ETSI TS 129 507 V16.7.0 (2021-04)

5G;
5G System;
Access and Mobility Policy Control Service;
Stage 3
(3GPP TS 29.507 version 16.7.0 Release 16)

Reference
RTS/TSGC-0329507vg70

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".

[23] 3GPP TS 23.316: "Wireless and wireling convergence access support for the 5G System (5GS)".

[24] 3GPP TS 29.531: "5G System; Network Slice Selection Services; Stage 3".

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].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [2], subclause 3.1 apply:

Allowed NSSAI

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].

5G-BRG	5G Broadband Residential Gateway
5G-RG	5G Residential Gateway
5GC	5G Core Network
5G-CRG	5G Cable Residential Gateway
5GS	5G System
AMBR	Aggregated Maximum Bit Rate
AMF	Access and Mobility Management Function
BBF	Broadband Forum
DNN	Data Network Name
EPS	Evolved Packet System
FN-BRG	Fixed Network Broadband Residential Gateway
FN-CRG	Fixed Network Cable Residential Gateway
FN-RG	Fixed Network Residential Gateway
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
GPSI	Generic Public Subscription Identifier
GUAMI	Globally Unique AMF Identifier
HFC	Hybrid Fiber-Coaxial
JSON	JavaScript Object Notation
LBO	Local Break Out (roaming)
NID	Network Identifier
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information

PCF	Policy Control Function
PEI	Permanent Equipment Identifier
PRA	Presence Reporting Area
QoS	Quality of Service
RFSP	RAT Frequency Selection Priority
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SNPN	Stand-alone Non-Public Network
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
V-PCF	Visited Policy Control Function
W-5GAN	Wireline 5G Access Network
W-5GBAN	Wireline BBF Access Network
W-5GCAN	Wireline 5G Cable Access Network
W-AGF	Wireline Access Gateway 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.

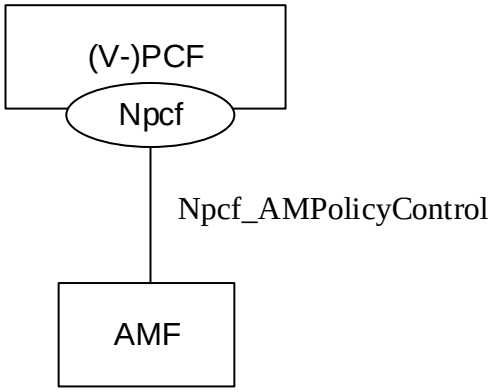

Figure 4.1.2-1: Reference Architecture for the Npcf_AMPolicyControl Service; SBI representation

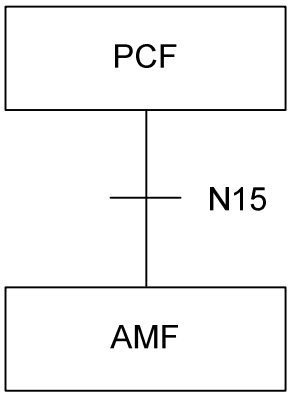

Figure 4.1.2-2: Non-roaming Reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

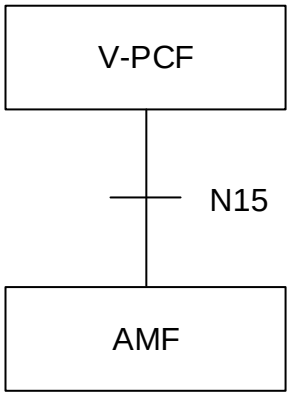

Figure 4.1.3-2: Roaming reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

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 an AM Policy Association and provides corresponding policies to the NF consumer when a policy control request trigger is met or the AMF is relocated due to 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 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.

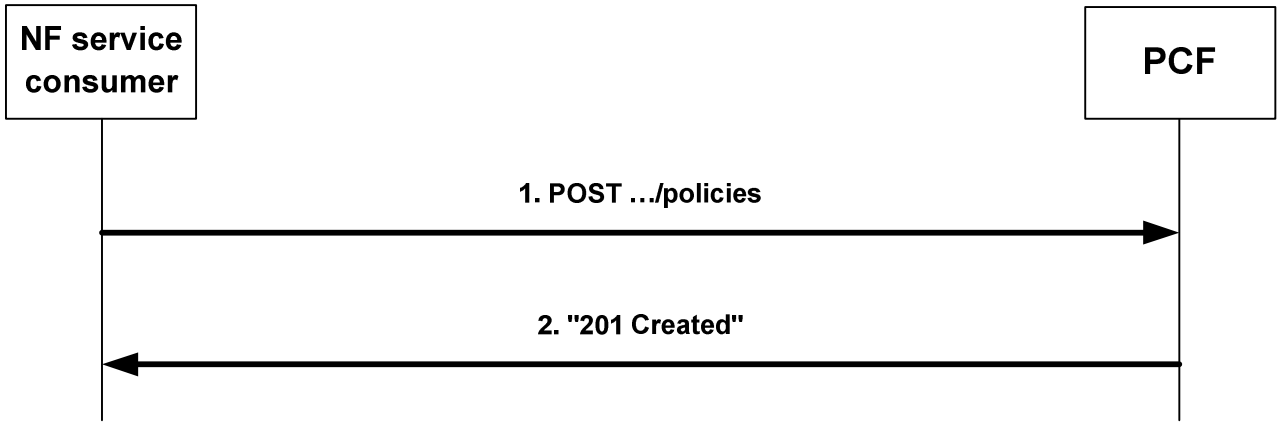

Figure 4.2.2.1-1: Creation of a policy association

When a UE registers and a UE context is being established, the AMF can obtain Service Area Restrictions, RFSP index, subscribed UE-AMBR and GPSI(s) from the UDM during the Access and Mobility Subscription Data retrieval procedure and the allowed NSSAI from local configuration or from the NSSF during the slice selection 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;
- SUPI encoded as "supi" attribute; and
- if the feature "SliceSupport" or the feature "DNNReplacementControl" is supported in the AMF and the UE is registered via a 3GPP access, the allowed NSSAI in the 3GPP access encoded in the "allowedSnssais" attribute;

and that shall include when available:

- GPSI encoded as "gpsi" attribute;
- if the feature "MultipleAccessTypes" is not supported, the 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 and for SNPN the NID encoded as "servingPlmn" attribute;
- if the feature "MultipleAccessTypes" is not supported, the 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;

- Alternate or backup FQDN(s) where to send Notifications encoded as "altNotifFqdns" attribute;
- trace control and configuration parameters information encoded as "traceReq" attribute;
- if the feature "UE-AMBR_Authorization" is supported in the AMF, the subscribed UE-AMBR (see subclause 4.2.2.3.3) in the "ueAmbr" attribute; and
- if the feature"DNNReplacementControl" is supported, the mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN encoded in the "mappingSnssais" attribute.

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

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

NOTE 1: The assigned policy association ID is part of the URI for the created resource and is thus associated with the SUPI.

and the PolicyAssociation data type as response body including:

- conditionally AMF Access and Mobility Policy (see subclause 4.2.2.3), i.e.:
  a) if the PCF received the "servAreaRes" attribute in the request, Service Area Restrictions encoded as "servAreaRes" attribute; and/or
  b) if the PCF received the "rfsp" attribute in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute; and/or
  c) if the feature "UE-AMBR_Authorization" is supported and the PCF received the "ueAmbr" attribute in the request, the authorized UE-AMBR encoded as "ueAmbr" 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
  c) if the "SliceSupport" feature or the "DNNReplacementControl" feature is supported, change of allowed NSSAI; and
  d) if the "DNNReplacementControl" feature is supported, change of SMF selection information; 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;

NOTE 2: If the PCF uses a Presence Reporting Area identifier referring to a Set of Core Network predefined Presence Reporting Areas as defined in 3GPP TS 23.501 [2], the PCF includes the identifier of this Presence Reporting Area set within the "praId" attribute.

- if the Policy Control Request Trigger "Change of SMF selection information" is provided, the SMF selection information representing the conditions upon which the AMF shall request a DNN replacement (see subclause 4.2.2.3.4) encoded as "smfSelInfo" attribute;

- if errors occur when processing the HTTP POST request, 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 rejects the AM policy association establishment, the NF service consumer shall apply the policy retrieved from the UDM if available; otherwise, the NF service consumer shall apply the operator configured policy.

If the PCF received a 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 "ServiceArea Restriction" 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].

4.2.2.3.3 UE-AMBR

The UE-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows of a UE. It shall be encoded using the Ambr data type defined in 3GPP TS 29.571 [11].

4.2.2.3.4 SMF Selection Management

If the "DNNReplacementControl" feature is supported, when SMF Selection Management is enabled, the SMF selection information is encoded using the "SmfSelectionData" data type, which consists of:

- the conditions upon which the AMF shall request to the PCF the replacement of SMF selection data, which may include:

  a) an indication of whether the AMF shall request DNN replacement when the UE requested an unsupported DNN during PDU session establishment encoded in the "unsuppDnn" attribute; and/or

  b) a list of candidate DNNs for replacement encoded in the "candidates" map, where:

i) the key of the map is the S-NSSAI; and

ii) each entry of the map is of "CandidateForReplacement" data type, which:

- shall include the S-NSSAI encoded in the "snssai" attribute; and
- may include the list of candidate DNNs for the S-NSSAI encoded in the "dnns" attribute;

NOTE 1: The S-NSSAIs included in the map are S-NSSAIs of the allowed NSSAI valid in the serving network. The PCF keeps updated information of the allowed NSSAI valid in the serving network by subscribing to the policy control request trigger Change of allowed NSSAI of the served UE.

- and,

a) when included within the Npcf_AMPolicyControl_Update request, the UE requested DNN and S-NSSAI at PDU session establishment that matched an entry of the "candidates" map, encoded in the "dnn" attribute and in the "snssai" attribute respectively, and the mapping to the home S-NSSAI encoded in the "mappingSnssai" attribute if available; and

b) when included within the Npcf_AMPolicyControl_Update response, the PCF selected DNN encoded in the "dnn" attribute;

NOTE 2: The PCF can select the same DNN and S-NSSAI as the UE requested DNN and S-NSSAI. When the PCF returns an unsupported DNN, the AMF applies internal policies to reject the PDU session establishment.

When the "dnns" attribute is omitted in an entry of the "candidates" map it represents that the AMF shall invoke the procedure for any UE request matching the S-NSSAI value included in the "snssai" attribute.

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 the old PCF to maintain the policy association and to update the Notification URI).

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

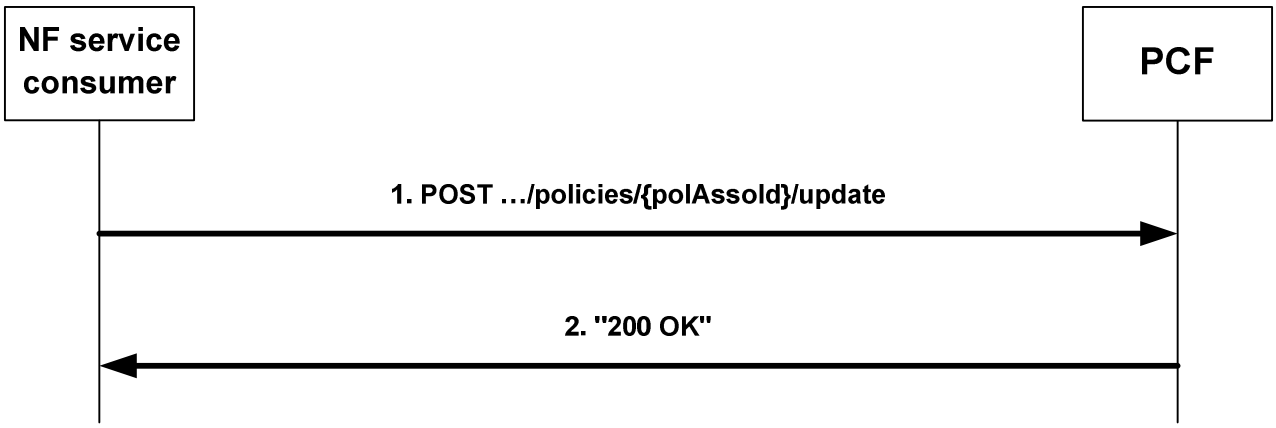

Figure 4.2.3.1-1: Update of a policy association

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 and/or the RFSP index change trigger occur, and/or the feature "UE-AMBR_Authorization" is supported and the subscribed UE-AMBR change trigger occurs, 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, to update the Notification URI, 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 the AM Policy Association by providing the 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;

  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.

NOTE 1: If the PCF included the identifer of a Core Network predefined Presence Reporting Area Set within the "praId" attribute during the subscription to changes of UE presence in PRA, the AMF only provides the presence reporting area information corresponding to the concerned individual Presence Reporting Area Identifier(s) within the Set. The "praId" attribute within each returned "PresenceInfo" data type hence includes the identifier of the concerned individual Presence Reporting Area.

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

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

  9. if the "SliceSupport" feature or the "DNNReplacementControl" feature is supported, the UE is registered via 3GPP access, the allowed NSSAI changed, and the Policy Control Request Trigger "Change of allowed NSSAI" was provided, then the allowed NSSAI encoded in the "allowedSnssais" attribute;

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

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

  12. for AMF relocation scenarios, if available, alternate or backup FQDN(s) where to send Notifications encoded as "altNotifFqdns" attribute;

  13. for AMF relocation scenarios, if available, the 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.

  14. if the feature "UE-AMBR_Authorization" is supported, and a subscribed UE-AMBR change occurred, the UE-AMBR (see subclause 4.2.2.3.x) as obtained from the UDM encoded as "ueAmbr" attribute;

  15. if the feature "DNNReplacementControl" is supported, DNN replacement applies and the Policy Control Request Trigger "Change of SMF selection information" is provided, the "smfSelInfo" attribute including:

- the UE requested DNN in the "dnn" attribute; and
- the UE requested S-NSSAI in the "snssai" attribute and, if available, the corresponding mapped home S-NSSAI in the "mappingSnssai" attribute;

when:

- the UE requested an unsupported DNN and the "unsuppDnn" attribute is set to "true"; or
- the UE requested DNN and S-NSSAI matched one of the S-NSSAI and DNN provided in the "candidates" attribute; and

16. if feature "DNNReplacementControl" is supported, the UE is registered via 3GPP access, the Allowed NSSAI changed and/or the mapping of a S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN changed, and the Policy Control Request Trigger" Change of allowed NSSAI" was provided, then the mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN encoded in the "mappingSnssais" attribute.

NOTE 3: When the feature "DNNReplacementControl" is supported, the AMF applies DNN replacement for non-roaming scenarios and LBO. For a PDU session with home routed roaming, whether to perform DNN replacement is based on operator agreement.

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;
- determine the applicable policy based on local policy;
- for the succesfull case, 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" attribute in the request, Service Area Restrictions encoded as "servAreaRes" attribute;
  b) if the PCF received the "rfsp" attribute in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute;
  c) if the feature "UE-AMBR_Authorization" is supported and the PCF received the "ueAmbr" attribute in the request, UE-AMBR encoded as "ueAmbr" attribute; and/or
  d) if the PCF received the "smfSelInfo" attribute in the request, the "smfSelInfo" attribute encoding the PCF selected DNN in the "dnn" attribute corresponding to the S-NSSAI received in the "snssai" attribute;
- if errors occur when processing the HTTP POST request, 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 "ES3XX" feature is supported and the PCF (service) instance has changed, the PCF may respond with an HTTP 3xx redirect response pointing to a new PCF (service) instance as defined in subclause 6.5.3.3 of 3GPP TS 29.500 [5].

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 and/or UE-AMBR from the UDM, the AMF shall remove the authorized Service Area Restrictions and/or RFSP and/or UE-AMBR provisioned by the PCF and apply the configured Service Area Restrictions and/or RFSP and/or UE-AMBR at the AMF without interacting with the PCF.

If feature "DNNReplacementControl" is supported and the AMF received the update of the SMF selection information within the "smfSelInfo" attribute in the response, the AMF shall apply the updated SMF selection information to the new PDU Sessions only, i.e. already established PDU Sessions are not affected.

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;
- "RFSP_CH", i.e. RFSP index change: the UDM notifies the AMF that the subscribed RFSP index has changed;
- "ALLOWED_NSSAI_CH", i.e. change of allowed NSSAI of the served UE;

NOTE 1: The "ALLOWED_NSSAI_CH" trigger only applies if the "SliceSupport" feature or the "DNNReplacementControl" feature is supported.

- "UE_AMBR_CH", i.e. UE-AMBR change: the UDM notifies the AMF that the subscribed UE-AMBR has changed;

NOTE 2: The "UE_AMBR_CH" trigger only applies if the "UE-AMBR_Authorization" feature is supported.

- "SMF_SELECT_CH", i.e. SMF selection information change: UE request for an unsupported DNN or UE request for a DNN within the list of DNN candidates for replacement per S-NSSAI; and

NOTE 3: The "SMF_SELECT_CH" trigger only applies if the "DNNReplacementControl" feature is supported and "ALLOWED_NSSAI_CH" trigger is also subscribed.

- "ACCESS_TYPE_CH", i.e. the access type change: the AMF notifies that the access type and the RAT type combinations available in the AMF for a UE with simultaneous 3GPP and non-3GPP connectivity has changed.

NOTE 4: The "ACCESS_TYPE_CH" trigger only applies if the "MultipleAccessTypes" feature is supported as specified in Annex B.

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;
- if the "UE-AMBR_Authorization" feature is supported, AMF Access and Mobility Policy (see subclause 4.2.2.3) UE-AMBR encoded as "ueAmbr" attribute;

  NOTE: PCF can stop applying policies to already provided attributes under PolicyUpdate data type. In that case, PCF will modify those attributes by e.g. providing configured values. How the PCF gets those values is out of specification.

- if the "DNNReplacementControl" feature is supported, AMF Access and Mobility Policy (see subclause 4.2.2.3) SMF selection information encoded as "smfSelInfo" 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); and/or

b) Change of UE presence in PRA; and/or

c) if the "SliceSupport" feature or the "DNNReplacementControl" feature is supported, change of allowed NSSAI; and/or

d) if the "DNNReplacementControl" feature is supported, SMF selection information change; 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.

- if the Policy Control Request Trigger "SMF selection information change" is provided or if that trigger was already set and the indication of DNN replacement when the requested DNN is unknown needs to be set or changed, the "unsuppDnn" attribute within "smfSelInfo" attribute shall be provided including the appropriate value.

- if the Policy Control Request Trigger "SMF selection information change" is provided or if that trigger was already set and the list of candidate DNNs for replacement needs to be set or changed, the "candidates" attribute within the "smfSelInfo" attribute is encoded as follows:

a) A new entry shall be added by supplying a new S-NSSAI as key and the corresponding CandidateForReplacement 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 S-NSSAI as key and the CandidateForReplacement 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 S-NSSAI 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;

e) The complete list of candidate DNNs for which reporting is required shall be removed by providing the "candidates" attribute with "NULL" as value.

- if the Policy Control Request Trigger "SMF selection information change" is removed, the candidate DNNs for which reporting was required shall be removed by providing the "smfSelInfo" 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.

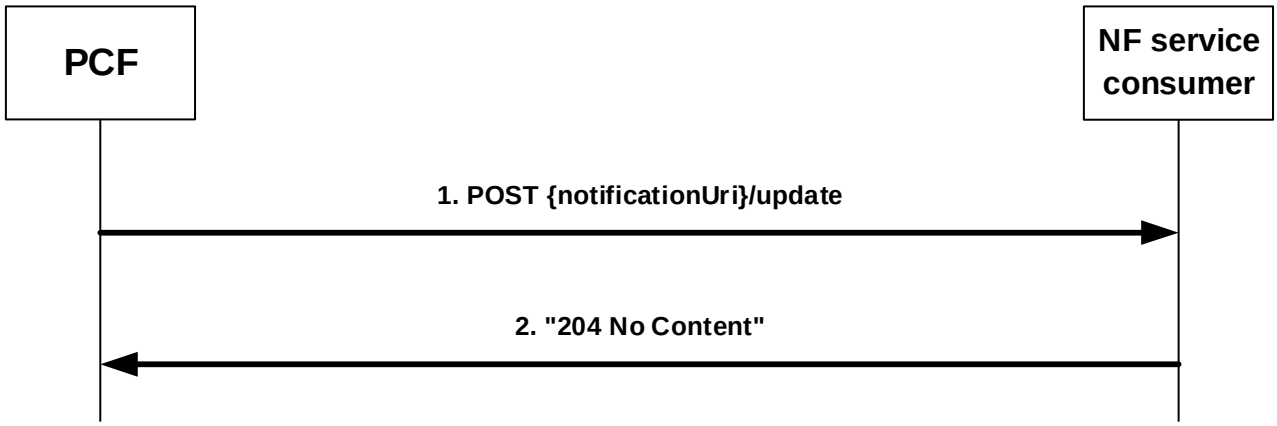

Figure 4.2.4.2-1: policy update notification

The PCF may decide to update Access and Mobility 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;
- 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, send an HTTP error response or, if the feature "ES3XX" is supported, an HTTP redirect response 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, 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, IPv6 Addess(es) or FQDN(s) where to send Notifications (e.g. via "altNotifIpv4Addrs", "altNotifIpv6Addrs" or "altNotifFqdns" attributes received when the policy association was created, 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 discover 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.

If the feature "DNNReplacementControl" is supported and the AMF received the update of the SMF selection information within the "smfSelInfo" attribute in the request, the AMF shall apply the updated SMF selection information to the new PDU Sessions only, i.e. already established PDU Sessions are not affected.

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.

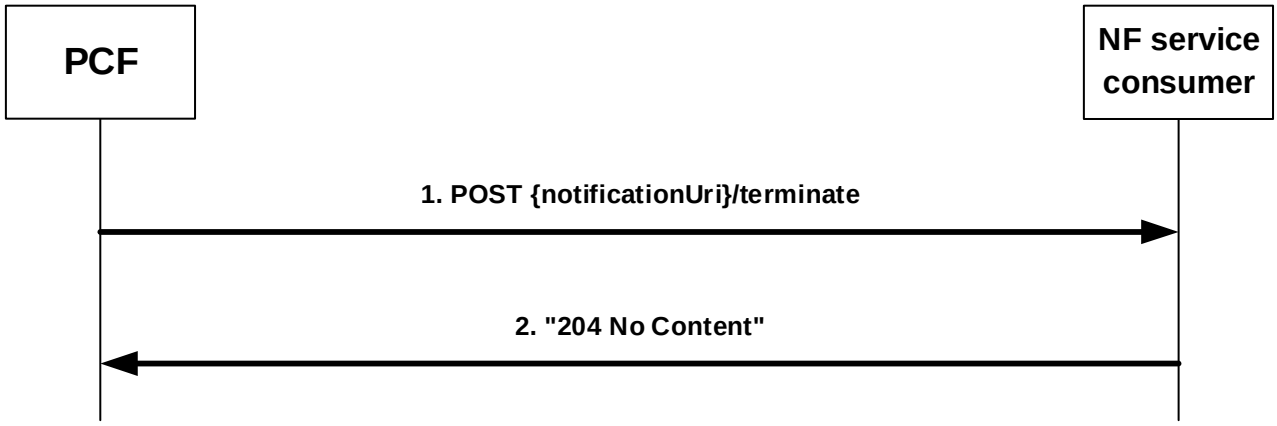

Figure 4.2.4.3-1: request for a termination of the policy association

The PCF may 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, send an HTTP error response or, if the feature "ES3XX" is supported, an HTTP redirect response 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, 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, IPv6 Addess(es) or FQDN(s) where to send Notifications (e.g. via "altNotifIpv4Addrs", "altNotifIpv6Addrs" or "altNotifFqdns" attributes received when the policy association was created, 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 discover 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 URI.

4.2.5 Npcf_AMPolicyControl_Delete Service Operation

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

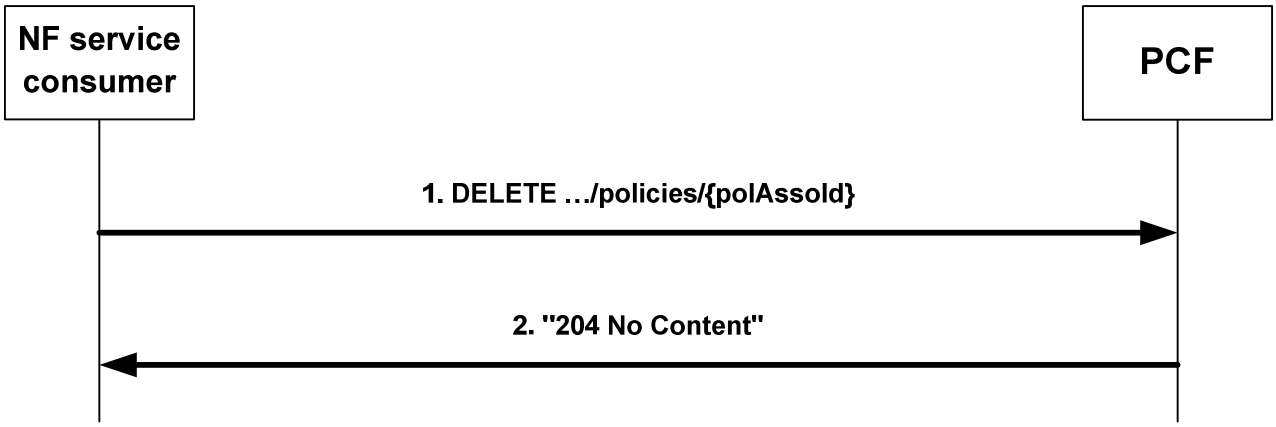

Figure 4.2.5-1: Deletion of a policy association

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, or when the UE moves from 5GS to EPS and the UE is not connected to the 5GC over a non-3GPP access.

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, send an HTTP error response or, if the feature "ES3XX" is supported, an HTTP redirect response 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 API URI of the Npcf_AMPolicyControl API shall be:

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

The request URIs used in HTTP requests from the NF service consumer towards the PCF shall have the Resource URI 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

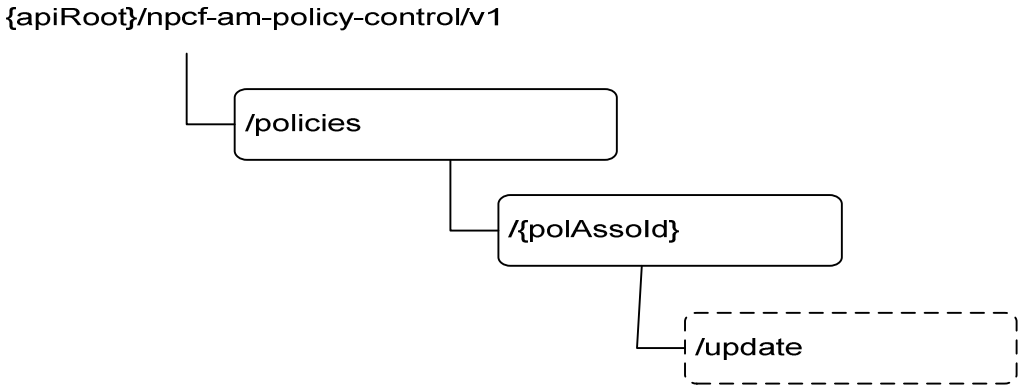

Figure 5.3.1-1: Resource URI structure of the Npcf_AMPolicyControl API

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	/policies/	POST	Create a new Individual AM Policy Association resource.
Individual AM Policy Association	/policies/{polAssoId}	GET	Read the Individual AM Policy Association resource.
		DELETE	Delete the Individual AM Policy Association resource.
	/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	Data type	Definition
apiRoot	string	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.				

Table 5.3.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}

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	Data type	Definition
apiRoot	string	See subclause 5.1.
polAssoId	string	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	
ProblemDetails	O	0..1	307 Temporary Redirect	Temporary redirection, during Individual AM policy retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
ProblemDetails	O	0..1	308 Permanent Redirect	Permanent redirection, during Individual AM policy retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
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.				

Table 5.3.3.3.1-4: Headers supported by the 307 Response Code on this resource

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

Table 5.3.3.3.1-5: Headers supported by the 308 Response Code on this resource

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

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.
ProblemDetails	O	0..1	307 Temporary Redirect	Temporary redirection, during Individual AM policy deletion. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
ProblemDetails	O	0..1	308 Permanent Redirect	Permanent redirection, during Individual AM policy deletion. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
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.				

Table 5.3.3.3.2-4: Headers supported by the 307 Response Code on this resource

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

Table 5.3.3.3.2-5: Headers supported by the 308 Response Code on this resource

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

5.3.3.4 Resource Custom Operations

5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

Operation Name	Custom operation URI	Mapped HTTP method	Description
Update	/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 of a policy control 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	307 Temporary Redirect	Temporary redirection, during Individual AM policy modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
ProblemDetails	O	0..1	308 Permanent Redirect	Permanent redirection, during Individual AM policy modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance. Applicable if the feature "ES3XX" is supported.
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.				

Table 5.3.3.4.2.2-3: Headers supported by the 307 Response Code on this resource

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

Table 5.3.3.4.2.2-4: Headers supported by the 308 Response Code on this resource

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

5.4 Custom Operations without associated resources

None.

5.5 Notifications

5.5.1 General

Table 5.5.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
Policy Update Notification	{notificationUri}/update	update (POST)	Policy Update Notification.
Request for termination of the policy association	{notificationUri}/terminate	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.
ProblemDetails	O	0..1	307 temporary redirect	Temporary redirection, during AM policy notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent. ProblemDetail may be included in the response if the feature "ES3XX" is supported.
ProblemDetails	O	0..1	308 Permanent Redirect	Permanent redirection, during AM policy notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent. Applicable if the feature "ES3XX" is supported.
ProblemDetails	O	0..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.				

Table 5.5.2.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF consumer (service) instance towards which the notification request is redirected. May be included if the feature "ES3XX" is supported.

Table 5.5.2.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

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.
ProblemDetails	O	0..1	307 temporary redirect	Temporary redirection, during AM policy notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent. ProblemDetail may be included in the response if the feature "ES3XX" is supported.
ProblemDetails	O	0..1	308 Permanent Redirect	Permanent redirection, during AM policy notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent. Applicable if the feature "ES3XX" is supported.
ProblemDetails	O	0..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.				

Table 5.5.3.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected. May be included if the feature "ES3XX" is supported.

Table 5.5.3.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance towards which the notification request is redirected

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
CandidateForReplacement	5.6.2.8	Contains the list of candidate DNNs for replacement per S-NSSAI	DNNReplacementControl
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.	
SmfSelectionData	5.6.2.7	Includes the SMF Selection information that may by replaced by the PCF	DNNReplacementControl
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]		
Ambr	3GPP TS 29.571 [11]	Aggregated Maximum Bit Rate.	UE-AMBR_Authorization
Dnn	3GPP TS 29.571 [11]	DNN	DNNReplacementControl
Fqdn	3GPP TS 29.510 [13]	FQDN	
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]		
MappingOfSnssai	3GPP TS 29.531 [24]	Identifies the mapping of an S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN.	DNNReplacementControl
Pei	3GPP TS 29.571 [11]	Permanent Equipment Identifier	
PlmnIdNid	3GPP TS 29.571 [11]	PLMN Identifier, and for SNPN NID	
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.	
ServiceName	3GPP TS 29.510 [13]	Name of the service instance.	
Snssai	3GPP TS 29.571 [11]	Identifies a S-NSSAI included in the Allowed NSSAI.	SliceSupport
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]		
WirelineServiceAreaRestriction	3GPP TS 29.571 [11]		WirelineWirelessConvergence

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", "ALLOWED_NSSAI_CH", "SMF_SELECT_CH", "PRA_CH" and "ACCESS_TYPE_CH" are permitted.	(NOTE)
servAreaRes	ServiceAreaRestriction	O	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF	
wlServAreaRes	WirelineServiceAreaRestriction	O	0..1	Wireline Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF	WirelineWirelessConvergence
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" and the "additionalPraId" attributes within the PresenceInfo data type shall not be supplied. The "praId" attribute within the PresenceInfo data type shall include the identifier of either a presence reporting area or a presence reporting area set.	
smfSelInfo	SmfSelectionData	O	0..1	If the trigger "SMF_SELECT_CH" is provided, the conditions for SMF selection information replacement, as determined by the PCF shall be provided.	DNNReplacementControl
ueAmbr	Ambr	O	0..1	UE-AMBR as part of the AMF Access and Mobility Policy as determined by the PCF.	UE-AMBR_Authorization
suppFeat	SupportedFeatures	M	1	Indicates the negotiated supported features.	

NOTE: The "ALLOWED_NSSAI_CH", "SMF_SELECT_CH" and "ACCESS_TYPE_CH" values in the "triggers" attribute apply under feature control as described in subclause 4.2.3.2.

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.	
altNotifFqdns	array(Fqdn)	O	1..N	Alternate or backup FQDN(s) 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.	
accessTypes	array(AccessType)	C	1..N	The Access Types where the served UE is camping. Shall be provided when available.	MultipleAccessTypes
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	PlmnIdNid	C	0..1	The serving PLMN where the served UE is camping. For an SNPN the NID together with the PLMN ID identifies the SNPN. Shall be provided when available.	
ratType	RatType	C	0..1	The 3GPP RAT Type where the served UE is camping. Shall be provided when available.	
ratTypes	array(RatType)	C	1..N	The 3GPP and non-3GPP RAT Types where the served UE is camping. Shall be provided when available.	MultipleAccessTypes
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.	
wlServAreaRes	WirelineServiceAreaRestriction	O	0..1	Wireline Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF	WirelineWirelessConvergence
rfsp	RfspIndex	C	0..1	RFSP Index as part of the AMF Access and Mobility Policy. Shall be provided when available.	
ueAmbr	Ambr	C	0..1	UE-AMBR as part of the AMF Access and Mobility Policy. Shall be provided when available.	UE-AMBR_Authorization
allowedSnssais	array(Snssai)	C	1..N	Represents the Allowed NSSAI in the 3GPP access and includes the S-NSSAIs values the UE can use in the serving PLMN. It shall be included if the feature "SliceSupport" or the feature "DNNReplacementControl" is supported in the AMF.	SliceSupport, DNNReplacementControl

mappingSnssais	array(MappingOfSnssai)	C	1..N	The mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN. It shall be included if available. If the feature "MultipleAccessTypes" is supported, this attribute contains also the mapping of the Allowed NSSAI in the non-3GPP access to the corresponding S-NSSAI of the HPLMN.	DNNReplacementControl
n3gAllowedSnssais	array(Snssai)	C	1..N	Represents the Allowed NSSAI in the non-3GPP access and includes the S-NSSAIs values the UE can use in the serving PLMN. It shall be included if the feature "MultipleAccessTypes" and, the feature "SliceSupport" or "DNNReplacementControl" are supported in the AMF and the UE is registered in the non-3GPP access.	SliceSupport, MultipleAccessTypes, DNNReplacementControl
guami	Guami	C	0..1	The Globally Unique AMF Identifier (GUAMI) shall be provided by an AMF as service consumer.	
serviceName	ServiceName	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.	
altNotifFqdns	array(Fqdn)	O	1..N	Alternate or backup FQDN(s) 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".	
wlServAreaRes	WirelineServiceAreaRestriction	C	0..1	Wireline Service Area Restriction as part of the AMF Access and Mobility Policy. Shall be provided for trigger "SERV_AREA_CH".	WirelineWirelessConvergence
rfsp	RfspIndex	C	0..1	RFSP Index as part of the AMF Access and Mobility Policy. Shall be provided for trigger "RFSP_CH".	
smfSelInfo	SmfSelectionData	C	0..1	The UE requested S-NSSAI and UE requested DNN. Shall be provided for trigger "SMF_SELECT_CH".	DNNReplacementControl
ueAmbr	Ambr	C	0..1	UE-AMBR as part of the AMF Access and Mobility Policy. Shall be provided for trigger "UE_AMBR_CH".	UE-AMBR_Authorization
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. The "additionalPraId" attribute within the PresenceInfo data type shall not be supplied. The "praId" attribute within the PresenceInfo data type shall include the identifier of an individual presence reporting area.	
userLoc	UserLocation	C	0..1	The location of the served UE shall be provided for trigger "LOC_CH".	
allowedSnssais	array(Snssai)	C	1..N	Represents the Allowed NSSAI in the 3GPP access and includes the S-NSSAIs values the UE can use in the serving PLMN. It shall be provided for trigger "ALLOWED_NSSAI_CH".	SliceSupport, DNNReplacementControl
mappingSnssais	array(MappingOfSnssai)	O	1..N	The mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN. It shall be provided for trigger "ALLOWED_NSSAI_CH" if available. If the feature "MultipleAccessTypes" is supported, this attribute contains also the mapping of the Allowed NSSAI in the non-3GPP access to the corresponding S-NSSAI of the HPLMN.	DNNReplacementControl

n3gAllowedSnssais	array(Snssai)	C	1..N	Represents the Allowed NSSAI in the non-3GPP access and includes the S-NSSAIs values the UE can use in the serving PLMN. It shall be provided for trigger "ALLOWED_NSSAI_CH" when the feature "MultipleAccessTypes" is supported.	SliceSupport, MultipleAccessTypes, DNNReplacementControl
accessTypes	array(AccessType)	C	1..N	The Access Types where the served UE is camping. Shall be provided for trigger "ACCESS_TYPE_CH".	MultipleAccessTypes
ratTypes	array(RatType)	C	1..N	The 3GPP RAT Type and non-3GPP RAT Type where the served UE is camping. Shall be provided for trigger "ACCESS_TYPE_CH".	MultipleAccessTypes
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. (NOTE 3)	
triggers	array(RequestTrigger)	O	1..N	Request Triggers that the PCF subscribes. Only values "LOC_CH", "ALLOWED_NSSAI_CH", "SMF_SELECT_CH", "PRA_CH" and "ACCESS_TYPE_CH" are permitted.	(NOTE 1) (NOTE 2)
servAreaRes	ServiceAreaRestriction	O	0..1	Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF.	
wlServAreaRes	WirelineServiceAreaRestriction	O	0..1	Wireline Service Area Restriction as part of the AMF Access and Mobility Policy as determined by the PCF	WirelineWirelessConvergence
rfsp	RfspIndex	O	0..1	RFSP Index as part of the AMF Access and Mobility Policy as determined by the PCF.	
smfSelInfo	SmfSelectionData	C	0..1	It may include updated conditions for SMF Selection information replacement. It shall include the PCF decision of the selected DNN when the "smfSelInfo" attribute containing the UE requested S-NSSAI and DNN was sent in the request.	DNNReplacementControl
ueAmbr	Ambr	C	0..1	UE-AMBR as part of the AMF Access and Mobility Policy.	UE-AMBR_Authorization
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. The "praId" attribute within the PresenceInfo data type shall include the identifier of either a presence reporting area or a presence reporting area set.	

NOTE 1: The "ALLOWED_NSSAI_CH", "SMF_SELECT_CH" and "ACCESS_TYPE_CH" values in the "triggers" attribute apply under feature control as described in subclause 4.2.3.2.
NOTE 2: The "SMF_SELECT_CH" trigger may be met only for new PDU sessions, i.e. it shall not apply to ongoing PDU sessions.
NOTE 3: When the PolicyUpdate data type is used in a policy update notify service operation, either the complete resource URI included in the "resourceUri" attribute or the "apiSpecificResourceUriPart" component (see subclause 5.1) of the resource URI included in the "resourceUri" attribute may be used by the NF service consumer (e.g. AMF) for the identification of the Individual AM Policy Association resource related to the notification.

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. (NOTE)	
cause	PolicyAssociationReleaseCause	M	1	The cause why the PCF requests the termination of the policy association.	
NOTE: Either the complete resource URI included in the "resourceUri" attribute or the "apiSpecificResourceUriPart" component (see subclause 5.1) of the resource URI included in the "resourceUri" attribute may be used by the NF service consumer (e.g. AMF) for the identification of the Individual AM Policy Association resource related to the notification.					

5.6.2.7 Type SmfSelectionData

Table 5.6.2.7-1: Definition of type SmfSelectionData

Attribute name	Data type	P	Cardinality	Description	Applicability
unsuppDnn	boolean	O	0..1	When it is set to "true", the AMF shall request DNN replacement when the UE requested an unsupported DNN at PDU session establishment request. The default value is "false".	
candidates	map(CandidateForReplacement)	O	1..N	Contains the list of DNNs per S-NSSAI that are candidate for replacement. The "snssai" attribute within the CandidateForReplacement data type shall also be the key of the map.	
snssai	Snssai	C	0..1	It shall be included in AM policy association update requests and represents the allowed S-NSSAI the UE includes in the PDU session establishment request.	
mappingSnssai	Snssai	O	0..1	It may be included in AM policy association update requests and represents the home mapping of the allowed S-NSSAI the UE includes in the PDU session establishment request.	
dnn	Dnn	C	0..1	It shall be included in AM policy association update requests and represents the UE requested DNN. It shall be included in AM policy association update response and represents the PCF selected DNN.	
NOTE: Either one of the "unsuppDnn" attribute and "candidates" attribute, or both attributes shall be present when the "smfSelInfo" attribute is included in the PolicyAssociation type or PolicyUpdate type when included in the Npcf_AMPolicyControl_UpdateNotify request.					

5.6.2.8 Type CandidateForReplacement

Table 5.6.2.8-1: Definition of type CandidateForReplacement

Attribute name	Data type	P	Cardinality	Description	Applicability
snssai	Snssai	M	1	The S-NSSAI in the serving PLMN. It shall contain a S-NSSAI within the Allowed NSSAI.	
dnns	array(Dnn)	O	1..N	List of candidate DNNs for replacement for the S-NSSAI included in the "snssai" attribute. If omitted, any DNN for the provided S-NSSAI is candidate for replacement.	

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.	
ALLOWED_NSSAI_CH	Allowed NSSAI change: the AMF notifies that the set of UE allowed S-NSSAIs has changed.	SliceSupport, DNNReplacementControl
UE_AMBR_CH	UE-AMBR change: the UDM notifies the AMF that the subscribed UE-AMBR has changed.	UE-AMBR_Authorization
SMF_SELECT_CH	SMF selection information change: UE request for an unsupported DNN or UE request for a DNN within the list of DNN candidates for replacement per S-NSSAI.	DNNReplacementControl
ACCESS_TYPE_CH	Access Type change: the AMF notifies that the access type and the RAT type combinations available in the AMF for a UE with simultaneous 3GPP and non-3GPP connectivity have changed.	MultipleAccessTypes

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].

Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [5] for HTTP redirections shall be supported if the feature "ES3XX" is supported.

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 and Table 5.7.3-2. 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 when PCF acts as a server. The AMF shall include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-2 when AMF acts as a server.

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.
PENDING_TRANSACTION	400 Bad Request	This error shall be used when the PendingTransaction feature is supported and the PCF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association and cannot handle the request as described in clause 9.2 of 3GPP TS 29.513 [7].

Table 5.7.3-2: Application errors when AMF acts as a server to receive a notification

Application Error	HTTP status code	Description
PENDING_TRANSACTION	400 Bad Request	This error shall be used when the PendingTransaction feature is supported and the AMF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association and cannot handle the request as described in clause 9.2 of 3GPP TS 29.513 [7].

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
1	SliceSupport	Indicates the support of AM policies differentiation based on the awareness of the allowed NSSAI.
2	PendingTransaction	This feature indicates support for the race condition handling as defined in 3GPP TS 29.513 [7].
3	UE-AMBR_Authorization	Indicates the support of UE-AMBR control by the PCF in the serving network.
4	DNNReplacementControl	Indicates the support of DNN replacement control.
5	MultipleAccessTypes	Indicates the support of AM policies for the multiple access types where the served UE is camping.
6	WirelineWirelessConvergence	Indicates the support of Wireline and Wireless access convergence.
8	ES3XX	Extended Support for 3xx redirections. This feature indicates the support of redirection for any service operation, according to Stateless NF procedures as specified in subclauses 6.5.3.2 and 6.5.3.3 of 3GPP TS 29.500 [5] and according to HTTP redirection principles for indirect communication, as specified in subclause 6.10.9 of 3GPP TS 29.500 [5].

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: 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 a Git-based repository that uses the GitLab software version control system (see clause 5B of the 3GPP TR 21.900 [22] and subclause 5.3.1 of the 3GPP TS 29.501 [6] for further information).

A.2 Npcf_AMPolicyControl API

```
openapi: 3.0.0
info:
  version: 1.1.3
  title: Npcf_AMPolicyControl
  description: |
    Access and Mobility Policy Control Service.
    © 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
externalDocs:
  description: 3GPP TS 29.507 V16.7.0; 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 4.4 of 3GPP TS 29.501
security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-am-policy-control
paths:
  /policies:
    post:
      operationId: CreateIndividualAMPolicyAssociation
      summary: Create individual AM policy association.
      tags:
        - AM Policy Associations (Collection)
      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 successful.
                '307':
                  description: temporary redirect
                  content:
                    application/problem+json:
                      schema:
                        $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
                  headers:
                    Location:
                      description: ' A URI pointing to the endpoint of an alternative NF consumer
(service) instance towards which the notification should be redirected.'
                      required: true
                      schema:
                        type: string
                    3gpp-Sbi-Target-Nf-Id:
                      description: 'Identifier of the target NF (service) instance towards which the
notification request is redirected'
                      schema:
                        type: string
                '308':
                  description: Permanent Redirect
                  content:
                    application/problem+json:
                      schema:
                        $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
                  headers:
                    Location:
                      required: true
                      description: 'A URI pointing to the endpoint of an alternative NF consumer
(service) instance towards which the notification should be redirected.'
                      schema:
                        type: string
                    3gpp-Sbi-Target-Nf-Id:
                      description: 'Identifier of the target NF (service) instance towards which the
notification request is redirected'
                      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 successful.
              '307':
                description: temporary redirect
                content:
                  application/problem+json:
                    schema:
                      $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
                headers:
                  Location:
                    description: ' A URI pointing to the endpoint of an alternative NF consumer
(service) instance towards which the notification should be redirected.'
                    required: true
                    schema:
                      type: string
                  3gpp-Sbi-Target-Nf-Id:
                    description: 'Identifier of the target NF (service) instance towards which the
notification request is redirected'
                    schema:
                      type: string
              '308':
                description: Permanent Redirect
                content:
                  application/problem+json:
                    schema:
                      $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
                headers:
                  Location:
                    required: true
                    description: 'A URI pointing to the endpoint of an alternative NF consumer
(service) instance towards which the notification should be redirected.'
                    schema:
                      type: string
                  3gpp-Sbi-Target-Nf-Id:
                    description: 'Identifier of the target NF (service) instance towards which the
notification request is redirected'
                    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:
      operationId: ReadIndividualAMPolicyAssociation
      summary: Read individual AM policy association.
      tags:
        - Individual AM Policy Association (Document)
      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'
        '307':
          description: Temporary Redirect
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
          headers:
            Location:
              description: 'An alternative URI of the resource located on an alternative PCF
(service) instance.'
              required: true
              schema:
                type: string
            3gpp-Sbi-Target-Nf-Id:
              description: 'Identifier of the target NF (service) instance towards which the request
is redirected'
              schema:
                type: string
        '308':
          description: Permanent Redirect
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
          headers:
            Location:
              description: 'An alternative URI of the resource located on an alternative PCF
(service) instance.'
              required: true
              schema:
                type: string
            3gpp-Sbi-Target-Nf-Id:
              description: 'Identifier of the target NF (service) instance towards which the request
is redirected'
              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'
        '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:
      operationId: DeleteIndividualAMPolicyAssociation
      summary: Delete individual AM policy association.
      tags:
        - Individual AM Policy Association (Document)
      parameters:
        - name: polAssoId
          in: path
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '204':
          description: No Content. Resource was successfully deleted.
        '307':
          description: Temporary Redirect
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
          headers:
            Location:
              description: 'An alternative URI of the resource located on an alternative PCF
(service) instance.'
              required: true
              schema:
                type: string
            3gpp-Sbi-Target-Nf-Id:
              description: 'Identifier of the target NF (service) instance towards which the request
is redirected'
              schema:
                type: string
        '308':
          description: Permanent Redirect
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
          headers:
            Location:
              description: 'An alternative URI of the resource located on an alternative PCF
(service) instance.'
              required: true
              schema:
                type: string
            3gpp-Sbi-Target-Nf-Id:
              description: 'Identifier of the target NF (service) instance towards which the request
is redirected'
              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'
        '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:
      operationId: ReportObservedEventTriggersForIndividualAMPolicyAssociation
      summary: Report observed event triggers and obtain updated policies for an individual AM
policy association.
      tags:
```

```
        - Individual AM Policy Association (Document)
      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'
        '307':
          description: Temporary Redirect
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
          headers:
            Location:
              description: 'An alternative URI of the resource located on an alternative PCF
(service) instance.'
              required: true
              schema:
                type: string
            3gpp-Sbi-Target-Nf-Id:
              description: 'Identifier of the target NF (service) instance towards which the request
is redirected'
              schema:
                type: string
        '308':
          description: Permanent Redirect
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
          headers:
            Location:
              description: 'An alternative URI of the resource located on an alternative PCF
(service) instance.'
              required: true
              schema:
                type: string
            3gpp-Sbi-Target-Nf-Id:
              description: 'Identifier of the target NF (service) instance towards which the request
is redirected'
              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'
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.
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        wlServAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/WirelineServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        smfSelInfo:
          $ref: '#/components/schemas/SmfSelectionData'
        ueAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        pras:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - suppFeat
    PolicyAssociationRequest:
      description: Information which the NF service consumer provides when requesting the creation
of a policy association. The serviveName property corresponds to the serviceName in the main body of
the specification.
      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.
        altNotifFqdns:
          type: array
          items:
            $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/Fqdn'
          minItems: 1
          description: Alternate or backup FQDN(s) 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'
        accessTypes:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
          minItems: 1
```

```
        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/PlmnIdNid'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        ratTypes:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
          minItems: 1
        groupIds:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
          minItems: 1
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        wlServAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/WirelineServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        ueAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        allowedSnssais:
          description: array of allowed S-NSSAIs for the 3GPP access.
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
          minItems: 1
        mappingSnssais:
          description: mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of
the HPLMN.
          type: array
          items:
            $ref: 'TS29531_Nnssf_NSSelection.yaml#/components/schemas/MappingOfSnssai'
          minItems: 1
        n3gAllowedSnssais:
          description: array of allowed S-NSSAIs for the Non-3GPP access.
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
          minItems: 1
        guami:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Guami'
        serviveName:
          $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/ServiceName'
        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.
        altNotifFqdns:
          type: array
```

```
          items:
            $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/Fqdn'
          minItems: 1
          description: Alternate or backup FQDN(s) 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'
        wlServAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/WirelineServiceAreaRestriction'
        rfsp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
        smfSelInfo:
          $ref: '#/components/schemas/SmfSelectionData'
        ueAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        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'
        allowedSnssais:
          description: array of allowed S-NSSAIs for the 3GPP access.
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
          minItems: 1
        mappingSnssais:
          description: mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of
the HPLMN.
          type: array
          items:
            $ref: 'TS29531_Nnssf_NSSelection.yaml#/components/schemas/MappingOfSnssai'
          minItems: 1
        accessTypes:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
          minItems: 1
        ratTypes:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
          minItems: 1
        n3gAllowedSnssais:
          description: array of allowed S-NSSAIs for the Non-3GPP access.
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
          minItems: 1
        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.
        servAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceAreaRestriction'
        wlServAreaRes:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/WirelineServiceAreaRestriction'
        rfsp:
```

```
        $ref: 'TS29571_CommonData.yaml#/components/schemas/RfspIndex'
      smfSelInfo:
        $ref: '#/components/schemas/SmfSelectionData'
      ueAmbr:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
      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
  SmfSelectionData:
    type: object
    properties:
      unsuppDnn:
        type: boolean
      candidates:
        type: object
        additionalProperties:
          $ref: '#/components/schemas/CandidateForReplacement'
        minProperties: 1
        nullable: true
      snssai:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
      mappingSnssai:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
      dnn:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
    nullable: true
  CandidateForReplacement:
    type: object
    properties:
      snssai:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
      dnns:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        minItems: 1
        nullable: true
    required:
      - snssai
    nullable: true
  RequestTrigger:
    anyOf:
    - type: string
      enum:
        - LOC_CH
        - PRA_CH
        - SERV_AREA_CH
        - RFSP_CH
        - ALLOWED_NSSAI_CH
        - UE_AMBR_CH
        - SMF_SELECT_CH
        - ACCESS_TYPE_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.
        - ALLOWED_NSSAI_CH: Allowed NSSAI change. The AMF notifies that the set of UE allowed S-
NSSAIs has changed.
        - UE_AMBR_CH: UE-AMBR change. The UDM notifies the AMF that the subscribed UE-AMBR has
changed.
        - SMF_SELECT_CH: SMF selection information change. The UE requested for an unsupported DNN
or UE requested for a DNN within the list of DNN candidates for replacement per S-NSSAI.
        - ACCESS_TYPE_CH: Access Type change. The AMF notifies that the access type and the RAT type
combinations available in the AMF for a UE with simultaneous 3GPP and non-3GPP connectivity 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 (normative): Wireless and wireline convergence access support

B.1 Scope

This annex defines procedures for wireless and wireline convergence access support for 5GS. The stage 2 definition and procedures are contained in 3GPP TS 23.316 [23]. The System Architecture for wireless and wireline convergence access is defined in 3GPP TS 23.501 [2].

B.2 Npcf_AMPolicyControl Service

B.2.1 Service Description

B.2.1.1 Overview

Subclause 4.1.1 applies with the modification that the UE is replaced by the 5G-RG and the W-AGF, which is acting as a UE towards the 5GC on behalf of the FN-RG.

B.2.1.2 Service Architecture

Subclause 4.1.2 applies with the exception that roaming functionality shall not apply in this Release of the specification for access and mobility policy control for 5G-RG connecting via W-5GAN and FN-RG. Roaming architecture is only applicable to a 5G-RG connecting to the 5GC via NG RAN.

B.2.1.3 Network Functions

B.2.1.3.1 Policy Control Function (PCF)

The PCF functionality defined in subclause 4.1.3.1 shall apply with the following modifications for wireline access:

- The UE-AMBR control by the serving network does not apply.
- The Service Area Restrictions for a FN-BRG do not apply.
- The PCF provides access and mobility related policy control as described in this Annex.

B.2.1.3.2 NF Service Consumers

The AMF functionality defined in subclause 4.1.3.2 shall apply with the following exceptions:

- The UE-AMBR control by the visited network is only applicable for a 5G-RG registered over 3GPP access.
- The AMF enforces access and mobility related policy control as described in this Annex.

B.3 Service Operation

B.3.1 Introduction

The descriptions in clause 4.2.1 are applied with the following differences:

- UE is replaced by the 5G-RG.

B.3.2 Npcf_AMPolicyControl_Create Service Operation

B.3.2.1 General

The procedure defined in clause 4.2.2.1 is applied with following differences:

- UE is replaced by the 5G-RG or FN-RG if applicable.
- Handling of RFSP information is not applicable if the 5G-RG or FN-RG connects the 5GC via wireline access.
- Global Line ID including the line Id and either PLMN Id or operator Id is encoded within the "gli" attribute of the "n3gaLocation" attribute included in the "userLoc" attribute within the PolicyAssociationRequest data structure when the 5G-RG or FN-RG connects the 5GC via W-5GBAN.
- The HFC Node Identifier in the "hfcNodeId" attribute of the "n3gaLocation" attribute included in the "userLoc" attribute within the PolicyAssociationRequest data structure when the 5G-CRG or FN-CRG connects to the 5GC via W-5GCAN.
- Only the policy control request triggers defined in subclause B.3.4.2 are provided by the PCF when the 5G-RG or FN-RG connects the 5GC via wireline access.
- The PolicyAssociationRequest data structure shall include, if available, and if the feature "WirelineWirelessConvergence" is supported, wireline access Service Area Restrictions (see subclause B.3.2.2.2) derived from the wireline access Service Area Restrictions obtained from the UDM by mapping any service areas denoted by geographical information into Line IDs (for a 5G-BRG) or HFC Node IDs (for a 5G-CRG and FN-CRG) encoded as "wlServAreaRes" attribute.
- The PolicyAssociation data type returned as body of the HTTP "201 Created" response shall include if the feature "WirelineWirelessConvergence" is supported, and if the PCF received the "wlServAreaRes" in the request, wireline Service Area Restrictions encoded as "wlServAreaRes" attribute.
- If the feature "MultipleAccessTypes" is supported, the NF service consumer (e.g. AMF) shall include:

  a) the RAT type entry corresponding to non-3GPP wireline access and/or the RAT type entry corresponding to the 3GPP access encoded in the "ratTypes" attribute, if available; and

  b) the "accessTypes" attribute indicating registration in the 3GPP access, or registration in the non-3GPP access, or registration in both 3GPP and non-3GPP access, if available.

NOTE: When both, 3GPP access and non-3GPP accesses are available, the "accessType" attribute and the "ratType" attribute within the PolicyAssociationRequest type contain the access type and RAT type corresponding to the 3GPP access.

- If the feature "SliceSupport" or the feature "DNNReplacementControl" is supported in the AMF, the UE is registered in the non-3GPP access, and the feature "MultipleAccessTypes" is supported, the NF service consumer (e.g. AMF) shall include the Allowed NSSAI in the non-3GPP access encoded in the "n3gAllowedSnssais" attribute.
- If the feature "DNNReplacementControl" is supported, the UE is registered in the non-3GPP access, and the feature "MultipleAccessTypes" is supported, the NF service consumer (e.g. AMF) may include the mapping of each S-NSSAI of the Allowed NSSAI in the non-3GPP access to the corresponding S-NSSAI of the HPLMN encoded in the "mappingSnssais" attribute.
- The PEI that may be included within the "pei" attribute shall have one of the following representations:

  a) If the 5G-BRG supports only wireline access, the PEI shall be the 5G-BRG MAC address.

  b) If the 5G-CRG supports only wireline access, the PEI shall be the cable modem MAC address.

  c) If the 5G-RG supports at least one 3GPP access technology, the PEI shall be the allocated IMEI or IMEISV.

  d) For the FN-BRG and FN-CRG, the PEI shall be the FN-RG MAC address.

NOTE: When the PEI includes an indication that the MAC address cannot be used as Equipment identifier of the FN-RG, the PEI cannot be trusted for regulatory purposes and cannot be used for equipment based policy evaluation.

B.3.2.2 AMF Access and Mobility Policy

B.3.2.2.1 General

The functionality defined in subclause 4.2.2.3 shall apply with the following modifications:

- UE-AMBR defined in subclause 4.2.2.3.3 shall not apply for wireline access.
- RFSP Index defined in subclause 4.2.2.3.2 shall not apply for wireline access.
- Service Area Restriction defined in subclause 4.2.2.3.1 is only applicable for a 5G-RG connected via NG-RAN. The wireline access Service Area Restriction defined in subclause B.3.2.2.2 shall apply for a FN-CRG and/or a 5G-RG (5G-BRG and 5G-CRG) connected via wireline access.

B.3.2.2.2 Wireline Service Area Restriction

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

- either a limited allowed area represented as both of:
  (i) a list of either Line IDs encoded as "globLineIds" (for a 5G-BRG) or HFC-Node IDs (for 5G-CRG and FN-CRG) encoded as "hfcNIds" attribute within the "areas" attribute; and
  (ii) the "restrictionType" attribute set to "ALLOWED_AREAS";
- or a limited not allowed area represented as both of:
  (i) a list of either Line IDs encoded as "globLineIds" (for a 5G-BRG) or HFC-Node IDs (for 5G-CRG and FN-CRG) encoded as "hfcNIds" attribute within the "areas" attribute; and
  (ii) the "restrictionType" attribute set to "NOT_ALLOWED_AREAS";

When the authorized wireline service area restrictions result in an unlimited set of HFC-Node IDs or Line IDs, the PCF shall include an empty "wlServAreaRes" attribute.

B.3.2.2.3 Void

B.3.3 Npcf_AMPolicyControl_UpdateNotify Service Operation

B.3.3.1 General

The functionality defined in subclause 4.2.4.2 and 4.2.4.3 shall apply.

B.3.4 Npcf_AMPolicyControl_Update Service Operation

B.3.4.1 General

The general procedure specified in subclause 4.2.3.2 to modify an existing AM policy association shall apply with the exception that for a FN-RG or a 5G-RG registering via wireline access only, the existing AM policy association shall not be updated due to location change (tracking area), change of UE presence in PRA, or RFSP index change.

If the feature "MultipleAccessTypes" is supported, the NF service consumer may include in the PolicyAssociationUpdateRequest data structure:

- if the Access Type and/or the RAT type changed and the access type change Policy Control Request Trigger was previously provisioned (see subclause B.3.4.2), the list of Access Type and RAT Type combinations available encoded in the "accessTypes" attribute, "ratTypes" attribute.

When the feature "MultipleAccessTypes" is supported the PCF may include in the PolicyUpdate data type the access type change Policy Control Request Trigger (see subclause B.3.4.2) encoded within the "triggers" attribute.

If the feature "SliceSupport" or the feature "DNNReplacementControl" is supported in the AMF, the UE is registered in the non-3GPP access, and the feature "MultipleAccessTypes" is supported, the NF service consumer (e.g. AMF) shall include the Allowed NSSAI in the non-3GPP access encoded in the "n3gAllowedSnssais" attribute together with the "ALLOWED_NSSAI_CH" policy control request trigger when a change of the Allowed NSSAI for the non-3GPP access occurred.

If the feature "DNNReplacementControl" is supported, the UE is registered in the non-3GPP access, and the feature "MultipleAccessTypes" is supported, the Allowed NSSAI changed and/or the mapping of a S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN changed, and the Policy Control Request Trigger "Change of allowed NSSAI" was provided then NF service consumer (e.g. AMF) may include the mapping of each S-NSSAI of the Allowed NSSAI in the non-3GPP access to the corresponding S-NSSAI of the HPLMN encoded in the "mappingSnssais" attribute.

In addition, if the feature "WirelineWirelessConvergence" is supported:

- the PolicyAssociationUpdateRequest data structure shall include if a wireline access Service Area restriction change occurred, the wireline access Service Area Restrictions (see subclause B.3.2.2.2) derived from the ones obtained from the UDM encoded as "wlServAreaRes" attribute;

- the PolicyUpdate data returned in the response, if the PCF received the " wlServAreaRes" attribute in the request, wireline access Service Area Restrictions encoded as "wlServAreaRes" attribute.

B.3.4.2 Policy Control Request Triggers

For a 5G-RG registering via NG-RAN, the Policy Control Request Triggers defined in subclause 4.2.3.2 shall apply.

For a FN-RG or a 5G-RG registering via wireline access, only the following Policy Control Request Triggers defined in subclause 4.2.3.2 shall apply:

- "SERV_AREA _CH", i.e. Service Area Restriction change: the UDM notifies the AMF that the subscribed service area restriction information has changed;

- "ALLOWED_NSSAI_CH", i.e. change of allowed NSSAI of the served UE;

NOTE 1: The "ALLOWED_NSSAI_CH" trigger only applies if the feature "SliceSupport" or the feature "DNNReplacementControl" is supported.

NOTE 2: The "SERV_AREA_CH" trigger is also used to notify that the subscribed wireline access service area restriction information has changed.

- "ACCESS_TYPE_CH", i.e. the access type change: the AMF notifies that the access type and the RAT type combinations available in the AMF for a UE with simultaneous 3GPP and non-3GPP connectivity has changed; and

NOTE 3: The "ACCESS_TYPE_CH" trigger only applies if the "MultipleAccessTypes" feature is supported.

- "SMF_SELECT_CH", i.e. SMF selection information change.

NOTE 4: The "SMF_SELECT_CH" trigger only applies if the "DNNReplacementControl" feature is supported.

B.3.4.3 Encoding of updated policy

Updated policies shall be encoded within the PolicyUpdate as specified in subclause 4.2.3.3 with the modifications listed in subclauses B.3.4.1, B.3.4.2, and this subclause.

- AMF Access and Mobility Policy (see subclause B.3.2.2.2) Service Area Restriction for wireline access is encoded as "wlServAreaRes" attribute.

B.3.5 Npcf_AMPolicyControl_Delete Service Operation

B.3.5.1 General

The functionality defined in subclause 4.2.5 shall apply.

Annex C (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-191089	0051	3	F	Support of Allowed NSSAI	16.0.0
2019-06	CT#84	CP-191089	0054	1	F	Correction on Policy Association termination	16.0.0
2019-06	CT#84	CP-191101	0055	2	F	API version Update	16.0.0
2019-06	CT#84	CP-191096	0056	1	F	Adding tags to OpenAPI File	16.0.0
2019-06	CT#84	CP-191089	0058	1	F	Race Condition handling	16.0.0
2019-09	CT#85	CP-192178	0061	-	B	Adding NID as input for policy decisions	16.1.0
2019-09	CT#85	CP-192156	0062	-	B	Serving PLMN UE AMBR control	16.1.0
2019-09	CT#85	CP-192140	0065	1	A	Correcting the resource URI of AM Policy Associations	16.1.0
2019-09	CT#85	CP-192176	0066	1	B	Support of wireline and wireless access convergence, NFs	16.1.0
2019-09	CT#85	CP-192152	0067	2	B	Support of 5WWC, Policy Control Request Triggers	16.1.0
2019-09	CT#85	CP-192152	0068	-	B	Annex of wireless and wireline convergence access support	16.1.0
2019-09	CT#85	CP-192152	0070	-	B	Npcf_AMPolicyControl_Create Service Operation of annex	16.1.0
2019-09	CT#85	CP-192140	0074	2	A	GUAMI included in the Update operation	16.1.0
2019-09	CT#85	CP-192173	0076	-	F	OpenAPI version update for TS 29.507 Rel-16	16.1.0
2019-12	CT#86	CP-193197	0078	1	F	Data type of the "serviceName" attribute	16.2.0
2019-12	CT#86	CP-193182	0080	-	A	Correction to PolicyUpdate	16.2.0
2019-12	CT#86	CP-193197	0081	2	B	DNN replacement	16.2.0
2019-12	CT#86	CP-193237	0084	2	B	Line Identifier	16.2.0
2019-12	CT#86	CP-193197	0086	1	B	AM Policy association establishment rejection	16.2.0
2019-12	CT#86	CP-193182	0088	1	A	Correction to Service Area Restrictions description	16.2.0
2019-12	CT#86	CP-193182	0090	1	A	Correction on 307 error, 29.507	16.2.0
2019-12	CT#86	CP-193232	0091	1	B	Support of simultaneous registration in multiple accesses	16.2.0
2019-12	CT#86	CP-193232	0092	2	B	Support of S-NSSAI for non-3GPP access	16.2.0
2019-12	CT#86	CP-193191	0093	1	B	Support of 5WWC, Service Area Restrictions	16.2.0
2019-12	CT#86	CP-193191	0094	1	B	Clarification of PEI format, 29.507	16.2.0
2019-12	CT#86	CP-193226	0095	2	B	HFC node Id in Location information	16.2.0
2019-12	CT#86	CP-193212	0096	-	F	Update of API version and TS version in OpenAPI file	16.2.0
2020-03	CT#87e	CP-200203	0097	1	B	Policy Control Request Triggers for wireline access	16.3.0
2020-03	CT#87e	CP-200203	0098	1	B	The data type of GlobalLineId	16.3.0
2020-03	CT#87e	CP-200207	0099	-	F	Corrections related to DNN replacement	16.3.0
2020-03	CT#87e	CP-200207	0100	-	F	Remove the possibility of SNSSAI change for DNN replacement	16.3.0
2020-03	CT#87e	CP-200207	0101	-	B	Mapping Of Allowed NSSAI	16.3.0
2020-03	CT#87e	CP-200207	0102	-	B	Completion of DNN replacement functionality	16.3.0
2020-03	CT#87e	CP-200207	0103	1	B	Completing the description of triggers values applicability in PolicyAssociation and PolicyUpdate types.	16.3.0
2020-03	CT#87e	CP-200216	0105	1	B	Update of OpenAPI version and TS version in externalDocs field	16.3.0
2020-06	CT#88e	CP-201215	0107	1	A	Corrections on Service Area Restriction	16.4.0
2020-06	CT#88e	CP-201215	0109	1	A	Location Header of 307 status code	16.4.0
2020-06	CT#88e	CP-201215	0111	1	A	Notification URI	16.4.0
2020-06	CT#88e	CP-201233	0112	3	B	Correction to the DNN replacement	16.4.0
2020-06	CT#88e	CP-201233	0113	1	B	Enable removing the policy decision	16.4.0
2020-06	CT#88e	CP-201233	0114	1	B	FQDN of alternative AMF	16.4.0
2020-06	CT#88e	CP-201228	0115	-	F	Removal of MAC address	16.4.0
2020-06	CT#88e	CP-201233	0116	3	D	OpenAPI: Removal of values from description of "triggers" property	16.4.0
2020-06	CT#88e	CP-201228	0117	1	F	Corrections on Annex B	16.4.0
2020-06	CT#88e	CP-201228	0118	1	B	Untrusted FN-RG PEI	16.4.0
2020-06	CT#88e	CP-201244	0119	1	F	Storage of YAML files in ETSI Forge	16.4.0
2020-06	CT#88e	CP-201256	0121	1	F	URI of the Npcf_AMPolicyControl service	16.4.0
2020-06	CT#88e	CP-201261	0122	1	F	Removal of RG_TMBR trigger	16.4.0
2020-06	CT#88e	CP-201228	0123	-	F	Correction to wireline service area restriction	16.4.0
2020-06	CT#88e	CP-201244	0125	-	F	Optionality of ProblemDetails	16.4.0
2020-06	CT#88e	CP-201244	0126	1	F	Supported headers, Resource Data type, Operation Name	16.4.0

2020-06	CT#88e	CP-201255	0128	-	F	Update of OpenAPI version and TS version in externalDocs field	16.4.0
2020-09	CT#89e	CP-202059	0129	1	F	correction to ACCESS_TYPE_CH trigger	16.5.0
2020-09	CT#89e	CP-202084	0135	-	F	Update of OpenAPI version and TS version in externalDocs field	16.5.0
2020-12	CT#90e	CP-203073	0136	2	F	Essential corrections and alignments	16.6.0
2020-12	CT#90e	CP-203139	0138	1	F	Storage of YAML files in 3GPP Forge	16.6.0
2020-12	CT#90e	CP-203143	0140	2	F	Correction to PRA	16.6.0
2020-12	CT#90e	CP-203112	0147	-	A	report initial presence status for PRA	16.6.0
2020-12	CT#90e	CP-203152	0150	-	F	Update of OpenAPI version and TS version in externalDocs field	16.6.0
2021-03	CT#91e	CP-210191	0151	1	F	Support of stateless NFs	16.7.0
2021-03	CT#91e	CP-210191	0161	-	F	Correction to resource identifiers descriptions used in notifications	16.7.0
2021-03	CT#91e	CP-210239	0164	-	F	Update of OpenAPI version and TS version in externalDocs field	16.7.0

History

Document history		
V16.4.0	August 2020	Publication
V16.5.0	November 2020	Publication
V16.6.0	January 2021	Publication
V16.7.0	April 2021	Publication