Content Provider to delete a session, the BM-SC will check whether the Content Provider is authenticated and authorized to delete services as described in clause 7. If the authorization is unsuccessful, the BM-SC shall send a 401 message as described in table 5.2.2.2.4-1. If the authorization is successful, the BM-SC checks to see if the service already exists with the given service resource identifier and a session exists with the given session resource identifier. If both of them exist, BM-SC delete the requested session for the given service. Upon successful deletion of requested session, the BM-SC shall respond to the Content Provider with a 200 success message indicating that the session is successfully deleted along with the service resource identifier and the session resource identifier. As an alternative to the 200 OK success message, BM-SC may send a 204 No Content success message without any message content to the Content Provider. If the session cannot be deleted, the BM-SC shall send a 403 message. If the session is not found or if the service was not found for which the session creation is sought, the BM-SC shall send a 404 message.

The possible response messages from the BM-SC, depending on whether the DELETE request is successful or unsuccessful, are shown in Table 5.2.2.2.4-1.

Table 5.2.2.2.4-1: Response status code, message, and contents for session deletion

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the session resource identifier of the session that is deleted and the service resource identifier of the corresponding service
204 No Content	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]

403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.2.2.5 Session Retrieval

Sessions can be read when the Content Provider wishes to know the latest representation of the session resources at the BM-SC.

Retrieval of a specific Session of a specific Service

GET /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}

The retrieval of a session shall be performed by the Content Provider using the HTTP GET method on the "session" instance resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

The {session-res-id} in the request URI is the session resource identifier of the session that is being retrieved.

Upon receipt of the HTTP GET request from the Content Provider, the BM-SC will check whether the Content Provider is authenticated and authorized to read services and sessions as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in table 5.2.2.2.5-1. If the authorization is successful, the BM-SC shall respond to the Content Provider with a 200 OK message and shall include the session resource representation of the session corresponding to the given service to the Content Provider. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the representation of the session configured at the BM-SC for the given service where the session representation is based on the JSON schema of session resource as described in sub-clause 5.2.2.1. The properties "session-start", "session-stop", "max-ingest-bitrate", "session-state", "geographical-area", "session-type", "session-announcement-mode", "session-type", "userplane-delivery-mode-configuration", "sdp-url", "application-service-description", "ingest-mode", "application-entryppoint-url", and "unicast-delivery" shall be included in the response to the Content Provider. All other properties of the session instance are optional to be returned to the Content Provider.

Alternatively, if the service was not found or if the session was not found, the BM-SC shall send a 404 Not Found message. If the request cannot be fulfilled, the BM-SC shall send 403 Forbidden message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.2.2.5-1.

Table 5.2.2.2.5-1: Response status code, message, and contents for service modification using HTTP GET

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the session representation of the session resource to the Content Provider
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]

403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

Retrieval of all Sessions of a Service

GET /xmb/v1.0/services/{service-res-id}/sessions

The retrieval of all sessions of a service shall be performed by the Content Provider using the HTTP GET method on the "sessions" instance resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/services/{service-res-id}/sessions
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

Upon receipt of the HTTP GET request from the Content Provider, the BM-SC will check whether the Content Provider is authenticated and authorized to read services and sessions as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in table 5.2.2.2.5-2. If the authorization is successful, the BM-SC shall respond to the Content Provider with a 200 OK message. If there are sessions configured at the BM-SC for the corresponding service, the BM-SC shall send the representation of the list of all session resources configured at the BM-SC for that service along with the 200 OK message. If there are no sessions configured at the BM-SC for that service, the BM-SC shall send message content in the 200 OK message indicating to the Content Provider that there are no sessions configured at the BM-SC for that service.

The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the representation of list of sessions configured at the BM-SC for the given service where each session representation is based on the JSON schema of session resource as described in subclause 5.2.2.1. The properties "session-start", "session-stop", "max-ingest-bitrate", "session-state", "geographical-area", "session-type", "session-announcement-mode", "session-type", "userplane-delivery-mode-configuration", "sdp-url", "application-service-description", "ingest-mode", "application-entryppoint-url", and "unicast-delivery" shall be included for each session representation in the response to the Content Provider. All other properties of the session instance are optional to be returned to the Content Provider.

Alternatively, if the request cannot be fulfilled, the BM-SC shall send 403 Forbidden message to the Content Provider. If the service was not found, the BM-SC shall send a 404 Not Found message

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.2.2.5-2.

Table 5.2.2.2.5-2: Response status code, message, and contents for service modification using HTTP GET

Status Code	Message	Contents
200 OK	The request has succeeded	If there are sessions configured at the BM-SC for that service, the BM-SC shall send the representations of all the configured sessions for that service to the Content Provider. If there are no sessions configured at the BM-SC for that service, the BM-SC shall send message content in this message indicating to the Content Provider that there are no sessions configured at the BM-SC for this service

401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.3 Reports

The BM-SC shall send reports to the Content Provider upon request by the Content Provider. Table 5.2.3-1 summarizes different report resources that the BM-SC manages for sending reports to the Content Provider.

Table 5.2.3-1: Resources for managing reports at BM-SC

Resource Name	Resource Type	Description
Report	Instance resource	Represents a single report resource. The BM-SC can send an individual report to the Content Provider using the report instance resource
Reports	Collection Resource	Represents a collection of report resources.

Reports can be generated separately for each service or for a session belonging to a particular service. Therefore, a report can be referenced with a given service resource identifier or for a combination of service resource identifier and session resource identifier.

5.2.3.1 Properties

Each report resource described in Table 5.2.3-1 has the set of properties described in Table 5.2.3.1-1. The BM-SC shall deliver the reports as indicated by this structure using the API operations described in sub-clause 5.2.3.2

Table 5.2.3.1-1 summarizes different service properties of a service resource.

Table 5.2.3.1-1: Resources for managing services at BM-SC

Property Token	JSON Value Type	Parameter Description
report-res-id	string	Report resource identifier
report-starttime	string	Report collection start time
report-endtime	string	Report collection end time
report-type	string	Type of report. Three types of reports can be generated by the BM-SC to send to the Content Provider: Consumption report: Report that provides service consumption information QoE report: Report that provides detailed QoE information of the content received File reception report: Report that provides detailed reception information for each file
report-url	string	Location of the report from where the Content Provider can retrieve the detailed report.
Report	string	Detailed report. This may not be included if report-url is included

Note: SA4 to clarify the report types and detail structure of a report that can be sent from BM-SC to the Content Provider.

The report instance resource with the properties defined above for each report can be shown using the following JSON schema:

```
 "report": {
        "type": "object",
        "description": "Report Description",
        "properties": {
                " report-starttime": {
                        "type": "string",
                        "description": "Report collection start time"
                },
                " report-endtime": {
                        "type": "string",
                        "description": "Report collection end time"
                },
                "report-type": {
                        "description": "Type of report",
                        "type": "string"
                },
                "report-url": {
                        "type": "string",
                        "description": "Location of the report from where the Content Provider can retrieve the detailed
                        report"
                },
                "report": {
                        "type": "string",
                        "description": "Detailed report"
                }
          }
      }
```

5.2.3.2 API Operations

5.2.3.2.1 Introduction

The Content Provider can request reports from the BM-SC for a given service or a session belonging to a given service.

5.2.3.2.2 Report Retrieval

Reports can be retrieved by the Content Provider for a service or for a session of a given service using HTTP GET method.

Report Retrieval for a Service

GET /xmb/v1.0/services/{service-res-id}/reports

The retrieval of reports of a service shall be performed by the Content Provider using the HTTP GET method on the "reports" collection resource as follows:

- the request URI with the "path" part set to: "/xmb/v1.0/services/{service-res-id}/reports"
- the Host field is set to the address of the BM-SC

QoE reports however are only available on session level. The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

Upon receipt of a HTTP GET request from the Content Provider to retrieve all the reports of a service, the BM-SC will check whether the Content Provider is authenticated and authorized to request reports for services and sessions configured at the BM-SC as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.3.2.2-1. If the authorization is successful, the BM-SC checks to see if the service with the given service resource identifier exists at the BM-SC. If the service exists at the BM-SC, the BM-SC shall respond to the Content Provider with a 200 success message along with the service resource identifier and the list of all reports for that service. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the list of report for that service. Each report in this list shall be based on the JSON schema of report resource as described in subclause 5.2.3.1.

Alternatively, if the report retrieval request cannot be fulfilled, the BM-SC shall send a 403 message. If the service was not found for which the report is sought, the BM-SC shall send a 404 message.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.3.2.2-1.

Table 5.2.3.2.2-1: Response status code, message, and contents for retrieval of all service reports

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier and all the reports for the service
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

GET /xmb/v1.0/services/{service-res-id}/reports/{report-res-id}

The Content Provider can request individual reports of a service if it is aware of the report resource identifiers of that service. A specific report for a service can be retrieved by the Content Provider using the HTTP GET method on the "report" instance resource as follows.

- the request URI with the "path" part set to: "/xmb/v1.0/services/{service-res-id}/reports/{report-res-id}"
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service whose reports are being sought.

The {report-res-id} in the request URI is the report resource identifier of that service.

It should be noted that QoE reports are only available on session level. Upon receipt of a HTTP GET request from the Content Provider to retrieve a specific report of a service with report resource identifier, the BM-SC will check whether the Content Provider is authenticated and authorized to request reports for services and sessions configured at the BM-SC as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.3.2.2-2. If the authorization is successful, the BM-SC checks to see if the service with the given service resource identifier and a report with given report resource identifier exists for that service at the BM-SC. If such report exists at the BM-SC, the BM-SC shall respond to the Content Provider with a 200 success message along with the service resource identifier and the report to the Content Provider. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the requested report resource for that service whose representation is based on the JSON schema of report resource as described in subclause 5.2.3.1.

Alternatively, if the report retrieval request cannot be fulfilled, the BM-SC shall send a 403 message. If the report is not found or if the service is not found for which the report is sought, the BM-SC shall send a 404 message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.3.2.2-2.

Table 5.2.3.2.2-2: Response status code, message, and contents for retrieval of a specific report of a service

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier and the requested report of the service
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

Report Retrieval for a Session of a given Service

GET /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}/reports

The retrieval of all the reports of a session for a given service shall be performed by the Content Provider using the HTTP GET method on the "reports" collection resource as follows:

- the request URI with the "path" part is set to: "/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}/reports.
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

The {session-res-id} in the request URI is the session resource identifier of the session whose reports are being sought.

Upon receipt of a HTTP GET request from the Content Provider to retrieve all the reports of a session of given service, the BM-SC will check whether the Content Provider is authenticated and authorized to request reports for services and sessions configured at the BM-SC as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.3.2.2-3. If the authorization is successful, BM-SC checks to see if the service with the given service resource identifier and a corresponding session with the given session identifier exists at the BM-SC. If such a session exists at the BM-SC, the BM-SC shall respond to the Content Provider with a 200 success message along with the list of all reports for that session. If there are no reports for that session at the BM-SC, the BM-SC shall send a 200 OK message with message content indicating that there are no reports for the session at the BM-SC. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the list of all reports for that session. Each report in this list of reports sent shall be based on the JSON schema of report resource as described in subclause 5.2.3.1.

Alternatively, if the report retrieval request cannot be fulfilled, the BM-SC shall send a 403 message. If the session is not found for which the report is sought, or if the service corresponding to the sessions is not found, the BM-SC shall send a 404 message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.3.2.2-3.

Table 5.2.3.2.2-3: Response status code, message, and contents for retrieval of all reports for a session

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier, session resource identifier, and all the reports of that session. If there are no reports for that session at the BM-SC, the BM-SC shall include message content indicating that there are no reports for the requested session at the BM-SC.
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

GET /xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}/reports/{report-res-id}

The Content Provider can request individual reports of a given session of a service if it is aware of the report resource identifiers of that session for that service. A specific report for a session can be retrieved by the Content Provider using the HTTP GET method on the "report" instance resource as follows.

- the request URI with the "path" part is set to: "/xmb/v1.0/services/{service-res-id}/sessions/{session-res-id}/reports/{report-res-id}"
- the Host field is set to the address of the BM-SC

The {service-res-id} in the request URI is the service resource identifier of the service as allocated by the BM-SC during service creation.

The {session-res-id} in the request URI is the session resource identifier of the session whose report is being sought.

The {report-res-id} in the request URI is the report resource identifier that is being sought.

Upon receipt of a HTTP GET request from the Content Provider to retrieve a specific report for a session of a service, the BM-SC will check whether the Content Provider is authenticated and authorized to request reports for services and sessions configured at the BM-SC as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in Table 5.2.3.2.2-4. If the authorization is successful, the BM-SC checks to see if a report with report resource identifier exists for a session with given session resource identifier whose service identifier is the given service resource identifier at the BM-SC. If such a report exists at the BM-SC, the BM-SC shall respond to the Content Provider with a 200 success message along with the requested report to the Content Provider. The response from the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the requested report resource for that session for the given service and whose representation is based on the JSON schema of report resource as described in subclause 5.2.3.1.

Alternatively, if the report retrieval request cannot be fulfilled, the BM-SC shall send a 403 message. If the session is not found for which the report is sought, or if the service corresponding to the sessions is not found, or if the report is not found, the BM-SC shall send a 404 message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.3.2.2-4.

Table 5.2.3.2.2-4: Response status code, message, and contents for retrieval of a specifc report of a session

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send the service resource identifier, session resource identifier, and the requested report for the service
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

5.2.4 Notifications

Notifications can be exchanged in two possible methods. In the first method, the Content Provider can "pull" the notifications from the BM-SC using HTTP GET method if and when the Content Provider wishes to acquire notification information as described in this subclause. The second method is that the notifications can be "pushed" from the BM-SC to the Content Provider via the push-notification-url as documented in clause 8.

Table 5.2.4-1 summarizes different notification resources that the BM-SC manages for sending notifications to the Content Provider.

Table 5.2.4-1: Resources for managing services at BM-SC

Resource Name	Resource Type	Description
Notification	Instance resource	Represents a single notification resource. The BM-SC can send an individual notification to the Content Provider using the notification instance resource
Notifications	Collection Resource	Represents a collection of notification resources.

5.2.4.1 Properties

Each notification resource described in Table 5.2.4-1 has the set of properties described in Table 5.2.4.1-1. The BM-SC shall deliver the notifications as indicated by this structure using the API operations described in sub clause 5.2.4.2.

Table 5.2.4.1-1 summarizes different properties of a notification resource.

Table 5.2.4.1-1: Resources for managing services at BM-SC

Property Token	JSON Value Type	Parameter Description
notification-res-id	string	Notification resource identifier
message-class	string	Enumeration with the following values (may be expanded in the future): **Critical**, **Warning**, **Information**, **Service**, **Session**. The message classes bear the following meaning: **Critical:** When some event drastically prevent the proper delivery of content **Warning:** When the service can be partially delivered but quality is reduced **Information:** When the service is properly delivered but some interesting event occurred **Session/Service**: Information about Service/Session related parameters Table 5.2.4.1-x shows the information that can be notified for each of the message classes.
message-name	string	Unique identifier of the message. Provides information about the message pertaining to the message-class of the notification Table 5.2.4.1-2 shows the information that can be notified for each of the message classes and message names.
Message-information	object	A dictionary of key values containing informations linked to the notification. Every message-information dictionary shall include the following two keys: date: The value of this key contains the UTC timestamp (in ms) of the date of the event source: The value of this key is hierarchical dot separated format of services and sessions in the format "service-resource-identifier:session-resource-identifier". If the notification is for a service, only the service-resource-identifier shall be included in this value. An empty value for this key represent a system wide notification. Table 5.2.4.1-x shows the additional key value pairs that can be included in the message-information for each of the message-class and message-name.

Table 5.2.4.1-2 shows the notification details that can be sent for each of the message classes.

Table 5.2.4.1-2: Notification Details for different message classes

Message Class	Possible Message Name	Additional Key Value Pairs in message-information dictionary
Critical	network-is-down	None
	service-badly-configured	bad-or-missing-parameters: [<property name>, ..]
	session-badly-configured	bad-or-missing-parameters: [<property name>, ..]

Warning	incoming-bitrate-exceed-session-capacity	incoming-bit-rate:<value in kbps>
	no-incoming-data	None
Information	qoe-report-available	None
	consumption-reports-available	None
	reception-reports-available	None
Service	service-announcement-change	None
Session	session-state-change	from-state:<from state> to-state: <to state> where the from state and to state have one of the values in the enumeration: Session Idle Session Announced Session Active Session Stopped
	file-ready-for-transmission	file-url:<file URL> file-size: <file-size> transmission-size: <transmission-size>
	file-download-started	file-url:<file URL>
	file-successfully-sent	file-url:<file URL>
	file-fetch-error	file-url:<file URL> http-error-code: <error-code>
Note 1: For the message-class "Service", the message-name service-announcement-change applies only when the session-state is in Session Announced or Session Active states. Note 2: For the message-class "Session", the message-name file-ready-for-transmission applies only when the session-type is "Files". Note 3: For the message-class "Session", the message-name file-download-started applies only when the session-type is "Files". Note 4: For the message-class "Session", the message-name file-successfully-sent applies only when the session-type is "Files".		

The notification instance resource with the properties defined in Table 5.2.4.1-1 can be shown using the following JSON schema:

```
 "Notification": {
        "type": "object",
        "description": "Notification Description",
        "properties": {
                "notification-res-id": {
                    "type": "string",

                    "description": "Identifier of the Notification Resource"

                },

                "message-class": {

                    "type": "string",

                    "description": "Indicates the message class of the notification",

                    "enum" : ["Critical: When some event drastically prevent the proper delivery of content",
                    "Warning: When the service can be partially delivered but quality is reduced", "Information:
                    When the service is properly delivered but some interesting event occurred", "transmitting",
                    "Session/Service: Information about Service/Session related parameters"]

                },

                "message name": {

                    "description": "Unique identifier of the message. Provides information about the message
                    pertaining to the message-class of the notification",

                    “type": "string",

                    "enum" : ["network-is-down", "service-badly-configured", "session-badly-configured",
                    "incoming-bitrate-exceed-session-capacity", "no-incoming-data", "qoe-report-available",
                    "consumption-reports-available", "reception-reports-available", "service-announcement-
                    change", "session-state-change", "file-ready-for-transmission", "file-download-started ", "file-
                    successfully-sent", "file-fetch-error"]

                },

                "message-information": {

                    "type": "object",

                    "description": "A dictionary of key values containing informations linked to the notification",

                    "additionalProperties": {

                        "type": "string"

                    }

                }

        }

    }
```

5.2.4.2 API Operations

5.2.4.2.1 Introduction

The Content Provider can request individual service and session level notifications and system-wide notifications from the BM-SC. The notifications are configured by the Content Provider when it creates services and sessions at the BM-SC. Notifications can be retrieved by the Content Provider from the BM-SC at times of its choice and shall use techniques such as long polling to poll the BM-SC for available notifications. Notifications can be retrieved from the BM-SC using HTTP methods on the notifications collection resource.

Editor's Note: The polling techniques that can be used by Content Provider to look for available notifications is FFS.

5.2.4.2.2 Notification Retrieval

Retrieval of All Notifications

GET /xmb/v1.0/notifications

The retrieval of all the notifications shall be performed by the Content Provider using the HTTP GET method on the "notifications" collection resource as follows:

- the request URI with the "path" part is set to: /xmb/v1.0/notifications
- the Host field is set to the address of the BM-SC

Upon receipt of a HTTP GET request from the Content Provider to retrieve all the notifications , the BM-SC will check whether the Content Provider is authenticated and authorized to request notifications as described in clause 7. If the authorization fails, the BM-SC shall send a 401 message as described in table 5.2.4.2.2-1. If the authorization is successful, the BM-SC shall respond to the Content Provider with a 200 success message along with the list of all notifications. If there are no available notifications at the BM-SC, the BM-SC shall send a 200 OK message with message content indicating that there are no available notifications. The response form the BM-SC to the Content Provider shall have the following:

- the Content-Type header field set to "application/json"
- the body of the message encoded in JSON format

The content body of this response message shall be the list of notifications available at the BM-SC. Each notification in this list shall be based on the JSON schema of notification resource as described in subclause 5.2.4.1.

Alternatively, if the notification retrieval request cannot be fulfilled, the BM-SC shall send a 403 message to the Content Provider.

The possible response messages from the BM-SC, depending on whether the GET request is successful or unsuccessful, are shown in Table 5.2.4.2.2-1.

Table 5.2.4.2.2-1: Response status code, message, and contents for retrieval of all notifications of service

Status Code	Message	Contents
200 OK	The request has succeeded	The BM-SC shall send all the notifications. If there are no notifications available at the BM-SC, the BM-SC shall include message content indicating that there are no notifications at the BM-SC.
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 2616 and IETF RFC 7231 [6]
403 Forbidden	Request cannot be fulfilled	The BM-SC may include optional text to indicate why the request could not fulfilled
Note: In addition to the above response codes, the BM-SC can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

Individual notifications can be accessed using HTTP GET method by referencing the "notification-res-id".

6 User Plane Procedures

6.1 Introduction

The xMB-U user plane procedures cover the transmission of service data between the Content Provider to the BM-SC. Only authorized and authenticated Content Provider sources shall be able to provide user plane data over xMB-U to the BM-SC. The following data transfer modes are supported:

- File Push: the Content Provider uploads or transmits files to the BM-SC either as soon as they become available, or in advance.
- File Pull: the Content Provider makes files available prior to the session start and at least during the lifetime of a session. The BM-SC will retrieve the files when it needs to deliver them.
- RTP Streaming: the BM-SC establishes an RTSP session to the Content Provider and starts the streaming session to relay media streams.
- Transport: the BM-SC listens on one IP address and one port number to receive UDP packets.

The details of these procedures are provided in the following sections.

6.2 File Session

6.2.1 General

Provisioning files for file distribution shall use one of the two options in the following sub-clauses.

6.2.2 Push Mode

WebDAV as described in IETF RFC 5246 [4] or HTTP v1.1 shall be used over TLS. The Content Provider shall use the PUT method and place the file in the message body of the request associated with the push-url. The Content Provider shall ensure that each file is available at the BM-SC latest at its provided file-earliest-fetch-time, or if not provided, prior to the session start. The Content Provider shall provide an authorization access token in the header with every HTTPS transaction. Potential response codes and their interpretation is provided in Table 6.2.2-1.

Table 6.2.2-1: Response status code, message, and contents of File Push mode

Status Code	Message	Contents
201 Created	File pushed successfully	None
401 Unauthorized	Request requires user authorization	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The Content Provider may include optional text to indicate why the request could not be fulfilled, e.g. incorrect URL used

6.2.3 Pull Mode

HTTP v1.1 shall be used over TLS in Pull mode. The BM-SC shall use GET method to request each file as defined by the file-list or alternatively by the manifest received from the file-delivery-manifest-url. The BM-SC shall pull each file earliest at its provided file-earliest-fetch-time, or if not provided, prior to the session start. Upon a successful GET, the Content Provider shall provide the requested file in the response body. Potential response codes and their interpretation is provided in Table 6.2.3-1.

Table 6.2.3-1: Response status code, message, and contents of File Pull mode

Status Code	Message	Contents
200 OK	The request has succeeded	The Content Provider shall send the requested file in the response body.

401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The Content Provider may include optional text to indicate why the request could not be fulfilled
404 Not Found	Requested resource not found	None
Note: If "file-delivery-manifest-url" is used, and if there is any error code in response to the request to get the manifest from the provided URL, the session is not started.		

6.3 Application Session

6.3.1 General

Application mode, including DASH service delivery shall use one of the two options in the following sub-clauses.

6.2.2 Push Mode

WebDAV as described in IETF RFC 5246 [4] or HTTP v1.1 shall be used over TLS. The Content Provider shall use PUT method with the resource (Application Session) or the Media Segment (DASH) in the message body, to place it at the push-url. The Content Provider shall ensure that each Segment is available at the BM-SC prior to its prescribed Segment availability start time in the MPD, or if not provided, prior to the session start. The Content Provider shall provide an authorization access token in the header with every HTTPS transaction. Potential response codes and their interpretation is provided in Table 6.2.2-1.

Table 6.2.2-1: Response status code, message, and contents of Application (including DASH) Push mode

Status Code	Message	Contents
201 Created	File pushed successfully	None
401 Unauthorized	Request requires user authorization	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The Content Provider may include optional text to indicate why the request could not be fulfilled, e.g. incorrect URL was used

6.2.3 Pull Mode

HTTP v1.1 shall be used over TLS in Pull mode. For DASH service, the BM-SC shall use the application-entry-point-url to retrieve the MPD. The BM-SC shall use GET method to request the resource, or for DASH, each Media Segment as defined by the MPD. Upon a successful GET, the Content Provider shall provide the requested resource or DASH Segment, respectively, in the response body. Potential response codes and their interpretation is provided in Table 6.2.3-1.

Table 6.2.3-1: Response status code, message, and contents of Application (including DASH) Pull mode

Status Code	Message	Contents
200 OK	The request has succeeded	The Content Provider shall send the requested resource or DASH Segment in the response body.
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The Content Provider may include optional text to indicate why the request could not be fulfilled

404 Not Found	Requested resource not found	None

The BM-SC shall ensure that each DASH Media Segment is fully received prior to its prescribed availability start time, or if not provided, prior to the session start.

Note: If "application-entry-point-url" is used, and if there is any error code in response to the request to get the MPD from the provided URL, the session is not started.

6.3 RTP Streaming

The Content Provider shall support PSS server functionality according to PSS as described in clause 5.3 of 3GPP TS 26.234 [5]. The streaming session shall be accessible prior to the start of the session. A URL to the SDP file that describes the streaming session between the Content Provider and the BM-SC is provided via the sdp-url, which shall be used for ingesting the streaming session. The SDP shall include the RTSP links for every media session as part of the “a=control” attribute to enable RTSP control of the session. The SDP shall also contain the required bitrate for each of the media sessions.

When the user plane data is provided via UDP, then SRTP over DTLS [127] shall be used for user plane protection. Establishment of TCP based user plane sessions with PSS is not supported.

If there is any error retrieving the SDP, the session is not started.

6.4 Transport

For Transport sessions, the BM-SC shall activate the receivers on the indicated IP address and port numbers and shall ensure that firewall and NAT traversal is enabled on these IP addresses and port numbers as defined in the SDP retrieved from the sdp-url. If there is any error retrieving the SDP, the session is not started. All traffic shall use DTLS as specified in 3GPP TS 33.210 [7] where both client and server certificates are verified.

7 Security

7.1 Overview

All xMB-C and xMB-U traffic shall only be send over secured transport channels that are established after successful authentication and authorization as described in subclauses 5 and 6.

7.2 Authentication & Authorization

HTTP over TLS,IETF RFC 2818 [13], shall be used to authenticate both ends of the connection. The TLS 1.2 as specified in IETF RFC 5246 [14] protocol shall be used. Both client and server shall refuse connections that do not use TLS version 1.2. The authentication shall be performed using valid X.509 certificates as defined in IETF RFC 2459 [15]. Both client and server shall validate the certificate of their peer using a trusted certificate authority before establishing the secure connection.

OAuth 2.0 as specified in IETF RFC 6749 [16] shall be used to authorize all requests over the xMB-C interface. Prior to any operations on the xMB interface, the client shall obtain an access token by authorizing with the BM-SC using the following URL path:

/v1.0/authorization

Both client and server shall at least support the HTTP Basic authentication scheme as defined in IETF RFC 7235 [17]. After successful authorization, the client will receive an OAuth2.0 access token.

Editor’s Note: 3GPP Working Group SA3 shall clarify the detail procedures for authentication and authorization.

7.3 Securing the APIs

The client shall use the access token with all xMB-C requests and as long as it is valid. The access token shall be provided as part of the HTTP Authorization header field. The BM-SC shall verify the validity of the provided access token and the grants that are associated with it.

8 Notification Push to the Content Provider

8.1 Introduction

The Content Provider configures the BM-SC with a push-notification-url and push-notification-configuration property as documented in subclause 5.2.1.1, where the BM-SC can post the notifications to the Content Provider.

8.2 Notification Post

To send a notification to the Content Provider, the BM-SC shall use HTTP POST as follows:

- the request URI with the "path" part is set to: {push-notification-url} HTTP/1.1
- the Host field is set to the address of the Content Provider
- the Content-Type header field is set to “application/json”
- the body of the message is encoded in JSON format

The {push-notification-url} in the URI above is the push notification URL configured by the Content Provider when the Content Provider configures the service using procedures described in subclause 5.2.1.2. The URL shall be an HTTP over TLS URL.

The content body of the above POST request shall contain the notification that the BM-SC intends to send to the Content Provider. The representation of the notification is based on the JSON schema of notification resource as described in subclause 5.2.4.1.

Upon receipt of HTTP POST from the BM-SC to notify the Content Provider about a notification, the Content Provider shall check whether the BM-SC is authenticated and authorized to send notifications to the Content Provider. If the authorization fails, the Content Provider shall send a 401 message. If the authorization is successful, the Content Provider shall accept the notification request and respond to the BM-SC with a 200 OK message indicating that it received the notification from the BM-SC. If the request cannot be fulfilled, the Content Provider shall send a 403 Forbidden message to the BM-SC.

The possible response messages from the Content Provider, depending on whether the notification request is accepted or not, are shown in Table 8.2-1.

Table 8.2-1: Response status code, message, and contents for notification request using HTTP POST

Status Code	Message	Contents
200 OK	The request has succeeded	None
401 Unauthorized	Request requires user authentication	In accordance to conditions as described in IETF RFC 7231 [6] and IETF RFC 7235 [8]
403 Forbidden	Request cannot be fulfilled	The Content Provider may include optional text to indicate why the request could not fulfilled
Note: In addition to the above response codes, the Content Provider can also send appropriate response codes described in IETF RFC 7231 [6] as applicable.		

Editor’s Note: The detail procedure for authentication and authorization of the BM-SC by the Content Provider is to be clarified by 3GPP Working Group SA3.

Annex A (informative): Call Flows

A.1 Introduction

The xMB-C procedures are used to create and control MBMS User Services from external sources. An MBMS User Service spans from the BM-SC to the UE and can contain one or more MBMS delivery methods. The provisioning procedure offer functions to create one or more delivery sessions (such as a MBMS Download Delivery session) and allows association of the delivery sessions to MBMS Bearer Services. As part of the xMB-C procedures for MBMS User Services, content ingestion for the user-plane data (i.e. xMB-U) are negotiated. As a result of the xMB-C procedures, the BM-SC can start service announcement and activates MBMS bearer services.

The Content Provider can query its entitlements, for instance the list of broadcast areas it is authorized to use.

The Content Provider can query the status of delivery sessions.

The Content Provider can request reception statistics.

A.2 xMB Procedure example for Live DASH services (MBMS Broadcast only)

This procedure example describes the xMB procedures for a Live DASH service (see 3GPP TS 26.247 [18] for the specification of DASH services) into a single broadcast area. A push interface like WebDAV is used here as ingestion method for the user-plane data (xMB-U). The push interface is identified by a unique URI. The source of the user plane data (CP Source) are the DASH Media Segments as produced by a Live Encoder / Segmenter and the source pushes each new segment when it becomes available. The Media Presentation Description (MPD) URL and Initialization Segment (IS) for the Live DASH session is provided to BM-SC during Session creation or on a subsequent update requestseparately to the BM-SC.

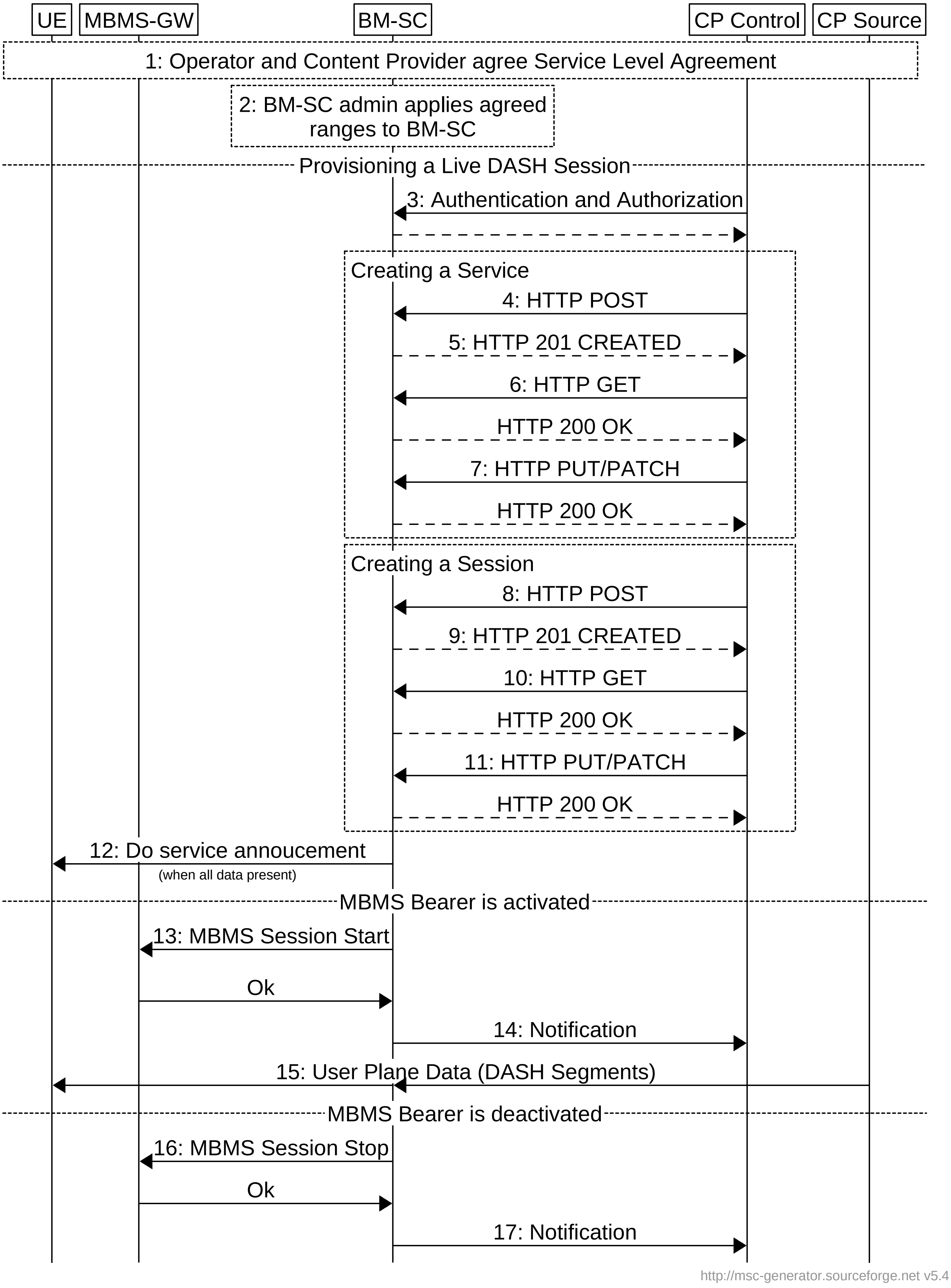
UE
MBMS-GW
BM-SC
CP Control
CP Source
1: Operator and Content Provider agree Service Level Agreement
2: BM-SC admin applies agreed ranges to BM-SC
Provisioning a Live DASH Session
3: Authentication and Authorization
Creating a Service
4: HTTP POST
5: HTTP 201 CREATED
6: HTTP GET
HTTP 200 OK
7: HTTP PUT/PATCH
HTTP 200 OK
Creating a Session
8: HTTP POST
9: HTTP 201 CREATED
10: HTTP GET
HTTP 200 OK
11: HTTP PUT/PATCH
HTTP 200 OK
12: Do service annoucement
(when all data present)
MBMS Bearer is activated
13: MBMS Session Start
Ok
14: Notification
15: User Plane Data (DASH Segments)
MBMS Bearer is deactivated
16: MBMS Session Stop
Ok
17: Notification
http://msc-generator.sourceforge.net v5.4

Figure A.2-1: xMB-C and xMB-U Procedures for a Live DASH Service

1: The operator and the Content Provider agree a Service Level Agreement (SLA), which entitles the Content Provider to use the MBMS system (in accordance to some rules) for content delivery. For instance, the SLA can include day time ranges, during which the Content Provider can distributed content. The SLA can also include geographical areas, in which the Content Provider is allowed to distribute content. The SLA also includes target bitrates and likely definitions of tolerable losses per service.

2: The BM-SC administrators (operator) apply the agreed ranges. This can imply to add additional Service Areas, and other system related configurations.

The Content Provider provisioning a single Live DASH session in a single broadcast area.

3: The Content Provider authenticates itself as authorized user. The Content Provider can only see those configurations, sessions and services, which belong to the Content Provider. On successful authentication, an access token is provided to Content Provider and shall be present in every subsequent message sent by Content Provider to BM-SC.

4: The Content Provider creates a new Service. The access token is provided by the Content Provider as input to the BM-SC. Optionally, the Content Provider may provide properties for the service like service class, service languages, service names, notification configuration as well as consumption reporting configuration. The Content Provider can select whether the Content Provider or the operator distributes service announcement by providing a list of Service Announcement Channel (SACH, as defined in Annex L.2 / L.3 of 3GPP TS 26.346 [3]) services used for operator-driven service announcement.

NOTE 1: BM-SC derives the required UE capabilities from the provided service and session properties.

5: Upon successful service creation by the BM-SC, the BM-SC shall provide a unique id of the service resource, that the Content Provider shall use for subsequent requests.

6: The Content Provider retrieves the current service properties. The access token and the unique resource id of the service are provided by the Content Provider as input to the BM-SC. The BM-SC responds with the service properties.

7: The Content Provider updates service properties. The access token, the unique resource id of the service and some or all service properties are provided by the Content Provider as input to the BM-SC

8: The Content Provider creates a session for the previously created service. The access token and the unique resource id of the service are provided by the Content Provider as input to the BM-SC. Optionally, the Content Provider may provide common session properties like: max ingest bitrate (excluding any FEC redundancy and transport overhead), scheduling information (start time, stop time), QoE Reporting configuration and session type (set to Application) as input. DASH specific session properties provided as input by Content Provider: MIME-type of MPD fragment (i.e. here set to application/dash+xml), Application Entry Point URL (i.e. here the MPD URL), xMB-U ingest mode (push/pull), Unicast Delivery Indicator, Components.

NOTE 2: BM-SC allocates following parameters for the SDP of the MBMS User Service: TMGI, FLUTE IP Multicast Address, UDP Port and TSI (see IETF RFC 3926 [19]).

NOTE 3: BM-SC derives the SAI list for the MBMS Service Area from Geographical Area provided in Content Provider request and from PLMN id negotiated in step 1. FEC information (codec and ratio) and MBMS Bearer QoS (ARP, QCI) are also negotiated in step 1.

NOTE 4: The Service Announcement start time can be provided in request. If not, BM-SC starts announcing service as soon as all required service and session properties are provided by Content Provider.

NOTE 5: In the case of regional services, i.e. that deliver region specific content, a session can be cloned so that all sessions of user service use same FLUTE parameters.

9: A unique resource id of the session, which identifies the created session, is responded. Additionally, the push URL (here, the required xMB-U ingest mode is set to push) and QoE Report URL are added to the response.

10: The Content provider queries the session configuration, providing the resource ids of the session and service. The Content Provider needs here the Push URL to configure the DASH segmenter.The BM-SC provides the information in response. All readable session properties are provided in response.

11: The Content Provider updates the session by providing here the DASH MPD URL (Application Entry Point URL). The BM-SC sends response with update status.

12: Once all information for service announcement is available, and if service announcement start time is ellapsed, the BM-SC starts announcing the service automatically. Service announcement is automatically updated following subsequent session updates.

The BM-SC activates automatically the MBMS Bearer at session start time. See 3GPP TS 26.346 [3] and 3GPP TS 29.061 [20] for further details.

13: The BM-SC activates the MBMS bearer by providing the TMGI, the Flow ID, the MBMS Service Area (MSA), the GBR and other parameters to the MBMS-GW.

14: When the Content Provider has configured a Notification URL for the service, the BM-SC notifies the Content Provider.

15: When the MBMS bearer is activated, then the BM-SC starts forwarding the xMB-U user plane data (push interface here). Any xMB-U user plane data received before activation of the MBMS bearer can be discarded.

16: At session stop time, the MBMS bearer is terminated.

17: The BM-SC can notify the Content Provider about the termination of the MBMS Bearer.

NOTE 6: The Content Provider terminates the service, when the service is not needed anymore. All sessions, which are still created or active will be deleted automatically by BM-SC with the termination of the service.

Editor’s Note: Protocol details for the specification of notification procedures (steps 14 & 17) are FFS.

A.3 xMB Procedure example for Live DASH services (with Service Continuity)

This procedure example describes the xMB-C procedures for a Live DASH service with service continuity. See 3GPP TS 26.247 [18] for the specification of DASH services. Service continuity allows UEs to enter or leave the MBMS service areas while receiving a Live DASH service. UEs can switch to unicast as defined in Clause 7.6 of 3GPP TS 26.346 [3] when leaving the MBMS service area.

In case of service continuity support, the system offers representations via unicast and via MBMS Bearers. A Unified MPD (cf. Clause 7.6 of 3GPP TS 26.346 [3]) contains the according retrieval information. When service continuity is supported, the Content Provider provides MPD and Initialization segments for both unicast and MBMS bearer access and also the according media segments. The Content Handler functions forwards the content to a DASH (unicast) Server. The DASH (unicast) server can use a Content Delivery Network (CDN) for unicast delivery.

A push interface is used here as ingestion method for the xMB-U user-plane data. The source of the user plane data (Content Provider Source) are the DASH Media Segments as produced by a Live Encoder / Segmenter, which produces the content for unicast and MBMS bearer delivery. The Media Presentation Description (MPD) and Initialization Segment (IS) for the Live DASH session is provided separately to the BM-SC.

The Service Announcement Function (SAF) of the BM-SC creates the needed metadata fragments for the MBMS User Service. To support service continuity, the SAF adds base pattern elements to the User Service Description element. The MBMS Client in the UE matches the base pattern against a portion of the entire request URL. The SAF creates unified MPD by adding information specific elements to it. The SAF makes the service announcement information available via unicast and via MBMS.

A content handler function of the BM-SC handles the separation of unicast and MBMS bearer content. The content handler function makes the content available in operators CDN for unicast access.

A.4 xMB Procedure example for File Delivery Services (without File Schedule)

This procedure example described the provisioning procedure for a File Delivery service without any file schedule element into a single broadcast area. The file schedule element is carried in the schedule description fragment during service announcement and contains transmission timings information for each URL. Consequently, the file URLs must be present when creating service announcement information.

This example assumes that the BM-SC automatically fetches the file using a pull method (xMB-U mode) and prepares the transmission. File URLs can be provided in session creation request or any subsequent session update request.When file preparation ends after session start time, the file is automatically added to user plane flow. It is up to Content Provider to secure that session scheduling is large enough to allow files preparation and transmission according to bitrate between BM-SC and file location, and bitrate of user plane.

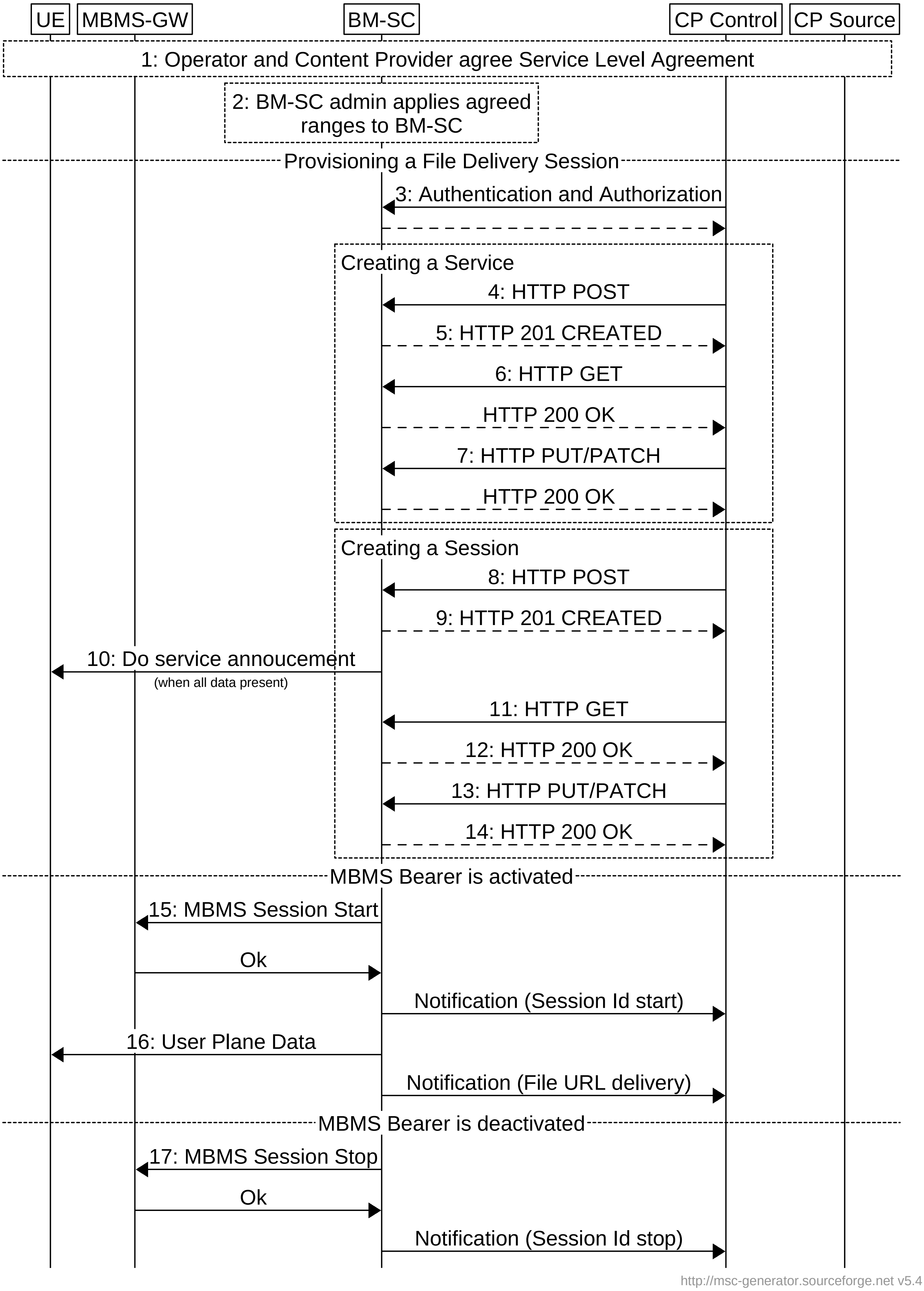
UE
MBMS-GW
BM-SC
CP Control
CP Source
1: Operator and Content Provider agree Service Level Agreement
2: BM-SC admin applies agreed ranges to BM-SC
Provisioning a File Delivery Session
3: Authentication and Authorization
Creating a Service
4: HTTP POST
5: HTTP 201 CREATED
6: HTTP GET
HTTP 200 OK
7: HTTP PUT/PATCH
HTTP 200 OK
Creating a Session
8: HTTP POST
9: HTTP 201 CREATED
10: Do service annoucement
(when all data present)
11: HTTP GET
12: HTTP 200 OK
13: HTTP PUT/PATCH
14: HTTP 200 OK
MBMS Bearer is activated
15: MBMS Session Start
Ok
Notification (Session Id start)
16: User Plane Data
Notification (File URL delivery)
MBMS Bearer is deactivated
17: MBMS Session Stop
Ok
Notification (Session Id stop)
http://msc-generator.sourceforge.net v5.4

Figure A.4 -1: xMB-C and xMB-U Procedures for a File Delivery Service

1: The operator and the Content Provider agree a Service Level Agreement (SLA), which entitles the Content Provider to use the MBMS system (in accordance to some rules) for content delivery. For instance, the SLA can include day time ranges, during which the Content Provider can distributed content. The SLA can also include geographical areas, in which the Content Provider is allowed to distribute content. The SLA also includes target bitrates and likely definitions of tolerable losses per service.

2: The BM-SC administrators (operator) apply the agreed ranges. This can imply to add additional Service Areas, and other system related configurations.

The Content Provider provisioning a file delivery session in a single broadcast area.

3: The Content Provider authenticates itself as authorized user. The Content Provider can only see those configurations, sessions and services, which belong to the Content Provider. On successful authentication, an access token is provided to CP and shall be present in every subsequent message sent by the Content Provider to BM-SC.

4: The Content Provider creates a new service. The access token is provided by the Content Provider as input to the BM-SC. Optionally, the Content Provider may provide properties for the service like service class, service languages, service names, notification configuration as well as consumption reporting configuration. The Content Provider can select whether the Content Provider or the operator distributes service announcement by providing a list of Service Announcement Channel (SACH, as defined in Annex L.2 / L.3 of 3GPP TS 26.346 [3]) services used for operator-driven service announcement.

NOTE 1: BM-SC derives the required UE capabilities from the provided service and session properties.

5: Upon successful service creation by the BM-SC, the BM-SC shall provide a unique resource id of the service, that the Content Provider can use for subsequent requests.

6: The Content Provider retrieves the current service properties. The access token and the unique resource id of the service are provided by the Content Provider as input to the BM-SC. The BM-SC responds with the service properties.

7: The Content Provider updates service properties. The access token, the unique resource id of the service and some or all service properties are provided by the Content Provider as in put to the BM-SC

8: The Content Provider creates a session for previously created service. The access token and the unique resource id of the service are provided by the Content Provider as input to the BM-SC. Optionally, the Content Provider may provide common session properties like max ingest bitrate (excluding any FEC redundancy and transport overhead), scheduling information (start time, stop time), Geographical Area and QoE Reporting configuration and session type (set to Files) as input. File specific session properties provided as input by Content Provider: xMB-U ingest mode (pull/push), file list if xMB-U pull mode.

NOTE 2: BM-SC allocates following parameters for SDP of the MBMS User Service: TMGI, FLUTE IP Multicast Address, UDP Port and TSI (see 3GPP TS 26.346 [3]).

NOTE 3: BM-SC derives the SAI list for the MBMS Service Area from Geographical Area provided in Content Provider request and from PLMN id negotiated in step 1. FEC information (codec and ratio) and MBMS Bearer QoS (ARP, QCI) are also negotiated in step 1.

NOTE 4: In xMB-U pull ingest mode, file URLs can be provided now (i.e. at session resource creation) or at a later stage (e.g. while the session is active) through the Session Update xMB-C procedure.

NOTE 5: Service Announcement start time can be provided in request. If not, BM-SC starts annoucing service as soon as all required service and session properties are provided by Content Provider

NOTE 6: In the case of regional services, i.e. that deliver region specific content, a session can be cloned so that all Sessions of user service use same FLUTE parameters.

9: A unique resource id of the session, which identifies the created Session, is responded. If xMB-U push ingest mode is used, BM-SC provides also the push URL the Content Provider shall use.

NOTE 7: For file URLs provided in session creation request, the BM-SC starts automatically to fetch the file resource(s) from the content location when file earliest fetch time elapses and generates the FLUTE and FEC symbols (if any). The BM-SC can notify the Content Provider when the process is finalized.

10: Once all information for service announcement is available, and if service announcement start time is elapsed, the BM-SC starts announcing the service automatically. Service announcement is automatically updated following subsequent Session updates. File schedule element can be present in Schedule fragment for files URLs provided in Session creation request.

11: The Content Provider queries the Session configuration, providing the resource ids of the session and service.

12: The BM-SC provides the information in response.

13: The Content Provider updates session by providing additional File URLs.

14: The BM-SC sends response with update status.

NOTE 8: The BM-SC starts automatically to fetch the new file resource(s) from the content location when file earliest fetch time elapses and generates the FLUTE and FEC symbols (if any). The BM-SC can notify the Content Provider when the process is finalized.

NOTE 9: Steps 9-12 can be executed at any time after Session is created and prior to the Session stop time. Any file URL added after Session start time will be automatically fetched, processed and sent on user plane.

The BM-SC activates automatically the MBMS Bearer at session start time.

15: The BM-SC activates the MBMS bearer by providing the TMGI, the Flow ID, the MBMS Service Area (MSA), the GBR and other parameters to the MBMS-GW. The BM-SC can notify the Content Provider about the activation of the MBMS Bearer.

16: When the MBMS Broadcast bearer is activated, then the BM-SC starts sending the user plane data, according to target reception completion time. The BM-SC can notify Content Provider of file delivery start/end.

17: At session stop time, the MBMS bearer is terminated. The BM-SC can notify the Content Provider about the termination of the MBMS Bearer.

NOTE 10: The Content Provider terminates the service. All sessions, which are still created or active will be deleted automatically by BM-SC with the termination of the service.

Editor’s Note: Protocol details for the specification of notification procedures (steps 14 & 17) are FFS.

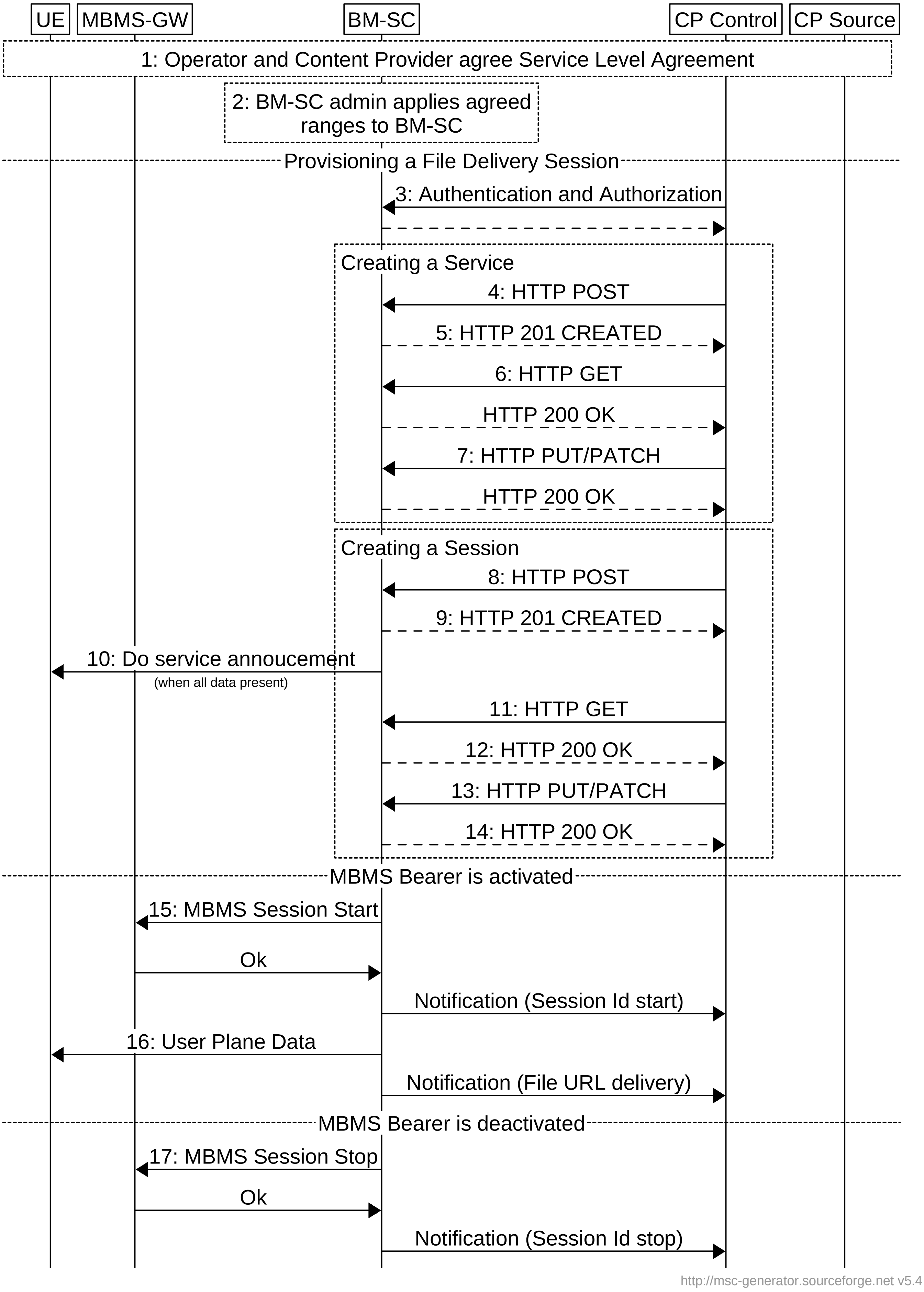
UE
MBMS-GW
BM-SC
CP Control
CP Source
1: Operator and Content Provider agree Service Level Agreement
2: BM-SC admin applies agreed ranges to BM-SC
Provisioning a File Delivery Session
3: Authentication and Authorization
Creating a Service
4: HTTP POST
5: HTTP 201 CREATED
6: HTTP GET
HTTP 200 OK
7: HTTP PUT/PATCH
HTTP 200 OK
Creating a Session
8: HTTP POST
9: HTTP 201 CREATED
10: Do service annoucement
(when all data present)
11: HTTP GET
12: HTTP 200 OK
13: HTTP PUT/PATCH
14: HTTP 200 OK
MBMS Bearer is activated
15: MBMS Session Start
Ok
Notification (Session Id start)
16: User Plane Data
Notification (File URL delivery)
MBMS Bearer is deactivated
17: MBMS Session Stop
Ok
Notification (Session Id stop)
http://msc-generator.sourceforge.net v5.4

Figure A.3-1: xMB-C and xMB-U Procedures for a File Delivery Service

1: The operator and the Content Provider agree a Service Level Agreement (SLA), which entitles the Content Provider to use the MBMS system (in accordance to some rules) for content delivery. For instance, the SLA can include day time ranges, during which the Content Provider can distributed content. The SLA can also include geographical areas, in which the Content Provider is allowed to distribute content. The SLA also includes target bitrates and likely definitions of tolerable losses per service.

2: The BM-SC administrators (operator) apply the agreed ranges. This can imply to add additional Service Areas, and other system related configurations.

The Content Provider provisioning a file delivery session in a single broadcast area.

3: The Content Provider authenticates itself as authorized user. The Content Provider can only see those configurations, sessions and services, which belong to the Content Provider. On successful authentication, an access token is provided to CP and shall be present in every subsequent message sent by the Content Provider to BM-SC.

4: The Content Provider creates a new service. The access token is provided by the Content Provider as input to the BM-SC. Optionally, the Content Provider may provide properties for the service like service class, service languages, service names, notification configuration as well as consumption reporting configuration. The Content Provider can select whether the Content Provider or the operator distributes service announcement by providing a list of Service Announcement Channel (SACH, as defined in Annex L.2 / L.3 of 3GPP TS 26.346 [3]) services used for operator-driven service announcement.

Note 1: BM-SC derives the required UE capabilities from the provided service and session properties.

5: Upon successful service creation by the BM-SC, the BM-SC shall provide a unique resource id of the service, that the Content Provider can use for subsequent requests.

6: The Content Provider retrieves the current service properties. The access token and the unique resource id of the service are provided by the Content Provider as input to the BM-SC. The BM-SC responds with the service properties.

7: The Content Provider updates service properties. The access token, the unique resource id of the service and some or all service properties are provided by the Content Provider as in put to the BM-SC

8: The Content Provider creates a session for previously created service. The access token and the unique resource id of the service are provided by the Content Provider as input to the BM-SC. Optionally, the Content Provider may provide common session properties like max ingest bitrate (excluding any FEC redundancy and transport overhead), scheduling information (start time, stop time), Geographical Area and QoE Reporting configuration and session type (set to Files) as input. File specific session properties provided as input by Content Provider: xMB-U ingest mode (pull/push), file list if xMB-U pull mode.

Note 2: BM-SC allocates following parameters for SDP of the MBMS User Service: TMGI, FLUTE IP Multicast Address, UDP Port and TSI (see IETF RFC 3926 [19]).

Note 3: BM-SC derives the SAI list for the MBMS Service Area from Geographical Area provided in Content Provider request and from PLMN id negotiated in step 1. FEC information (codec and ratio) and MBMS Bearer QoS (ARP, QCI) are also negotiated in step 1.

Note 4: In xMB-U pull ingest mode, file URLs can be provided now (i.e. at session resource creation) or at a later stage (e.g. while the session is active) through the Session Update xMB-C procedure.

Note 5: Service Announcement start time can be provided in request. If not, BM-SC starts annoucing service as soon as all required service and session properties are provided by Content Provider

Note 6: In the case of regional services, i.e. that deliver region specific content, a session can be cloned so that all Sessions of user service use same FLUTE parameters.

9: A unique resource id of the session, which identifies the created Session, is responded. If xMB-U push ingest mode is used, BM-SC provides also the push URL the Content Provider shall use.

Note 7: For file URLs provided in session creation request, the BM-SC starts automatically to fetch the file resource(s) from the content location when file earliest fetch time elapses and generates the FLUTE and FEC symbols (if any). The BM-SC can notify the Content Provider when the process is finalized.

10: Once all information for service announcement is available, and if service announcement start time is elapsed, the BM-SC starts announcing the service automatically. Service announcement is automatically updated following subsequent Session updates. File schedule element can be present in Schedule fragment for files URLs provided in Session creation request.

11: The Content Provider queries the Session configuration, providing the resource ids of the session and service.

12: The BM-SC provides the information in response.

13: The Content Provider updates session by providing additional File URLs.

14: The BM-SC sends response with update status.

Note 8: The BM-SC starts automatically to fetch the new file resource(s) from the content location when file earliest fetch time elapses and generates the FLUTE and FEC symbols (if any). The BM-SC can notify the Content Provider when the process is finalized.

Note 9: Steps 9-12 can be executed at any time after Session is created and prior to the Session stop time. Any file URL added after Session start time will be automatically fetched, processed and sent on user plane.

The BM-SC activates automatically the MBMS Bearer at session start time.

15: The BM-SC activates the MBMS bearer by providing the TMGI, the Flow ID, the MBMS Service Area (MSA), the GBR and other parameters to the MBMS-GW. The BM-SC can notify the Content Provider about the activation of the MBMS Bearer.

16: When the MBMS Broadcast bearer is activated, then the BM-SC starts sending the user plane data, according to target reception completion time. The BM-SC can notify Content Provider of file delivery start/end.

17: At session stop time, the MBMS bearer is terminated. The BM-SC can notify the Content Provider about the termination of the MBMS Bearer.

Note 10: The Content Provider terminates the service. All sessions, which are still created or active will be deleted automatically by BM-SC with the termination of the service.

Editor’s Note: Protocol details for the specification of notification procedures (steps 14 & 17) are FFS.

Annex B (normative): JSON Schema

```
{
   "swagger":"2.0",
   "info":{
      "title":"BM-SC API",
      "description":"BM-SC Content Provider ingestion API",
      "version":"1.0"
   },
   "host":"<xMB_Entry_Point>",
   "schemes":[
      "https"
   ],
   "basePath":"/xmb/v1.0",
   "produces":[
      "application/json"
   ],
   "paths":{
      "/services":{
         "get":{
            "description":"Return all supported services",
            "produces":[
               "application/json"
            ],
            "responses":{
               "200":{
                  "description":"A list of services.",
                  "schema":{
                     "type":"array",
                     "items":{
                        "$ref":"#/definitions/Service"
                     }
                  }
               },
          "default":{
            "description":"Unexpected error",
            "schema":{
              "$ref":"#/definitions/Error"
            }
          }
        }
      },
      "post":{
        "description":"Creates a service",
        "produces":[
          "application/json"
        ],
        "responses":{
          "201":{
            "description":"Service successfully created..",
            "schema":{
              "$ref":"#/definitions/services-response"
            }
          },
          "401":{
            "description":"Request requires user authentication"
          },
          "403":{
            "description":"Request cannot be fulfilled"
          }
        }
      }
    },
    "/services/{service-id}":{
      "get":{
        "description":"Returns resource for a given service-id",
        "produces":[
          "application/json"
        ],
        "parameters":[
          {
            "name":"service-id",
            "in":"path",
            "description":"Service Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          }
        ],
        "responses":{
          "200":{
            "description":"OK.",
            "schema":{
              "$ref":"#/definitions/Service"
            }
          }
        }
      },
      "patch":{
        "description":"Update a service",
        "produces":[
          "application/json"
        ],
        "parameters":[
          {
            "name":"body",
            "in":"body",
            "required":true,
            "description":"Service that needs to be created",
            "schema":{
              "$ref":"#/definitions/Service"
            }
          },
          {
```

```
      "name":"service-id",
      "in":"path",
      "description":"Service Id",
      "required":true,
      "type":"integer",
      "format":"int32"
    }
  ],
  "responses":{
    "200":{
      "description":"The request has succeeded"
    },
    "401":{
      "description":"Request requires user authentication"
    },
    "403":{
      "description":"Request cannot be fulfilled"
    },
    "404":{
      "description":"Request not found"
    }
  }
},
"put":{
  "description":"Updates a service",
  "produces":[
    "application/json"
  ],
  "parameters":[
    {
      "name":"body",
      "in":"body",
      "required":true,
      "description":"Service that needs to be created",
      "schema":{
        "$ref":"#/definitions/Service"
      }
    },
    {
      "name":"service-id",
      "in":"path",
      "description":"Service Id",
      "required":true,
      "type":"integer",
      "format":"int32"
    }
  ],
  "responses":{
    "200":{
      "description":"The request has succeeded"
    },
    "401":{
      "description":"Request requires user authentication"
    },
    "403":{
      "description":"Request cannot be fulfilled"
    },
    "404":{
      "description":"Request not found"
    }
  }
},
"delete":{
  "description":"Delete a service",
  "produces":[
    "application/json"
  ],
  "parameters":[
    {
      "name":"service-id",
        "in":"path",
        "description":"Service Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      }
    ],
    "responses":{
      "200":{
        "description":"The request has succeeded"
      },
      "401":{
        "description":"Request requires user authentication"
      },
      "403":{
        "description":"Request cannot be fulfilled"
      },
      "404":{
        "description":"Request not found"
      }
    }
  }
},
"/services/{service-id}/sessions":{
  "get":{
    "description":"Return all sessions of a given service",
    "produces":[
      "application/json"
    ],
    "parameters":[
      {
        "name":"service-id",
        "in":"path",
        "description":"Service Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      }
    ],
    "responses":{
      "200":{
        "description":"A list of sessions.",
        "schema":{
          "type":"array",
          "items":{
            "$ref":"#/definitions/Session"
          }
        }
      },
      "default":{
        "description":"Unexpected error",
        "schema":{
          "$ref":"#/definitions/Error"
        }
      }
    }
  },
  "post":{
    "description":"Create a session for a given service",
    "produces":[
      "application/json"
    ],
    "parameters":[
      {
        "name":"service-id",
        "in":"path",
        "description":"Service Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      }
    ],
    "responses":{
      "201":{
        "description":"Session successfully created..",
        "schema":{
          "$ref":"#/definitions/session-response"
        }
      },
      "401":{
        "description":"Request requires user authentication"
      },
      "403":{
        "description":"Request cannot be fulfilled"
      }
    }
  }
},
"/services/{service-id}/sessions/{session-id}":{
  "get":{
    "description":"Return a session of a given service",
    "produces":[
      "application/json"
    ],
    "parameters":[
      {
        "name":"service-id",
        "in":"path",
        "description":"Service Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      },
      {
        "name":"session-id",
        "in":"path",
        "description":"Session Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      }
    ],
    "responses":{
      "200":{
        "description":"OK.",
        "schema":{
          "$ref":"#/definitions/Session"
        }
      }
    }
  },
  "patch":{
    "description":"Updates a session of a given service",
    "produces":[
      "application/json"
    ],
    "parameters":[
      {
        "name":"body",
        "in":"body",
        "required":true,
        "description":"Session that needs to be created",
        "schema":{
          "$ref":"#/definitions/Session"
        }
      },
      {
        "name":"service-id",
        "in":"path",
        "description":"Service Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      },
      {
        "name":"session-id",
        "in":"path",
        "description":"Session Id",
        "required":true,
        "type":"integer",
        "format":"int32"
      }
    ],
    "responses":{
      "200":{
        "description":"The request has succeeded"
      },
      "401":{
        "description":"Request requires user authentication"
      },
      "403":{
        "description":"Request cannot be fulfilled"
      },
      "404":{
        "description":"Request not found"
      }
    }
  },
  "put":{
    "description":"Update a session of a given service",
    "produces":[
      "application/json"
    ],
    "parameters":[
      {
```

```
    "name":"body",
    "in":"body",
    "required":true,
    "description":"Session that needs to be created",
    "schema":{
      "$ref":"#/definitions/Session"
    }
  },
  {
    "name":"service-id",
    "in":"path",
    "description":"Service Id",
    "required":true,
    "type":"integer",
    "format":"int32"
  },
  {
    "name":"session-id",
    "in":"path",
    "description":"Session Id",
    "required":true,
    "type":"integer",
    "format":"int32"
  }
],
"responses":{
  "200":{
    "description":"The request has succeeded"
  },
  "401":{
    "description":"Request requires user authentication"
  },
  "403":{
    "description":"Request cannot be fulfilled"
  },
    "404":{
      "description":"Request not found"
    }
  }
},
"delete":{
  "description":"Delete a session of a given service",
  "produces":[
    "application/json"
  ],
  "parameters":[
    {
      "name":"service-id",
      "in":"path",
      "description":"Service Id",
      "required":true,
      "type":"integer",
      "format":"int32"
    },
    {
      "name":"session-id",
      "in":"path",
      "description":"Session Id",
      "required":true,
      "type":"integer",
      "format":"int32"
    }
  ],
  "responses":{
    "200":{
      "description":"The request has succeeded"
    },
    "401":{
      "description":"Request requires user authentication"
    },
          "403":{
            "description":"Request cannot be fulfilled"
          },
          "404":{
            "description":"Request not found"
          }
        }
      }
    },
    "/services/{service-id}/reports":{
      "get":{
        "description":"Returns all reports of a given service",
        "produces":[
          "application/json"
        ],
        "parameters":[
          {
            "name":"service-id",
            "in":"path",
            "description":"Service Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          }
        ],
        "responses":{
          "200":{
            "description":"A list of reports.",
            "schema":{
              "type":"array",
              "items":{
                "$ref":"#/definitions/Report"
              }
            }
          },
          "401":{
            "description":"Request requires user authentication"
          },
          "403":{
            "description":"Request cannot be fulfilled"
          },
          "404":{
            "description":"Request not found"
          },
          "default":{
            "description":"Unexpected error",
            "schema":{
              "$ref":"#/definitions/Error"
            }
          }
        }
      }
    },
    "/services/{service-id}/reports/{report-id}":{
      "get":{
        "description":"Returns all reports of a given service",
        "produces":[
          "application/json"
        ],
        "parameters":[
          {
            "name":"service-id",
            "in":"path",
            "description":"Service Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          },
          {
            "name":"report-id",
            "in":"path",
            "description":"Report Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          }
        ],
        "responses":{
          "200":{
            "description":"A report with given report-id",
            "schema":{
              "$ref":"#/definitions/Report"
            }
          },
          "401":{
            "description":"Request requires user authentication"
          },
          "403":{
            "description":"Request cannot be fulfilled"
          },
          "404":{
            "description":"Request not found"
          },
          "default":{
            "description":"Unexpected error",
            "schema":{
              "$ref":"#/definitions/Error"
            }
          }
        }
      }
    },
    "/services/{service-id}/sessions/{session-id}/reports":{
      "get":{
        "description":"Return all reports of a given session of a given service",
        "produces":[
          "application/json"
        ],
        "parameters":[
          {
            "name":"service-id",
            "in":"path",
            "description":"Service Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          },
          {
            "name":"session-id",
            "in":"path",
            "description":"Session Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          }
        ],
        "responses":{
          "200":{
            "description":"OK.",
            "schema":{
              "$ref":"#/definitions/Report"
            }
          },
          "401":{
            "description":"Request requires user authentication"
          },
          "403":{
            "description":"Request cannot be fulfilled"
          },
          "404":{
```

```
            "description":"Request not found"
          }
        }
      }
    },
    "/services/{service-id}/sessions/{session-id}/reports/{report-id}":{
      "get":{
        "description":"Return all reports of a given session of a given service",
        "produces":[
          "application/json"
        ],
        "parameters":[
          {
            "name":"service-id",
            "in":"path",
            "description":"Service Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          },
          {
            "name":"session-id",
            "in":"path",
            "description":"Session Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          },
          {
            "name":"report-id",
            "in":"path",
            "description":"Report Id",
            "required":true,
            "type":"integer",
            "format":"int32"
          }
        ],
        "responses":{
          "200":{
            "description":"OK.",
            "schema":{
              "$ref":"#/definitions/Report"
            }
          },
          "401":{
            "description":"Request requires user authentication"
          },
          "403":{
            "description":"Request cannot be fulfilled"
          },
          "404":{
            "description":"Request not found"
          }
        }
      }
    },
    "/notifications":{
      "get":{
        "description":"Returns all notifications.",
        "produces":[
          "application/json"
        ],
        "responses":{
          "200":{
            "description":"A list of notifications.",
            "schema":{
              "type":"array",
              "items":{
                "$ref":"#/definitions/Notification"
              }
            }
          },
          "401":{
            "description":"Request requires user authentication"
          },
          "403":{
            "description":"Request cannot be fulfilled"
          },
          "default":{
            "description":"Unexpected error",
            "schema":{
              "$ref":"#/definitions/Error"
            }
          }
        }
      }
    }
  },
  "definitions":{
    "Service":{
      "type":"object",
      "description":"Service Description",
      "properties":{
        "id":{
          "type":"number",
          "description":"Service Resource Identifier"
        },
        "service-id":{
          "type":"string",
          "description":"Identifies the MBMS User Service as defined in Clause 11.2.1.1."
        },
        "service-class":{
          "description":"Service Class",
          "type":"string"
        },
        "service-languages":{
          "type":"array",
          "description":"List of service languages",
          "items":{
            "type":"string"
          }
        },
        "service-names":{
          "type":"array",
          "description":"List of service names",
          "items":{
            "type":"string"
          }
        },
        "service-announce-mode":{
          "description":"Enumeration that the BM-SC creates according service announcement fragments for the sessions and / or do service announcement on SACH. Additional service announcement modes may be added in future",
          "type":"string"
        },
        "consumption-reporting-configuration":{
          "type":"object",
          "description":"The Content Provider wishes to collect consumption reports (enabling precision, i.e. combination of sample percentage and reporting interval)",
          "properties":{
            "reporting-interval":{
              "type":"number",
              "description":"The interval for which the BM-SC has to aggregate the statistics for"
            },
            "sample-percentage":{
              "type":"number",
              "description":"Percentage of users to collect reports from"
            },
            "start-time":{
              "type":"string",
              "description":"Start time of consumption report collection"
            },
            "end-time":{
              "type":"string",
              "description":"End time of consumption report collection"
            }
          }
        },
        "push-notification-url":{
          "type":"string",
          "description":"The Content Provider provides Notification URL over which it will receive notifications
“pushed” by the BM-SC. The Notification procedure is described in Clause 5.4A.4.6."
        },
        "push-notification-configuration":{
          "type":"string",
          "description":"If the Content Provider enables push delivery of notifications, then the Content Provider may
provide notification filters. This parameter contains a comma separated list of Classes it wishes to receive among the
following options: Critical, Warning, Information, Service, Session, or All to get all types of notification. The
notification message shall be sent immediately to the Content Provider upon becoming available."
        }
      }
    },
    "services-response": {
            "required": [
                "service-res-id"
            ],
            "properties": {
                "service-res-id": {
                    "type": "integer",
      "format": "int32",
      "description": "The resource identifier of the service."
                }
            }
        },
    "Session":{
      "type":"object",
      "description":"Session Description",
      "properties":{
        "id":{
          "type":"string",
          "description":"Session Resource Identifier"
        },
        "session-start":{
          "description":"Start time when the MBMS Bearer is active",
          "type":"number"
        },
        "session-stop":{
          "description":"Stop time until the MBMS bearer is active",
          "type":"number"
        },
        "max-ingest-bitrate":{
          "description":"The requested bitrate excludes FEC overhead and transport overhead. The BM-SC calculates the MBMS Bearer bitrate from it, considering overhead like FEC and other transport overheads. The session bitrate is always larger or equal to the payload bitrate",
          "type":"number",
          "format":"float"
        },
        "max-delay":{
          "description":"Specifies the maximum delay the MBMS System should add, i.e. from the time the data is received to the time by when the data is released from the MBMS system",
          "type":"number",
          "format":"float"
        },
        "session-state":{
          "description":"The BM-SC may automatically change the state of the session. Possible states: Session Idle, Session Announced, Session Active",
          "type":"string"
        },
        "service-announcement-start-time":{
          "description":"When present, this time at which the BM-SC shall start service announcement",
          "type":"number"
        },
        "geographical-area":{
          "description":"Geographics Area, where the service is provided, either through unicast or through MBMS Bearers. The BM-SC derives the MBMS Service Area and the SAI list for the availability information from Geographical Area as provided by the Content Provider. The content of each string item is left to the business agreement between the Content Provider and the Operator.",
          "type":"array",
          "items":{
            "type":"string"
          }
        },
        "qoe-reporting-configuration":{
          "type":"array",
          "description":"The Content Provider wishes to collect QoE reports for this session. If this configuration is included, the QoE reporting configuration shall be applied only for this session. If this configuration is present, the Content Provider requests overriding of service level configuration for this session with this configuration. The possible QoE metrics that the Content Provider may request can be either found in or derived from sub-clauses 8.4.2 and 10 of 3GPP TS 26.347 [21], as well as the reception reporting information that is available in sub-clause 9.4.6 of 3GPP TS 26.346 [3]. The detailed or aggregated reports shall not contain information such as clientId, which might pose privacy concerns, or networkResourceCellId, which would expose mobile network information.",
          "items":{
            "type":"object",
            "description":"QoE metric configuration",
            "properties":{
              "metric-name":{
                "type":"string",
                "description":"Name of QoE metric"
              },
              "metric-type":{
                "type":"string",
                "description":"Type of metric"
              },
              "reporting-interval":{
                "type":"number",
                "description":"The interval for which the BM-SC has to aggregate the statistics for"
              },
              "sample-percentage":{
                "type":"number",
                "description":"Percentage of users to collect reports from"
              },
              "start-time":{
                "type":"string",
                "description":"Start time of consumption report collection"
              },
              "end-time":{
                "type":"string",
                "description":"End time of consumption report collection"
              }
            }
          }
        },
        "session-type":{
          "description":"The session type is how the Content Provider is providing the content to the BM-SC. The BM-SC is selecting the appropriate delivery methods from the session type. The session type shall be extensible for further session types",
          "type":"string",
          "enum":[
            "Streaming: When the session type is set to Streaming, the BM-SC expects a Streaming type input (RTP). When the method is set to streaming, then the format is compliant to MBMS streaming (as defined in 3GPP TS 26.346 [3]).",
            "Files: When the session type is set to Files, the BM-SC expects generic files as input. The files can be provided either by on-request pull interactions or continuous push ingest",
            "Application: When the session type is set to Application, then the ingest depends on the application service description. When the Application Service Description is set to DASH, the BM-SC expects an MPD and optionally one or more IS’s. The content is assumed to be 3GP-DASH compliant (as defined by 3GPP TS 26.247). The BM-SC may either pull the Media Segments from the Content Provider or the Content Provider continuously pushes Segments into the BM-SC",
            "Transport-Mode: When the session type is set to Transport-Mode, the BM-SC provides transport of data/TV content in a transparent manner. The content provide may provide some configuration parameters for the distributions"
          ]
        },
        "transport-mode-session":{
          "description":"Describes a transport mode session",
          "type":"object",
          "properties":{
            "session-announcement-mode":{
              "description":"The session announcement mode is either Other or MBMS",
              "type":"string",
              "enum":[
                "Other: the BMSC generates the session parameters and provides those to the Content Provider.",
                "MBMS: the session announcement is done by the MBMS system through the SACH."
              ]
```

```
        },
        "userplane-session-description-parameters":{
          "description":"The session description parameters for the user plane provide the information on where and how the to access the session at the Content Provider. The parameters Type and Access URL. Note the BM-SC may get input on session properties from the Content Provider, e.g. bitrate, dependening on the ingest session.",
          "type":"object",
          "properties":{
            "session-description-type":{
              "type":"string",
              "description":"The type of the session that describes the session, typically for proper interpretation of the Location element, for example the Internet Media Type of the document, of the URL in an HTTP URL."
            },
            "session-description-access-url":{
              "type":"string",
              "description":"A URL that enables to access and possibly control the ingest session. The URL may for example be an RTSP URL or a URL to an SDP that describes a multicast stream or an HTTP URL to retrieve a ready packaged MPEG2-TS stream, etc."
            }
          }
        },
        "userplane-delivery-mode-configuration":{
          "description":"This mode configures how the session needs to be delivered to the application, i.e. it basically establishes the delivery mode",
          "type":"string",
          "enum":[
            "Forward-only: The BM-SC receives complete IP Multicast packets for to be forwarded",
            "Proxy: Proxy the incoming UDP payloads to the outgoing UDP payloads"
          ]
        },
        "delivery-session-description-parameters":{
          "description":"If the Service Announcement Mode is set to Other, then at least the following information is provided by the BM-SC: TMGI of the MBMS Bearer. Note that additional parameters may be provided, based on the configuration options of the delivery method for transport only.",
          "type":"string"
        }
      }
    },
    "streaming-session":{
      "description":"Describes a streming session",
      "type":"object",
      "properties":{
        "sdp-url":{
          "description":"A URL to the SDP that describes the streaming session between the Content Provider and the BM-SC, that will be used for ingesting the streaming session. The SDP shall include the RTSP links for every media session as part of the “a=control” attribute to enable RTSP control of the session. The SDP shall also contain the required bitrate for each of the media sessions. The content shall conform to the constraints of this specification.",
          "type":"string"
        },
        "time-shifting":{
          "description":"Indicates if and for how long time shifting access to the content (using unicast) may be provided for this session.",
          "type":"number"
        }
      }
    },
    "application-session":{
      "description":"Describes an application session",
      "type":"object",
      "properties":{
        "application-service":{
          "description":"Mimetype of the Application Service",
          "type":"string"
        },
        "ingest-mode":{
          "description":"The ingest mode enumerates how resources are ingested into the BM-SC",
          "type":"string",
          "enum":[
            "Pull: The BM-SC pulls the resources as described by the application entry point document. If DASH resources are Media Segments, the BM-SC pulls the Media Segments as described by the Segment availability start time from a DASH MPD.",
            "Push: The Content Provider pushes resources. The BM-SC needs to provide a push URL. If DASH resources are Media Segments, Content Provider pushes Media Segments, so that the Media Segment is available on the BM-SC according to Segment availability start time. The BM-SC needs to provide a push URL."
          ]
        },
        "application-entry-point-url":{
          "description":"The application entry point refers to an MPD when Application Service Description is set to DASH. When the Ingest Mode is set to Push, then the MPD Url refers to a DASH MPD which should be fetched, optionally conditioned and inserted into Service Announcement. When the Ingest Mode is set to Pull, then the BM-SC starts fetching the Segments using unicast.",

          "type":"string"

        },

        "push-url":{

          "description":"If the Session Type is set to Application: A resource locator for ingesting Media Segments using HTTP. The Content Provider may create additional sub-resources using WebDAV procedures. This is a read-only parameter managed by the BM-SC and only present when Ingest Mode is set to Push. If the Session Type is set to Files: This parameter contains the Push URL the Content Provider shall use when using the Push ingestion mode. This is a read-only parameter managed by the BM-SC and only present when Ingest Mode is set to Push. ",

          "type":"string"

        },

        "unicast-delivery":{

          "description":"Indicator whether the content is also available for unicast retrieval",

          "type":"boolean"

        },

        "components":{

          "description":"List of Components of the application, which are recommended to be made available on MBMS Bearers. In case of DASH, each component is identified by a representation identifier. ",

          "type":"array",

          "items":{

                   "type":"string"

          }

        }

      }

    },

    "files-session":{

      "description":"Describes a file session",

      "type":"object",

      "properties":{

        "ingest-mode":{

          "description":"The ingest mode enumerates how resources are ingested into the BM-SC",

          "type":"string",

          "enum":[

            "Pull: The Content Provider adds files URLs that the BM-SC will fetch. The Content Provider may tell the BM-SC when to start fetching the file",
            "Push: The Content Provider shall push the file to the BM-SC that will immediately process and deliver as soon as it is ready. The BM-SC may be configured to ignore all files that are pushed before session active time, or stage them. The BM-SC shall provide back to the Content Provider the URL the Content Provider shall use to push the files."

          ]

        },

        "file-list":{

          "type":"array",

          "description":"List of files to be sent. In the Push mode, the file list is not used since the BM-SC will monitor its push folder and send the files it receives on a first-come first-served basis. In Pull mode, the file list contains the following information per file entry:",

          "items":{

            "type":"object",

            "properties":{

              "file-url":{

                "type":"string",

                "description":"the URL to the file"

              },

              "file-earliest-fetch-time":{

                "type":"string",

                "description":"The BM-SC shall fetch the file no sooner than this UTC timestamp. If absent, then the file shall be present on the Content Provider server and the BM-SC may fetch it when it wants",

                "format":"date-time"

              },

              "file-size":{

                "type":"integer",

                "format":"int32",

                "description":"The Content Provider may provide the precise or an file size estimate as input. The BM-SC may update the file size once it has started to fetch the file"

              },

              "file-status":{

                "type":"string",

                "description":"Enumeration stating the state of the file. Possible values are pending, fetched, prepared, transmitting, sent",

                "enum":[

                  "pending",

                  "fetched",

                  "prepared",
                  "transmitting",
                  "sent"
                ]
              },
              "target-reception-completion-time":{
                "type":"string",
                "description":"(On the MBMS Client) hint on the due date, when the file should be completely received by the UE. The BM-SC should schedule and order the transmission etc accordingly",
                "format":"date-time"
              },
              "keep-update-interval":{
                "type":"string",
                "description":"The BM-SC checks the file resources with the given interval for changes"
              },
              "file-repeat-duration":{
                "type":"integer",
                "format":"int32",
                "description":"The number of times the file shall be sent on the session (a value of 1 means the file shall be sent only once). This counter shall be decreased each time the file has been transmitted. When equals to zero, no more file repeat is scheduled. The BM-SC may send FEC instead of source information"
              }
            }
          }
        },
        "file-delivery-manifest-url":{
          "description":"Alternative to the file list. The resource may describe scheduling information for the file",
          "type":"string"
        },
        "display-base-url": {
          "type": "string",
          "description": "When ingest mode is set to Push, the Base URL is seen by the UE."
        }
      }
    }
  }
},
"session-response": {
        "required": [
            "session-res-id"
        ],
        "properties": {
            "session-res-id": {
                "type": "integer",
   "format": "int32",
   "description": "The resource identifier of the session."
            }
        }
    },
"Report":{
  "type":"object",
  "description":"Report Description",
  "properties":{
    "id":{
      "type":"string",
      "description":"Report Resource Identifier"
    },
    "report-type":{
      "description":"Type of report",
      "type":"string"
    },
    "report-url":{
      "type":"string",
      "description":"Location of the report from where the Content Provider can retrieve the detailed report"
    },
    "report":{
      "type":"string",
      "description":"Detailed report"
    },
    "report-starttime":{
      "type":"string",
      "description":"Report collection start time"
    },
    "report-endtime":{
      "description":"Report collection end time",
      "type":"string"
    }
  }
},
"Notification": {
    "type": "object",
    "description": "Notification Description",
    "properties": {
      "id": {
        "type": "string",
        "description": "Notification Resource Identifier"
      },
      "message-class": {
        "type": "string",
        "description": "Indicates the message class of the notification",
        "enum" : ["Critical: When some event drastically prevent the proper delivery of content", "Warning: When the service can be partially delivered but quality is reduced", "Information: When the service is properly delivered but some interesting event occurred", "transmitting", "Session/Service: Information about Service/Session related parameters"]
      },
      "message-name": {
         "description": "Unique identifier of the message. Provides information about the message pertaining to the message-class of the notification",
        "type": "string",
        "enum" : ["network-is-down", "service-badly-configured", "session-badly-configured", "incoming-bitrate-exceed-session-capacity", "no-incoming-data", "qoe-report-available", "consumption-reports-available", "reception-reports-available", "service-announcement-change", "session-state-change", "file-ready-for-transmission", "file-download-started ", "file-successfully-sent", "file-fetch-error"]
      },
      "message-information": {
        "type": "object",
        "description": "A dictionary of key values containing informations linked to the notification",
        "additionalProperties": {
            "type": "string"
        }
```

```
           }
        }
     },
    "Error":{
      "type":"object",
      "properties":{
        "code":{
          "type":"integer",
          "format":"int32"
        },
        "message":{
          "type":"string"
        }
      }
    }
  }
}
```

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
01-2017						TS initial skeleton	0.0.0
01-2017						C3A170064, C3A170066, C3A170069 agreed in Adhoc	0.1.0
02-2017						Specification of the xMB user- and control-plane procedures, accompanied by the corresponding JSON schema.	0.2.0
03-2017	CT#75	CP-170102				TS sent for approval to Plenary	1.0.0
03-2017	CT#75	CP-170102				TS under change control	14.0.0

History

Document history		
V14.0.0	April 2017	Publication