ETSI TS 129 537 V17.2.0 (2023-04)

5G;
5G System;
Multicast/Broadcast Policy Control services;
Stage 3
(3GPP TS 29.537 version 17.2.0 Release 17)

Reference
RTS/TSGC-0329537vh20

Keywords
5G

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found under https://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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the stage 3 protocol and data model for the Service Based Interfaces of the Multicast/Broadcast Policy Control Services. It provides stage 3 protocol definitions and message flows, and specifies the APIs of the Multicast/Broadcast Services provided by the PCF.

The 5G System stage 2 architecture and procedures are specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]. The stage 2 architecture and procedures for 5G Multicast/Broadcast Services are specified in 3GPP TS 23.247 [14].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition are specified in 3GPP TS 29.500 [4] and 3GPP TS 29.501 [5].

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 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[5] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[6] OpenAPI: "OpenAPI Specification Version 3.0.0", https://spec.openapis.org/oas/v3.0.0.

[7] 3GPP TR 21.900: "Technical Specification Group working methods".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[10] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[11] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[12] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[13] IETF RFC 7807: "Problem Details for HTTP APIs".

[14] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[15] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[16] 3GPP TS 29.532: "5G System; 5G Multicast-Broadcast Session Management Services; Stage 3".

[17] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[18] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

[19] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[20] 3GPP TS 29.519: "5G System; Usage of the Unified Data Repository service for Policy Data, Application Data and Structured Data for Exposure; Stage 3".

[21] 3GPP TS 29.521: "5G System; Binding Support Management Service; Stage 3".

[22] IETF RFC 7396: "JSON Merge Patch".

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].

For the purpose of the present document, the terms and definitions given in clause 3 of 3GPP TS 23.247 [14] also apply, including the ones referencing other specifications.

3.2 Symbols

None.

3.3 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].

MBS	Multicast/Broadcast Service
MB-SMF	Multicast/Broadcast Session Management Function
MBSF	Multicast/Broadcast Service Function

4 Overview

In the frame of supporting Multicast/Broadcast Services (MBS), the Policy Control Function (PCF) provides services to NF service consumers (e.g. MB-SMF) via the Npcf Service Based Interface. The PCF supports for this purpose the functionalities defined in 3GPP TS 23.247 [14], i.e. MBS related Policy and Charging Control procedures.

Figures°4-1 and 4.2 depict the Multicast/Broadcast related reference architecture of the PCF respectively in SBI representation and reference point representation.

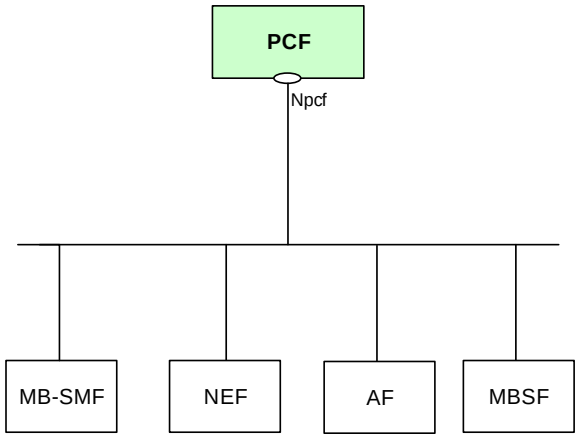

Figure 4-1: Reference model for the MBS PCF Services – SBI representation

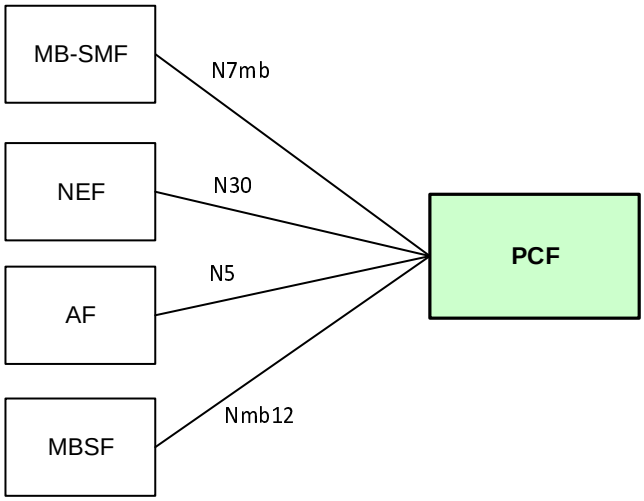

Figure 4-2: Reference Model for the MBS PCF Services – Reference point representation

5 Services offered by the PCF

5.1 Introduction

Table 5.1-1 summarizes the corresponding APIs defined for this specification.

Table 5.1-1: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Npcf_MBSPolicyControl	5.2	MBS Policy Control Service	TS29537_Npcf_MBSPolicyControl.yaml	npcf-mbspolicycontrol	A.2
Npcf_MBSPolicyAuthorization	5.3	MBS Policy Authorization Service	TS29537_Npcf_MBSPolicyAuthorization.yaml	npcf-mbspolicyauth	A.3

5.2 Npcf_MBSPolicyControl Service

5.2.1 Service Description

The MBS Session Policy Control Service enables the Policy Control Function (PCF) to provision, update and remove MBS session related policies to NF service consumers (e.g. MB-SMF), i.e.:

- enable an NF service consumer to request the creation, update and deletion of an MBS Policy Association for an MBS session; and
- enable the PCF to provision/update/remove MBS policies towards an NF service consumer.

5.2.2 Service Operations

5.2.2.1 Introduction

The service operations defined for the Npcf_MBSPolicyControl Service are shown in table 5.2.2.1-1.

Table 5.2.2.1-1: Npcf_MBSPolicyControl Operations

Service Operation Name	Description	Initiated by
Npcf_MBSPolicyControl_Create	Request the creation of an MBS Policy Association at the PCF in order to receive MBS policies for an MBS session.	NF service consumer (e.g. MB-SMF)
Npcf_MBSPolicyControl_Update	Request the update of an existing MBS Policy Association at the PCF in order to receive the updated MBS policies for an MBS session.	NF service consumer (e.g. MB-SMF)
Npcf_MBSPolicyControl_Delete	Request the deletion of an existing MBS Policy Association.	NF service consumer (e.g. MB-SMF)

5.2.2.2 Npcf_MBSPoliyControl_Create

5.2.2.2.1 General

The Npcf_MBSPolicyControl_Create service operation enables an NF service consumer (e.g. MB-SMF) to request the creation of an MBS Policy Association at the PCF and the provisioning of MBS policies for a multicast or a broadcast MBS session.

The following procedures using the Npcf_MBSPolicyControl_Create service operation are supported:

- MBS Policy Association Establishment.

5.2.2.2.2 MBS Policy Association Establishment

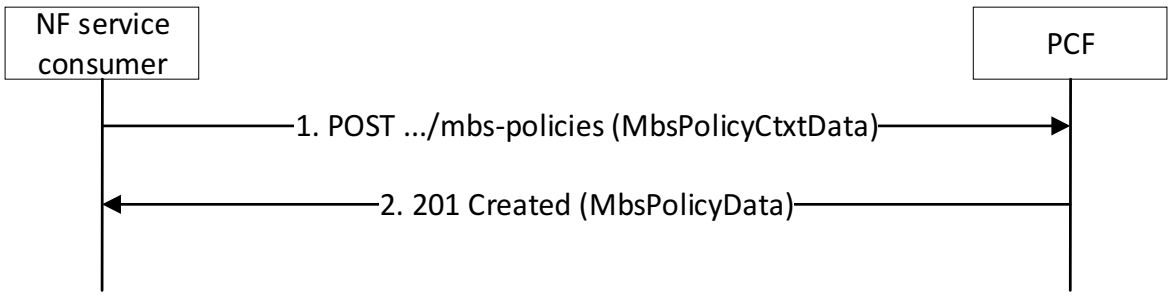

Figure 5.2.2.2.2-1: Procedure for MBS Policy Association establishment

1. In order to request the creation of an MBS Policy Association, the NF service consumer (e.g. MB-SMF) shall send an HTTP POST request to the PCF targeting the URI of the "MBS Policies" collection resource, with the request body containing the MbsPolicyCtxtData data structure that shall contain:

   - the identifier of the concerned MBS Session, within the "mbsSessionId" attribute;

   - the MBS Service Information, if available, within the "mbsServInfo" attribute; and

   - the list of supported features, if feature negotiation needs to take place, within the "suppFeat" attribute;

   and may contain:

   - the DNN of the MBS session, within the "dnn" attribute; and

   - the S-NSSAI of the MBS session, within the "snssai" attribute.

2. Upon reception of the HTTP POST request from the NF service consumer:

   - if MBS Service Information is present within the "mbsServInfo" attribute, the MBS session is an instance of a location-dependent MBS service and the PCF is not already serving this location-dependent MBS service, or if the MBS Service Information is not present, the PCF may interact with the BSF by invoking the Nbsf_Management_Register service operation, as specified in clause 4.2.2.4 of 3GPP TS 29.521 [21], to check whether there is already a PCF serving the MBS Session, and if it is not the case, register itself as the PCF serving the MBS session;

NOTE 1: Interacting with the BSF is not necessary in a deployment with a single PCF.

   - if MBS Service Information is present within the "mbsServInfo" attribute, then:

     - the PCF may interact with the UDR to retrieve MBS Session policy control data for the MBS session, as specified in 3GPP TS 29.519 [20];

NOTE 2: Interacting with the UDR for MBS Session policy control data retrieval is not necessary in a deployment where MBS Policy Session policy control data is stored locally at the PCF.

     - the PCF shall then perform MBS policy authorization based on the received MBS Service Information, the operator policies that are pre-configured at the PCF and the MBS Session policy control data retrieved from the UDR, if any;

     - if MBS policy authorization is successful, the PCF shall derive the required MBS policies (e.g. QoS parameters) and determine whether they are allowed or not;

     - if the required MBS policies are allowed:

       - the PCF shall store the generated MBS policies for the MBS session together with the corresponding MBS session ID; and

     - if MBS policy authorization is not successful or the required MBS policies are not allowed, the PCF shall reject the request with an appropriate error response as specified below in this clause;

   - otherwise, when MBS Service Information is not present within the "mbsServInfo" attribute and the PCF has previously derived the necessary MBS policies for the MBS session using the procedure defined in clause 5.3.2.2, the PCF shall provide these MBS policies in the response message returned to the NF service consumer (MB-SMF) as described below;

   - upon success, the PCF shall:

     - create a new "Individual MBS Policy" resource; and

     - respond to the NF service consumer with an HTTP "201 Created" status code including a Location header field containing the URI of the created "Individual MBS Policy" resource, and the response body including the MbsPolicyData data structure that shall contain:

       - the received input parameters within the corresponding request body, within the "mbsPolicyCtxtData" attribute;

- the provisioned MBS Policy Decision containing the MBS policies derived by the PCF as defined above in this clause, within the "mbsPolicies" attribute; and

- the list of supported features, if feature negotiation is taking place, within the "suppFeat" attribute;

- if errors occur when processing the HTTP POST request, the PCF shall apply the error handling procedures specified in clause 6.1.7;

NOTE 3: The PCF also deregisters at the BSF from being the PCF serving the MBS Session using the procedure defined in clause 4.2.3.4 of 3GPP TS 29.521 [21], if the PCF created such MBS Session binding as defined above in this clause. Interacting with the BSF to deregister from being the PCF serving the MBS Session is not necessary in a deployment with a single PCF.

- if MBS Service Information is provided but is invalid, incorrect or insufficient for the PCF to perform MBS policy authorization, the PCF shall reject the request with an HTTP "400 Bad Request" response message including the ProblemDetails data structure with the "cause" attribute set to "INVALID_MBS_SERVICE_INFO";

- if MBS Service Information is provided, but the MBS IP flow(s) description provided within the MBS Service Information cannot be handled by the PCF because the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [19] are not respected, the PCF shall reject the request with an HTTP "400 Bad Request" status code including the ProblemDetails data structure with the "cause" attribute set to "FILTER_RESTRICTIONS_NOT_RESPECTED";

- if from an application level point of view, the provided set of input parameters is incomplete, erroneous or missing necessary information for the PCF to perform MBS policy control, the PCF shall reject the request with an HTTP "400 Bad Request" response message including the ProblemDetails data structure with the "cause" attribute set to "ERROR_INPUT_PARAMETERS";

- if MBS Service Information is provided but is not authorized, the PCF shall reject the request with an HTTP "403 Forbidden" status code including the MbsExtProblemDetails data structure that shall contain:

  - the ProblemDetails data structure with the "cause" attribute set to "MBS_SERVICE_INFO_NOT_AUTHORIZED";

  and may contain:

  - the AcceptableMbsServInfo data structure including the MBS Service Information that is acceptable for the PCF;

  and

- if the PCF denies the creation of the "Individual MBS Policy" resource based on local configuration and/or operator policies, the PCF shall reject the request within an HTTP "403 Forbidden" status code including the "cause" attribute of the ProblemDetails data structure set to "MBS_POLICY_CONTEXT_DENIED". At the reception of this error code and based on the internally configured failure actions, the NF service consumer may reject or allow, by applying local policies, the establishment of the corresponding MBS session.

5.2.2.3 Npcf_MBSPolicyControl_Update

5.2.2.3.1 General

The Npcf_MBSPolicyControl_Update service operation enables the NF service consumer (e.g. MB-SMF) to request the update of an existing "Individual MBS Policy" resource for a multicast or a broadcast MBS session and/or report MBS Policy Decision installation and/or enforcement failure(s) to the PCF.

The following procedures using the Npcf_MBSPolicyControl_Update service operation are supported:

- MBS Policy Association Update.

5.2.2.3.2 MBS Policy Association Update

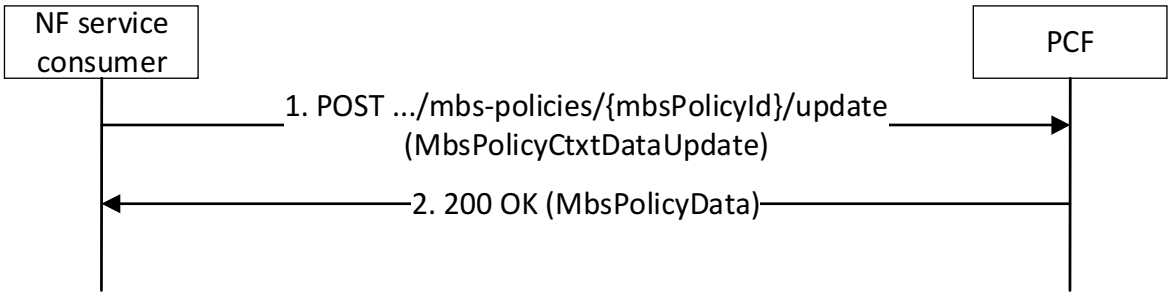

Figure 5.2.2.3.2-1: Procedure for MBS Policy Association Update

1. In order to request the update of an existing MBS Policy Association, the NF service consumer shall invoke the "Update" resource custom operation by sending an HTTP POST request to the PCF targeting the URI of the corresponding "Individual MBS Policy" resource custom operation, i.e. "{apiRoot}/npcf-mbspolicycontrol/<apiVersion>/mbs-policies/{mbsPolicyId}/update", with the request body including the MbsPolicyCtxtDataUpdate data structure that may contain:

   - the updated MBS Service Information, within the "mbsServInfo" attribute;
   - the MBS Policy Control Request Triggers that are met, within the "mbsPcrts" attribute, and/or
   - the MBS Error reporting containing the MBS Policy Decision installation and/or enforcement failure(s), within the "mbsErrorReport" attribute.

   If the PCF determines that the received HTTP POST request needs to be redirected, the PCF shall respond with an HTTP redirect response, as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

2. Upon reception of the HTTP POST request from the NF service consumer:

   - if the MBS Policy Control Request Trigger "MBS_SESSION_UPDATE" is triggered and updated MBS Service Information is present within the "mbsServInfo" attribute, then the PCF shall perform MBS policy authorization for the received updated MBS Service Information taking into account the operator policies pre-configured at the PCF and/or the MBS Session policy control data retrieved from the UDR. Then:
     - if MBS policy authorization is successful, the PCF shall determine whether updated MBS policies (e.g. QoS parameters) need to be derived and provisioned. If it is the case, the PCF shall derive these required updated MBS policies (e.g. QoS parameters) and determine whether they are allowed or not;
     - if updated MBS policies are derived and allowed, the PCF shall store the generated updated MBS policies for the MBS session together with the corresponding MBS session ID; and
     - if MBS policy authorization is not successful or the required updated MBS policies, if any, are not allowed, the PCF shall reject the request with an appropriate error response as specified below in this clause;
   - if the MBS Policy Control Request Trigger "MBS_SESSION_UPDATE" is triggered and no updated MBS Service Information is provided, then the PCF may identify whether there are any updated MBS policies that need to be applied as per the procedure defined in clause 5.3.2.3 and/or based on local configuration;

   NOTE: If updated MBS Service Information is not present in the received request, then the PCF has previously determined and generated the required updated MBS policies for the MBS session as specified in clause 5.3.

   - if MBS error reporting is present in the request and contains a set of MBS Policy Decision installation and/or enforcement failure(s), the PCF may take it into account when deriving the required updated MBS policies as specified in clause 5.2.4.1;
   - upon success, the PCF shall:
     - update the corresponding "Individual MBS Policy" resource accordingly; and

- respond to the NF service consumer with an HTTP "200 OK" status code with the response body including the MbsPolicyData data structure that shall contain:

  - the updated complete list of input parameters, within the "mbsPolicyCtxtData" attribute;

  and may contain:

  - the updated MBS Policy Decision containing the updated, deleted and/or newly provisioned MBS policies, within the "mbsPolicies" attribute;

- if errors occur when processing the HTTP POST request, the PCF shall apply the error handling procedures specified in clause 6.1.7;

- if updated MBS Service Information is provided but is invalid, incorrect or insufficient for the PCF to perform MBS policy authorization, the PCF shall reject the request with an HTTP "400 Bad Request" response message including the ProblemDetails data structure with the "cause" attribute set to "INVALID_MBS_SERVICE_INFO";

- if updated MBS Service Information is provided, but the MBS IP flow(s) description provided within the MBS Service Information cannot be handled by the PCF because the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [19] are not respected, the PCF shall reject the request with an HTTP "400 Bad Request" status code including the ProblemDetails data structure with the "cause" attribute set to "FILTER_RESTRICTIONS_NOT_RESPECTED";

- if from an application level point of view, the provided set of input parameters is incomplete, erroneous or missing necessary information for the PCF to perform MBS policy control, the PCF shall reject the request with an HTTP "400 Bad Request" response message including the ProblemDetails data structure with the "cause" attribute set to "ERROR_INPUT_PARAMETERS";

- if updated MBS Service Information is provided but is not authorized, the PCF shall reject the request with an HTTP "403 Forbidden" status code including the MbsExtProblemDetails data structure that shall contain:

  - the ProblemDetails data structure with the "cause" attribute set to "MBS_SERVICE_INFO_NOT_AUTHORIZED";

  and may contain:

  - the AcceptableMbsServInfo data structure including the MBS Service Information that is acceptable for the PCF;

- if the PCF denies the update of the "Individual MBS Policy" resource based on local configuration and/or operator policies, the PCF shall reject the request within an HTTP "403 Forbidden" status code including the ProblemDetails data structure with the "cause" attribute set to "MBS_POLICY_CONTEXT_DENIED". At the reception of this error code and based on the internally configured failure actions, the NF service consumer (MB-SMF) may reject or allow, by applying local policies, the update of the corresponding MBS session; and

- if the targeted "Individual MBS Policy" resource does not exist, the PCF shall reject the request with an HTTP "404 Not Found" status code including the ProblemDetails data structure with the "cause" attribute set to "MBS_POLICY_ASSOCIATION_NOT_FOUND".

5.2.2.4 Npcf_MBSPolicyControl_Delete

5.2.2.4.1 General

The Npcf_MBSPolicyControl_Delete service operation enables the NF service consumer (e.g. MB-SMF) to request the deletion of an existing "Individual MBS Policy" resource.

The following procedures using the Npcf_MBSPolicyControl_Delete service operation are supported:

- MBS Policy Association Deletion.

5.2.2.4.2 MBS Policy Association Deletion

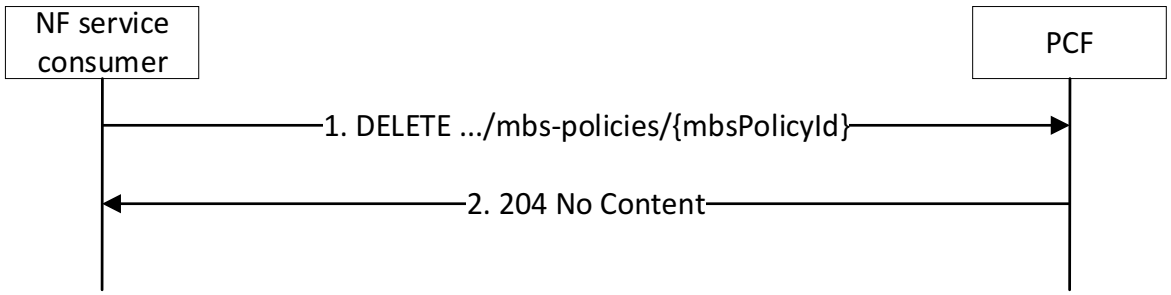

Figure 5.2.2.4.2-1: MBS Policy Association Deletion procedure

1. In order to request the deletion of an existing MBS Policy Association, the NF service consumer shall send an HTTP DELETE request to the PCF, targeting the URI of the corresponding "Individual MBS Policy" resource.

   If the PCF determines that the received HTTP DELETE request needs to be redirected, the PCF shall respond with an HTTP redirect response, as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

2. On successful deletion of the targeted MBS Policy Association:

   - the PCF may deregister at the BSF from being the PCF serving the MBS Session using the procedure defined in clause 4.2.3.4 of 3GPP TS 29.521 [21], if the PCF created such MBS Session binding during the creation of the MBS Policy Association, as specified in clause 5.2.2.2; and
   - the PCF shall respond to the NF service consumer (MB-SMF) with an HTTP "204 No Content" status code.

   If errors occur when processing the HTTP DELETE request, the PCF shall apply the error handling procedures specified in clause 6.1.7.

   If the targeted "Individual MBS Policy" resource does not exist, the PCF shall reject the request with an HTTP "404 Not Found" status code including the ProblemDetails data structure with the "cause" attribute set to "MBS_POLICY_ASSOCIATION_NOT_FOUND".

5.2.3 MBS Policy Decision Management

5.2.3.1 General

An MBS Policy Decision enables to provide the necessary MBS policies for controlling an MBS Session. An MBS Policy Decision is encoded via the MbsPolicyDecision data structure defined in clause 6.1.6.2.3 and composed of the following information:

- MBS PCC rule(s), within the "mbsPccRules" attribute.
- MBS QoS decision(s), which can be referred by MBS PCC rules, within the "mbsQosDecs" attribute.
- Set(s) of MBS QoS characteristics for non-standardized and non-preconfigured 5QIs, within the "mbsQosChars" attribute.
- The authorized MBS Session-AMBR, within the "authMbsSessAmbr" attribute.
- The MBS Policy Control Request Trigger(s), within the "mbsPcrts" attribute.

The following clauses describe the above components of an MBS Policy Decision.

5.2.3.1.1 MBS PCC Rule definition

An MBS PCC rule enables to provide MBS policy control for an MBS service data flow. It is composed of the following information, as defined in table 5.2.3.1.1-1.

- Information enabling the detection of the MBS service data flow.

- A set of MBS Policy Control parameters to be enforced for the MBS service data flow.

Table 5.2.3.1.1-1: Content of an MBS PCC rule

Name	Description	Category
MBS PCC Rule identifier	Uniquely identifies the MBS PCC rule, within an MBS Session. It is used between the PCF and the MB-SMF for referencing the MBS PCC rules of an MBS Session.	Mandatory
	MBS service data flow detection	
Precedence	Determines the order in which the MBS service data flow template of the MBS PCC rule is applied relative to the MBS service data flow templates of the other MBS PCC rules of the MBS session, during MBS service data flow detection and policy enforcement.	Mandatory
MBS Service Data Flow Template	The list of MBS service data flow filter(s) for the detection of the MBS service data flow.	Mandatory
	MBS policy control parameters	
5QI	Identifier of the authorized set of QoS parameters for the MBS service data flow.	Mandatory
ARP	The authorized Allocation and Retention Priority for the MBS service data flow, consisting of the priority level, the pre-emption capability and the pre-emption vulnerability.	Mandatory
MBR – Maximum BitRate (DL)	The downlink maximum bitrate authorized for the MBS service data flow.	Optional
GBR – Guaranteed BitRate (DL)	The downlink guaranteed bitrate authorized for the MBS service data flow.	Optional
Averaging Window	Represents the duration over which the guaranteed and maximum bitrates shall be calculated.	Optional
Priority Level	Indicates the level of priority in scheduling resources among MBS QoS flows.	Optional
Maximum Data Burst Volume	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB.	Optional

An MBS PCC rule is encoded via the MbsPccRule data structure defined in clause 6.1.6.2.7 and is composed of the following information:

- An MBS PCC rule identifier that uniquely identifies the MBS PCC rule within the related MBS Session, within the "mbsPccRuleId" attribute.

- The MBS service data flow template for MBS service data flow detection, within the "mbsDlIpFlowInfo" attribute.

- The precedence information, i.e. the order in which the MBS service data flow template of the MBS PCC rule is applied relative to the MBS service data flow templates of the other MBS PCC rules of the MBS session, during MBS service data flow detection and policy enforcement, within the "precedence" attribute.

- The MBS authorized QoS to be applied for the MBS service data flow corresponding to the MBS PCC rule, i.e. a reference to an MBS QoS decision instance provisioned by the PCF at MBS Policy Decision level, within the "refMbsQosDec" attribute.

The following operations are allowed on MBS PCC rule(s):

- Installation, i.e. to provision MBS PCC rule(s).

- Modification, i.e. to modify MBS PCC rule(s).

- Removal, i.e. to remove MBS PCC rule(s).

5.2.3.1.2 MBS QoS Decision

An MBS Policy Decision based on MBS QoS contains the QoS parameters to be applied for an MBS service data flow. It defines the QoS parameters (e.g. 5QI, ARP, maximum/guaranteed bitrates, etc.) to be applied for the corresponding MBS PCC rule. An MBS QoS decision is encoded via the MbsQosDec data structure defined in clause 6.1.6.2.8 and composed of the following information:

- An identifier of the MBS QoS Decision that uniquely identifies the MBS QoS Decision within the related MBS Session, within the "mbsQosId" attribute.
- The 5QI information, i.e. an identifier of the set of QoS parameters to be applied to an MBS service data flow, within the "5qi" attribute;
- The 5QI Priority Level, within the "priorityLevel" attribute.
- The Allocation and Retention Priority information to be applied for an MBS service data flow, within the "arp" attribute.
- The Maximum Downlink Bit Rate for to be applied for an MBS service data flow, within the "mbrDl" attribute.
- The Guaranteed Downlink Bit Rate to be applied for an MBS service data flow, within the "gbrDl" attribute.
- The averaging window, i.e. the duration over which the guaranteed and maximum bitrates shall be calculated, within the "averWindow" attribute.
- The MBS Maximum Data Burst Volume to be applied for an MBS service data flow, within the "mbsMaxDataBurstVol" attribute.

5.2.3.1.3 MBS QoS Characteristics

A set of MBS QoS Characteristics contains the QoS parameters for a non-standardized and non-preconfigured 5QI. It defines the QoS parameters (e.g. 5QI, ARP, maximum/guaranteed bitrates, etc.) to be applied for an MBS PCC rule and the corresponding MBS service data flow. A set of MBS QoS Characteristics is encoded via the MbsQosChars data structure defined in clause 6.1.6.2.9 and composed of the following information:

- The 5QI information, i.e. an identifier of the set of non-standardized and non-preconfigured QoS parameters for an MBS service data flow, within the "5qi" attribute. It applies at MBS PCC rule level and MBS session level.
- The resource type (i.e. GBR, delay critical GBR or non-GBR), within the "resourceType" attribute.
- The 5QI priority level, within the "priorityLevel" attribute.
- The Packet Delay Budget, within the "packetDelayBudget" attribute.
- The Packet Error Rate, within the "packetErrorRate" attribute.
- The averaging window, within the "averWindow" attribute.
- The MBS Maximum Data Burst Volume, within the "mbsMaxDataBurstVol" attribute.

5.2.3.1.4 MBS Session-AMBR

The MBS Session-AMBR contains the Aggregated Maximum Bit Rate to be applied for an MBS session.

5.2.3.1.5 MBS Policy Control Request Triggers

The MBS Policy Control Request Triggers identify the conditions based on which the NF service consumer (MB-SMF) shall trigger the MBS Policy Association Update procedure defined in clause 5.2.2.3. They can be either pre-configured at the NF service consumer (MB-SMF), i.e. implicitly subscribed by default by the PCF, or explicitly provisioned by the PCF to the NF service consumer (MB-SMF) during the MBS Policy Association Creation/Update procedures defined in clause 5.2.2.

The MBS Policy Control Request Triggers are encoded using the MbsPcrt Enumeration data type defined in clause 6.1.6.3.3. The possible values are the following:

- "MBS_SESSION_UPDATE", i.e. MBS Session Update: the MBS policies may need to be updated due to updated MBS Session information. This MBS Policy Control Request Trigger is pre-configured at the NF service consumer (MB-SMF), i.e. implicitly subscribed by the PCF.

5.2.3.2 Provisioning and enforcement of MBS Policy Decisions

5.2.3.2.1 General

MBS Policy Decisions are provided by the PCF to the NF service consumer (MB-SMF) as part of the following service operations:

- the Npcf_MBSPolicyControl_Create service operation defined in clause 5.2.2.2; and
- the Npcf_MBSPolicyControl_Update service operation defined in clause 5.2.2.3.

For the Npcf_MbsPolicyControl_Create service operation, the MbsPolicyDecision data structure shall contain the MBS Policy Decision containing a full description of all the MBS policies provisioned by the PCF for the MBS Policy Association.

For the Npcf_MBSPolicyControl_Update service operation for, the MbsPolicyDecision data structure shall contain the updated MBS Policy Decision containing a full description of all the updated MBS policies (if any) provisioned for the MBS Policy Association.

5.2.3.2.2 Provisioning and enforcement of MBS PCC rules

The PCF provisions/updates/removes MBS PCC rule(s) via the "mbsPccRules" attribute of the MbsPolicyDecision data structure as part of the provisioning/update/removal of an MBS Policy Decision (cf. clause 5.2.3.2.1).

- For provisioning or modifying a dynamic PCF-provisioned MBS PCC rule, the corresponding MbsPccRule data structure shall be provided as a map entry value of the "mbsPccRules" attribute within the MbsPolicyDecision data structure representing the related MBS Policy Decision. The corresponding map key shall be set to the value of the "mbsPccRuleId" attribute of the MbsPccRule data structure.
- For removing a previously provisioned MBS PCC rule, the corresponding map entry value shall be set to "NULL" and map key to the value of the "mbsPccRuleId" attribute of the MbsPccRule data structure representing the targeted MBS PCC rule.

5.2.3.2.3 Provisioning and enforcement of authorized MBS QoS for an MBS service data flow

The authorized MBS QoS for an MBS service data flow is provisioned along with the corresponding MBS PCC rule, as specified in the clause 5.2.3.2.2.

The MBS authorized QoS per MBS service data flow shall be provisioned within the MbsQosDec data structure representing the MBS QoS Decision to be applied for the MBS service data flow. For this purpose:

- the PCF shall include this MBS QoS Decision instance as a map entry within the "mbsQosDecs" attribute of the MbsPolicyDecision data structure of the corresponding MBS Policy Decision, as specified in clause 5.2.3.1.2, and include the reference to this MBS QoS Decision instance within the "refMbsQosDec" attribute of the MbsPccRule data structure representing the corresponding MBS PCC rule;
- when the PCF provisions a standardized 5QI value, but the Priority Level, the Averaging Window and/or the Maximum Data Burst Volume shall be different from the standardized values defined in the table 5.7.4-1 of 3GPP TS 23.501 [2], the PCF shall include within the corresponding MbsQosDec data structure the required Priority Level within the "priorityLevel" attribute, the Averaging Window within the "averWindow" attribute and/or the MBS Maximum Data Burst Volume within the "mbsMaxDataBurstVol" attribute;
- if the PCF needs to provision dynamically assigned 5QI value(s) (from the non-standardized and non-preconfigured value range) and the associated set(s) of MBS QoS Characteristics, the PCF shall include within the MbsPolicyDecision data structure representing the related MBS Policy Decision the "mbsQosChars" map attribute containing one or more set(s) of MBS QoS Characteristics, with each one of them encoded using the MbsQosChar data structure as specified in clause 5.2.3.1.3. The PCF shall not update nor remove previously provisioned set(s) of MBS QoS Characteristics during the lifetime of the concerned MBS Policy Association;
- when the PCF provisions a dynamically assigned 5QI value (from the non-standardized and non-preconfigured value range) for the MBS PCC rule within the referred MBS QoS Decision instance, then the "5qi" attribute of

the corresponding MbsQosDec data structure shall be set to the value of the dynamically assigned 5QI which points to the MBS QoS Characteristics instance containing the related QoS parameters;

NOTE: Operator configuration is assumed to ensure that a dynamically assigned 5QI value is unique and references at a given time the same set of MBS QoS characteristics within the whole PLMN.

Upon reception of an MBS PCC rule provisioning including the corresponding authorized MBS QoS information from the PCF, the NF service consumer (MB-SMF) shall perform MBS QoS flow binding as specified in clause 6.10 of 3GPP TS 23.247 [14]. The NF service consumer (MB-SMF) shall also reserve the necessary resources for the guaranteed bitrate of the MBS PCC rule, if provided. For GBR MBS QoS flows, the NF service consumer (MB-SMF) should set the MBS QoS flow's GBR to the sum of the GBR(s) of all the MBS PCC rule(s) that are active/installed and bound to that GBR MBS QoS flow, and the MBS QoS flow's MBR to the sum of the MBR(s) of all the MBS PCC rule(s) that are active/installed and bound to that GBR MBS QoS flow.

The NF service consumer (MB-SMF) shall assign a new MBS QFI if a new MBS QoS flow needs to be established and derive the MBS QoS profile required towards the Access Network, if applicable, and the MBS QoS information with PDRs towards the MB-UPF.

During an MBS session policy association update procedure that results in updating all the MBS PCC rule(s) bound to a certain MBS QoS flow, if all these MBS PCC rule(s) are updated with the same values of the QoS parameters (e.g. 5QI, ARP, Priority level, Averaging Window and Maximum Data Burst Volume), the NF service consumer (MB-SMF) should not perform a new MBS QoS flow binding and simply modify this MBS QoS flow with the updated QoS parameters.

5.2.3.2.4 Provisioning and enforcement of authorized MBS Session-AMBR

The Provisioning of the authorized MBS Session-AMBR for an MBS session is part of the provisioning of the corresponding MBS Policy Decision, as specified in the clause 5.2.3.2.1.

Upon reception of the authorized MBS Session-AMBR from the PCF, the NF service consumer (MB-SMF) shall trigger the necessary procedures towards the MB-UPF for the provisioning and enforcement of the MBS Session-AMBR for the concerned MBS session.

NOTE: For an MBS session, the authorized MBS Session-AMBR is not propagated to neither the access network nor the UE.

5.2.3.2.5 Provisioning and enforcement of MBS Policy Control Request Triggers

The PCF may provision one or more MBS Policy Control Request Triggers(s) to the NF service consumer (MB-SMF). In order to do so, the PCF shall include the "mbsPcrts" attribute containing one or more MBS Policy Control Request Triggers(s) within the MbsPolicyDecision data structure.

During the lifetime of the MBS Policy Association, the PCF may update and/or remove previously provisioned MBS Policy Control Request Triggers(s):

- In order to update a previously subscribed set of MBS Policy Control Request Triggers(s), the PCF shall provide the complete list of the subscribed MBS Policy Control Request Triggers(s) within the "mbsPcrts" attribute of the MbsPolicyDecision data structure.

- In order to remove all the previously subscribed MBS Policy Control Request Triggers(s), the PCF shall provide the "mbsPcrts" attribute set to the value "NULL" within the MbsPolicyDecision data structure. Upon reception of a "NULL" value within the "mbsPcrts" attribute, the NF service consumer (MB-SMF) shall only trigger the MBS Policy Association Update procedure for the pre-configured MBS Policy Control Request Triggers(s), i.e. the ones implicitly subscribed by the PCF.

MBS Policy Control Request Triggers(s) may also be pre-configured at the NF service consumer as specified in clause 5.2.3.1.5. In such case, the PCF is implicitly subscribed and does not need to explicitly subscribe to these MBS Policy Control Request Triggers(s) towards the NF service consumer (MB-SMF). A combination of pre-configured MBS Policy Control Request Triggers(s) and explicitly subscribed MBS Policy Control Request Triggers(s) may be present for an MBS Policy Association.

5.2.4 MBS Policy Error Handling

5.2.4.1 MBS Policy Error Reporting

Following an MBS Policy Association Creation or Update procedure, as defined in clause 5.2.2.2.2 or 5.2.2.3.2, the NF service consumer (MB-SMF) may report the potentially encountered failure(s) during the installation and/or enforcement of the provisioned MBS Policy Decision, both for MBS Policy Decision level failure(s) (e.g. MBS QoS Decision failure) and MBS PCC rule level failure(s) (e.g. the installation of one or more MBS PCC rule(s) fails or the PCF installed or modified one or more MBS PCC rules but resource allocation for these MBS PCC rule(s) was unsuccessful).

In order to do so, the NF service consumer (MB-SMF) shall trigger the MBS Policy Association Update procedure defined in clause 5.2.2.3.2 and include within the "mbsErrorReport" attribute of the MbsPolicyCtxtDataUpdate data structure the necessary information on the failure(s) that occurred within one or more MBS Report instance(s), each one of them encoded using the MbsReport data structure that shall include:

- the failure reason, if available, within the "failureCode" attribute;
- the affected MBS PCC rule(s), if the reported failure is at MBS PCC rule level, within the "mbsPccRuleIds" attribute; and
- the MBS PCC rule status, if the reported failure is at MBS PCC rule level, within the "mbsPccRuleStatus" attribute.

Depending on the value of the "failureCode" attribute, the PCF may decide on the necessary updates to be applied to the MBS Policy Decision, if any, including whether to retain, re-install, modify or remove the existing MBS PCC rule(s), or any other action applies.

For MBS PCC rule level failure(s), the following handling shall apply:

- if the installation of one or more new MBS PCC rule(s) (i.e. MBS PCC rule(s) which were not successfully installed previously) fails, the NF service consumer (MB-SMF) shall set the "mbsPccRuleStatus" attribute to the value "INACTIVE";
- if one or more MBS PCC rule(s) were successfully installed but can no longer be enforced by the NF service consumer (MB-SMF), the MB-SMF shall set the "mbsPccRuleStatus" attribute to "INACTIVE";

NOTE: When the PCF receives the "mbsPccRuleStatus" set to the value "INACTIVE", the PCF does not need to request the MB-SMF to remove the concerned MBS PCC rule(s) within the "mbsPccRuleIds" attribute.

- if the requested modifications to currently active MBS PCC rule(s) fails, the NF service consumer (MB-SMF) shall:
  - retain the targeted existing MBS PCC rule(s) active in their current version (i.e. without any modification), unless the failure reason also impacts the current version of these existing MBS PCC rule(s); and
  - report the modification failure to the PCF;

and

- the removal of MBS PCC rule(s) shall not fail. The NF service consumer (MB-SMF) shall retain the MBS PCC rule(s) removal request and perform the related necessary actions/procedures in the network when it is possible.

5.3 Npcf_MBSPolicyAuthorization Service

5.3.1 Service Description

The MBS Policy Authorization Service enables the Policy Control Function (PCF) to authorize the MBS Service Information provided by an NF service consumer (e.g. AF, NEF, MBSF) and derive the related MBS policies, i.e.:

- enable an NF service consumer (e.g. AF, NEF, MBSF) to request the creation, update or removal of an MBS Application Session Context, based on the provisioning of MBS Service Information; and

- enable the PCF to authorize the provided MBS Service Information and derive the MBS policies related to the targeted MBS session.

5.3.2 Service Operations

5.3.2.1 Introduction

The service operations defined for the Npcf_MBSPolicyAuthorization Service are shown in table 5.3.2.1-1.

Table 5.3.2.1-1: Npcf_MBSPolicyAuthorization Service Operations

Service Operation Name	Description	Initiated by
Npcf_MBSPolicyAuthorization_Create	Request the creation of an MBS Application Session Context at the PCF, to enable MBS policy authorization for the provided MBS Service Information.	NF service consumer (e.g. NEF, MBSF, AF)
Npcf_MBSPolicyAuthorization_Update	Update an existing MBS Application Session Context at the PCF, to enable MBS policy authorization for the provided updated MBS Service Information.	NF service consumer (e.g. NEF, MBSF, AF)
Npcf_MBSPolicyAuthorization_Delete	Delete an existing MBS Application Session Context at the PCF.	NF service consumer (e.g. NEF, MBSF, AF)

5.3.2.2 Npcf_MBSPoliyAuthorization_Create

5.3.2.2.1 General

The Npcf_MBSPolicyAuthorization_Create service operation enables an NF service consumer (e.g. AF, NEF, MBSF) to request the creation of an MBS Application Session Context at the PCF, for the purpose of requesting MBS policy authorization for a multicast or a broadcast MBS session.

The following procedures using the Npcf_MBSPolicyAuthorization_Create service operation are supported:

- MBS Application Session Context Establishment.

5.3.2.2.2 MBS Application Session Context Establishment

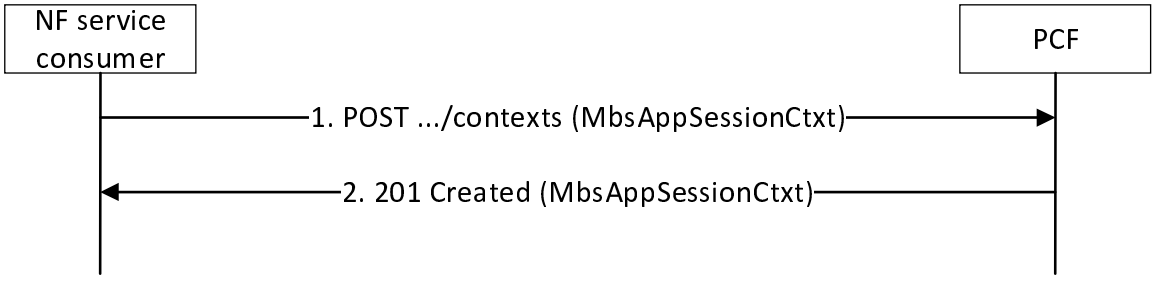

Figure 5.3.2.2.2-1: MBS Application Session Context establishment procedure

1. In order to request the creation of a new MBS Application Session Context, the NF service consumer (e.g. AF, NEF, MBSF) shall send an HTTP POST request to the PCF, targeting the URI of the "MBS Application Session Contexts" collection resource, with the request body containing the MbsAppSessionCtxt data structure that shall contain:

   - the MBS session identifier, within the "mbsSessionId" attribute;
   - the MBS Service Information, if available, within the "mbsServInfo" attribute; and
   - the list of supported features, if feature negotiation needs to take place, within the "suppFeat" attribute;

   and may contain:

- the DNN of the MBS session, within the "dnn" attribute; and

- the S-NSSAI of the MBS session, within the "snssai" attribute.

2. Upon reception of the HTTP POST request from the NF service consumer:

- the PCF may interact with the UDR to retrieve MBS Session policy control data for the MBS session, as specified in clause 5.2.16 of 3GPP TS 29.519 [20] ;

NOTE 1: Interacting with the UDR for MBS Session policy control data retrieval is not necessary in a deployment where MBS Policy Session policy control data is stored locally at the PCF.

- the PCF shall perform MBS policy authorization based on the MBS Service Information received from the NF service consumer and the operator policies that are pre-configured at the PCF and/or the MBS Session policy control data retrieved from the UDR. Then:

  - if MBS policy authorization is successful, the PCF shall derive the required MBS policies (e.g. QoS parameters) and determine whether they are allowed or not;

  - if the required MBS policies are allowed:

    - the PCF shall store the generated MBS policies for the MBS session together with the corresponding MBS session ID;

    - the PCF shall create a new "Individual MBS Application Session Context" resource and respond to the NF service consumer with an HTTP "201 Created" status code, including an HTTP Location header field containing the URI of the created "Individual MBS Application Session Context" resource and the response body containing a representation of the created resource within the MbsAppSessionCtxt data structure; and

    - the PCF may register itself at the BSF as the PCF handling the MBS session as specified in clause 4.2.2.4 of 3GPP TS 29.521 [21];

NOTE 2: Registering at the BSF as the PCF serving the MBS Session is not necessary in a deployment with a single PCF.

  - otherwise, when MBS policy authorization is not successful or the required MBS policies are not allowed, the PCF shall reject the request with an appropriate error response as specified below in this clause;

- if errors occur when processing the HTTP POST request, the PCF shall apply the error handling procedures specified in clause 6.2.7;

- if the provided MBS Service Information is invalid, incorrect or insufficient for the PCF to perform MBS policy authorization, the PCF shall reject the request with an HTTP "400 Bad Request" status code including the ProblemDetails data structure with the "cause" attribute set to "INVALID_MBS_SERVICE_INFO";

- if the MBS IP flow(s) description provided within the MBS Service Information cannot be handled by the PCF because the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [19] are not respected, the PCF shall reject the request with an HTTP "400 Bad Request" status code including the ProblemDetails data structure with the "cause" attribute set to "FILTER_RESTRICTIONS_NOT_RESPECTED"; and

- if the provided MBS Service Information are not authorized, the PCF shall reject the request with an HTTP "403 Forbidden" status code including the MbsExtProblemDetails data structure that shall contain:

  - the ProblemDetails data structure with the "cause" attribute set to "MBS_SERVICE_INFO_NOT_AUTHORIZED";

  and may contain:

  - the AcceptableMbsServInfo data structure including the MBS Service Information that is acceptable for the PCF.

5.3.2.3 Npcf_MBSPoliyAuthorization_Update

5.3.2.3.1 General

The Npcf_MBSPolicyAuthorization_Update service operation enables an NF service consumer (e.g. AF, NEF, MBSF) to request the update of an existing MBS Application Session Context, for the purpose of requesting the authorization of updated MBS Service Information.

The following procedures using the Npcf_MBSPolicyAuthorization_Update service operation are supported:

- MBS Application Session Context Update.

5.3.2.3.2 MBS Application Session Context Update

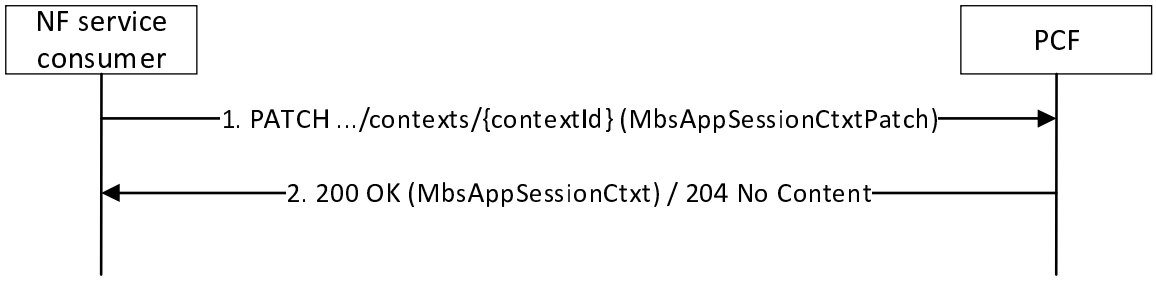

Figure 5.3.2.3.2-1: MBS Application Session Context update procedure

1. In order to request the modification of an existing MBS Application Session Context, the NF service consumer (e.g. AF, NEF, MBSF) shall send an HTTP PATCH request to the PCF, targeting the URI of the corresponding "Individual MBS Application Session Context" resource, with the request body containing the MbsAppSessionCtxtPatch data structure that may contain:

   - the requested modifications to the MBS Service Information, within the "mbsServInfo" attribute.

2. Upon reception of the HTTP PATCH request from the NF service consumer:

   - the PCF may interact with the UDR to retrieve MBS Session policy control data for the MBS session, as specified in 3GPP TS 29.519 [20];

   - the PCF shall perform MBS policy authorization based on the requested modifications to the MBS Service Information received from the NF service consumer and the operator policies that are pre-configured at the PCF and/or the MBS session policy control data retrieved from the UDR. Then:

     - if MBS policy authorization of the requested modifications to the MBS Service Information is successful, the PCF shall derive the required updated MBS policies (e.g. QoS parameters), if any, and determine whether they are allowed or not;

     - if the required updated MBS policies are allowed:

       - the PCF shall store the generated updated MBS policies for the MBS session, if any, together with the corresponding MBS session ID;

       - the PCF shall update the associated "Individual MBS Application Session Context" resource accordingly and respond to the NF service consumer with either an HTTP "200 OK" status code with the response body containing a representation of the updated resource within the MbsAppSessionCtxt data structure, or an HTTP "204 No Content" status code; and

       - if the authorized MBS policies have been changed, the PCF shall include the "contactPcfInd" attribute set to "true" within the returned MbsAppSessionCtxt data structure to indicate that the PCF shall be contacted, i.e. to indicate to the NF service consumer (MB-SMF) that it needs to trigger the MBS Policy Association Update procedure, as defined in clause 5.2.2.3, to receive updated MBS policies from the PCF;

- otherwise, when MBS policy authorization is not successful or the required updated MBS policies are not allowed, the PCF shall reject the request with an appropriate error response as specified below in this clause;

- if errors occur when processing the HTTP PATCH request, the PCF shall apply the error handling procedures specified in clause 6.2.7;

- if the targeted "Individual MBS Application Session Context" resource does not exist, the PCF shall reject the request with an HTTP "404 Not Found" status code including the ProblemDetails data structure with the "cause" attribute set to "MBS_SESSION_POL_AUTH_CTXT_NOT_FOUND";

- if the provided MBS Service Information is invalid, incorrect or insufficient for the PCF to perform MBS policy authorization, the PCF shall reject the request with an HTTP "400 Bad Request" status code including the ProblemDetails data structure with the "cause" attribute set to "INVALID_MBS_SERVICE_INFO";

- if the MBS IP flow(s) description provided within the MBS Service Information cannot be handled by the PCF because the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [19] are not respected, the PCF shall reject the request with an HTTP "400 Bad Request" status code including the ProblemDetails data structure with the "cause" attribute set to "FILTER_RESTRICTIONS_NOT_RESPECTED"; and

- if the provided MBS Service Information is not authorized, the PCF shall reject the request with an HTTP "403 Forbidden" status code including the MbsExtProblemDetails data structure that shall contain:

  - the ProblemDetails data structure with the "cause" attribute set to "MBS_SERVICE_INFO_NOT_AUTHORIZED";

  and may contain:

  - the AcceptableMbsServInfo data structure including the MBS Service Information that is acceptable for the PCF.

5.3.2.4 Npcf_MBSPoliyAuthorization_Delete

5.3.2.4.1 General

The Npcf_MBSPolicyAuthorization_Delete service operation enables an NF service consumer (e.g. AF, NEF, MBSF) to request the deletion of an existing MBS Application Session Context at the PCF.

The following procedures using the Npcf_MBSPolicyAuthorization_Delete service operation are supported:

- MBS Application Session Context Deletion.

5.3.2.4.2 MBS Application Session Context Deletion

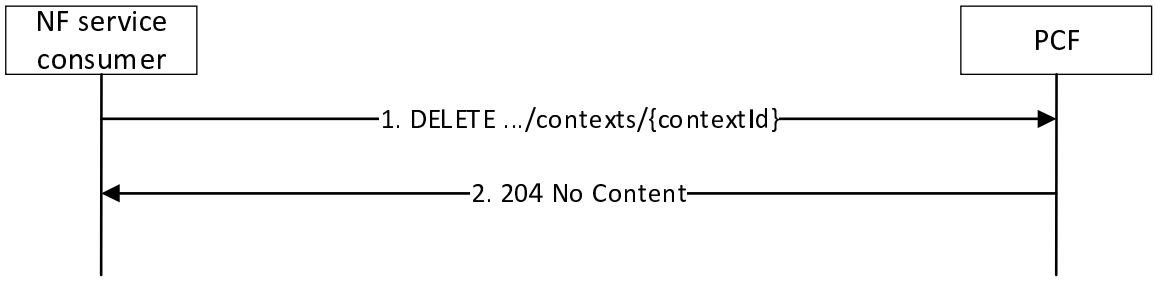

Figure 5.3.2.4.2-1: MBS Application Session Context deletion procedure

1. In order to request the deletion of an existing MBS Application Session Context, the NF service consumer (e.g. AF, NEF, MBSF) shall send an HTTP DELETE request to the PCF targeting the URI of the corresponding "Individual MBS Application Session Context" resource.

2. Upon success, the PCF shall respond with an HTTP "204 No Content" status code.

If errors occur when processing the HTTP DELETE request, the PCF shall apply the error handling procedures specified in clause 6.2.7.

If the targeted Individual MBS Application Session Context does not exist, the PCF shall reject the request with an HTTP "404 Not Found" status code including the ProblemDetails data structure with the "cause" attribute set to "MBS_SESSION_POL_AUTH_CTXT_NOT_FOUND".

6 API Definitions

6.1 Npcf_MBSPolicyControl Service API

6.1.1 Introduction

The Npcf_MBSPolicyControl Service shall use the Npcf_MBSPolicyControl API.

The API URI of the Npcf_MBSPolicyControl Service shall be:

{apiRoot}/<apiName>/<apiVersion>

The request URIs used in HTTP requests from the NF service consumer towards the NF service producer shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [5], i.e.:

{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].
- The <apiName> shall be "npcf-mbspolicycontrol".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.1.3.

6.1.2 Usage of HTTP

6.1.2.1 General

HTTP/2, IETF RFC 7540 [11], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [4].

The OpenAPI [6] specification of HTTP messages and content bodies for the Npcf_MBSPolicyControl API is contained in Annex A.2.

6.1.2.2 HTTP standard headers

6.1.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

6.1.2.2.2 Content type

JSON, IETF RFC 8259 [12], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

The "Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [13].

6.1.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4] may be supported.

6.1.3 Resources

6.1.3.1 Overview

This clause describes the structure for the resource URIs and the resources and methods used for the Npcf_MBSPolicyControl service.

Figure 6.1.3.1-1 depicts the resource URIs structure for the Npcf_MBSPolicyControl API.

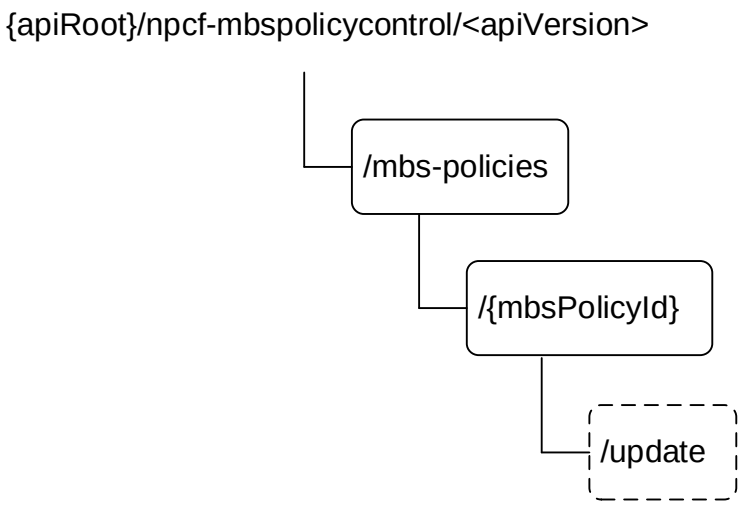

Figure 6.1.3.1-1: Resource URI structure of the Npcf_MBSPolicyControl API

Table 6.1.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.1.3.1-1: Resources and methods overview

Resource purpose/name	Resource URI (relative path after API URI)	HTTP method or custom operation	Description (service operation)
MBS Policies	/mbs-policies	POST	Request the creation of a new Individual MBS Policy resource.
Individual MBS Policy	/mbs-policies/{mbsPolicyId}	GET	Request the retrieval of an existing Individual MBS Policy resource.
		DELETE	Request the deletion of an existing Individual MBS Policy resource.
		Update (POST)	Request the update of an existing Individual MBS Policy resource.

6.1.3.2 Resource: MBS Policies

6.1.3.2.1 Description

This resource represents the collection of "Individual MBS Policy" resources managed by the PCF.

6.1.3.2.2 Resource Definition

Resource URI: **{apiRoot}/npcf-mbspolicycontrol/<apiVersion>/mbs-policies**

This resource shall support the resource URI variables defined in table 6.1.3.2.2-1.

Table 6.1.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.1.1.

6.1.3.2.3 Resource Standard Methods

6.1.3.2.3.1 POST

This method enables an NF service consumer (e.g. MB-SMF) to request the creation of an MBS Policy Association at the PCF.

This method shall support the URI query parameters specified in table 6.1.3.2.3.1-1.

Table 6.1.3.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.1.3.2.3.1-2 and the response data structures and response codes specified in table 6.1.3.2.3.1-3.

Table 6.1.3.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
MbsPolicyCtxtData	M	1	Contains the parameters to request the creation of an MBS Policy Association.

Table 6.1.3.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MbsPolicyData	M	1	201 Created	Successful case. An Individual MBS Policy resource is successfully created.
n/a			308 Permanent Redirect	Permanent Redirection. Another PCF already serves the MBS Session.
ProblemDetails	O	0..1	400 Bad Request	(NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
MbsExtProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 6.1.7.				

Table 6.1.3.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/npcf-mbspolicycontrol/<apiVersion>/mbs-policies/{mbsPolicyId}

Table 6.1.3.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI (i.e. "apiRoot") of the PCF currently handling the MBS Session and towards which the request is redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Contains the identifier of the PCF (service) instance towards which the request is redirected.

6.1.3.2.4 Resource Custom Operations

There are no resource custom operations defined for this resource in this release of the specification.

6.1.3.3 Resource: Individual MBS Policy

6.1.3.3.1 Description

This resource represents an "Individual MBS Policy" resource managed by the PCF.

6.1.3.3.2 Resource Definition

Resource URI: **{apiRoot}/npcf-mbspolicycontrol/<apiVersion>/mbs-policies/{mbsPolicyId}**

This resource shall support the resource URI variables defined in table 6.1.3.3.2-1.

Table 6.1.3.3.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.1.1.
mbsPolicyId	string	Represents the unique identifier of the "Individual MBS Policy" resource.

6.1.3.3.3 Resource Standard Methods

6.1.3.3.3.1 GET

This method enables an NF service consumer (e.g. MB-SMF) to retrieve an existing "Individual MBS Policy" resource at the PCF.

This method shall support the URI query parameters specified in table 6.1.3.3.3.1-1.

Table 6.1.3.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.1.3.3.3.1-2 and the response data structures and response codes specified in table 6.1.3.3.3.1-3.

Table 6.1.3.3.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 6.1.3.3.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MbsPolicyData	M	1	200 OK	Successful case. The requested Individual MBS Policy resource is successfully returned in the response body.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
NOTE: The mandatory HTTP error status codes for the GET method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.1.3.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

Table 6.1.3.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

6.1.3.3.3.2 DELETE

This method enables an NF service consumer (e.g. MB-SMF) to request the deletion of an existing "Individual MBS Policy" resource at the PCF.

This method shall support the URI query parameters specified in table 6.1.3.3.3.2-1.

Table 6.1.3.3.3.2-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.1.3.3.3.2-2 and the response data structures and response codes specified in table 6.1.3.3.3.2-3.

Table 6.1.3.3.3.2-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 6.1.3.3.3.2-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response Codes	Description
n/a			204 No Content	Successful response. The Individual MBS Policy resource was successfully deleted.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
ProblemDetails	O	0..1	404 Not Found	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the DELETE method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 6.1.7.				

Table 6.1.3.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

Table 6.1.3.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

6.1.3.3.4 Resource Custom Operations

6.1.3.3.4.1 Overview

Table 6.1.3.3.4.1-1: Custom operations

Operation name	Custom operaration URI	Mapped HTTP method	Description
Update	/mbs-policies/{mbsPolicyId}/update	Update (POST)	Request the update of an existing MBS Policy Association.

6.1.3.3.4.2 Operation: Update

6.1.3.3.4.2.1 Description

This resource custom operation enables an NF service consumer (e.g. MB-SMF) to request the update of an existing MBS Policy Association at the PCF.

6.1.3.3.4.2.2 Operation Definition

This operation shall support the request data structures specified in table 6.1.3.3.4.2.2-1 and the response data structure and response codes specified in table 6.1.3.3.4.2.2-2.

Table 6.1.3.3.4.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
MbsPolicyCtxtDataUpdate	M	1	Contains the parameters to request the update of the Individual MBS Policy resource.

Table 6.1.3.3.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MbsPolicyData	M	1	200 OK	Successful case. The targeted Individual MBS Policy resource is successfully updated.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
ProblemDetails	O	0..1	400 Bad Request	(NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
MbsExtProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
ProblemDetails	O	0..1	404 Not Found	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 6.1.7.				

Table 6.1.3.3.4.2.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

Table 6.1.3.3.4.2.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

6.1.4 Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

6.1.5 Notifications

There are no notifications defined for this API in this release of the specification.

6.1.6 Data Model

6.1.6.1 General

This clause specifies the application data model supported by the API.

Table 6.1.6.1-1 specifies the data types defined for the Npcf_MBSPolicyControl service based interface protocol.

Table 6.1.6.1-1: Npcf_MBSPolicyControl specific Data Types

Data type	Clause defined	Description	Applicability
MbsErrorReport	6.1.6.2.10	Contains the reporting of MBS Policy decision level failure(s) and/or MBS PCC rule level failure(s).	
MbsFailureCode	6.1.6.3.4	Represents the reason behind the MBS Policy Decision(s) enforcement failure or the MBS PCC rule(s) installation failure.	
MbsMaxDataBurstVol	6.1.6.3.2	Represents the maximum MBS data burst volume.	
MbsPccRule	6.1.6.2.7	Represents the parameters constituting an MBS PCC rule.	
MbsPcrt	6.1.6.3.3	Represents an MBS Policy Control Request Trigger.	
MbsPolicyCtxtData	6.1.6.2.2	Contains the parameters used to request the creation of an Individual MBS Policy resource.	
MbsPolicyCtxtDataUpdate	6.1.6.2.11	Contains the parameters to update an existing MBS Policy Association.	
MbsPolicyData	6.1.6.2.4	Contains the MBS policy data of an Individual MBS Policy resource.	
MbsPolicyDecision	6.1.6.2.3	Contains the parameters constituting an MBS Policy Decision.	
MbsPccRuleStatus	6.1.6.3.5	Represents the status of an MBS PCC rule.	
MbsQosChar	6.1.6.2.9	Represents the parameters constituting a set of explicitly signalled QoS Characteristics.	
MbsQosDec	6.1.6.2.8	Represents the parameters constituting an MBS QoS Decision.	
MbsReport	6.1.6.2.12	Includes the information about the MBS Policy Decision level failure(s) and/or the MBS PCC rule level failure(s).	

Table 6.1.6.1-2 specifies data types re-used by the Npcf_MBSPolicyControl service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Npcf_MBSPolicyControl service based interface.

Table 6.1.6.1-2: Npcf_MBSPolicyControl re-used Data Types

Data type	Reference	Comments	Applicability
5Qi	3GPP TS 29.571 [15]	Indicates the 5G QoS Identifier.	
5QiPriorityLevel	3GPP TS 29.571 [15]	Indicates the 5QI Priority Level.	
Arp	3GPP TS 29.571 [15]	Indicates the allocation and retention priority.	
AverWindow	3GPP TS 29.571 [15]	Indicates the Averaging Window.	
BitRate	3GPP TS 29.571 [15]	Indicates the Bit Rate.	
Dnn	3GPP TS 29.571 [15]	Identifies a DNN.	
FlowDescription	3GPP TS 29.512 [18]	Represents packet filtering information for an IP flow.	
MbsExtProblemDetails	Clause 6.2.6.4.1	Identifies the MBS related extensions to the ProblemDetails data structure.	
MbsServiceInfo	3GPP TS 29.571 [15]	Represents MBS Service Information.	
MbsSessionId	3GPP TS 29.571 [15]	Represents an MBS Session Identifier.	
PacketDelBudget	3GPP TS 29.571 [15]	Indicates the Packet Delay Budget.	
PacketErrRate	3GPP TS 29.571 [15]	Indicates the Packet Error Rate.	
ProblemDetails	3GPP TS 29.571 [15]	Contains error related additional information.	
QosResourceType	3GPP TS 29.571 [15]	Indicates the QoS resource type.	
RedirectResponse	3GPP TS 29.571 [15]	Contains redirection related information.	
Snssai	3GPP TS 29.571 [15]	Identifies an S-NSSAI.	
SupportedFeatures	3GPP TS 29.571 [15]	Represents the list of supported features. It is used to negotiate the applicability of the optional features.	
Uinteger	3GPP TS 29.571 [15]	Represents an unsigned integer.	

6.1.6.2 Structured data types

6.1.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

6.1.6.2.2 Type: MbsPolicyCtxtData

Table 6.1.6.2.2-1: Definition of type MbsPolicyCtxtData

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsSessionId	MbsSessionId	M	1	Represents the identifier of the MBS Session.	
dnn	Dnn	O	0..1	Represents the DNN of the MBS session.	
snssai	Snssai	O	0..1	Represents the S-NSSAI of the MBS session.	
mbsServInfo	MbsServiceInfo	O	0..1	Represents the MBS Service Information. This attribute shall be provided, if available.	
suppFeat	SupportedFeatures	C	0..1	Contains the list of the supported features among the ones defined in clause 6.1.8. This attribute shall be present when feature negotiation needs to take place.	

6.1.6.2.3 Type: MbsPolicyDecision

Table 6.1.6.2.3-1: Definition of type MbsPolicyDecision

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsPccRules	map(MbsPccRule)	O	1..N	A map of MBS PCC rule(s) with the content being the MbsPccRule as described in clause 6.1.6.2.7. The key used in this map for each entry is the "mbsPccRuleId" attribute of the corresponding MbsPccRule instance.	
mbsQosDecs	map(MbsQosDec)	O	1..N	Map of MBS QoS Decision(s). The key used in this map for each entry is the "mbsQosId" attribute of the corresponding MbsQosDec instance. (NOTE)	
mbsQosChars	map(MbsQosChar)	O	1..N	Map of QoS characteristics for non-standard 5QIs and non-preconfigured 5QIs. The key of the map is the 5QI value within the "5qi" attribute of the corresponding MbsQosChar instance. (NOTE)	
authMbsSessAmbr	BitRate	O	0..1	The Authorized MBS Session-AMBR.	
mbsPcrts	array(MbsPcrt)	O	1..N	The MBS Policy Control Request Triggers(s) that the PCF requests to subscribe to.	
NOTE: This attribute shall not be removed if it was provisioned.					

6.1.6.2.4 Type: MbsPolicyData

Table 6.1.6.2.4-1: Definition of type MbsPolicyData

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsPolicyCtxtData	MbsPolicyCtxtData	M	1	Contains the parameters used to request MBS Policy Association creation/update.	
mbsPolicies	MbsPolicyDecision	C	0..1	Contains the provisioned MBS Policy Decision containing the MBS policies authorized by the PCF. This attribute shall be present in the response to a request to create an MBS Policy Association or a request to retrieve the properties of an existing MBS Policy Association, and may be present in the response to a request to update an existing MBS Policy Association.	
suppFeat	SupportedFeatures	C	0..1	Contains the list of negotiated supported features. This parameter shall be provided by the PCF in the response to a request in which the NF service consumer provided the list of features that it supports.	

6.1.6.2.5 Void

6.1.6.2.6 Void

6.1.6.2.7 Type: MbsPccRule

Table 6.1.6.2.7-1: Definition of type MbsPccRule

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsPccRuleId	string	M	1	Univocally identifies the MBS PCC rule within the related MBS session.	
mbsDlIpFlowInfo	array(FlowDescription)	C	1..N	Contains the MBS downlink IP flow packet filter(s) information. (NOTE 3)	
precedence	Uinteger	O	0..1	Determines the order in which this MBS PCC rule is applied relative to other MBS PCC rules within the same MBS session. (NOTE 1)	
refMbsQosDec	array(string)	C	1..N	A reference to the MbsQosDec policy decision type. It contains the value of the "mbsQosId" attribute of the referred MbsQosDec policy decision defined in clause 6.1.6.2.8. (NOTE 2, NOTE 3)	

NOTE 1: The "precedence" attribute is used to specify the precedence of the MBS PCC rule among all MBS PCC rules associated to an MBS session. It includes an integer value in the range of 0 to 255 (decimal). The higher the value of the "precedence" attribute, the lower the precedence of the MBS PCC rule to which it applies.
NOTE 2: Arrays are only introduced for future compatibility. In this release of the specification, the maximum number of elements in the array is 1.
NOTE 3: This attribute shall be present in the response to an MBS Policy Association Creation request and may be present in the response to an MBS Policy Association Update request.

6.1.6.2.8 Type: MbsQosDec

Table 6.1.6.2.8-1: Definition of type MbsQosDec

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsQosId	string	M	1	Univocally identifies the MBS QoS Decision within the related MBS session.	
5qi	5Qi	O	0..1	Contains the identifier of the authorized QoS parameters for the MBS service data flow. (NOTE 2)	
priorityLevel	5QiPriorityLevel	O	0..1	Indicates a priority in scheduling resources among MBS QoS flows. (NOTE 1)	
mbrDl	BitRate	O	0..1	Indicates the maximum bandwidth in downlink.	
gbrDl	BitRate	O	0..1	Indicates the guaranteed bandwidth in downlink.	
arp	Arp	O	0..1	Indicates the allocation and retention priority.	
averWindow	AverWindow	O	0..1	Represents the duration over which the guaranteed and maximum bitrates shall be calculated. (NOTE 1)	
mbsMaxDataBurstVol	MbsMaxDataBurstVol	O	0..1	Denotes the largest amount of data that is required to be transferred within a period. (NOTE 1)	

NOTE 1: This attribute is applicable only when a value different from the standardized 5QI values, defined in table 5.7.4-1 3GPP TS 23.501 [2], is provided.
NOTE 2: When the provided 5QI value is a dynamically assigned 5QI (i.e. from the non-standardized and non-preconfigured value range), the corresponding QoS parameters (e.g. Packet Delay Budget, Packet Error Rate, etc.) are provided in the corresponding MbsQosChar data structure.

6.1.6.2.9 Type: MbsQosChar

Table 6.1.6.2.9-1: Definition of type MbsQosChar

Attribute name	Data type	P	Cardinality	Description	Applicability
5qi	5Qi	M	1	Represents the identifier of the set of non-standardized and non-preconfigured MBS QoS parameters for an MBS service data flow.	
resourceType	QosResourceType	M	1	Indicates whether the MBS QoS resource type is GBR, delay critical GBR or non-GBR.	
priorityLevel	5QiPriorityLevel	M	1	Indicates the 5QI Priority Level within a range of 1 to 127 and encoded as an unsigned integer.	
packetDelayBudget	PacketDelBudget	M	1	Indicates the packet delay budget expressed in milliseconds and encoded as an unsigned integer.	
packetErrorRate	PacketErrRate	M	1	Indicates the packet error rate encoded as a string. Examples: - A Packer Error Rate of $4x10^{-6}$ shall be encoded as "4E-6". - A Packer Error Rate of 10^{-2} shall be encoded as"1E-2".	
averWindow	AverWindow	C	0..1	Indicates the averaging window. This attribute shall be present only for a GBR QoS flow or a Delay Critical GBR QoS flow.	
mbsMaxDataBurstVol	MbsMaxDataBurstVol	M	1	Indicates the maximum data burst volume, encoded as an unsigned integer.	

6.1.6.2.10 Type: MbsErrorReport

Table 6.1.6.2.11-1: Definition of type MbsErrorReport

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsReports	array(MbsReport)	O	1..N	Contains the reporting of MBS Policy decision level failure(s) and/or MBS PCC rule level failure(s).	

6.1.6.2.11 Type: MbsPolicyCtxtDataUpdate

Table 6.1.6.2.11-1: Definition of type MbsPolicyCtxtDataUpdate

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsServInfo	MbsServiceInfo	O	0..1	Represents the updated MBS Service Information.	
mbsPcrts	array(MbsPcrt)	O	1..N	Represents the list of MBS Policy Control Request Triggers that are met.	
mbsErrorReport	MbsErrorReport	O	0..1	Contains the reporting of MBS Policy decision level failure(s) and/or MBS PCC rule level failure(s).	

6.1.6.2.12 Type: MbsReport

Table 6.1.6.2.12-1: Definition of type MbsReport

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsPccRuleIds	array(string)	C	1..N	Contains the identifier(s) of the affected MBS PCC rule(s). This attribute shall be present if the reported failure is related to the MBS PCC rule(s) installation. (NOTE)	
mbsPccRuleStatus	MbsPccRuleStatus	C	0..1	Indicates the status of the MBS PCC rule(s) identified by the "mbsPccRuleIds" attribute. This attribute shall be present only if the "mbsPccRuleIds" attribute is present.	
failureCode	MbsFailureCode	C	0..1	Indicates the reason of the failure of the MBS Policy Decision or the MBS PCC rule(s) identified by the "mbsPccRuleIds" attribute. This attribute shall be present when available. (NOTE)	
NOTE: If the reported failure is due to MBS Policy Decision failure, then the "mbsPccRuleIds" attribute shall not be present and the "failureCode" attribute indicates the appropriate failure cause illustrating the MBS Policy Decision failure that occurred.					

6.1.6.3 Simple data types and enumerations

6.1.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

6.1.6.3.2 Simple data types

The simple data types defined in table 6.1.6.3.2-1 shall be supported.

Table 6.1.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
MbsMaxDataBurstVol	Integer	Represents MBS Maximum Data Burst Volume expressed in Bytes. Minimum = 1. Maximum = 2000000.	

6.1.6.3.3 Enumeration: MbsPcrt

The enumeration MbsPcrt represents the MBS Policy Control Request Triggers. It shall comply with the provisions defined in table 6.1.6.3.3-1.

Table 6.1.6.3.3-1: Enumeration MbsPcrt

Enumeration value	Description	Applicability
MBS_SESSION_UPDATE	Indicates the MBS Session Update policy control request trigger. This MBS Policy Control Request Trigger is implicitly subscribed by the PCF, i.e. pre-configured at the NF service consumer (MB-SMF).	

6.1.6.3.4 Enumeration: MbsFailureCode

The enumeration MbsFailureCode represents the reason behind the MBS Policy Decision failure. It shall comply with the provisions of table 6.1.6.3.4-1.

Table 6.1.6.3.4-1: Enumeration MbsFailureCode

Enumeration value	Description	Applicability
NF_MALFUNCTION	Indicates that the MBS PCC rule could not be successfully installed due to MB-SMF/MB-UPF malfunction.	
NF_RESOURCES_UNAVAILABLE	Indicates that the MBS PCC rule could not be successfully installed due to resources unavailable at the MB-SMF/MB-UPF.	
RESOURCE_ALLOCATION_FAILURE	Indicates that the MBS PCC rule could not be successfully installed or maintained since the associated MBS QoS flow establishment/modification failed or the associated MBS QoS flow was released.	
MBS_QOS_VALIDATION_FAILURE	Indicate that MBS QoS validation has failed.	
NO_MBS_QOS_FLOW	Indicates that there is no MBS QoS flow to which the MB-SMF can bind the MBS PCC rule(s).	
MBS_QOS_DECISION_ERROR	Indicates failure in the provisioning of MBS QoS Decision data.	
MBS_POLICY_PARAM_ERROR	Indicates that the information related to the provisioned MBS policy parameter(s) is incorrect, incomplete or inconsistent.	

6.1.6.3.5 Enumeration: MbsPccRuleStatus

The enumeration MbsPccRuleStatus represents the status of an MBS PCC rule. It shall comply with the provisions of table 6.1.6.3.5-1.

Table 6.1.6.3.5-1: Enumeration MbsPccRuleStatus

Enumeration value	Description	Applicability
ACTIVE	Indicates that the MBS PCC rule(s) are successfully installed.	
INACTIVE	Indicates that the MBS PCC rule(s) are removed.	

6.1.6.4 Data types describing alternative data types or combinations of data types

There are no data types describing alternative data types or combinations of data types defined for this API in this release of the specification.

6.1.6.5 Binary data

6.1.6.5.1 Binary Data Types

Table 6.1.6.5.1-1: Binary Data Types

Name	Clause defined	Content type

6.1.7 Error Handling

6.1.7.1 General

For the Npcf_MBSPolicyControl API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [5]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses are applicable for the Npcf_MBSPolicyControl API.

6.1.7.2 Protocol Errors

No specific procedures for the Npcf_MBSPolicyControl service are specified.

6.1.7.3 Application Errors

The application errors defined for the Npcf_MBSPolicyControl service are listed in Table 6.1.7.3-1.

Table 6.1.7.3-1: Application errors

Application Error	HTTP status code	Description
INVALID_MBS_SERVICE_INFO	400 Bad Request	The HTTP request is rejected because the provided MBS Service Information is invalid (e.g. invalid QoS reference), incorrect or insufficient for the PCF to perform MBS policy authorization.
FILTER_RESTRICTIONS_NOT_RESPECTED	400 Bad Request	The HTTP request is rejected because the MBS IP flow(s) description provided within the MBS Service Information cannot be handled due to the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [19] not being respected.
ERROR_INPUT_PARAMETERS	400 Bad Request	The HTTP request is rejected because the provided set of input parameters are incomplete, erroneous or missing necessary information for the PCF to perform MBS policy control.
MBS_SERVICE_INFO_NOT_AUTHORIZED	403 Forbidden	The HTTP request is rejected because the provided MBS Service Information is not authorized by the PCF.
MBS_POLICY_CONTEXT_DENIED	403 Forbidden	The HTTP request is rejected because the PCF does not accept the NF service consumer request due to operator policies and/or local configuration.
MBS_POLICY_ASSOCIATION_NOT_FOUND	404 Not Found	The HTTP request is rejected because the targeted MBS Policy Association does not exist at the PCF.

6.1.8 Feature negotiation

The optional features listed in table 6.1.8-1 are defined for the Npcf_MBSPolicyControl API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.1.8-1: Supported Features

Feature number	Feature Name	Description

6.1.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Npcf_MBSPolicyControl API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [9]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [10]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Npcf_MBSPolicyControl API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [10], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Npcf_MBSPolicyControl service.

The Npcf_MBSPolicyControl API defines a single scope "npcf-mbspolicycontrol" for the entire service, and it does not define any additional scopes at resource or operation level.

6.2 Npcf_MBSPolicyAuthorization Service API

6.2.1 Introduction

The Npcf_MBSPolicyAuthorization Service shall use the Npcf_MBSPolicyAuthorization API.

The API URI of the Npcf_MBSPolicyAuthorization Service shall be:

{apiRoot}/<apiName>/<apiVersion>

The request URIs used in HTTP requests from the NF service consumer towards the NF service producer shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [5], i.e.:

{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].
- The <apiName> shall be "npcf-mbspolicyauth".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.2.3.

6.2.2 Usage of HTTP

6.2.2.1 General

HTTP/2, IETF RFC 7540 [11], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [4].

The OpenAPI [6] specification of HTTP messages and content bodies for the Npcf_MBSPolicyAuthorization API is contained in Annex A.2.

6.2.2.2 HTTP standard headers

6.2.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

6.2.2.2.2 Content type

JSON, IETF RFC 8259 [12], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

JSON object used in the HTTP PATCH request shall be encoded according to "JSON Merge Patch" and shall be signalled by the content type "application/merge-patch+json", as defined in IETF RFC 7396 [22].

The "Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [13].

6.2.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4] may be supported.

6.2.3 Resources

6.2.3.1 Overview

This clause describes the structure of the resource URIs and the resources and methods used for the Npcf_MBSPolicyAuthorization service.

Figure 6.2.3.1-1 depicts the resource URIs structure for the Npcf_MBSPolicyAuthorization API.

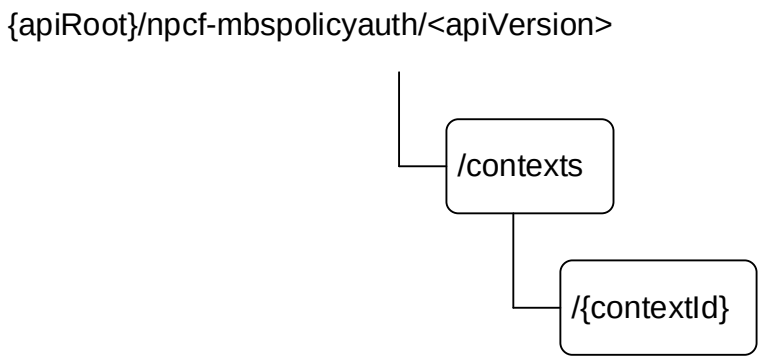

Figure 6.2.3.1-1: Resource URI structure of the Npcf_MBSPolicyAuthorization API

Table 6.2.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.2.3.1-1: Resources and methods overview

Resource purpose/name	Resource URI (relative path after API URI)	HTTP method or custom operation	Description (service operation)
MBS Application Session Contexts	/contexts	POST	Create a new MBS Application Session Context.
Individual MBS Application Session Context	/contexts/{contextId}	GET	Retrieve an existing Individual MBS Application Session Context resource.
		PATCH	Modify an existing Individual MBS Application Session Context resource.
		DELETE	Delete an existing Individual MBS Application Session Context resource.

6.2.3.2 Resource: MBS Application Session Contexts

6.2.3.2.1 Description

This resource represents the collection of "Individual MBS Application Session Context" resources managed by the PCF.

6.2.3.2.2 Resource Definition

Resource URI: **{apiRoot}/npcf-mbspolicyauth/<apiVersion>/contexts**

This resource shall support the resource URI variables defined in table 6.2.3.2.2-1.

Table 6.2.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.2.1.

6.2.3.2.3 Resource Standard Methods

6.2.3.2.3.1 POST

This method enables an NF service consumer (e.g. NEF, MBSF, AF) to request the creation of an MBS Application Session Context at the PCF.

This method shall support the URI query parameters specified in table 6.2.3.2.3.1-1.

Table 6.2.3.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.2.3.2.3.1-2 and the response data structures and response codes specified in table 6.2.3.2.3.1-3.

Table 6.2.3.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
MbsAppSessionCtxt	M	1	Contains the parameters to create an Individual MBS Application Session Context for MBS policy authorization.

Table 6.2.3.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MbsAppSessionCtxt	M	1	201 Created	Successful case. An Individual MBS Application Session Context resource is successfully created and a representation of the created resource is returned in the response body. A Location header field containing the URI of the created resource is also included.
ProblemDetails	O	0..1	400 Bad Request	(NOTE 2)
MbsExtProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the HTTP POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 6.2.7.				

Table 6.2.3.2.3.1-4: Headers supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/npcf-mbspolicyauth/<apiVersion>/contexts/{contextId}

6.2.3.2.4 Resource Custom Operations

There are no resource custom operations defined for this resource in this release of the specification.

6.2.3.3 Resource: Individual MBS Application Session Context

6.2.3.3.1 Description

This resource represents an "Individual MBS Application Session Context" resource managed by the PCF.

6.2.3.3.2 Resource Definition

Resource URI: **{apiRoot}/npcf-mbspolicyauth/<apiVersion>/contexts/{contextId}**

This resource shall support the resource URI variables defined in table 6.2.3.3.2-1.

Table 6.2.3.3.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.2.1.
contextId	string	Represents the unique identifier of the "Individual MBS Application Session Context" resource.

6.2.3.3.3 Resource Standard Methods

6.2.3.3.3.1 GET

This method enables an NF service consumer (e.g. NEF, MBSF, AF) to retrieve an existing "Individual MBS Application Session Context" resource at the PCF.

This method shall support the URI query parameters specified in table 6.2.3.3.3.1-1.

Table 6.2.3.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.2.3.3.3.1-2 and the response data structures and response codes specified in table 6.2.3.3.3.1-3.

Table 6.2.3.3.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 6.2.3.3.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MbsAppSessionCtxt	M	1	200 OK	Successful case. The requested Individual MBS Application Session Context resource is successfully returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
NOTE: The mandatory HTTP error status codes for the HTTP GET method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.2.3.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

Table 6.2.3.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

6.2.3.3.3.2 PATCH

This method enables an NF service consumer (e.g. NEF, MBSF, AF) to request the modification of an existing "Individual MBS Application Session Context" resource at the PCF.

This method shall support the URI query parameters specified in table 6.2.3.3.3.2-1.

Table 6.2.3.3.3.2-1: URI query parameters supported by the PATCH method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.2.3.3.3.2-2 and the response data structures and response codes specified in table 6.2.3.3.3.2-3.

Table 6.2.3.3.3.2-2: Data structures supported by the PATCH Request Body on this resource

Data type	P	Cardinality	Description
MbsAppSessionCtxtPatch	M	1	Contains the parameters to request the modification of an existing Individual MBS Application Session Context resource.

Table 6.2.3.3.3.2-3: Data structures supported by the PATCH Response Body on this resource

Data type	P	Cardinality	Response codes	Description
MbsAppSessionCtxt	M	1	200 OK	Successful case. The corresponding Individual MBS Application Session Context resource is successfully modified and a representation of the updated resource is returned in the response body.
n/a			204 No Content	Successful case. The corresponding Individual MBS Application Session Context resource is successfully modified and no content is returned in the response body.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
ProblemDetails	O	0..1	400 Bad Request	(NOTE 2)
MbsExtProblemDetails	O	0..1	403 Forbidden	(NOTE 2)
ProblemDetails	O	0..1	404 Not Found	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the HTTP PATCH method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 6.2.7.				

Table 6.2.3.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

Table 6.2.3.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

6.2.3.3.3 DELETE

This method enables an NF service consumer (e.g. NEF, MBSF, AF) to request the deletion of an existing "Individual MBS Application Session Context" resource at the PCF.

This method shall support the URI query parameters specified in table 6.2.3.3.3.3-1.

Table 6.2.3.3.3.3-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.2.3.3.3.3-2 and the response data structures and response codes specified in table 6.2.3.3.3.3-3.

Table 6.2.3.3.3.3-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 6.2.3.3.3.3-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Successful case. The corresponding Individual MBS Application Session Context resource is successfully deleted.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.
ProblemDetails	O	0..1	404 Not Found	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the HTTP DELETE method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: Failure cases are described in clause 6.2.7.				

Table 6.2.3.3.3.3-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

Table 6.2.3.3.3.3-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative PCF (service) instance.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the request is redirected.

6.2.3.3.4 Resource Custom Operations

There are no resource custom operations defined for this resource in this release of the specification.

6.2.4 Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

6.2.5 Notifications

There are no notifications defined for this API in this release of the specification.

6.2.6 Data Model

6.2.6.1 General

This clause specifies the application data model supported by the API.

Table 6.2.6.1-1 specifies the data types defined for the Npcf_MBSPolicyAuthorization service based interface protocol.

Table 6.2.6.1-1: Npcf_MBSPolicyAuthorization specific Data Types

Data type	Clause defined	Description	Applicability
AcceptableMbsServInfo	6.2.6.2.4	Contains the MBS Service Information that can be accepted by the PCF.	
MbsExtProblemDetails	6.2.6.4.1	Identifies the MBS related extensions to the ProblemDetails data structure.	
MbsAppSessionCtxt	6.2.6.2.2	Represents the parameters of an MBS Application Session Context.	
MbsAppSessionCtxtPatch	6.2.6.2.3	Represents the modifications to an existing MBS Application Session Context.	

Table 6.2.6.1-2 specifies data types re-used by the Npcf_MBSPolicyAuthorization service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Npcf_MBSPolicyAuthorization service based interface.

Table 6.2.6.1-2: Npcf_MBSPolicyAuthorization re-used Data Types

Data type	Reference	Comments	Applicability
BitRate	3GPP TS 29.571 [15]	Represents a bit rate.	
Dnn	3GPP TS 29.571 [15]	Identifies a DNN.	
MbsMediaComp	3GPP TS 29.571 [15]	Represents an MBS Media Component.	
MbsServiceInfo	3GPP TS 29.571 [15]	Represents MBS Service Information.	
MbsSessionId	3GPP TS 29.571 [15]	Represents an MBS Session Identifier.	
ProblemDetails	3GPP TS 29.571 [15]	Contains error related additional information.	
RedirectResponse	3GPP TS 29.571 [15]	Contains redirection related information.	
Snssai	3GPP TS 29.571 [15]	Identifies an S-NSSAI.	
SupportedFeatures	3GPP TS 29.571 [15]	Represents the list of supported features. It is used to negotiate the applicability of the optional features.	

6.2.6.2 Structured data types

6.2.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

6.2.6.2.2 Type: MbsAppSessionCtxt

Table 6.2.6.2.2-1: Definition of type MbsAppSessionCtxt

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsSessionId	MbsSessionId	M	1	Represents the identifier of the corresponding MBS Session.	
mbsServInfo	MbsServiceInfo	C	0..1	Represents the MBS Service Information. This attribute shall be provided, if available.	
dnn	Dnn	O	0..1	Represents the DNN of the MBS session.	
snssai	Snssai	O	0..1	Represents the S-NSSAI of the MBS session.	
contactPcfInd	boolean	O	0..1	Indicates whether the PCF shall be contacted or not, i.e.: - "true" means that the PCF shall be contacted; and - "false" means that the PCF shall not be contacted. When this attribute is not present, the default value is "false". This attribute may only be present in the response to an MBS Application Session Context update request.	
suppFeat	SupportedFeatures	C	0..1	Contains the list of the supported features (among the ones defined in clause 6.2.8). This parameter shall be provided if feature negotiation needs to take place.	

6.2.6.2.3 Type: MbsAppSessionCtxtPatch

Table 6.2.6.2.3-1: Definition of type MbsAppSessionCtxtPatch

Attribute name	Data type	P	Cardinality	Description	Applicability
mbsServInfo	MbsServiceInfo	O	0..1	Represents the updated MBS Service Information.	

6.2.6.2.4 Type: AcceptableMbsServInfo

Table 6.2.6.2.4-1: Definition of type AcceptableMbsServInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
accMbsServInfo	map(MbsMediaComp)	C	1..N	Contains the maximum acceptable bandwidth per media component that can be accepted and authorized by the PCF. Each map entry encoded using the MbsMediaComp data structure shall only include the "mbsMedCompNum" attribute and the "maxReqMbsBwDl" attribute indicating the maximum acceptable bandwidth. The key of the map is the "medCompN" attribute of the corresponding MbsMediaComp data structure provided as a map entry. (NOTE)	
accMaxMbsBw	BitRate	C	0..1	Contains the maximum acceptable bandwidth. (NOTE)	
NOTE: When the acceptable MBS bandwidth is per MBS media component, only the "accMbsServInfo" attribute shall be present. When the acceptable MBS bandwidth applies to all the MBS media components, only the "accMaxMbsBw" attribute shall be present.					

6.2.6.3 Simple data types and enumerations

6.2.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

6.2.6.3.2 Simple data types

The simple data types defined in table 6.2.6.3.2-1 shall be supported.

Table 6.2.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability

6.2.6.4 Data types describing alternative data types or combinations of data types

6.2.6.4.1 Type: MbsExtProblemDetails

Table 6.2.6.4.1-1: Definition of type MbsExtProblemDetails as a list of to be combined data types

Data type	Cardinality	Description	Applicability
ProblemDetails	1	Contains the details of the encountered problem, as defined in 3GPP TS 29.571 [15].	
AcceptableMbsServInfo	0..1	Contains the MBS Service Information that can be accepted by the PCF.	

6.2.6.5 Binary data

6.2.6.5.1 Binary Data Types

Table 6.2.6.5.1-1: Binary Data Types

Name	Clause defined	Content type

6.2.7 Error Handling

6.2.7.1 General

For the Npcf_MBSPolicyAuthorization API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [5]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses are applicable for the Npcf_MBSPolicyAuthorization API.

6.2.7.2 Protocol Errors

No specific procedures for the Npcf_MBSPolicyAuthorization service are specified.

6.2.7.3 Application Errors

The application errors defined for the Npcf_MBSPolicyAuthorization service are listed in table 6.2.7.3-1.

Table 6.2.7.3-1: Application errors

Application Error	HTTP status code	Description
INVALID_MBS_SERVICE_INFO	400 Bad Request	The HTTP request is rejected because the provided MBS Service Information is invalid (e.g. invalid QoS reference), incorrect or insufficient for the PCF to perform MBS policy authorization.
FILTER_RESTRICTIONS_NOT_RESPECTED	400 Bad Request	The HTTP request is rejected because the MBS IP flow(s) description provided within the MBS Service Information cannot be handled due to the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [19] not being respected.
MBS_SERVICE_INFO_NOT_AUTHORIZED	403 Forbidden	The HTTP request is rejected because the provided MBS Service Information is not authorized by the PCF.
MBS_SESSION_POL_AUTH_CTXT_NOT_FOUND	404 Not Found	The HTTP request is rejected because the targeted Individual MBS Application Session Context does not exist at the PCF.

6.2.8 Feature negotiation

The optional features listed in table 6.2.8-1 are defined for the Npcf_MBSPolicyAuthorization API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.2.8-1: Supported Features

Feature number	Feature Name	Description

6.2.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Npcf_MBSPolicyAuthorization API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [9]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [10]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Npcf_MBSPolicyAuthorization API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [10], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Npcf_MBSPolicyAuthorization service.

The Npcf_MBSPolicyAuthorization API defines a single scope "npcf-mbspolicyauth" for the entire service, and it does not define any additional scopes at resource or operation level.

Annex A (normative): OpenAPI specification

A.1 General

This Annex specifies the formal definition of the API(s) defined in the present specification. It consists of OpenAPI specifications in YAML format.

This Annex takes precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API(s).

NOTE 1: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification files contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see clause 5.3.1 of 3GPP TS 29.501 [5] and clause 5B of 3GPP TR 21.900 [7]).

A.2 Npcf_MBSPolicyControl API

```
openapi: 3.0.0
info:
  title: Npcf_MBSPolicyControl API
  version: 1.0.1
  description: |
    MBS Policy Control Service
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: >
    3GPP TS 29.537 V17.1.0; 5G System; Multicast/Broadcast Policy Control Services.
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.537/'

security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-mbspolicycontrol

servers:
  - url: '{apiRoot}/npcf-mbspolicycontrol/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501.

paths:
  /mbs-policies:
    post:
      summary: Request the creation of a new MBS Policy Association.
      operationId: CreateMBSPolicy
      tags:
        - MBS Policies (Collection)
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MbsPolicyCtxtData'
      responses:
        '201':
          description: >
            Created. An Individual MBS Policy resource is successfully created.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MbsPolicyData'
          headers:
            Location:
              description: >
                Contains the URI of the newly created Individual MBS Policy resource.
              required: true
              schema:
                type: string
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          description: Forbidden.
          content:
            application/problem+json:
              schema:
                $ref:
'TS29537_Npcf_MBSPolicyAuthorization.yaml#/components/schemas/MbsExtProblemDetails'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
```

```
      '429':
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'

  /mbs-policies/{mbsPolicyId}:
    parameters:
      - name: mbsPolicyId
        in: path
        description: >
          Contains the identifier of the concerned Individual MBS Policy resource.
        required: true
        schema:
          type: string

    get:
      summary: Read an Individual MBS Policy resource.
      operationId: GetIndMBSPolicy
      tags:
        - Individual MBS Policy (Document)
      responses:
        '200':
          description: >
            OK. The requested Individual MBS Policy resource is successfully returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MbsPolicyData'
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

    delete:
      summary: Deletes an existing Individual MBS Policy resource.
      operationId: DeleteIndMBSPolicy
      tags:
        - Individual MBS Policy  (Document)
      parameters:
        - name: mbsPolicyId
          in: path
          description: >
            Contains the identifier of the concerned Individual MBS Policy resource.
          required: true
          schema:
            type: string
      responses:
        '204':
          description: >
            No Content. The concerned Individual MBS Policy resource is successfully deleted.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
```

```
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

  /mbs-policies/{mbsPolicyId}/update:
    post:
      summary: Request the update of an existing MBS Policy Association.
      operationId: UpdateIndMBSPolicy
      tags:
        - Individual MBS Policy  (Document)
      parameters:
        - name: mbsPolicyId
          in: path
          description: >
            Contains the identifier of the concerned Individual MBS Policy resource.
          required: true
          schema:
            type: string
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MbsPolicyCtxtDataUpdate'
      responses:
        '200':
          description: >
            OK. The targeted Individual MBS Policy resource is successfully updated.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MbsPolicyData'
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          description: Forbidden.
          content:
            application/problem+json:
              schema:
                $ref:
'TS29537_Npcf_MBSPolicyAuthorization.yaml#/components/schemas/MbsExtProblemDetails'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

components:
```

```
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            npcf-mbspolicycontrol: Access to the Npcf_MBSPolicyControl API

  schemas:
    MbsPolicyCtxtData:
      description: >
        Contains the parameters used to request the creation of an MBS Policy
        Association.
      type: object
      properties:
        mbsSessionId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsSessionId'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        snssai:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        mbsServInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsServiceInfo'
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - mbsSessionId

    MbsPolicyDecision:
      description: >
        Represents the parameters constituting an MBS Policy Decision.
      type: object
      properties:
        mbsPccRules:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MbsPccRule'
          minProperties: 1
          description: >
            A map of MBS PCC rule(s) with each map entry containing the MbsPccRule data structure.
            The key of the map for each entry is the mbsPccRuleId attribute of the corresponding
            MbsPccRule data structure.
          nullable: true
        mbsQosDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MbsQosDec'
          minProperties: 1
          description: >
            A map of MBS QoS Decision(s) with each map entry containing the MbsQosDec data
structure.
            The key of the map for each entry is the mbsQosId attribute of the corresponding
            MbsQosDec data structure.
        mbsQosChars:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MbsQosChar'
          minProperties: 1
          description: >
            A map of MBS QoS Characteristics set(s) with each map entry containing the MbsQosChar
data
            structure. The key of the map for each entry is the 5QI attribute of the corresponding
            MbsQosDec data structure.
        authMbsSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        mbsPcrts:
          type: array
          items:
            $ref: '#/components/schemas/MbsPcrt'
          minItems: 1
          nullable: true

    MbsPolicyData:
      description: >
        Contains the MBS policy data provisioned as part of an MBS Policy Association.
      type: object
      properties:
```

```
      mbsPolicyCtxtData:
        $ref: '#/components/schemas/MbsPolicyCtxtData'
      mbsPolicies:
        $ref: '#/components/schemas/MbsPolicyDecision'
      suppFeat:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
    required:
      - mbsPolicyCtxtData

  MbsPccRule:
    description: Represents the parameters constituting an MBS PCC rule.
    type: object
    properties:
      mbsPccRuleId:
        type: string
      mbsDlIpFlowInfo:
        type: array
        items:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/FlowDescription'
        minItems: 1
      precedence:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
      refMbsQosDec:
        type: array
        items:
          type: string
        minItems: 1
        maxItems: 1
    required:
      - mbsPccRuleId

  MbsQosDec:
    description: Represents the parameters constituting an MBS QoS Decision.
    type: object
    properties:
      mbsQosId:
        type: string
      5qi:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
      priorityLevel:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevel'
      mbrDl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
      gbrDl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
      arp:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Arp'
      averWindow:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindow'
      mbsMaxDataBurstVol:
        $ref: '#/components/schemas/MbsMaxDataBurstVol'
    required:
      - mbsQosId

  MbsQosChar:
    description: >
      Represents the parameters constituting a set of explicitly signalled QoS characteristics.
    type: object
    properties:
      5qi:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
      priorityLevel:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevel'
      resourceType:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/QosResourceType'
      packetDelayBudget:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
      packetErrorRate:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketErrRate'
      averWindow:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindow'
      mbsMaxDataBurstVol:
        $ref: '#/components/schemas/MbsMaxDataBurstVol'
    required:
      - 5qi
      - resourceType
      - priorityLevel
      - packetDelayBudget
```

```
        - packetErrorRate
        - mbsMaxDataBurstVol

    MbsPolicyCtxtDataUpdate:
      description: >
        Contains the parameters to request the modification of an existing MBS Policy Association.
      type: object
      properties:
        mbsServInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsServiceInfo'
        mbsPcrts:
          type: array
          items:
            $ref: '#/components/schemas/MbsPcrt'
          minItems: 1
        mbsErrorReport:
          $ref: '#/components/schemas/MbsErrorReport'

    MbsErrorReport:
      description: >
        Represents the reporting of MBS Policy decision level failure(s) and/or MBS PCC rule level
        failure(s).
      type: object
      properties:
        mbsReports:
          type: array
          items:
            $ref: '#/components/schemas/MbsReport'
          minItems: 1

    MbsReport:
      description: >
        Contains information about the MBS Policy Decision level failure(s) and/or the MBS PCC
        rule level failure(s).
      type: object
      properties:
        mbsPccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
        mbsPccRuleStatus:
          $ref: '#/components/schemas/MbsPccRuleStatus'
        failureCode:
          $ref: '#/components/schemas/MbsFailureCode'

# Simple data types:

    MbsMaxDataBurstVol:
      description: Represents the MBS Maximum Data Burst Volume expressed in Bytes.
      type: integer
      minimum: 1
      maximum: 2000000

# ENUMS:

    MbsPcrt:
      anyOf:
      - type: string
        enum:
          - MBS_SESSION_UPDATE
      - type: string
        description: >
          Represents MBS Policy Control Request Triggers.
      description: |
        Possible values are
        - MBS_SESSION_UPDATE: Indicates the MBS Session Update policy control request trigger.

    MbsPccRuleStatus:
      anyOf:
      - type: string
        enum:
          - ACTIVE
          - INACTIVE
      - type: string
        description: >
          Represents the MBS PCC rule status.
      description: |
```

```
        Possible values are
        - ACTIVE: Indicates that the MBS PCC rule(s) are successfully installed.
        - INACTIVE: Indicates that the MBS PCC rule(s) are removed.

    MbsFailureCode:
      anyOf:
      - type: string
        enum:
          - NF_MALFUNCTION
          - NF_RESOURCES_UNAVAILABLE
          - RESOURCE_ALLOCATION_FAILURE
          - MBS_QOS_VALIDATION_FAILURE
          - NO_MBS_QOS_FLOW
          - MBS_QOS_DECISION_ERROR
          - MBS_POLICY_PARAM_ERROR
      - type: string
        description: >
          Represents the reason for the MBS Policy Decision(s) enforcement failure or the MBS PCC
          rule(s) installation failure.
      description: |
        Possible values are:
        - NF_MALFUNCTION: Indicates that the MBS PCC rule could not be successfully installed due to
MB-SMF/MB-UPF malfunction.
        - NF_RESOURCES_UNAVAILABLE: Indicates that the MBS PCC rule could not be successfully
installed due to resources unavailable at the MB-SMF/MB-UPF.
        - RESOURCE_ALLOCATION_FAILURE: Indicates that the MBS PCC rule could not be successfully
installed or maintained since the associated MBS QoS flow establishment/modification failed or the
associated MBS QoS flow was released.
        - MBS_QOS_VALIDATION_FAILURE: Indicates that MBS QoS validation has failed.
        - NO_MBS_QOS_FLOW: Indicates that there is no MBS QoS flow to which the MB-SMF can bind the
MBS PCC rule(s).
        - MBS_QOS_DECISION_ERROR: Indicates failure in the provisioning of MBS QoS Decision data.
        - MBS_POLICY_PARAM_ERROR: Indicates that the information related to the provisioned MBS
policy parameter(s) is incorrect, incomplete or inconsistent.
```

A.3 Npcf_MBSPolicyAuthorization API

```
openapi: 3.0.0
info:
  title: Npcf_MBSPolicyAuthorization API
  version: 1.0.1
  description: |
    MBS Policy Authorization Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: >
    3GPP TS 29.537 V17.1.0; 5G System; Multicast/Broadcast Policy Control Services.
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.537/'

security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-mbspolicyauth

servers:
  - url: '{apiRoot}/npcf-mbspolicyauth/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in subclause 4.4 of 3GPP TS 29.501.

paths:
  /contexts:
    post:
      summary: Request the creation of a new Individual MBS Application Session Context resource.
      operationId: CreateMBSAppSessionCtxt
      tags:
        - MBS Application Session Contexts (Collection)
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/MbsAppSessionCtxt'
      responses:
        '201':
          description: >
            Created. An Individual MBS Application Session Context resource is successfully created
            and a representation of the created resource is returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MbsAppSessionCtxt'
          headers:
            Location:
              description: >
                Contains the URI of the newly created Individual MBS Application Session Context
                resource.
              required: true
              schema:
                type: string
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          description: Forbidden.
          content:
            application/problem+json:
              schema:
                $ref: '#/components/schemas/MbsExtProblemDetails'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
```

```
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'

  /contexts/{contextId}:
    parameters:
      - name: contextId
        in: path
        description: >
          Contains the identifier of the Individual MBS Application Session Context resource.
        required: true
        schema:
          type: string

    get:
      summary: Read an existing Individual MBS Application Session Context resource.
      operationId: GetMBSAppSessionCtxt
      tags:
        - Individual MBS Application Session Context (Document)
      responses:
        '200':
          description: >
            OK. The requested Individual MBS Application Session Context resource is successfully
            returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MbsAppSessionCtxt'
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

    patch:
      summary: Request the modification of an existing Individual MBS Application Session Context
resource.
      operationId: ModifyMBSAppSessionCtxt
      tags:
        - Individual MBS Application Session Context (Document)
      requestBody:
        required: true
        content:
          application/merge-patch+json:
            schema:
              $ref: '#/components/schemas/MbsAppSessionCtxtPatch'
      responses:
        '200':
          description: >
            OK. The requested Individual MBS Application Session Context resource is successfully
            modified and a representation of the updated resource is returned in the response body.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/MbsAppSessionCtxt'
        '204':
          description: >
```

```
            No Content. The corresponding Individual MBS Application Session Context resource is
            successfully modified and no content is returned in the response body.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          description: Forbidden.
          content:
            application/problem+json:
              schema:
                $ref: '#/components/schemas/MbsExtProblemDetails'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

    delete:
      summary: Request the deletion of an existing Individual MBS Application Session Context
resource.
      operationId: DeleteMBSAppSessionCtxt
      tags:
        - Individual MBS Application Session Context (Document)
      responses:
        '204':
          description: >
            No Content. The corresponding Individual MBS Application Session Context resource is
            successfully deleted.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            npcf-mbspolicyauth: Access to the Npcf_MBSPolicyAuthorization API

  schemas:
    MbsAppSessionCtxt:
      description: >
        Represents the parameter of an MBS Application Session Context.
      type: object
```

```
      properties:
        mbsSessionId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsSessionId'
        mbsServInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsServiceInfo'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        snssai:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        contactPcfInd:
          type: boolean
          default: false
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - mbsSessionId

    MbsAppSessionCtxtPatch:
      description: >
        Represents the modifications to an existing MBS Application Session Context resource.
      type: object
      properties:
        mbsServInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsServiceInfo'

    AcceptableMbsServInfo:
      description: >
        Contains the MBS Service Information that can be accepted by the PCF.
      type: object
      properties:
        accMbsServInfo:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/MbsMediaComp'
          minProperties: 1
        accMaxMbsBw:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
      oneOf:
        - required: [accMbsServInfo]
        - required: [accMaxMbsBw]

# Data types describing alternative data types or combinations of data types:

    MbsExtProblemDetails:
      description: Identifies the MBS related extensions to the ProblemDetails data structure.
      allOf:
        - $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        - $ref: '#/components/schemas/AcceptableMbsServInfo'
```

Annex B (informative): Withdrawn API versions

B.1 General

This Annex lists withdrawn API versions of the APIs defined in the present specification. Clause 4.3.1.6 of 3GPP TS 29.501 [5] describes the withdrawal of API versions.

B.2 Npcf_MBSPolicyControl API

The API versions listed in table B.2-1 are withdrawn for the Npcf_MBSPolicyControl API.

Table B.2-1: Withdrawn API versions of the Npcf_MBSPolicyControl service

API version number	Remarks

B.3 Npcf_MBSPolicyAuthorization API

The API versions listed in table B.3-1 are withdrawn for the Npcf_MBSPolicyAuthorization API.

Table B.3-1: Withdrawn API versions of the Npcf_MBSPolicyAuthorization service

API version number	Remarks

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-01	CT3#119bis-e	C3-220401				TS Skeleton	0.0.0
2022-01	CT3#119bis-e	C3-220457				Inclusion of C3-220113, C3-220114, C3-220115, C3-220116, C3-220402, C3-220403, C3-220404 C3-220491, C3-220492, C3-220493	0.1.0
2022-04	CT3#121-e	C3-222483				Inclusion of C3-222056, C3-222124, C3-222127, C3-222403, C3-222404, C3-222405, C3-222406 C3-222407, C3-222462	0.2.0
2022-05	CT3#122-e	C3-223506				Inclusion of C3-223561, C3-223574, C3-223562, C3-223563, C3-223564, C3-223568, C3-223565 C3-223566, C3-223573, C3-223308	0.3.0
2022-06	CT#96	CP-221097				Presentation to TSG CT for information	1.0.0
2022-06						Update of info and externalDocs fields in OpenAPI specs by MCC	1.0.1
2022-09	CT3#123-e					Inclusion of C3-224644, C3-224645, C3-224646, C3-224709, C3-224710, C3-224711	1.0.2
2022-09	CT#97e	CP-222129				Presentation to TSG CT for approval	2.0.0
2022-09	CT#97e	CP-222129				Approved by TSG CT	17.0.0
2022-12	CT#98e	CP-223167	0001	1	F	Attribute corrections in the description and data model clause in Npcf_MBSPolicyControl Service	17.1.0
2022-12	CT#98e	CP-223166	0005	-	F	Wrong data type for MBS QoS information	17.1.0
2022-12	CT#98e	CP-223167	0006	1	F	Add 404 NOT FOUND for the Npcf_MBSPolicyauthorization update and delete service	17.1.0
2022-12	CT#98e	CP-223166	0007	-	F	Correction to architecture figure	17.1.0
2022-12	CT#98e	CP-223167	0008	1	F	Correction to content type of Npcf_MBSPolicyAuthorization API	17.1.0
2022-12	CT#98e	CP-223166	0009	-	F	Correction to Individual MBS Policy	17.1.0
2022-12	CT#98e	CP-223166	0010	-	F	Correction to MbsAppSessionCtxt	17.1.0
2022-12	CT#98e	CP-223167	0011	1	F	Correction to Npcf_MBSPoliyControl_Create operation	17.1.0
2022-12	CT#98e	CP-223167	0012	1	F	Correction to reponse of create operation	17.1.0
2022-12	CT#98e	CP-223166	0013	-	F	Correction to the indication that the PCF has to be contacted	17.1.0
2022-12	CT#98e	CP-223167	0014	1	F	Corrections for Npcf_MBSPolicyControl service	17.1.0
2022-12	CT#98e	CP-223188	0015	-	F	Update of info and externalDocs fields	17.1.0
2023-03	CT#99	CP-230131	0018	1	F	Miscellaneous essential corrections to the MBS PCF APIs	17.2.0

History

Document history		
V17.0.0	September 2022	Publication
V17.1.0	January 2023	Publication
V17.2.0	April 2023	Publication