ETSI TS 129 507 V15.9.0 (2022-03)

5G;
5G System;
Access and Mobility Policy Control Service;
Stage 3
(3GPP TS 29.507 version 15.9.0 Release 15)

Reference
RTS/TSGC-0329507vf90

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 http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

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

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present specification provides the stage 3 definition of the Access and Mobility Policy Control Service (Npcf_AMPolicyControl) of the 5G System.

The stage 2 definition and procedures of the Access and Mobility Policy Control Service are contained in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4]. The 5G System Architecture is defined in 3GPP TS 23.501 [2].

Stage 3 call flows are provided in 3GPP TS 29.513 [7].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition of the 5G System are specified in 3GPP TS 29.500 [5] and 3GPP TS 29.501 [6].

The Access and Mobility Policy Control Service is provided by the Policy Control Function (PCF). This service provides Access and Mobility Policies.

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 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

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

[6] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[7] 3GPP TS 29.513: "5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3".

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

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

[10] OpenAPI, "OpenAPI 3.0.0 Specification", https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md.

[11] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[12] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[13] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[14] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[15] void.

[16] void.

[17] 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".

[18] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[19] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

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

[22] 3GPP TR 21.900: "Technical Specification Group working methods".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

AMF	Access and Mobility Management Function
DNN	Data Network Name
GPSI	Generic Public Subscription Identifier
GUAMI	Globally Unique AMF Identifier
JSON	JavaScript Object Notation
NRF	Network Repository Function
PCF	Policy Control Function
PEI	Permanent Equipment Identifier
PRA	Presence Reporting Area
RFSP	RAT Frequency Selection Priority
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
V-PCF	Visited Policy Control Function

4 Access and Mobility Policy Control Service

4.1 Service Description

4.1.1 Overview

The Access and Mobility Policy Control Service, as defined in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4], is provided by the Policy Control Function (PCF).

This service provides AMF access control and mobility management related policies to the AMF and offers the following functionalities:

- policy creation based on a request from the AMF during UE registration;
- notification of the AMF of the updated policies which are subscribed; and

- deletion of the policy context for a UE.

4.1.2 Service Architecture

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The Policy and Charging related 5G architecture is also described in 3GPP TS 29.513 [7].

The Access and Mobility Policy Control Service (Npcf_AMPolicyControl) is part of the Npcf service-based interface exhibited by the Policy Control Function (PCF).

The known consumer of the Npcf_AMPolicyControl service is the Access and Mobility Management Function (AMF).

The AMF accesses the Access and Mobility Policy Control Service at the PCF via the N15 Reference point. In the roaming scenario, the N15 reference point is located between the V-PCF in the visited network and the AMF.

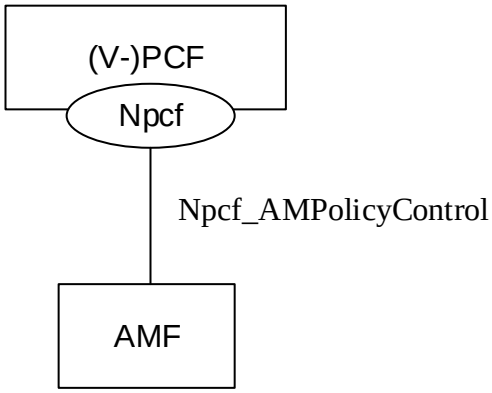

Figure 4.1.2-1: Reference Architecture for the Npcf_AMPolicyControl Service; SBI representation

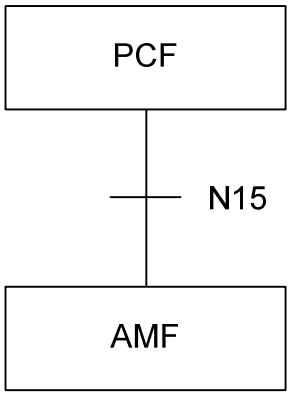

Figure 4.1.2-2: Non-roaming Reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

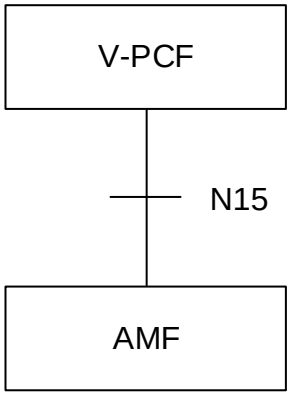

Figure 4.1.3-2: Roaming reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

4.1.3 Network Functions

4.1.3.1 Policy Control Function (PCF)

The Policy Control Function (PCF):

- Supports unified policy framework to govern network behaviour; and
- Provides Access and Mobility Management related policies to the AMF that enforces them.

In the roaming scenario, the Visited Policy Control Function (V-PCF) provides the functions described in this subclause towards the visited network.

4.1.3.2 NF Service Consumers

The Access and Mobility Management function (AMF) provides:

- Registration management;
- Connection management;
- Reachability management; and
- Mobility Management.

4.2 Service Operations

4.2.1 Introduction

Table 4.2.1-1: Operations of the Npcf_AMPolicyControl Service

Service operation name	Description	Initiated by
Npcf_AMPolicyControl_Create	Creates an AM Policy Association and provides corresponding policies to the NF consumer.	NF consumer (AMF)
Npcf_AMPolicyControl_Update	Updates of an AM Policy Association and provides corresponding policies to the NF consumer when the policy control request trigger is met or the AMF is relocated due to the UE mobility and the old PCF is selected.	NF consumer (AMF)
Npcf_AMPolicyControl_UpdateNotify	Provides updated policies to the NF consumer.	PCF (V-PCF in roaming case)
Npcf_AMPolicyControl_Delete	Provides means for the NF consumer to delete the AM Policy Association.	NF consumer (AMF)

4.2.2 Npcf_AMPolicyControl_Create Service Operation

4.2.2.1 General

The procedure in the present subclause is applicable when the NF service consumer creates an AM policy association when the UE registers to the network, and when the the AMF is relocated (between the different AMF sets) and the new AMF selects a new PCF. The procedure for the case where the AMF is relocated and the new AMF selects the old PCF is defined in subclause 4.2.3.1.

The creation of an AM policy association only applies for normally registered UEs, i.e., it does not apply for Emergency Registered UEs.

Figure 4.2.2.1-1 illustrates the creation of a policy association.

Figure 4.2.2.1-1: Creation of a policy association

When a UE registers and a UE context is being established, the AMF can obtain Service Area Restrictions, RFSP index, and GPSI from the UDM during the update location procedure and shall decide based on local policies whether to request policies from the PCF.

To request policies from the PCF, the NF service consumer (e.g. AMF) shall send an HTTP POST request with: "{apiRoot}/npcf-am-policy-control/v1/policies" as Resource URI and the PolicyAssociationRequest data structure as request body that shall include:

- Notification URI encoded as "notificationUri" attribute; and

- SUPI encoded as "supi" attribute,

and that shall include when available:

- GPSI encoded as "gpsi" attribute;
- Access type encoded as "accessType" attribute;
- Permanent Equipment Identifier (PEI) encoded as "pei" attribute;
- User Location Information encoded as "userLoc" attribute;
- UE Time Zone encoded as "timeZone" attribute;
- Serving PLMN Identifier encoded as "servingPlmn" attribute;
- RAT type encoded as "ratType" attribute;
- Service Area Restrictions (see subclause 4.2.2.3.1) derived from the Service Area Restrictions obtained from the UDM by mapping any service areas denoted by geographical information into Tracking Area Identities (TAIs) and encoded as "servAreaRes" attribute;
- RFSP index (see subclause 4.2.2.3.2) as obtained from the UDM encoded as "rfsp" attribute;
- A list of Internal Group Identifiers encoded as "groupIds" attribute;
- if the NF service consumer is an AMF, the GUAMI encoded as "guami" attribute;
- if the NF service consumer is an AMF, the name of a service produced by the AMF that expects to receive information within Npcf_AMPolicyControl_UpdateNotify service operation encoded as "serviceName" attribute;
- Alternate or backup IPv4 Address(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute;
- Alternate or backup IPv6 Address(es) where to send Notifications encoded as "altNotifIpv6Addrs" attribute; and
- trace control and configuration parameters information encoded as "traceReq" attribute.

Upon the reception of the HTTP POST request, the PCF:

- shall assign a policy association ID;
- shall determine the applicable policy (taking into consideration and optionally modifying possibly received Service Area Restrictions and/or RFSP index);
- for the succesfull case shall send a HTTP "201 Created" response with the URI for the created resource in the "Location" header field

NOTE: The assigned policy association ID is part of the URI for the created resource and is thus associated with the SUPI.

and the the PolicyAssociation data type as body including:

- conditionally AMF Access and Mobility Policy (see subclause 4.2.2.3), i.e.:

  a) if the PCF received the "servAreaRes" in the request, Service Area Restrictions encoded as "servAreaRes" attribute; and/or

  b) if the PCF received the "rfsp" attributes in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute;

- optionally one or several of the following Policy Control Request Trigger(s) encoded as "triggers" attribute (see subclause 4.2.3.2):

  a) Location change (tracking area); and

  b) Change of UE presence in PRA; and

- if the Policy Control Request Trigger "Change of UE presence in PRA" is provided, the presence reporting areas for which reporting is required encoded as "pras" attribute;

- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7 and according to the following provisions:

  - if the user information received within the "supi" attribute is unknown, the PCF shall reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "USER_UNKNOWN";

  - if the PCF is, due to incomplete, erroneous or missing information in the request not able to provision an AM policy decision, the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR_REQUEST_PARAMETERS".

If the PCF received an GUAMI, the PCF may subscribe to GUAMI changes using the AMFStatusChange service operation of the Namf_Communication service specified in 3GPP TS 29.518 [14], and it may use the Nnrf_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the obtained GUAMI and possibly service name) to query the other AMFs within the AMF set.

If the PCF received a "traceReq" attribute, it shall perform trace procedures as defined in 3GPP TS 32.422 [18].

4.2.2.2 Void

4.2.2.2.0 Void

4.2.2.2.1 Void

4.2.2.2.2 Void

4.2.2.3 AMF Access and Mobility Policy

4.2.2.3.1 Service Area Restriction

If service area restrictions are enabled, the Service Area Restriction information is encoded using the "ServiceAreaRestriction" data type defined in 3GPP TS 29.571 [11] and consists of:

- a limited allowed area represented as:

  a) the maximum number of allowed TAs that can be traversed encoded as "maxNumOfTAs" attribute; or

  b) both of:

     (i) a list of allowed Tracking Area Identities (TAIs) encoded as "tacs" attributes within the "areas" attribute; and

     (ii) the "restrictionType" attribute set to "ALLOWED_AREAS"; or

  c) both a) and b) above;

- or a limited allowed area represented as:

  a) the maximum number of allowed TAs that can be traversed encoded as "maxNumOfTAsForNotAllowedAreas" attribute; or

  b) all of:

     (i) a list of not allowed Tracking Area Identities (TAIs) encoded as "tacs" attributes within the "areas" attribute; and

     (ii) the "restrictionType" attribute set to "NOT_ALLOWED_AREAS"; and

(iii) the maximum number of allowed TAs that can be traversed encoded as "maxNumOfTAsForNotAllowedAreas" attribute;

- or a not allowed area represented as:

a) a list of not allowed Tracking Area Identities (TAIs) encoded as "tacs" attributes within the "areas" attribute; and

b) the "restrictionType" attribute set to "NOT_ALLOWED_AREAS".

When the "restrictionType" attribute is set to "NOT_ALLOWED_AREAS", the "maxNumOfTAs" attribute shall not be present.

When the "restrictionType" attribute is set to "ALLOWED_AREAS", the "maxNumOfTAsForNotAllowedAreas" attribute shall not be present.

When for a limited allowed area both, "maxNumOfTAs" and "areas" attributes are present, the "maxNumOfTAs" attribute represents the upper limit of the limited allowed area. The AMF may add any not yet visited tracking areas to the allowed area represented by the "areas" attribute until the total number of TAs reaches the "maxNumOfTAs" attribute value.

NOTE 1: The "maxNumOfTAs" attribute value represents the maximum number of TAs of the limited allowed area. When "maxNumOfTAs" attribute value is lower than the number of TAs in the "areas" attribute it represents the maximum number of TAs allowed inside the limited allowed area defined by the TAs contained in the "areas" attribute. When the "maxNumOfTAs" attribute value is higher than the number of TAs in the "areas" attribute it represents that additional TAs up to the "maxNumOfTAs" attribute value can be dynamically added to the area defined by the TAs contained in the "areas" attribute..

When for a limited allowed area the following three attributes are present:

- "maxNumOfTAsForNotAllowedAreas" attribute; and
- the "restrictionType" attribute set to "NOT_ALLOWED_AREAS"; and
- the "areas" attribute,

the "maxNumOfTAsForNotAllowedAreas" attribute represents the maximum number of TAs allowed in a limited allowed area outside the not allowed area represented in the "areas" attribute. The limited allowed area is dynamically calculated by the AMF, and the TAs outside of the dynamically calculated limited allowed area become not allowed TAs.

NOTE 2: Both, the "maxNumOfTAsForNotAllowedAreas" attribute and the "maxNumOfTAs" attribute, when present in a "ServiceAreaRestriction" data type instance that does not include the "areas" attribute and the "restrictionType" attribute, represent a maximum number of allowed TAs in a limited allowed area dynamically calculated by the AMF.

When the authorized service area restrictions result in an unlimited set of tracking areas, the PCF shall include an empty "servAreaRes" attribute.

4.2.2.3.2 RFSP Index

The RFSP Index is an index referring to a UE information used locally by the Access Network in order to apply specific radio resource management strategies. It shall be encoded using the RfspIndex data type defined in 3GPP TS 29.571 [11].

4.2.3 Npcf_AMPolicyControl_Update Service Operation

4.2.3.1 General

The procedure in the present subclause is applicable when the NF service consumer modifies an existing AM policy association (including the case where the AMF is relocated and the new AMF selects to maintain the policy association with the old PCF and to update the Notification URI).

Figure 4.2.3.1-1 illustrates the update of a policy association.

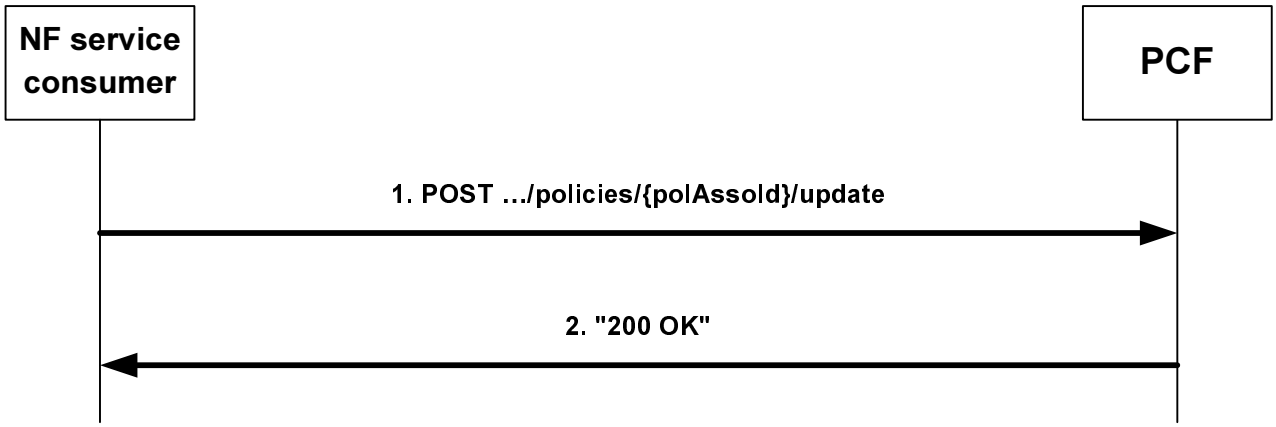

Figure 4.2.3.1-1: Update of a policy association

The AMF as NF service consumer invokes this procedure when a policy control request trigger (see subclause 4.2.3.2) occurs. When the Service Area restriction change trigger or the RFSP index change trigger occur, the AMF shall always invoke the procedure. When the location change trigger or the change of UE presence in PRA trigger occurs, the AMF shall only invoke the procedure if the PCF has subscribed to that event trigger.

If an AMF knows by implementation specific means that the UE context has been transferred to an AMF with another GUAMI within the AMF set, it may also invoke this procedure to update the Notification URI and the GUAMI.

NOTE 1: Either the old or the new AMF can invoke this procedure.

During the AMF relocation, if the new AMF received the resource URI of the individual AM Policy from the old AMF and selects the old PCF, the new AMF shall also invoke this procedure to update the Notification URI and the GUAMI. The new AMF may also update the alternate or backup IP addresses.

To request policies from the PCF and/or to update the Notification URI, and/or to update the trace control configuration, and/or to request the termination of trace, the NF Service Consumer (e.g. AMF) shall request the update of an AM Policy Association by providing relevant parameters about the UE context by sending an HTTP POST request with "{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}/update" as Resource URI and the PolicyAssociationUpdateRequest data structure as request body that shall include:

- at least one of the following:

  1. a new Notification URI encoded in the "notificationUri" attribute; and/or

  2. observed Policy Control Request Trigger(s) (see subclause 4.2.3.2) encoded as "triggers" attribute;

  3. if a Service Area restriction change occurred, the Service Area Restrictions (see subclause 4.2.2.3.1) as obtained from the UDM encoded as "servAreaRes" attribute;

  4. if a RFSP index change occurred, the RFSP index (see subclause 4.2.2.3.2) as obtained from the UDM encoded as "rfsp" attribute;

  5. if a UE location change occurred, the UE location encoded as "userLoc" attribute;

  6. if the Policy Control Request Trigger "Change of UE presence in PRA" is provided, the current presence status of the UE for the presence reporting areas for which reporting was requested, if not previously provided, or the presence reporting areas for which reporting was requested and the status has changed encoded as "praStatuses" attribute.

  7. if the trace control configuration needs to be updated, trace control and configuration parameters information encoded as "traceReq" attribute;and

  8. if trace needs to be terminated, the "traceReq" attribute set to the Null value;

  9. for AMF relocation scenarios, if available, alternate or backup IPv4 Address(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute;

10. for AMF relocation scenarios, if available, alternate or backup IPv6 Address(es) where to send Notifications encoded as "altNotifIpv6Addrs" attribute; and/or

11. for AMF relocation scenarios, if available, the new GUAMI encoded as "guami" attribute.

NOTE 2: An alternate NF service consumer than the one that requested the generation of the subscription resource can send the request. For instance, an AMF as service consumer can change.

Upon the reception of the HTTP POST request, the PCF:

- shall update the corresponding individual AM Policy resource based on the information provided by the AMF;
- shall determine the applicable policy based on local policy;
- for the succesfull case shall send a HTTP "200 OK" response with the PolicyUpdate data type as body with possible updates for that applicable policy and Policy Control Request Trigger(s) encoded as described in subclause 4.2.3.3 and according to the following provisions:

  a) if the PCF received the "servAreaRes" in the request, Service Area Restrictions encoded as "servAreaRes" attribute; and/or

  b) if the PCF received the "rfsp" attributes in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute;

- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7 and according to the following provisions:

  - if the PCF is, due to incomplete, erroneous or missing information in the request not able to provision an AM policy decision, the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR_REQUEST_PARAMETERS".

If the PCF received a "traceReq" attribute, it shall perform trace procedures as defined in 3GPP TS 32.422 [18].

If the AMF received the request of removal of Service Area Restrictions and/or RFSP from the UDM, the AMF shall remove the authorized Service Area Restrictions and/or RFSP provisioned by the PCF and apply the configured Service Area Restrictions and/or RFSP at the AMF to the UE without the interaction with the PCF.

If the PCF received a new GUAMI, the PCF may subscribe to GUAMI changes using the AMFStatusChange service operation of the Namf_Communication service specified in 3GPP TS 29.518 [14], and it may use the Nnrf_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the obtained GUAMI and possibly service name) to query the other AMFs within the AMF set.

4.2.3.2 Policy Control Request Triggers

The following Policy Control Request Triggers are defined (see subclause 6.1.2.5 of 3GPP TS 23.503 [4]):

- "LOC_CH", i.e. location change (tracking area): the tracking area of the UE has changed;
- "PRA_CH", i.e. change of UE presence in PRA: the UE is entering/leaving a Presence Reporting Area, this includes reporting the initial status at the time the request for reports is initiated;
- "SERV_AREA _CH", i.e. Service Area Restriction change: the UDM notifies the AMF that the subscribed service area restriction information has changed; and
- "RFSP_CH", i.e. RFSP index change: the UDM notifies the AMF that the subscribed RFSP index has changed.

4.2.3.3 Encoding of updated policy

Updated policies shall be encoded within the PolicyUpdate data type that may include:

- AMF Access and Mobility Policy (see subclause 4.2.2.3) Service Area Restriction encoded as "servAreaRes" attribute;
- AMF Access and Mobility Policy (see subclause 4.2.2.3) RFSP Index encoded as "rfsp" attribute;

- updated Policy Control Request Trigger(s) (see subclause 4.2.3.2) encoded as "triggers" attribute i.e.:

  1) either a new complete list of applicable Policy Control Request Trigger(s) including one or several of the following:

     a) Location change (tracking area);

     b) Change of UE presence in PRA; or

  2) a "NULL" value to request the removal of all previously installed Policy Control Request Trigger(s); and

- if the Policy Control Request Trigger "Change of UE presence in PRA" is provided or if that trigger was already set but the requested presence reporting areas need to be changed, the presence reporting areas for which reporting is required encoded as "pras" attribute encoded as follows:

  a) A new entry shall be added by supplying a new identifier as key and the corresponding PresenceInfo data type instance with complete contents as value as an entry within the map.

  b) An existing entry shall be modified by supplying the existing identifier as key and the PresenceInfo data type instance with complete contents as value as an entry within the map.

  c) An existing entry shall be deleted by supplying the existing identifier as key and "NULL" as value as an entry within the map.

  d) For an unmodified entry, no entry needs to be provided within the map; and

- if the Policy Control Request Trigger "Change of UE presence in PRA" is removed, the presence reporting areas for which reporting was required shall be removed by providing the "pras" attribute with "NULL" as value.

4.2.4 Npcf_AMPolicyControl_UpdateNotify Service Operation

4.2.4.1 General

The PCF may decide to update policies or to request the termination of the policy association and shall then use an Npcf_AMPolicyControl_UpdateNotify service operation.

The following procedures using the Npcf_AMPolicyControl_UpdateNotify service operation are supported:

- policy update notification; and
- request for termination of the policy association.

4.2.4.2 Policy update notification

Figure 4.2.4.2-1 illustrates the policy update notification.

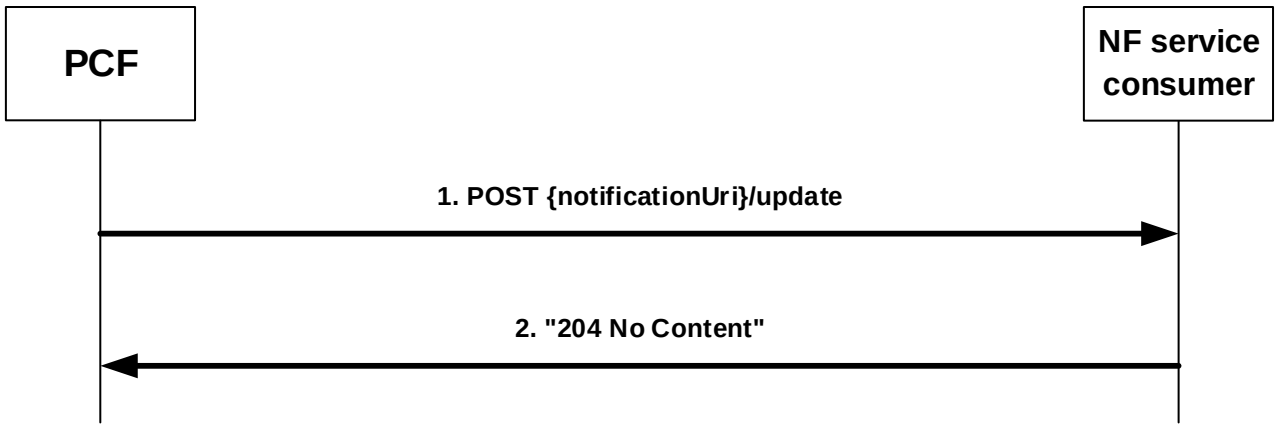

Figure 4.2.4.2-1: policy update notification

The PCF may decide to update policies and shall then send an HTTP POST request with "{notificationUri}/update" as URI (where the Notification URI was previously supplied by the NF service consumer) and the PolicyUpdate data structure as request body encoded as described in subclause 4.2.3.3.

Upon the reception of the HTTP POST request, the NF service consumer:

- shall enforce the received updated policy;
- shall either send a HTTP "204 No Content" response indicating the success of the enforcement or an appropriate failure response; and
- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7.

If the AMF as NF service consumer is not able to handle the notification but knows by implementation specific means that another AMF is able to handle the notification, it shall reply with an HTTP "307 temporary redirect" error response pointing to the URI of the new AMF. If the AMF is not able to handle the notification but another unknown AMF could possibly handle the notification, it shall reply with an HTTP "404 Not found" error response.

If the PCF receives a "307 temporary redirect" response, the PCF shall resend the failed policy update notification request using the received URI in the Location header field as Notification URI. Subsequent policy update notifications, triggered after the failed one, shall be sent to the Notification URI provided by the NF service consumer during the corresponding policy association creation/update.

If the PCF becomes aware that a new AMF is requiring notifications (e.g. via the "404 Not found" response or via Namf_Communication service AMFStatusChange Notifications, see 3GPP TS 29.518 [14], or via link level failures), and the PCF knows alternate or backup IPv4 or IPv6 Addess(es) where to send Notifications (e.g. via "altNotifIpv4Addrs" or "altNotifIpv6Addrs" attributes received when the policy association was created or via AMFStatusChange Notifications, or via the Nnrf_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the service name and GUAMI obtained during the creation of the subscription) to query the other AMFs within the AMF set), the PCF shall exchange the authority part of the corresponding Notification URI with one of those addresses and shall use that URI in any subsequent communication.

If the PCF received a "404 Not found" response, the PCF should resend the failed policy update notification request to that URI.

4.2.4.3 Request for termination of the policy association

Figure 4.2.4.3-1 illustrates the request for a termination of the policy association.

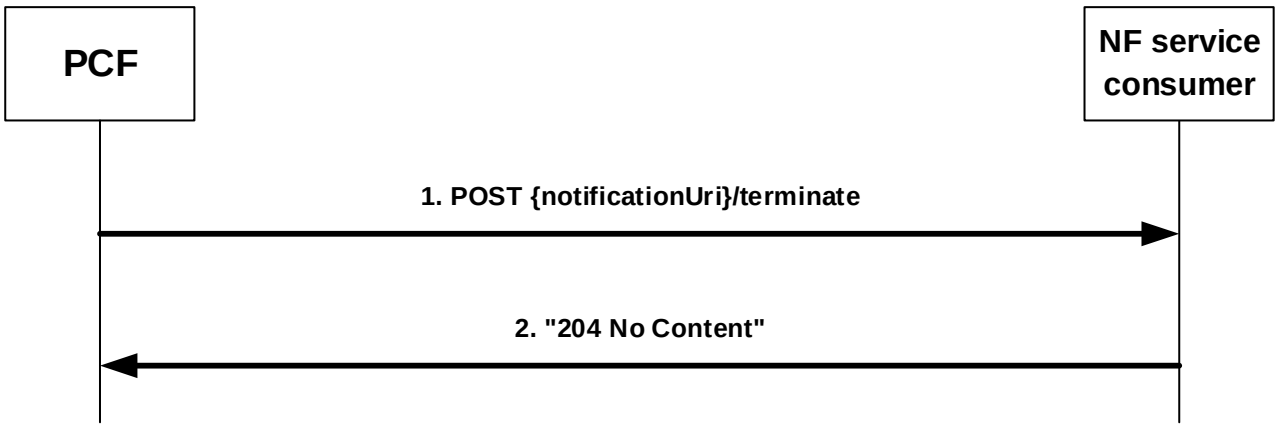

Figure 4.2.4.3-1: request for a termination of the policy association

The PCF may to request the termination of the policy association and shall then send an HTTP POST request with "{notificationUri}/terminate" as URI (where the Notification URI was previously supplied by the NF service consumer) and the TerminationNotification data structure as request body that shall include:

- the policy association ID encoded as "polAssoId" attribute; and
- the cause why the PCF requests the termination of the policy association encoded as "cause" attribute.

Upon the reception of the HTTP POST request, the NF service consumer:

- shall either send a HTTP "204 No Content" responsefor the succesfull processing of the HTTP POST request or an appropriate failure response; and
- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7.

After the succesfull processing of the HTTP POST request, the NF service consumer shall remove the context related to the policy association but still apply the provisioned AM policies to the UE and invoke the Npcf_AMPolicyControl_Delete Service Operation defined in subclause 4.2.5 to terminate the policy association.

If the AMF as NF service consumer is not able to handle the notification but knows by implementation specific means that another AMF is able to handle the notification, it shall reply with an HTTP "307 temporary redirect" error response pointing to the URI of the new AMF. If the AMF is not able to handle the notification but another unknown AMF could possibly handle the notification, it shall reply with an HTTP "404 Not found" error response.

If the PCF receives a "307 temporary redirect" response, the PCF shall resend the failed request for termination of the policy association using the received URI in the Location header field as Notification URI.

If the PCF becomes aware that a new AMF is requiring notifications (e.g. via the "404 Not found" response or via Namf_Communication service AMFStatusChange Notifications, see 3GPP TS TS 29.518 [14], or via link level failures), and the PCF knows alternate or backup IPv4 or IPv6 Addess(es) where to send Notifications (e.g. via "altNotifIpv4Addrs" or "altNotifIpv6Addrs" attributes received when the policy association was created or via AMFStatusChange Notifications, or via the Nnrf_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the service name and GUAMI obtained during the creation of the subscription) to query the other AMFs within the AMF set), the PCF shall exchange the authority part of the corresponding Notification URI with one of those addresses and shall resend the failed request for termination of the policy association to that URI.

If the PCF received a "404 Not found" response, the PCF should resend the failed request for termination of the policy association to that URL.

4.2.5 Npcf_AMPolicyControl_Delete Service Operation

Figure 4.2.5-1 illustrates the deletion of a policy association.

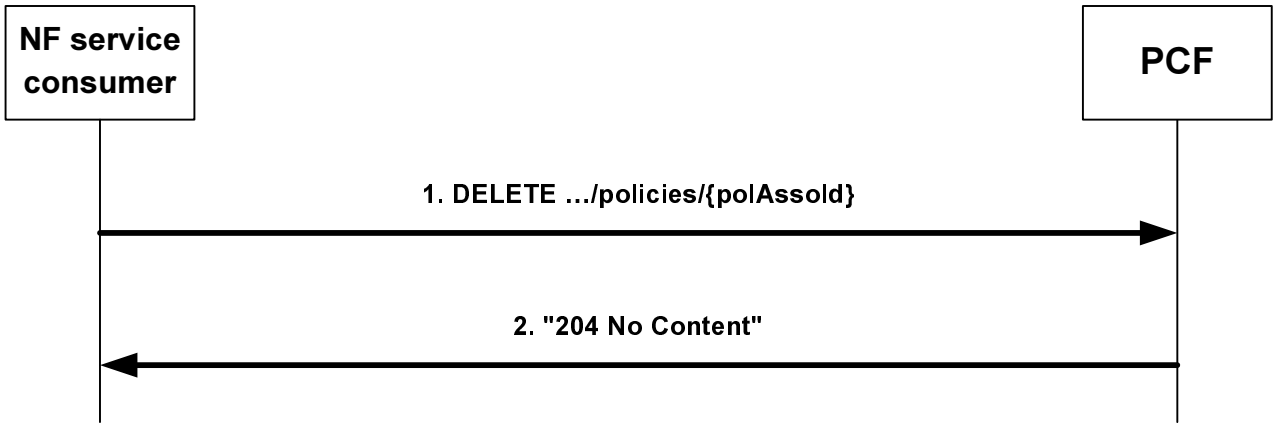

Figure 4.2.5-1: Deletion of a policy association

The AMF as NF service consumer requests that the policy association is deleted when the corresponding UE context is terminated, e.g. during UE de-registration from the network.

During the AMF relocation, the old AMF shall invoke this procedure when:

- the resource URI of the "Individual AM Policy Association" resource is not transferred to the new AMF; or
- the new AMF informs the old AMF that the "Individual AM Policy Association" resource is not being reused (i.e. the old PCF is not being reused).

To request that the policy association is deleted, the NF service consumer (e.g. AMF) shall send an HTTP DELETE request with "{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}" as Resource URI.

Upon the reception of the HTTP DELETE request, the PCF shall:

- delete the policy association;
- send either an HTTP "204 No Content" response indicating the success of the deletion or an appropriate failure response; and
- if errors occur when processing the HTTP DELETE request, apply error handling procedures as specified in subclause 5.7.

5 Npcf_AMPolicyControl API

5.1 Introduction

The Access and Mobility Policy Control Service shall use the Npcf_AMPolicyControl API.

The request URI used in HTTP request from the NF service consumer towards the PCF shall have the structure defined in subclause 4.4.1 of 3GPP TS 29.501 [6], i.e.:

{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [6].
- The {apiName} shall be "npcf-am-policy-control".
- The {apiVersion} shall be "v1".
- The {apiSpecificResourceUriPart} shall be set as described in subclause 5.3.

5.2 Usage of HTTP

5.2.1 General

HTTP/2, IETF RFC 7540 [8], shall be used as specified in clause 5 of 3GPP TS 29.500 [5].

HTTP/2 shall be transported as specified in subclause 5.3 of 3GPP TS 29.500 [5].

The OpenAPI [10] specification of HTTP messages and content bodies for the Npcf_AMPolicyControl is contained in Annex A.

5.2.2 HTTP standard headers

5.2.2.1 General

See subclause 5.2.2 of 3GPP TS 29.500 [5] for the usage of HTTP standard headers.

5.2.2.2 Content type

JSON, IETF RFC 8259 [9], shall be used as content type of the HTTP bodies specified in the present specification as specified in subclause 5.4 of 3GPP TS 29.500 [5] The use of the JSON format shall be signalled by the content type "application/json".

"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 [21].

5.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in subclause 5.2.3.2 of 3GPP TS 29.500 [5] shall be applicable

5.3 Resources

5.3.1 Resource Structure

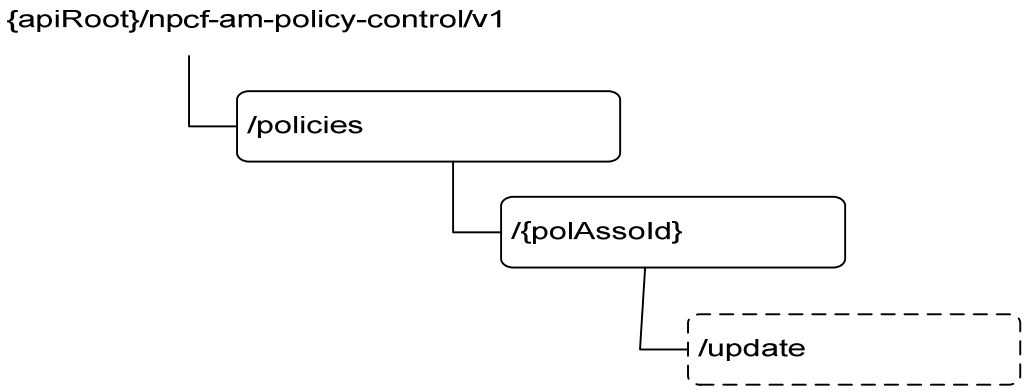

Figure 5.3.1-1: Resource URI structure of the Npcf_AMPolicyControl API

Table 5.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 5.3.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
AM Policy Associations	{apiRoot}/ npcf-am-policy-control/ v1/policies	POST	Create a new Individual AM Policy Association resource.
Individual AM Policy Association	{apiRoot} /npcf-am-policy-control/ v1/policies/ {polAssoId}	GET	Read the Individual AM Policy Association resource.
		DELETE	Delete the Individual AM Policy Association resource.
	{apiRoot} /npcf-am-policy-control/ v1/policies/ {polAssoId}/update	update (POST)	Report observed event trigger and obtain updated policies.

5.3.2 Resource: AM Policy Associations

5.3.2.1 Description

This resource represents a collection of Individual AM policy Associations.

5.3.2.2 Resource definition

Resource URI: **{apiRoot}/npcf-am-policy-control/v1/policies**

This resource shall support the resource URI variables defined in table 5.3.2.2-1.

Table 5.3.2.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See subclause 5.1

5.3.2.3 Resource Standard Methods

5.3.2.3.1 POST

This method shall support the URI query parameters specified in table 5.3.2.3.1-1.

Table 5.3.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.3.2.3.1-2 and the response data structures and response codes specified in table 5.3.2.3.1-3.

Table 5.3.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
PolicyAssociationRequest	M	1	Input parameters for the creation of a policy association.

Table 5.3.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
PolicyAssociation	M	1	201 Created	Policy association was created and policies are being provided.
ProblemDetails	O	0..1	400 Bad Request	(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 [5] also apply. NOTE 2: Failure cases are described in subclause 5.7.				

5.3.3 Resource: Individual AM Policy Association

5.3.3.1 Description

This document resource represents an individual AM policy association.

5.3.3.2 Resource definition

Resource URI: **{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}**

This resource shall support the resource URI variables defined in table 5.3.2.2-1.

Table 5.3.2.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See subclause 5.1.
polAssoId	Identifier of a policy association.

5.3.3.3 Resource Standard Methods

5.3.3.3.1 GET

This method shall support the URI query parameters specified in table 5.3.2.3.1-1.

Table 5.3.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.3.2.3.1-2 and the response data structures and response codes specified in table 5.3.2.3.1-3.

Table 5.3.3.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 5.3.3.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
PolicyAssociation	M	1	200 OK	
NOTE: The mandatory HTTP error status codes for the GET method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

5.3.3.3.2 DELETE

This method shall support the URI query parameters specified in table 5.3.3.3.2-1.

Table 5.3.3.3.2-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.3.3.3.2-2 and the response data structures and response codes specified in table 5.3.3.3.2-3.

Table 5.3.3.3.2-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 5.3.3.3.2-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The policy association was successfully deleted.
NOTE: The mandatory HTTP error status codes for the DELETE method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

5.3.3.4 Resource Custom Operations

5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

Custom operation URI	Mapped HTTP method	Description
{apiRoot} /npcf-am-policy-control/v1/ policies/ {polAssoId}/update	POST	Report observed event trigger and obtain updated policies.

5.3.3.4.2 Operation: Update

5.3.3.4.2.1 Description

The update custom operation allows an NF service consumer to report the occurrence on a police request trigger and to obtain related updated policies.

5.3.3.4.2.2 Operation Definition

This operation shall support the request data structures specified in table 5.3.3.4.2.2-1 and the response data structure and response codes specified in table 5.3.3.4.2.2-2.

Table 5.3.3.4.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
PolicyAssociationUpdateRequest	M	1	Describes the observed event trigger(s).

Table 5.3.3.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
PolicyUpdate	M	1	200 OK	Describes updated policies.
ProblemDetails	O	0..1	400 Bad Request	(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 [5] also apply. NOTE 2: Failure cases are described in subclause 5.7.				

5.4 Custom Operations without associated resources

None.

5.5 Notifications

5.5.1 General

Table 5.5.1-1: Notifications

Custom operation URI	Mapped HTTP method	Description
{notificationUri}/update	POST	Policy Update Notification.
{notificationUri}/terminate	POST	Request for termination of the policy association.

5.5.2 Policy Update Notification

5.5.2.1 Description

This notification is used by the PCF to provide updates of access and mobility policies to the NF service consumer.

5.5.2.2 Operation Definition

This operation shall support the request data structures specified in table 5.5.2.2-1 and the response data structure and response codes specified in table 5.5.2.2-2.

Table 5.5.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
PolicyUpdate	M	1	Updated policies.

Table 5.5.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The policies were successfully updated.
n/a			307 temporary redirect	The NF service consumer shall generate a Location header field containing a URI pointing to another NF service consumer to which the notification should be send.
ProblemDetails	M	1	404 Not Found	The NF service consumer can use this response when the notification can be sent to another unknown host.
NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

5.5.3 Request for termination of the policy association

5.5.3.1 Description

This notification is used by the PCF to request the termination of a policy association.

5.5.3.2 Operation Definition

This operation shall support the request data structures specified in table 5.5.3.2-1 and the response data structure and response codes specified in table 5.5.3.2-2.

Table 5.5.3.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
TerminationNotification	M	1	Request to terminate the policy association.

Table 5.5.3.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The request for policy association termination was received.
n/a			307 temporary redirect	The NF service consumer shall generate a Location header field containing a different URI pointing to another NF service consumer to which the notification should be send.
ProblemDetails	M	1	404 Not Found	The NF service consumer can use this response when the notification can be sent to another unknown host.
NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

5.6 Data Model

5.6.1 General

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

Table 5.6.1-1 specifies the data types defined for the Npcf_AMPolicyControl service based interface protocol.

Table 5.6.1-1: Npcf_AMPolicyControl specific Data Types

Data type	Section defined	Description	Applicability
PolicyAssociation	5.6.2.2	Description of a policy association that is returned by the PCF when a policy Association is created, or read.	
PolicyAssociationReleaseCause	5.6.3.4	The cause why the PCF requests the termination of the policy association.	
PolicyAssociationRequest	5.6.2.3	Information that NF service consumer provides when requesting the creation of a policy association.	
PolicyAssociationUpdateRequest	5.6.2.4	Information that NF service consumer provides when requesting the update of a policy association.	
PolicyUpdate	5.6.2.5	Updated policies that the PCF provides in a notification or in the reply to an Update Request.	
RequestTrigger	5.6.3.3	Enumeration of possible Request Triggers.	
TerminationNotification	5.6.2.6	Request to terminate a policy Association that the PCF provides in a notification.	

Table 5.6.1-2 specifies data types re-used by the Npcf_AMPolicyControl 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_AMPolicyControl service based interface.

Table 5.6.1-2: Npcf_AMPolicyControl re-used Data Types

Data type	Reference	Comments	Applicability
AccessType	3GPP TS 29.571 [11]		
Gpsi	3GPP TS 29.571 [11]	Generic Public Subscription Identifier	
GroupId	3GPP TS 29.571 [11]		
Guami	3GPP TS 29.571 [11]	Globally Unique AMF Identifier	
Ipv4Addr	3GPP TS 29.571 [11]		
Ipv6Addr	3GPP TS 29.571 [11]		
NetworkId	3GPP TS 29.571 [11]		
Pei	3GPP TS 29.571 [11]	Permanent Equipment Identifier	
PresenceInfo	3GPP TS 29.571 [11]	Presence reporting area information	
PresenceInfoRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "PresenceInfo" data type, but with the OpenAPI "nullable: true" property.	
ProblemDetails	3GPP TS 29.571 [11]		
Uri	3GPP TS 29.571 [11]		
UserLocation	3GPP TS 29.571 [11]		
RatType	3GPP TS 29.571 [11]		
RfspIndex	3GPP TS 29.571 [11]		
ServiceAreaRestriction	3GPP TS 29.571 [11]	Within the areas attribute, only tracking area codes shall be included.	
Supi	3GPP TS 29.571 [11]	Subscription Permanent Identifier	
SupportedFeatures	3GPP TS 29.571 [11]	Used to negotiate the applicability of the optional features defined in table 5.8-1.	
TimeZone	3GPP TS 29.571 [11]		
TraceData	3GPP TS 29.571 [11]		

5.6.2 Structured data types

5.6.2.1 Introduction

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

5.6.2.2 Type PolicyAssociation

Table 5.6.2.2-1: Definition of type PolicyAssociation

Attribute name	Data type	P	Cardinality	Description	Applicability
request	PolicyAssociationRequest	O	0..1	The information provided by the NF service consumer when requesting the creation of a policy association	
triggers	array(RequestTrigger)	O	1..N	Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH" are permitted.	
servAreaRes	ServiceAreaRestriction	O	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF	
rfsp	RfspIndex	O	0..1	RFSP Index as part of the AMF Access and Mobility Policy as determined by the PCF.	
pras	map(PresenceInfo)	C	1..N	If the Trigger "PRA_CH" is provided, the presence reporting area(s) for which reporting is requested shall be provided. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState" attribute within the PresenceInfo data type shall not be supplied.	
suppFeat	SupportedFeatures	M	1	Indicates the negotiated supported features.	

5.6.2.3 Type PolicyAssociationRequest

Table 5.6.2.3-1: Definition of type PolicyAssociationRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	M	1	Identifies the recipient of Notifications sent by the PCF.	
altNotifIpv4Addrs	array(Ipv4Addr)	O	1..N	Alternate or backup IPv4 Addess(es) where to send Notifications.	
altNotifIpv6Addrs	array(Ipv6Addr)	O	1..N	Alternate or backup IPv6 Addess(es) where to send Notifications.	
supi	Supi	M	1	Subscription Permanent Identifier.	
gpsi	Gpsi	C	0..1	Generic Public Subscription Identifier. Shall be provided when available.	
accessType	AccessType	C	0..1	The Access Type where the served UE is camping. Shall be provided when available.	
pei	Pei	C	0..1	The Permanent Equipment Identifier of the served UE. Shall be provided when available.	
userLoc	UserLocation	C	0..1	The location of the served UE. Shall be provided when available.	
timeZone	TimeZone	C	0..1	The time zone where the served UE is camping. Shall be provided when available.	
servingPlmn	NetworkId	C	0..1	The serving PLMN where the served UE is camping. Shall be provided when available.	
ratType	RatType	C	0..1	The RAT Type where the served UE is camping. Shall be provided when available.	
groupIds	array(GroupId)	C	1..N	List of Internal Group Identifiers of the served UE. Shall be provided when available.	
servAreaRes	ServiceAreaRestriction	C	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy. Shall be provided when available.	
rfsp	RfspIndex	C	0..1	RFSP Index as part of the AMF Access and Mobility Policy. Shall be provided when available.	
guami	Guami	C	0..1	The Globally Unique AMF Identifier (GUAMI) shall be provided by an AMF as service consumer.	
serviceName	string	O	0..1	If the NF service consumer is an AMF, it should provide the name of a service produced by the AMF that makes use of information received within the Npcf_AMPolicyControl_UpdateNotify service operation.	
suppFeat	SupportedFeatures	M	1	Indicates the features supported by the service consumer.	
traceReq	TraceData	C	0..1	Trace control and configuration parameters information defined in 3GPP TS 32.422 [18] shall be included if trace is required to be activated.	

5.6.2.4 Type PolicyAssociationUpdateRequest

Table 5.6.2.4-1: Definition of type PolicyAssociationUpdateRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	O	0..1	Identifies the recipient of Notifications sent by the PCF.	
altNotifIpv4Addrs	array(Ipv4Addr)	O	1..N	Alternate or backup IPv4 Address(es) where to send Notifications.	
altNotifIpv6Addrs	array(Ipv6Addr)	O	1..N	Alternate or backup IPv6 Address(es) where to send Notifications.	
triggers	array(RequestTrigger)	C	1..N	Request Triggers that the NF service consumer observes.	
servAreaRes	ServiceAreaRestriction	C	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy. Shall be provided for trigger "SERV_AREA_CH".	
rfsp	RfspIndex	C	0..1	RFSP Index as part of the AMF Access and Mobility Policy. Shall be provided for trigger "RFSP_CH".	
praStatuses	map(PresenceInfo)	C	1..N	If the Trigger "PRA_CH" is reported, the UE presence status for tracking area for which changes of the UE presence occurred shall be provided. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState" attribute within the PresenceInfo data type shall be supplied.	
userLoc	UserLocation	C	0..1	The location of the served UE shall be provided for trigger "LOC_CH".	
traceReq	TraceData	C	0..1	Trace control and configuration parameters information defined in 3GPP TS 32.422 [18] shall be included if trace is required to be activated, modified or deactivated. For trace modification, it shall contain a complete replacement of trace data. For trace deactivation, it shall contain the Null value.	
guami	Guami	O	0..1	The Globally Unique AMF Identifier (GUAMI) shall be provided by an AMF as service consumer.	

5.6.2.5 Type PolicyUpdate

Table 5.6.2.5-1: Definition of type PolicyUpdate

Attribute name	Data type	P	Cardinality	Description	Applicability
resourceUri	Uri	M	1	The resource URI of the individual AM policy related to the notification.	
triggers	array(RequestTrigger)	O	1..N	Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH" are permitted.	
servAreaRes	ServiceAreaRestriction	O	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF.	
rfsp	RfspIndex	O	0..1	RFSP Index as part of the AMF Access and Mobility Policy as determined by the PCF.	
pras	map(PresenceInfoRm)	C	1..N	If the Trigger "PRA_CH" is provided or if that trigger was already set but the requested presence reporting areas need to be changed, the presence reporting area(s) for which reporting is requested shall be provided. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState"attribute within the PresenceInfo data type shall not be supplied.	

5.6.2.6 Type TerminationNotification

Table 5.6.2.6-1: Definition of type TerminationNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
resourceUri	Uri	M	1	The resource URI of the individual AM policy related to the notification.	
cause	PolicyAssociationReleaseCause	M	1	The cause why the PCF requests the termination of the policy association.	

5.6.3 Simple data types and enumerations

5.6.3.1 Introduction

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

5.6.3.2 Simple data types

The simple data types defined in table 5.6.3.2-1 shall be supported.

Table 5.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
n/a			

5.6.3.3 Enumeration: RequestTrigger

The enumeration RequestTrigger represents the possible Policy Control Request Triggers.. It shall comply with the provisions defined in table 5.6.3.3-1.

Table 5.6.3.3-1: Enumeration RequestTrigger

Enumeration value	Description	Applicability
LOC_CH	Location change (tracking area): the tracking area of the UE has changed.	
PRA_CH	Change of UE presence in PRA: the AMF reports the current presence status of the UE in a Presence Reporting Area, and notifies that the UE enters/leaves the Presence Reporting Area.	
SERV_AREA_CH	Service Area Restriction change: the UDM notifies the AMF that the subscribed service area restriction information has changed.	
RFSP_CH	RFSP index change: the UDM notifies the AMF that the subscribed RFSP index has changed.	

5.6.3.4 Enumeration: PolicyAssociationReleaseCause

The enumeration SessionReleaseCause represents the cause why the PCF requests the termination of the policy association. It shall comply with the provisions defined in table 5.6.3.4-1.

Table 5.6.3.4-1: Enumeration PolicyAssociationReleaseCause

Enumeration value	Description	Applicability
UNSPECIFIED	This value is used for unspecified reasons.	
UE_SUBSCRIPTION	This value is used to indicate that the session needs to be terminated because the subscription of UE has changed (e.g. was removed).	
INSUFFICIENT_RES	This value is used to indicate that the server is overloaded and needs to abort the session.	

5.7 Error handling

5.7.1 General

For the Npcf_AMPolicyControl API, HTTP error responses shall be supported as specified in subclause 4.8 of 3GPP TS 29.501 [6]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [5] 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 [5].

In addition, the requirements in the following subclauses are applicable for the Npcf_AMPolicyControl API.

5.7.2 Protocol Errors

No specific protocol errors for the Npcf_AMPolicyControl APIservice are specified.

5.7.3 Application Errors

The application errors defined for the Npcf_AMPolicyControl service are listed in Table 5.7.3-1. The PCF may include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-1.

Table 5.7.3-1: Application errors

Application Error	HTTP status code	Description
USER_UNKNOWN	400 Bad Request	The HTTP request is rejected because the end user specified in the request is unknown to the PCF.
ERROR_REQUEST_PARAMETERS	400 Bad Request	The HTTP request is rejected because the set of information needed by the PCF for AM Policy selection is incomplete or erroneous or not available for the decision to be made.

NOTE: Including a "ProblemDetails" data structure with the "cause" attribute in the HTTP response is optional unless explicitly mandated in the service operation subclauses.

5.8 Feature negotiation

The optional features in table 5.8-1 are defined for the Npcf_AMPolicyControl API. They shall be negotiated using the extensibility mechanism defined in subclause 6.6 of 3GPP TS 29.500 [5].

Table 5.8-1: Supported Features

Feature number	Feature Name	Description

5.9 Security

As indicated in 3GPP TS 33.501 [19] and 3GPP TS 29.500 [5], the access to the Npcf_AMPolicyControl API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [20]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [13]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Npcf_AMPolicyControl API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [13], subclause 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_AMPolicyControl service.

The Npcf_AMPolicyControl API defines a single scope "npcf-am-policy-control" 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

The present Annex contains an OpenAPI [10] specification of HTTP messages and content bodies used by the Npcf_AMPolicyControl API.

This Annex shall take precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API.

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 file contained in this 3GPP Technical Specification are available on the public 3GPP file server in the following locations (see clause 5B of the 3GPP TR 21.900 [22] for further information):

- https://www.3gpp.org/ftp/Specs/archive/OpenAPI/<Release>/, and
- https://www.3gpp.org/ftp/Specs/<Plenary>/<Release>/OpenAPI/.

NOTE 2: To fetch the OpenAPI specification file after CT#83 plenary meeting for Release 15 in the above links <Plenary> must be replaced with the date the CT Plenary occurs, in the form of year-month (yyyy-mm), e.g. for CT#83 meeting <Plenary> must be replaced with value "2019-03" and <Release> must be replaced with value "Rel-15".

A.2 Npcf_AMPolicyControl API

```
openapi: 3.0.0
info:
  version: 1.0.4
  title: Npcf_AMPolicyControl
  description: |
    Access and Mobility Policy Control Service.
    © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
externalDocs:
  description: 3GPP TS 29.507 V15.8.0; 5G System; Access and Mobility Policy Control Service.
  url: 'http://www.3gpp.org/ftp/Specs/archive/29_series/29.507/'
servers:
  - url: '{apiRoot}/npcf-am-policy-control/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in subclause subclause 4.4 of 3GPP TS 29.501
security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-am-policy-control
paths:
  /policies:
    post:
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PolicyAssociationRequest'
      responses:
        '201':
          description: Created
          content:
            application/json:
```

```
              schema:
                $ref: '#/components/schemas/PolicyAssociation'
          headers:
            Location:
              description: 'Contains the URI of the newly created resource, according to the
structure: {apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}'
              required: true
              schema:
                type: string
        '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'
        '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:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        policyUpdateNotification:
          '{$request.body#/notificationUri}/update':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/PolicyUpdate'
              responses:
                '204':
                  description: No Content, Notification was succesfull
                '307':
                  description: temporary redirect
                  headers:
                    Location:
                      description: 'A URI pointing to the endpoint of another NF service consumer to
which the notification should be sent'
                      required: true
                      schema:
                        type: string
                '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'
                '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:
                  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
        policyAssocitionTerminationRequestNotification:
          '{$request.body#/notificationUri}/terminate':
            post:
```

```
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/TerminationNotification'
              responses:
                '204':
                  description: No Content, Notification was succesfull
                '307':
                  description: temporary redirect
                  headers:
                    Location:
                      description: 'A URI pointing to the endpoint of another NF service consumer to
which the notification should be sent'
                      required: true
                      schema:
                        type: string
                '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'
                '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'
  /policies/{polAssoId}:
    get:
      parameters:
        - name: polAssoId
          in: path
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '200':
          description: OK. Resource representation is returned
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PolicyAssociation'
        '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:
      parameters:
        - name: polAssoId
          in: path
```

```
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '204':
          description: No Content. Resource was succesfully deleted
        '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'
        '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'
  /policies/{polAssoId}/update:
    post:
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PolicyAssociationUpdateRequest'
      parameters:
        - name: polAssoId
          in: path
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '200':
          description: OK. Updated policies are returned
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PolicyUpdate'
        '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'
        '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-am-policy-control: Access to the Npcf_AMPolicyControl API
  schemas:
    PolicyAssociation:
```

```
      type: object
      properties:
        request:
          $ref: '#/components/schemas/PolicyAssociationRequest'
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 1
          description: Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH"
are permitted.
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        pras:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - suppFeat
    PolicyAssociationRequest:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        altNotifIpv4Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
          minItems: 1
          description: Alternate or backup IPv4 Address(es) where to send Notifications.
        altNotifIpv6Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
          minItems: 1
          description: Alternate or backup IPv6 Address(es) where to send Notifications.
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        userLoc:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        timeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        servingPlmn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        groupIds:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
          minItems: 1
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        guami:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Guami'
        serviveName:
          type: string
          description: If the NF service consumer is an AMF, it should provide the name of a service
produced by the AMF that makes use of information received within the
Npcf_AMPolicyControl_UpdateNotify service operation. It corresponds to serviceName in the main body.
        traceReq:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TraceData'
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
```

```
        - notificationUri
        - suppFeat
        - supi
    PolicyAssociationUpdateRequest:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        altNotifIpv4Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
          minItems: 1
          description: Alternate or backup IPv4 Address(es) where to send Notifications.
        altNotifIpv6Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
          minItems: 1
          description: Alternate or backup IPv6 Address(es) where to send Notifications.
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 1
          description: Request Triggers that the NF service consumer observes.
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        praStatuses:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
          description: Map of PRA status information.
        userLoc:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        traceReq:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TraceData'
        guami:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Guami'
    PolicyUpdate:
      type: object
      properties:
        resourceUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 1
          nullable: true
          description: Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH"
are permitted.
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        pras:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfoRm'
          description: Map of PRA information.
          minProperties: 1
          nullable: true
      required:
        - resourceUri
    TerminationNotification:
      type: object
      properties:
        resourceUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        cause:
          $ref: '#/components/schemas/PolicyAssociationReleaseCause'
      required:
        - resourceUri
        - cause
```

```
    RequestTrigger:
      anyOf:
      - type: string
        enum:
          - LOC_CH
          - PRA_CH
          - SERV_AREA_CH
          - RFSP_CH
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - LOC_CH: Location change (tracking area). The tracking area of the UE has changed.
        - PRA_CH: Change of UE presence in PRA. The AMF reports the current presence status of the
UE in a Presence Reporting Area, and notifies that the UE enters/leaves the Presence Reporting Area.
        - SERV_AREA_CH: Service Area Restriction change. The UDM notifies the AMF that the
subscribed service area restriction information has changed.
        - RFSP_CH: RFSP index change. The UDM notifies the AMF that the subscribed RFSP index has
changed.
    PolicyAssociationReleaseCause:
      anyOf:
      - type: string
        enum:
          - UNSPECIFIED
          - UE_SUBSCRIPTION
          - INSUFFICIENT_RES
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - UNSPECIFIED: This value is used for unspecified reasons.
        - UE_SUBSCRIPTION: This value is used to indicate that the session needs to be terminated
because the subscription of UE has changed (e.g. was removed).
        - INSUFFICIENT_RES: This value is used to indicate that the server is overloaded and needs
to abort the session.
```

Annex B (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	New
2017-10						TS skeleton of Access and Mobility Policy Control Service specification	0.0.0
2017-10	CT3#92					C3-175324, C3-175338 and C3-17525	0.1.0
2017-12	CT3#93					C3-176355, C3-176354, C3-176237, C3-176238 and C3-176239	0.2.0
2018-01	CT3#94					C3-180033, C3-180195 C3-182307, C3-182308, C3-182309, C3-182442, C3-182311, C3-182312, C3-182313 and C3-182314.	0.3.0
2018-05	CT3#97					C3-183447, C3-183803, C3-183449, C3-183804, C3-183805, C3-183806, C3-183807, C3-183844, C3-183650 and C3-183650	0.5.0
2018-06	CT#80	CP-181025				TS sent to plenary for approval	1.0.0
2018-06	CT#80	CP-181025				TS approved by plenary	15.0.0
2018-09	CT#81	CP-182023	0002	1	B	Trace activation	15.1.0
2018-09	CT#81	CP-182015	0003	3	F	AM Policy Association management during the AMF relocation	15.1.0
2018-09	CT#81	CP-182015	0004	4	F	Completion of Error Codes in OpenAPI file	15.1.0
2018-09	CT#81	CP-182015	0005	1	F	Stateless AMF support updates	15.1.0
2018-09	CT#81	CP-182015	0006	7	F	Removal of editor´s note about additional parameters to further qualify event triggers	15.1.0
2018-09	CT#81	CP-182029	0007	3	F	Service Area Restrictions	15.1.0
2018-09	CT#81	CP-182015	0008	3	F	UE Policies	15.1.0
2018-09	CT#81	CP-182015	0009	1	F	V-PCF procedures	15.1.0
2018-09	CT#81	CP-182015	0010		F	Alignment of resource URIs to resource URI structure	15.1.0
2018-09	CT#81	CP-182015	0011	1	F	Including location information when a location change event is met	15.1.0
2018-09	CT#81	CP-182015	0012	1	F	Description of Structured data types	15.1.0
2018-09	CT#81	CP-182015	0014	1	F	Update of notification	15.1.0
2018-09	CT#81	CP-182015	0015		F	Update the consumer of Npcf_AMPolicyControl service	15.1.0
2018-09	CT#81	CP-182015	0016	1	F	Type of Rfsp attribute in PolicyAssociation data type	15.1.0
2018-09	CT#81	CP-182015	0017	3	F	Encoding to provide only updated parts of policies	15.1.0
2018-09	CT#81	CP-182015	0018	1	F	Termination Causes	15.1.0
2018-09	CT#81	CP-182015	0019	1	F	Update of resource figure	15.1.0
2018-09	CT#81	CP-182015	0020		F	Correction of cardinality of arrays	15.1.0
2018-12	CT#82	CP-183205	0021	1	F	Cleanup of UE policy	15.2.0
2018-12	CT#82	CP-183205	0022	2	F	AM Policy association handling during the AMF relocation	15.2.0
2018-12	CT#82	CP-183205	0023	1	F	Removal of unused abbreviations	15.2.0
2018-12	CT#82	CP-183205	0024	1	F	Correction of HTTP header field with URL of created resource	15.2.0
2018-12	CT#82	CP-183205	0025		F	Type of servAreaRes attribute within Type PolicyAssociation	15.2.0
2018-12	CT#82	CP-183205	0026		F	HTTP Error responses for Notifications	15.2.0
2018-12	CT#82	CP-183205	0028	2	F	Individual AM policy deletion at AMF relocation	15.2.0
2018-12	CT#82	CP-183205	0029	1	F	Correction of the update of Policy Control Request triggers	15.2.0
2018-12	CT#82	CP-183205	0030		F	Default value for apiRoot	15.2.0
2018-12	CT#82	CP-183205	0031		F	API version	15.2.0
2018-12	CT#82	CP-183205	0032		F	ExternalDocs OpenAPI field	15.2.0
2018-12	CT#82	CP-183205	0033		F	Location header field in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0034	1	F	Security	15.2.0
2018-12	CT#82	CP-183205	0035		F	supported content types	15.2.0
2018-12	CT#82	CP-183205	0036	2	F	HTTP Error responses	15.2.0
2018-12	CT#82	CP-183205	0037	1	F	Correction to the PolicyAssociation data type	15.2.0
2018-12	CT#82	CP-183205	0039		F	Re-use PresenceInfoRm data type	15.2.0
2018-12	CT#82	CP-183205	0040		F	Correction to the PresenceInfo data type	15.2.0
2018-12	CT#82	CP-183205	0041	1	F	Alternate IP address in Npcf_AMPolicyControl_Update	15.2.0
2018-12	CT#82	CP-183205	0042	2	F	Corrections on authorized service area restrictions and RFSP index	15.2.0
2018-12	CT#82	CP-183205	0043	2	F	Corrections on encoding of Service Area Restrictions	15.2.0
2018-12	CT#82	CP-183205	0044	1	F	AM Policy Control support for Emergency Registration	15.2.0
2018-12	CT#82	CP-183205	0045	1	F	Multiple Internal Group identifiers	15.2.0
2018-12	CT#82	CP-183205	0046	2	F	Corrections on Protocol and Application errors	15.2.0
2018-12	CT#82	CP-183205	0047	1	F	Correction of Resource name	15.2.0
2018-12	CT#82	CP-183205	0048	1	F	Removal of pras attribute	15.2.0
2018-12	CT#82	CP-183176	0049		F	Corrections of Cardinality in OpenAPI	15.2.0
2019-03	CT#83	CP-190114	0050	2	F	Correction on PCF-initiated AM Policy association termination	15.3.0
2019-06	CT#84	CP-191187	0053	1	F	Precedence of OpenAPI file	15.4.0
2019-06	CT#84	CP-191187	0057	1	F	Correction to Service Area Restriction and RFSP	15.4.0
2019-06	CT#84	CP-191187	0059	1	F	Copyright Note in YAML file	15.4.0
2019-06	CT#84	CP-191187	0060	1	F	API version Update	15.4.0
2019-09	CT#85	CP-192140	0064	1	F	Correcting the resource URI of AM Policy Associations	15.5.0
2019-09	CT#85	CP-192140	0073	1	F	GUAMI included in the Update operation	15.5.0
2019-09	CT#85	CP-192172	0077		F	OpenAPI version update TS 29.507 Rel-15	15.5.0
2019-12	CT#86	CP-193182	0079		F	Correction to PolicyUpdate	15.6.0
2019-12	CT#86	CP-193182	0087	1	F	Correction to Service Area Restrictions description	15.6.0
2019-12	CT#86	CP-193182	0089	1	F	Correction on 307 error, 29.507	15.6.0

2020-06	CT#88e	CP-201215	0106	1	F	Corrections on Service Area Restriction	15.7.0
2020-06	CT#88e	CP-201215	0108	1	F	Location Header of 307 status code	15.7.0
2020-06	CT#88e	CP-201215	0110	1	F	Notification URI	15.7.0
2020-06	CT#88e	CP-201254	0127		F	Update of OpenAPI version and TS version in externalDocs field	15.7.0
2020-12	CT#90e	CP-203112	0146		F	report initial presence status for PRA	15.8.0
2020-12	CT#90e	CP-203151	0149		F	Update of OpenAPI version and TS version in externalDocs field	15.8.0
2022-03	CT#95e	CP-220167	0202	1	F	Handling of error responses	15.9.0

History

Document history		
V15.0.0	June 2018	Publication
V15.1.0	October 2018	Publication
V15.2.0	April 2019	Publication
V15.3.0	April 2019	Publication
V15.4.0	July 2019	Publication
V15.5.0	October 2019	Publication
V15.6.0	January 2020	Publication
V15.7.0	August 2020	Publication
V15.8.0	January 2021	Publication
V15.9.0	March 2022	Publication