TTA Standard

정보통신단체표준(기술규격) 제정일: 2018 년 9 월
TTAT.3G-29.507(R15-15.0.0)

3GPP-(Technical Speciation Group Core Network and Terminals; 5G System; Access and Mobility Policy Control Service; Stage 3)

한국정보통신기술협회
Telecommunications Technology Association

3GPP TS 29.507 V15.0.0 (2018-06)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Access and Mobility Policy Control Service; Stage 3 (Release 15)

Keywords

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 and UE 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".

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
API	Application Programming Interface
DNN	Data Network Name
eMBB	enhanced Mobile Broadband
GPSI	Generic Public Subscription Identifier
HTTP	Hypertext Transfer Protocol
H-PCF	Home Policy Control Function
JSON	JavaScript Object Notation
MIoT	Massive IoT
NF	Network Function
NSSAI	Network Slice Selection Assistance Information
PCF	Policy Control Function
PEI	Permanent Equipment Identifier
PSI	Policy Section Identifier
RFSP	RAT Frequency Selection Priority
SSC	Session and Service Continuity
SUPI	Subscription Permanent Identifier
TA	Tracking Area
TAI	Tracking Area Identity
UDM	Unified Data Management
UDR	Unified Data Repository
URLLC	Ultra-Reliable Low Latency Communications
URSP	UE Route Selection Policy
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
- UE policies such as the UE Route Selection Policy to the UE via 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 consumers of the Npcf_AMPolicyControl service are the Access and Mobility Management Function (AMF) and the Visited Policy Control Function (V-PCF).

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. The V-PCF accesses the Access and Mobility Policy Control Service at the Home Policy Control Function (H-PCF) via the N24 Reference point.

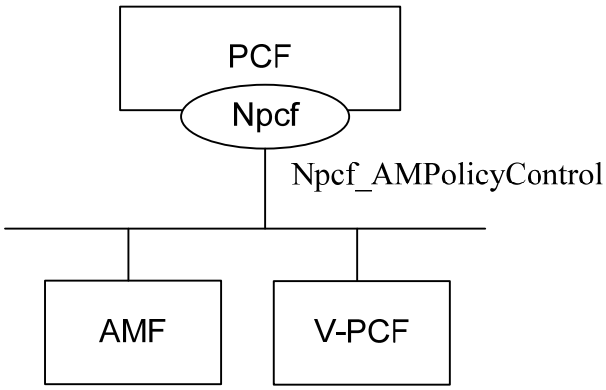

Figure 4.1.2-1: Reference Architecture for the Npcf_AMPolicyControl Service; SBI representation

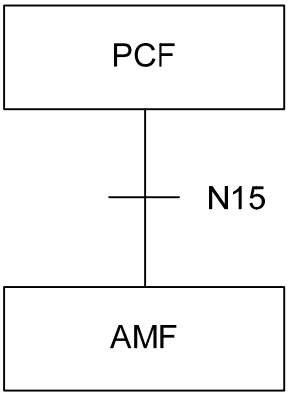

Figure 4.1.2-2: Non-roaming Reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

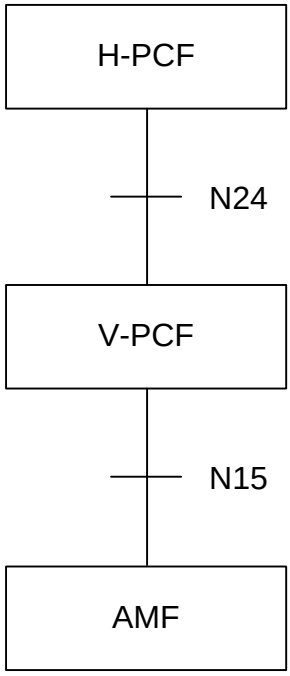

Figure 4.1.3-2: Roaming reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

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 policy rules to Control Plane function(s) that enforce them, including:

  a) Access and Mobility Management related policies for the AMF; and

  b) UE policies that include Access Network discovery and selection policies and UE Route Selection Policies.

4.1.3.2 NF Service Consumers

The Access and Mobility Management function (AMF) provides:

- Registration management;
- Connection management;
- Reachability management;
- Mobility Management; and
- Sending of UE Policy towards the served UE.

The Visited Policy Control Function (V-PCF) provides the functions described in subclause 4.1.3.1 towards the visited network.

4.2 Service Operations

Editor's note: V-PCF procedures when communicating as client with the H-PCF as service producer are FFS.

Editor´s note: Requirements and protocol support in CT4 for a possible transfer of AM policy associations during AMF relocation are FFS. If transfer of AM policy associations during AMF relocation is supported, this should be mentioned in the procedures.

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.	NF consumer (AMF)
Npcf_AMPolicyControl_UpdateNotify	Provides updated policies to the NF consumer.	PCF
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

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 that shall include when available:

- SUPI encoded as "supi" attribute;

NOTE 1: The SUPI is always available except for some emergency sessions where the PEI is 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 Restriction s (see subclause 4.2.2.3.1) as obtained from the UDM 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 PSIs denoting fragments of UE Policy stored in the UE, as obtained from the UE encoded as "psis" attribute;
- V-PCF ID (if the consumer is AMF, when receiving the PCF ID from old AMF during inter-AMF mobility) encoded as "vPcfId" attribute;
- H-PCF ID (if the consumer is V-PCF, when receiving the H-PCF ID from AMF) encoded as "hPcfId" attribute;
- Internal Group Identifier encoded as "groupId" attribute;
- Alternate or backup IPv4 Addess(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute; and
- Alternate or backup IPv6 Addess(es) where to send Notifications encoded as "altNotifIpv6Addrs" 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 possibly modifying possibly received Service Area Restrictions and/or RFSP index) and for the succesfull case shall send a HTTP "201 Created" response with the assigned policy association ID in the "Link" header field

NOTE 2: The assigned policy association ID is thus associated with the SUPI (or PEI in case of emergency PDU Session without SUPI).

and the the PolicyAssociation data type as body including:

- optionally UE policy (see subclause 4.2.2.2) encoded as "uePolicy" attribute, i.e.:
  a) UE Access Network discovery and selection policies; and/or
  b) UE Route Selection Policies (URSP); and/or,
- optionally AMF Access and Mobility Policy (see subclause 4.2.2.3), i.e.:
  a) Service Area Restrictions encoded as "servAreaRes" attribute; and/or
  b) RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute; and
- 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.

If errors occur when processing the HTTP POST request, the PCF shall apply error handling procedures as specified in subclause 5.7.

Editor's note: It is ffs is additional parameters to further qualify event triggers, e.g. a tracking area or PRA description, are required.

4.2.2.2 UE Policy

Editor's note: The structure of the UE policies will be defined by CT1 and related references need to be added. The present specification needs to describe PCF procedures to handle UE policies and related PSIs.

4.2.2.2.1 UE Access Network discovery and selection policies

UE Access Network discovery and selection policies are used by the UE to select non-3GPP accesses and to decide how to route traffic between the selected 3GPP and non 3GPP accesses.

In this release of the specification, the Access Network Discovery & Selection policy shall contain only rules that aid the UE in selecting a WLAN access network. Rules for selecting other types of non-3GPP access networks are not specified.

The WLAN access network selected by the UE with the use of Access Network Discovery & Selection policy may be used for direct traffic offload (i.e. sending traffic to the WLAN outside of a PDU Session) and for registering to 5GC via a N3IWF.

The Access Network Discovery & Selection policy shall contain one or more WLAN Selection Policy (WLANSP) rules defined in subclause 4.8.2.1.6 of 3GPP TS 23.402 [12].

Editor's note: It is ffs if a substructure needs to be defined in the present specification. Alternatives to consider is that a RAN specification or a CT1 specification are referenced.

4.2.2.2.2 UE Route Selection Policy(URSP)

The UE Route Selection Policy is used by the UE to determine how to route outgoing traffic.

Editor's note: It is ffs if a substructure needs to be defined in the present specification. Alternatives to consider is that a RAN specification or a CT1 specification are referenced.

The UE Route Selection Policy shall consist of one or several URSP rules.

Each URSP rule shall contain:

- a rule precedence that is different from the precedence of any other URSP rule within the UE Route Selection Policy;

NOTE 1: The rule precedence values within the URSP determine the order in which the URSP rules are enforced in the UE.

- a traffic descriptor that shall consist of one or several of the following:

  a) one or several application identifier(s);

  b) one or several IP descriptor(s) consisting of destination IP address or IPv6 network prefix, destination port number and protocol ID of the protocol above IP; or

  c) Non-IP descriptors; and

Editor's note: Details of the Non-IP descriptor are FFS.

  d) "Match all" traffic indicator.

NOTE 2: The "Match all" traffic indicator can be used in the USRP rule with lowest rule precedence value and with the only one route selection descriptor in the USRP rule.

- one or several route selection descriptor(s) that shall each contain:

  a) a route selection descriptor precedence that is different from the precedence of any other route selection descriptor within the URSP rule; and

NOTE 3: The route selection descriptor precedence values within the URSP determine the order in which the route selection descriptors are to be applied.

  b) a route selection component that shall contain one of:

    1. either non-seamless Offload indication; or

    2. one or several of the following:

i) Session and Service Continuity (SSC) Mode as defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2] [SSC Mode 1, SSC Mode 2, SSC Mode 3] that indicates that the matching traffic shall be routed via a PDU Session supporting that SSC Mode;

ii) for network slice selection, one or several S-NSSAI(s) as defined in subclause 515.2 of 3GPP TS 23.501 [2] that indicate that the matching traffic shall be routed via a PDU Session supporting any of those S-NSSAI(s) and that each consist of:

+ a mandatory Slice/Service type (SST) with standardized values "1" for enhanced Mobile Broadband (eMBB), "2" for ultra- reliable low latency communications (URLLC), and "3" for massive IoT (MIoT), as specified in table 5.15.2.2-1 in 3GPP TS 23.501 [2] and non-standardized values; and

+ an optional Slice Differentiator that complements the Slice/Service type(s) to allow further differentiation for selecting a Network Slice instance from the potentially multiple Network Slice instances that all comply with the indicated Slice/Service type;

iii) one or several DNN(s) that indicate that the matching traffic shall be routed via a PDU Session supporting any of those DNN(s); or

iv) the preferred Access Type (3GPP or non-3GPP) when the UE establishes a PDU Session for the matching application.

Editor's note: This text needs to be enhanced with encoding details such as attribute names once they are defined.

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 consists of:

- either:

  a) a list of allowed Tracking Area Identities (TAIs); and/or

  b) the maximum number (that can be unlimited) of allowed TAs within a list of allowed TAs defined in the AMF (and not explicitly provided by the PCF);

- or:

  a) a list of not allowed Tracking Area Identities (TAIs).

Editor's note: This text needs to be enhanced with encoding details such as attribute names once they are defined.

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

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

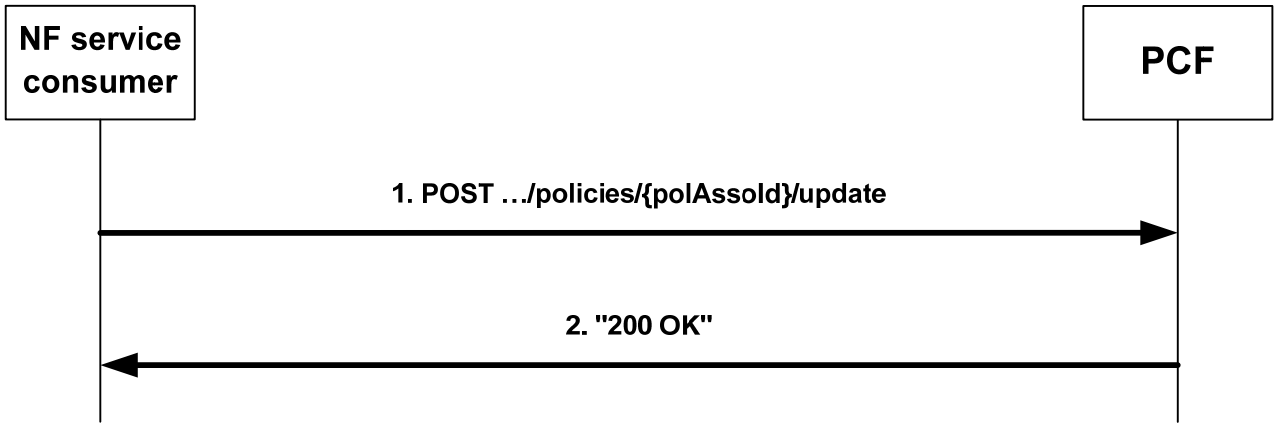

Figure 4.2.3.1-1: Update of a policy association

The AMF 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.

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

To request policies from the PCF or to update the Notification URI, 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; and

  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.

NOTE: 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 determine the applicable policy and 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) including:

- updated policies, i.e.:

  1) UE policy (see subclause 4.2.2.2) encoded as "uePolicy" attribute;

  2) AMF Access and Mobility Policy (see subclause 4.2.2.3) Service Area Restriction encoded as "servAreaRes" attribute;

  3) AMF Access and Mobility Policy (see subclause 4.2.2.3) RFSP Index encoded as "rfsp" attribute; and/or

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

     a) Location change (tracking area); and

     b) Change of UE presence in PRA.

If errors occur when processing the HTTP POST request, the PCF shall apply error handling procedures as specified in subclause 5.7.

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;
- "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.

4.2.4 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.

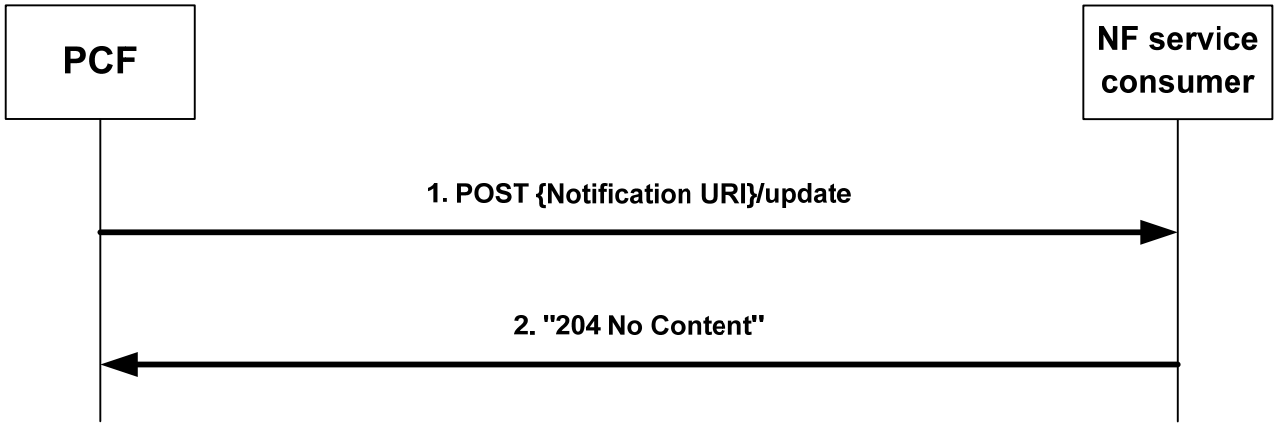

Figure 4.2.4.2-1: policy update notification

The PCF may decide to update policies and shall then send an HTTP POST request with "{Notification URI}/update" as URI (where the Notification URI was previously supplied by the NF service consumer) and the PolicyUpdate data structure as request body that shall include:

- the policy association ID encoded as "polAssoId" attribute; and
- updated policies, i.e.:
  1) UE policy (see subclause 4.2.2.2) encoded as "uePolicy" attribute;
  2) AMF Access and Mobility Policy (see subclause 4.2.2.3) Service Area Restriction encoded as "servAreaRes" attribute;

3) AMF Access and Mobility Policy (see subclause 4.2.2.3) RFSP Index encoded as "rfsp" attribute; and/or

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

   a) Location change (tracking area) encoded as "LOC_CH"; and/or

   b) Change of UE presence in PRA encoded as "PRA_CH".

Upon the reception of the HTTP POST request, the NF service consumer (e.g. AMF) shall enforce the received updated policy and shall either send a HTTP "204 No Content" response indicating the success of the enforcement or an appropriate failure response.

If errors occur when processing the HTTP POST request, the NF service consumer shall apply error handling procedures as specified in subclause 5.7.

If the AMF 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 use this URL as Notification URL in subsequent communication and shall resend the failed policy update notification request to that URL.

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 23.502 [3], 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), the PCF shall exchange the authority part of the corresponding Notification URL with one of those addresses and shall use that URL in subsequent communication. If the PCF received a "404 Not found" response, the PCF should resend the failed policy update notification request to that URL.

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.

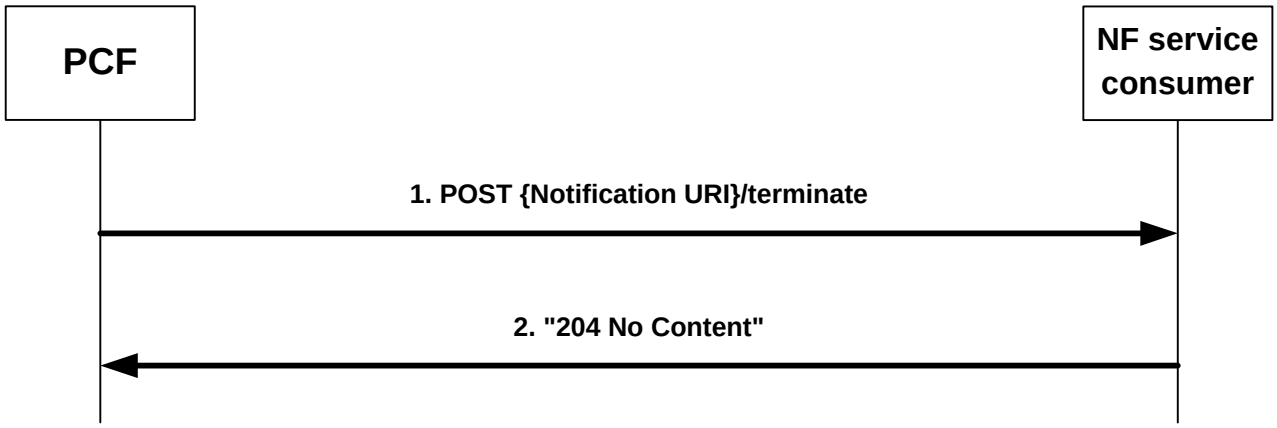

Figure 4.2.4.3-1: request for a termination of the policy association

The PCF may to request the termination of the policy association and shall then send an HTTP POST request with "{Notification URI}/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.

Upon the reception of the HTTP POST request, the NF service consumer (e.g. AMF) shall either send a HTTP "204 No Content" responsefor the succesfull processing of the HTTP POST request or an appropriate failure response.

If errors occur when processing the HTTP POST request, the NF service consumer 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 invoke the Npcf_AMPolicyControl_Delete Service Operation defined in subclause 4.2.5 to terminate the policy association.

If the AMF 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 use this URL as Notification URL in subsequent communication and shall resend the failed request for termination of the policy association to that URL.

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 23.502 [3], 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), the PCF shall exchange the authority part of the corresponding Notification URL with one of those addresses and shall use that URL in subsequent communication. 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.

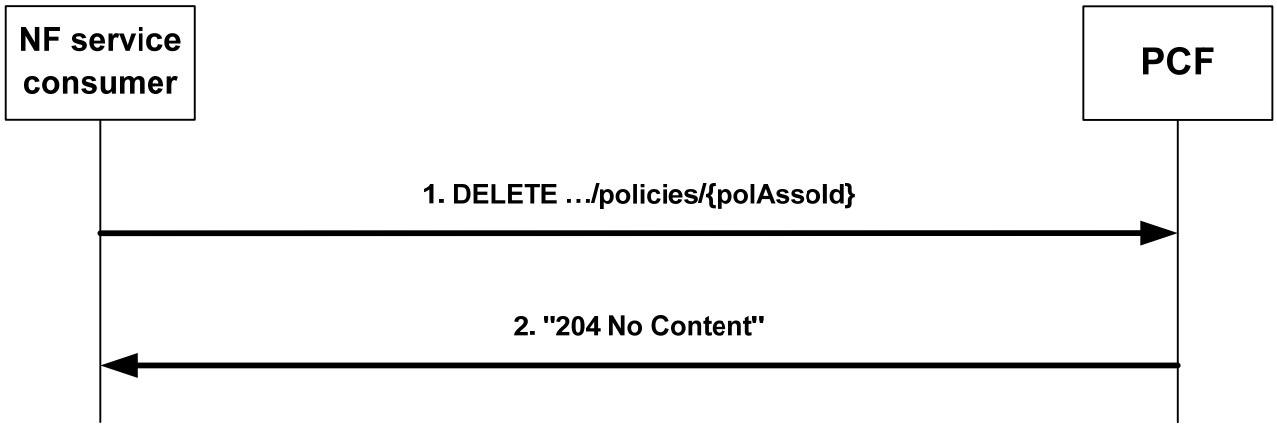

Figure 4.2.5-1: deletion of a policy association

The AMF requests that the policy association is deleted when the corresponding UE context is terminated, e.g. during UE de-registration or handover.

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 and send either a an HTTP "204 No Content" response indicating the success of the deletion or an appropriate failure response.

If errors occur when processing the HTTP DELETE request, the PCF shall 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 [2], i.e.:

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

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [2].
- 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 [4].

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 [4] 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 [4].

5.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in subclause 5.2.3.2 of 3GPP TS 29.500 [4] shall be applicable

5.3 Resources

5.3.1 Resource Structure

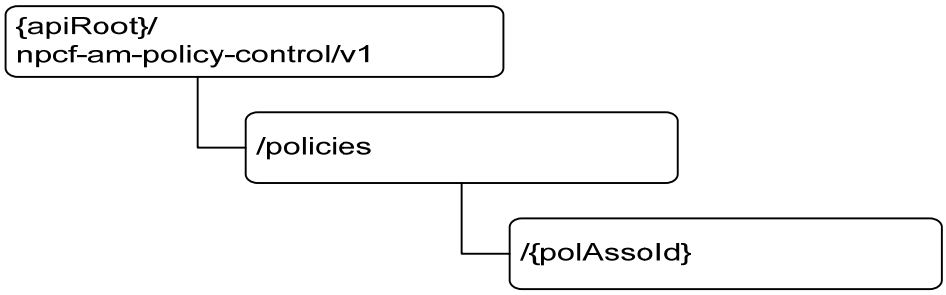

Figure 5.3.1-1: Resource URI structure of the Npcf_AMPolicyControl API

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 Policies	{apiRoot}/ npcf-am-policy-control/ v1/policies/	POST	Create a new Individual AM Policy resource.
Individual AM Policy	{apiRoot} /npcf-am-policy-control/ v1/policies/ {policyId}	GET	Read the Individual AM Policy resource.
		DELETE	Delete the Individual AM Policy 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 Policies

5.3.2.1 Description

This resource represents a collection of 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.
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.				

5.3.3 Resource: Individual AM Policy

5.3.3.1 Description

This 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/ {policyId}/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.
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.				

5.4 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
{Notification URI}/update	POST	Policy Update Notification.
{Notification URI}/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.

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.

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, updated, or read.	
PolAssoId	5.6.3.2	Policy association identifier.	
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]		
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	
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]		
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]		

5.6.2 Structured data types

5.6.2.1 Introduction

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

Allowed structures are: array, object.

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		
uePolicy	FFF	O	0..1	The UE policy as determined by the PCF.	
triggers	array(RequestTrigger)	O	0..N	Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH" are permitted.	
servAreaRes	FFS	O	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF	
rfsp	FFS	O	0..1	RFSP Index as part of the AMF Access and Mobility Policy as determined by the PCF.	
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	0..N	Alternate or backup IPv4 Addess(es) where to send Notifications.	
altNotifIpv6Addrs	array(Ipv6Addr)	O	0..N	Alternate or backup IPv6 Addess(es) where to send Notifications.	
supi	Supi	C	0..1	Subscription Permanent Identifier. Shall be provided when available.	
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.	
groupId	GroupId	C	0..1	Internal Group Identifier of the served UE. Shall be provided when available.	
vPcfId	string	C	0..1	V-PCF Identifier. Shall be provided when available.	
hPcfId	string	C	0..1	H-PCF Identifier. 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.	
psis	array(FFS)	C	0..N	A list of PSIs denoting fragments of UE Policy stored in the UE, as obtained from the UE. Shall be provided when available.	
suppFeat	SupportedFeatures	M	1	Indicates the features supported by the service consumer.	

Editor's note: The type for PSI is FFS and needs to be alligned with CT1.

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.	
triggers	array(RequestTrigger)	M	1..N	Request Triggers that the NF service consumer observes.	
servAreaRes	FFS	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".	

5.6.2.5 Type PolicyUpdate

Table 5.6.2.5-1: Definition of type PolicyUpdate

Attribute name	Data type	P	Cardinality	Description	Applicability
polAssoId	PolAssoId	C	0..1	Policy Association ID assigned by the PCF. Shall be included when policy is supplied as part of the Npcf_AMPolicyControl_UpdateNotify Service Operation.	
uePolicy	FFF	O	0..1	The UE policy as determined by the PCF.	
triggers	array(RequestTrigger)	O	0..N	Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH" are permitted.	
servAreaRes	FFS	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.	

Editor's note: The included data types need to allow that only updated parts of policies are provided.

5.6.2.6 Type TerminationNotification

Table 5.6.2.6-1: Definition of type TerminationNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
polAssoId	PolAssoId	M	1	Policy Association ID assigned by the PCF.	

Editor's note: Addition of termination causes is ffs.

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
PolAssoId	string	Policy Association Identifier	

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 UE is entering/leaving a 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.	

5.7 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 procedures for the Nsmf_EventExposure service are specified.

5.7.3 Application Errors

The application errors defined for the Npcf_AMPolicyControl service are listed in Table 5.7.3-1.

Table 5.7.3-1: Application errors

Application Error	HTTP status code	Description

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

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.

In case of conflicts between the main body of the present document and the present Annex, the information in the main body shall be applicable.

A.2 Npcf_AMPolicyControl API

Editor's note: HTTP Error responses need to be alligned with updates to Table 5.2.7.1-1 of 3GPP TS 29.500 [4].

Editor's note: The ServiceAreaRestriction data type is not yet defined in 3GPP TS 29.571 [11].

```
openapi: 3.0.0
info:
  description: Access and Mobility Policy Control Service API
  version: "1.PreR15.0.0"
  title: Npcf_AMPolicyControl
externalDocs:
  description: 3GPP TS 29.507 V15.0.0 (2018-06) 5G System; Access and Mobility Policy Control
Service; Stage 3
  url: http://www.3gpp.org/ftp/Specs/archive/29_series/29.507/
servers:
  - url: https://{apiRoot}/npcf-am-policy-control/v1
    variables:
      apiRoot:
        default: demohost.com
        description: apiRoot as defined in subclause subclause 4.4 of 3GPP TS 29.501, excluding the
http:// part
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'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        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
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              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
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              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'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        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'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        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'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
components:
  schemas:
    PolicyAssociation:
      type: object
      properties:
        request:
          $ref: '#/components/schemas/PolicyAssociationRequest'
        uePolicy:
          type: string
    # Editor's note:  The type is FFS and string is only used as temporary placeholder to pass syntax checks

        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 0
          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'
        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: 0
          description: Alternate or backup IPv4 Addess(es) where to send Notifications.
        altNotifIpv6Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
          minItems: 0
          description: Alternate or backup IPv6 Addess(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'
        groupId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
        vPcfId:
          type: string
          description: V-PCF Identifier. Shall be provided when available.
        hPcfId:
          type: string
          description: H-PCF Identifier. Shall be provided when available.
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        psis:
          type: array
          items:
            type: string
    # Editor's note:  The type is FFS and string is only used as temporary placeholder to pass syntax checks

          minItems: 0
          description: A list of PSIs denoting fragments of UE Policy stored in the UE, as obtained
from the UE. Shall be provided when available.
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - notificationUri
        - suppFeat
    PolicyAssociationUpdateRequest:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 0
          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'
    PolicyUpdate:
      type: object
      properties:
        polAssoId:
          $ref: '#/components/schemas/PolAssoId'
        uePolicy:
          type: string
    # Editor's note:  The type is FFS and string is only used as temporary placeholder to pass syntax checks

        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 0
          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'
    TerminationNotification:
      type: object
      properties:
        polAssoId:
          $ref: '#/components/schemas/PolAssoId'
      required:
        - polAssoId
    PolAssoId:
      type: string
      description: Policy Association Identifier
    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 UE is entering/leaving a 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.
```

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