ETSI TS 129 537 V18.3.0 (2024-05)

5G;
5G System;
Multicast/Broadcast Policy Control services;
Stage 3
(3GPP TS 29.537 version 18.3.0 Release 18)

Reference
RTS/TSGC-0329537vi30

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 9113: "HTTP/2".

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

[13] IETF RFC 9457: "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.

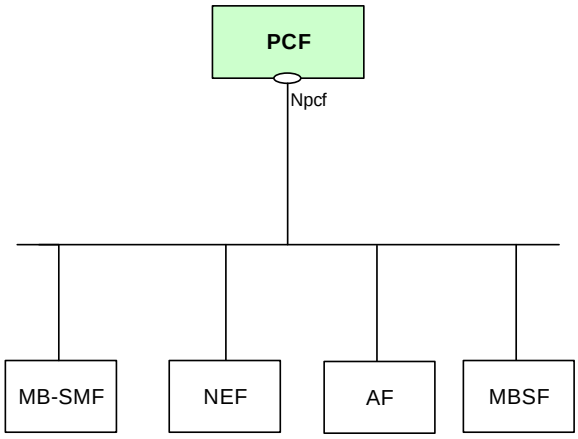

Figure 4-1: Reference model for the MBS PCF Services – SBI representation

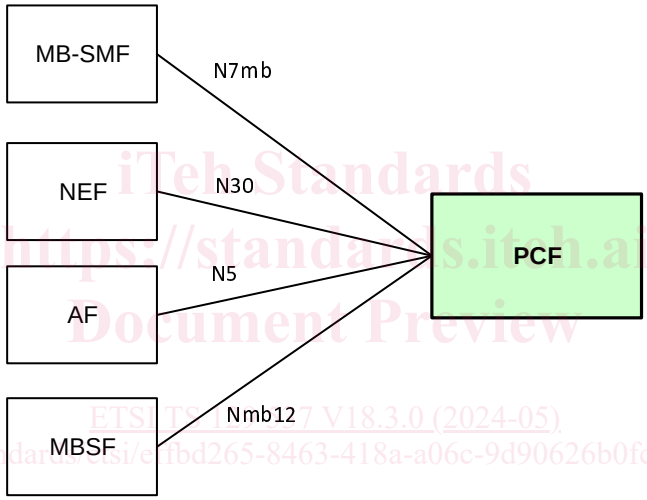

Figure 4-2: Reference Model for the MBS PCF Services – Reference point representation

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

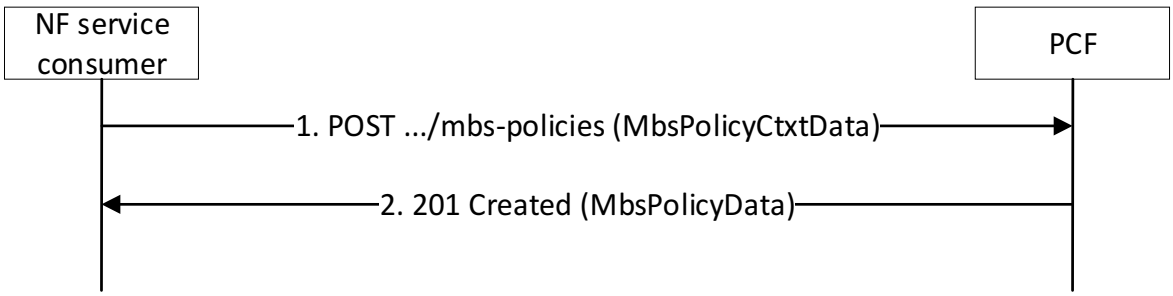

Figure 5.2.2.2.2-1: Procedure for MBS Policy Association establishment

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;
   - the list of supported features, if feature negotiation needs to take place, within the "suppFeat" attribute; and
   - the Area Session Policy ID within the "areaSessPolId" attribute, if the "AreaSessPolicy" feature is supported and the request corresponds to an MBS Session that is an instance of a location-dependent MBS service.

   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 if the "AreaSessPolicy" feature is supported, the Area Session Policy ID is present within the "areaSessPolId" attribute, and the PCF is not already serving this location-dependent MBS service (i.e., there is no MBS Policy Association at the PCF for the MBS Session ID provided within "mbsSessionId" attribute), 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 the "AreaSessPolicy" feature is supported and the MBS session is an instance of a location-dependent MBS service, the corresponding Area Session Policy 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.

NOTE 4: For a location-dependent MBS service, the PCF deregisters at the BSF from being the PCF serving the MBS Session as indicated in NOTE 3 above only if it is the last MBS Policy Association associated to the location-dependent MBS service (i.e., associated to the corresponding MBS Session ID).

- 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.