ETSI TS 129 525 V15.0.0 (2019-04)

5G;
5G System;
UE Policy Control Service;
Stage 3
(3GPP TS 29.525 version 15.0.0 Release 15)

Reference
DTS/TSGC-0329525vf00

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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 UE Policy Control Service (Npcf_UEPolicyControl) of the 5G System.

The stage 2 definition and procedures of UE 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 UE Policy Control Service is provided by the Policy Control Function (PCF). This service provides UE policies.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

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

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

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

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

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

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

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

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

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

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

[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] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[16] 3GPP TS 24.526: "UE policies for 5G System (5GS); Stage 3".

[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".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

AMF	Access and Mobility Management Function
API	Application Programming Interface
DNN	Data Network Name
GPSI	Generic Public Subscription Identifier
GUAMI	Globally Unique AMF Identifier
HTTP	Hypertext Transfer Protocol
H-PCF	Home Policy Control Function
JSON	JavaScript Object Notation
N3AN	Non-3GPP access network
NF	Network Function
NRF	Network Repository Function
PCF	Policy Control Function
PEI	Permanent Equipment Identifier
PRA	Presence Reporting Area
SUPI	Subscription Permanent Identifier
UDR	Unified Data Repository
UPSC	UE policy section code
UPSI	UE policy section identifier
URSP	UE Route Selection Policy
V-PCF	Visited Policy Control Function

4 UE Policy Control Service

4.1 Service Description

4.1.1 Overview

The UE 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 UE policies such as the UE Route Selection Policy to the UE via the AMF;

and offers the following functionalities:

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

- deletion of the policy context for a UE.

4.1.2 Service Architecture

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

The UE Policy Control Service (Npcf_UEPolicyControl) is part of the Npcf service-based interface exhibited by the Policy Control Function (PCF).

The known consumers of the Npcf_UEPolicyControl service are the Access and Mobility Management Function (AMF) and the Visited Policy Control Function (V-PCF).

The AMF accesses the UE Policy Control Service at the PCF via the N15 Reference point. In the roaming scenario, the N15 reference point is located between the V-PCF in the visited network and the AMF. The V-PCF accesses the UE Policy Control Service at the Home Policy Control Function (H-PCF) via the N24 Reference point.

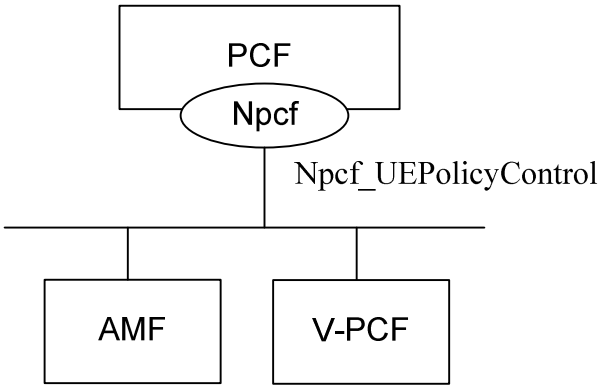


Figure 4.1.2-1: Reference Architecture for the Npcf_UEPolicyControl Service; SBI representation

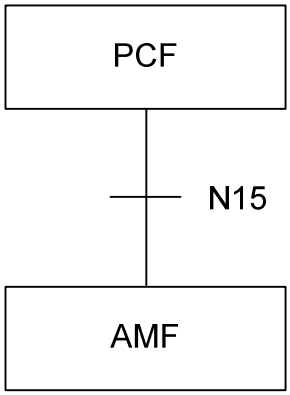


Figure 4.1.2-2: Non-roaming Reference Architecture for the Npcf_UEPolicyControlService; reference point representation

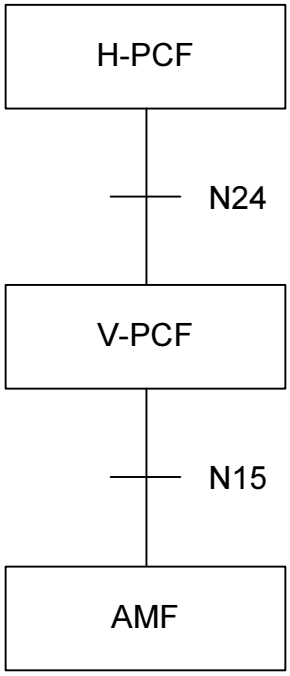


Figure 4.1.3-2: Roaming reference Architecture for the Npcf_UEPolicyControlService; reference point representation

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 UE policy rules, including Access Network discovery and selection policies and UE Route Selection Policies.

4.1.3.2 NF Service Consumers

The Access and Mobility Management function (AMF) provides:

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

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

4.2 Service Operations

4.2.1 Introduction

Table 4.2.1-1: Operations of the Npcf_UEPolicyControl Service

Service operation name	Description	Initiated by
Npcf_UEPolicyControl_Create	Creates a UE Policy Association.	NF consumer (AMF, V-PCF in roaming case)
Npcf_UEPolicyControl_Update	Updates of an UE Policy Association and provides corresponding policies to the NF consumer when the policy control request trigger is met or the AMF is relocated due to the UE mobility and the old PCF is selected.	NF consumer (AMF, V-PCF in roaming case)
Npcf_UEPolicyControl_UpdateNotify	Provides updated policies to the V-PCF by the H-PCF or initiates the UE Policy association termination towards to the NF consumer by the NF producer.	H-PCF for policy update, PCF for initiating the UE policy association termination (H-PCF and V-PCF in roaming case)
Npcf_UEPolicyControl_Delete	Provides means for the NF consumer to delete the UE Policy Association.	NF consumer (AMF, V-PCF in roaming case)

4.2.2 Npcf_UEPolicyControl_Create Service Operation

4.2.2.1 General

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

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

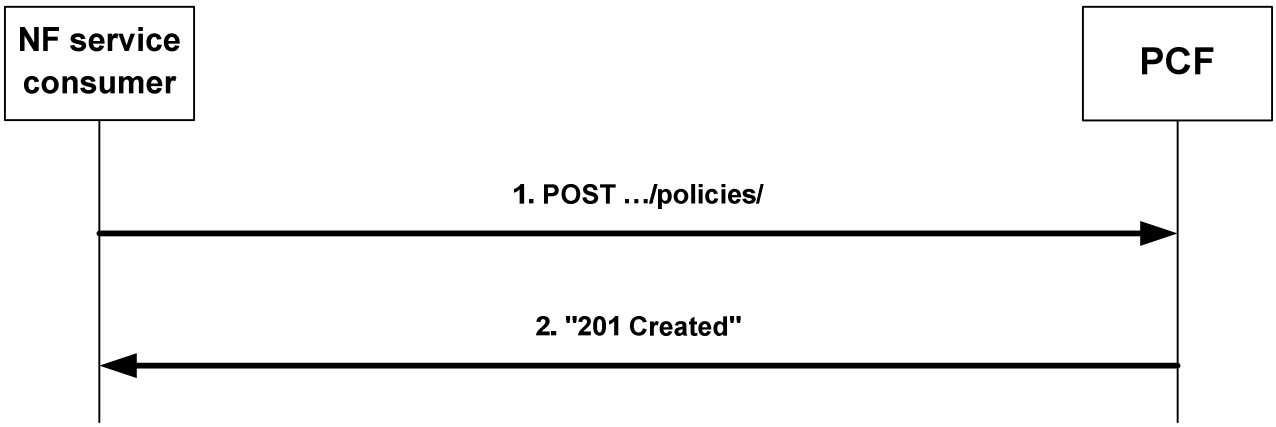


Figure 4.2.2.1-1: Creation of a UE policy association

When a UE registers and a UE context is being established, the AMF can obtain from the UE an UPSI LIST TRANSPORT" message of the UE policy delivery protocol defined in Annex D of 3GPP TS 24.501 [15] and shall decide based on local policies and that message whether to establish a UE policy association with the PCF.

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

- Notification URI encoded as "notificationUri" attribute,

and that shall include when available:

- SUPI encoded as "supi" attribute;

NOTE 1: The SUPI is always available except for some emergency sessions where the UEPolicyControl Service is not required.

- GPSI encoded as "gpsi" attribute;
- Access type encoded as "accessType" attribute;
- Permanent Equipment Identifier (PEI) encoded as "pei" attribute;
- User Location Information encoded as "userLoc" attribute;
- UE Time Zone encoded as "timeZone" attribute;
- Serving PLMN Identifier encoded as "servingPlmn" attribute;
- RAT type encoded as "ratType" attribute;
- any received "UPSI LIST TRANSPORT" message of the UE policy delivery protocol defined in Annex D of 3GPP TS 24.501 [15] encoded as "uePolReq" attribute;
- H-PCF ID (if the consumer is V-PCF, when receiving the H-PCF ID from AMF) encoded as "hPcfId" attribute;
- Internal Group Identifier encoded as "groupId" attribute;
- 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_UEPolicyControl_UpdateNotify service operation encoded as "serviceName" attribute;
- Alternate or backup IPv4 Address(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute; and
- Alternate or backup IPv6 Address(es) where to send Notifications encoded as "altNotifIpv6Addrs" attribute.

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

- shall assign a UE policy association ID;
- if the PCF is a V-PCF, may determine based on operator policy to send as the NF service consumer towards the H-PCF a request for the Creation of a UE policy association as described in the present clause;
- shall determine the applicable UE policy, for the V-PCF taking into consideration any policy received from the H-PCF in the reply to the possible request for the Creation of a policy association;
- for the succesfull case shall send a HTTP "201 Created" response with the URI for the created resource in the "Location" header field

NOTE 2: The assigned policy association ID is part of the URI for the created resource and is thus associated with the SUPI.

and the the PolicyAssociation data type as body including:

- optionally for the H-PCF as service producer communicating with the V-PCF, UE policy (see subclause 4.2.2.2) encoded as "uePolicy" attribute;
- optionally one or several of the following Policy Control Request Trigger(s) encoded as "triggers" attribute (see subclause 4.2.3.2):

  a) Location change (tracking area); and

  b) Change of UE presence in PRA; and

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

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

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

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

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

4.2.2.2 UE Policy

4.2.2.2.1 General

The UE policy consists of UE Access Network discovery and selection policies and UE Route Selection Policy (URSP). The encoding of UE policies is defined in 3GPP TS 24.526 [16].

The UE Policy is transferred to the UE using the UE policy delivery protocol defined in Annex D of 3GPP TS 24.501 [15]. The PCF will receive "MANAGE UE POLICY COMPLETE" messages, "MANAGE UE POLICY COMMAND REJECT" messages and "UPSI LIST TRANSPORT" message and shall send UE policy using the "MANAGE UE POLICY COMMAND" messages. Those messages are transparently forwarded by the AMF.

The "UPSI LIST TRANSPORT" message is transferred transparently during the creation of a policy association, as described in subclause 4.2.2.1.

The V-PCF shall use the Namf_Communication Service defined in 3GPP TS 29.519 [17] to receive "MANAGE UE POLICY COMPLETE" and "MANAGE UE POLICY COMMAND REJECT" messages from the UE and to send MANAGE UE POLICY COMMAND" messages to the UE. The V-PCF shall only send "MANAGE UE POLICY COMMAND" messages below a predefined size limit.

The H-PCF shall use procedures as defined in the present specification to receive "MANAGE UE POLICY COMPLETE" and "MANAGE UE POLICY COMMAND REJECT" messages from the V-PCF and to send MANAGE UE POLICY COMMAND" messages to the V-PCF. The H-PCF shall encode the "MANAGE UE POLICY COMMAND" message in an "uePolicy" attribute.

The PCF may deliver the UE policy to the UE in several "MANAGE UE POLICY COMMAND" messages.

For the purpose of such fragmented delivery and subsequent partial updates of UE policies, the UE policy is divided into policy sections. Such policy sections may be predefined in the PCF, may be retrieved by the PCF from the UDR as specified in 3GPP TS 29.519 [17], or may be dynamically generated by the PCF, but shall comply to the rules below. The PCF may combine several policy sections into one "MANAGE UE POLICY COMMAND" message if the predefined size limit is observed.

The following rules apply for policy sections:

- The size shall be below the predefined size limit.

- The policy section shall only contain complete URSP rule(s), WLANSP rule(s), and/or complete N3AN node configuration information, but no fractions of such rules or configuration information.

- To ease a subsequent partial update of UE policies, policy sections should only contain a small number of URSP rule(s), and/or WLANSP rule(s).

- The entire content of a policy section shall be provided by a single PLMN.

A PCF shall only determine policy sections of its own PLMN. However, a V-PCF may forward UE policy sections received from the H-PCF to the UE.

Each UE policy section is identified by a UE policy section identifier (UPSI). The UPSI is composed of two parts:

a) a PLMN ID part containing the PLMN ID for the PLMN of the PCF which provides the UE policies; and

b) a UE policy section code (UPSC) containing a unique value within the PLMN selected by the PCF.

The PCF provides an UPSI when providing a new UE policy section and can then identify that policy section using that UPSI when requesting that this UE policy section is modified or deleted, as specified in Annex D of 3GPP TS 24.501 [15].

The H-PCF may store and retrieve UPSCs and related policy sections of the own PLMN it provided to a UE in the UDR as specified in 3GPP TS 29.519 [17]. The H-PCF will use the SUPI of the UE as data key and store separate information for each UE in the UDR.

The V-PCF may retrieve UPSCs and related policy sections applicable for all UEs from a HPLMN from the UDR, using the HPLMN ID as key as specified in 3GPP TS 29.519 [17].

When receiving the "UPSI LIST TRANSPORT" message, the PCF shall determine based on the UPSIs indicated in that message, UPCS stored in the UDR and local policy whether any new UE policy sections need to be installed and any existing UE policy section need to be updated or deleted. A V-PCF may also send an "UPSI LIST TRANSPORT" message with the UPSIs of the HPLMN received in the original "UPSI LIST TRANSPORT" message to the H-PCF and will then receive possible new or modified policy sections determined by the HPLMN in a "MANAGE UE POLICY COMMAND". If the PCF determines that changes are required and/or receives possible new or modified policy sections determined by the HPLMN, it shall send the determined new, updated or deleted policy sections using one or several "MANAGE UE POLICY COMMAND" messages towards the NF service consumer.

After sending a "MANAGE UE POLICY COMMAND" messages, the PCF shall wait for a related confirmation in a "MANAGE UE POLICY COMPLETE" messages or failure indication in a "MANAGE UE POLICY COMMAND REJECT" message. When receiving no such message until the expiry of a supervision timer specified in Annex D of 3GPP TS 24.501 [15], or when receiving a failure indication, the PCF should re-send related instructions for the policy sections.

4.2.2.2.2 UE Access Network discovery and selection policies

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

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

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

The Access Network Discovery & Selection policy contains one or more WLAN Selection Policy (WLANSP) rules and Non-3GPP access network (N3AN) node configuration information.

N3AN node configuration information is used to control UE behaviour related to selection of either N3IWF or ePDG for accessing 5GCN via non-3GPP access.

UE Access Network discovery and selection policies are encoded as defined in 3GPP TS 24.526 [16].

UE Access Network discovery and selection policies may be provided by a V-PCF or a H-PCF.

4.2.2.2.3 UE Route Selection Policy(URSP)

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

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

URSP rules are encoded as defined in 3GPP TS 24.526 [16].

UE Route Selection Policy may only be provided by a H-PCF, but shall not be provided by a V-PCF.

4.2.3 Npcf_UEPolicyControl_Update Service Operation

4.2.3.1 General

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

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

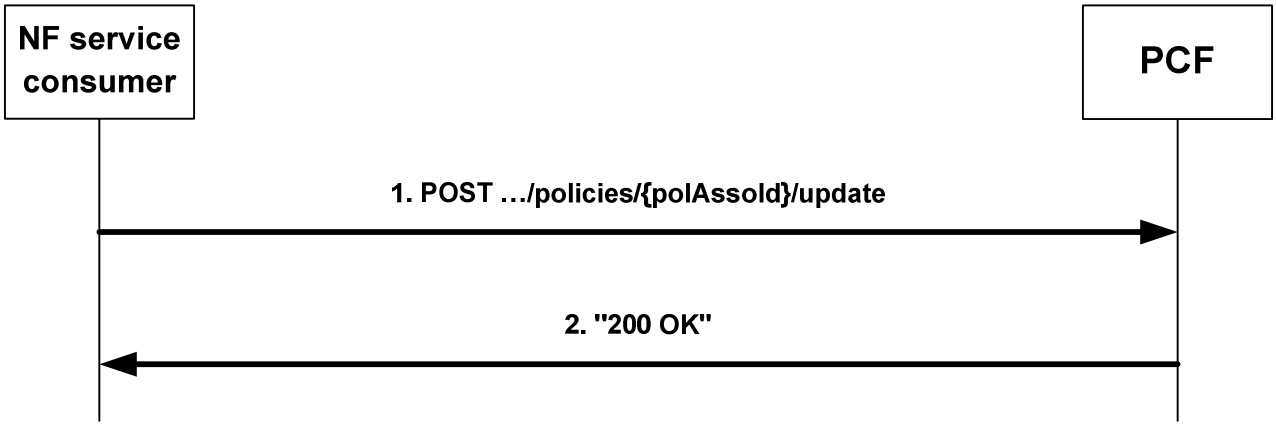


Figure 4.2.3.1-1: Update of a UE policy association

The AMF as NF service consumer invokes this procedure when a policy control request trigger (see subclause 4.2.3.2) occurs. When the "UE_POLICY", 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.

NOTE: 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. The new AMF may also update the alternate or backup IP addresses.

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

- at least one of the following:

  1. a new Notification URI encoded in the "notificationUri" attribute; and/or
  2. observed Policy Control Request Trigger(s) (see subclause 4.2.3.2) encoded as "triggers" attribute;
  3. if a UE location change occurred, the UE location encoded as "userLoc" attribute;
  4. if a "MANAGE UE POLICY COMPLETE" message or a "MANAGE UE POLICY COMMAND REJECT" message of the UE policy delivery protocol defined in Annex D of 3GPP TS 24.501 [15] has been received by the NF service consumer, the message encoded as "uePolDelResult" attribute;
  5. if the Policy Control Request Trigger "Change of UE presence in PRA" is provided, the presence reporting areas for which reporting was requested and the status has changed encoded as "praStatuses" attribute;
  6. for AMF relocation scenarios, if available, alternate or backup IPv4 Address(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute; and/or

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

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

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

- if the PCF is a V-PCF and has an established policy association, shall determine based on operator policy and requested event triggers of the H-PCF whether to send as the NF service consumer towards the H-PCF a request for the update of the policy association as described in the present clause;
- shall determine the applicable policy based on local policy and for the V-PCF any policy received from the H-PCF in the reply to the possible request for the update of a policy association;
- for the succesfull case shall send a HTTP "200 OK" response with the PolicyUpdate data type as body with possible updates for that applicable policy and Policy Control Request Trigger(s) encoded as described in subclause 4.2.3.3; and
- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7 and according to the following provisions:
  - if the PCF is, due to incomplete, erroneous or missing information in the request not able to provision a UE 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".

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; and
- "UE_POLICY", i.e. a "MANAGE UE POLICY COMPLETE" message or a "MANAGE UE POLICY COMMAND REJECT" message, as defined in Annex D.5 of 3GPP TS 24.501 [15], has been received by the AMF and is being forwarded.

4.2.3.3 Encoding of updated policy

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

- UE policy (see subclause 4.2.2.2) encoded as "uePolicy" 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); or
     b) Change of UE presence in PRA; or
  2) a "NULL" value to request the removal of all previously installed Policy Control Request Trigger(s); and
- if the Policy Control Request Trigger "Change of UE presence in PRA" is provided or if that trigger was already set but the requested presence reporting areas need to be changed, the presence reporting areas for which reporting is required encoded as "pras" attribute encoded as follows:
  a) A new entry shall be added by supplying a new identifier as key and the corresponding PresenceInfo data type instance with complete contents as value as an entry within the map.
  b) An existing entry shall be modified by supplying the existing identifier as key and the PresenceInfo data type instance with complete contents as value as an entry within the map.

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

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

4.2.4 Npcf_UEPolicyControl_UpdateNotify Service Operation

4.2.4.1 General

The H-PCF may decide to update policies or the PCF (H-PCF in the roaming case) may decide to request the termination of the policy association and shall then use an Npcf_UEPolicyControl_UpdateNotify service operation.

The following procedures using the Npcf_UEPolicyControl_UpdateNotify service operation are supported:

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

4.2.4.2 Policy update notification

Figure 4.2.4.2-1 illustrates the policy update notification.

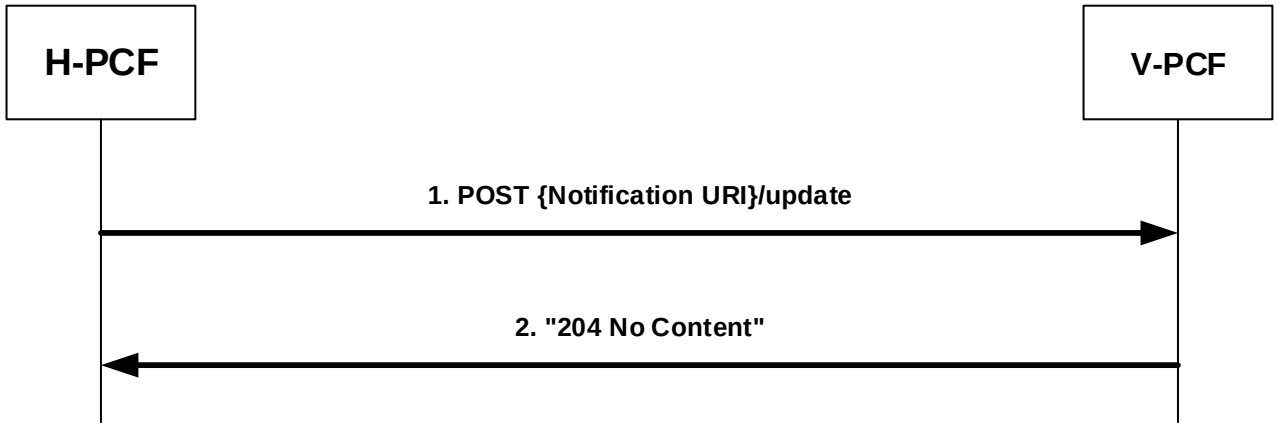


Figure 4.2.4.2-1: policy update notification

The H-PCF may decide to update policies and shall then send an HTTP POST request with "{Notification URI}/update" as URI (where the Notification URI was previously supplied by the V-PCF 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 V-PCF:

- shall use the Namf_Communication Service defined in 3GPP TS 29.519 [17] to send "MANAGE UE POLICY COMMAND" message(s) with the received policy to the UE;
- shall either send a HTTP "204 No Content" response indicating the success of the enforcement or an appropriate failure response, taking into consideration a reply received from the Namf_Communication Service according to the previous bullet; and
- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7.

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.

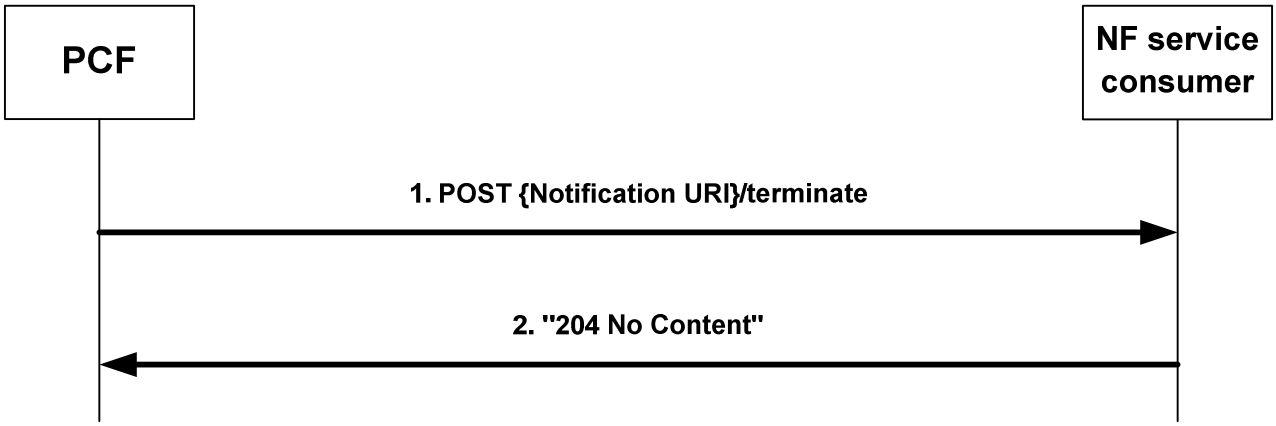


Figure 4.2.4.3-1: request for a termination of theUE policy association

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

- the policy association ID encoded as "polAssoId" attribute; 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:

- if the V-PCF is the NF service consumer, shall send as NF service producer for the corresponding policy association (towards the AMF) a request for a termination of the policy association according to the present clause;
- shall either send a HTTP "204 No Content" responsefor the succesfull processing of the HTTP POST request or an appropriate failure response, for the V-PCF as the NF service consumer taking into consideration a reply received for the possible corresponding policy update notification request according to the previous bullet; and
- if errors occur when processing the HTTP POST request, shall apply error handling procedures as specified in subclause 5.7.

After the succesfull processing of the HTTP POST request, any NF service consumer except for the V-PCF shall invoke the Npcf_UEPolicyControl_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 use this URL as Notification URL in subsequent communication and shall resend the failed request for termination of the policy association to that URL.

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

4.2.5 Npcf_UEPolicyControl_Delete Service Operation

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

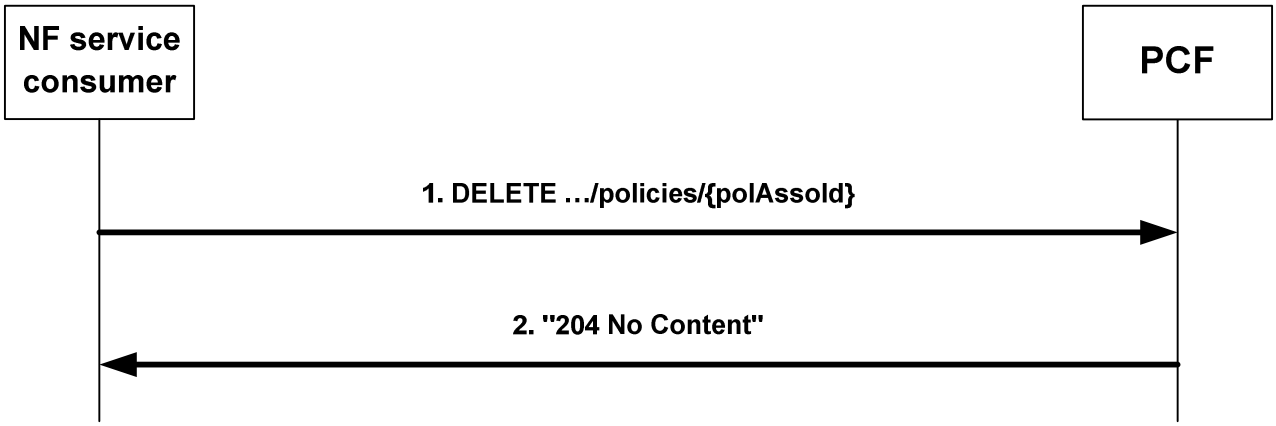


Figure 4.2.5-1: Deletion of a policy association

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

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

- the resource URI of the individual UE Policy Association resource is not transferred to the new AMF; or
- the new AMF informs the old AMF that the individual UE Policy Association resource is not being reused.

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

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

- delete the policy association;
- if the PCF is a V-PCF and has an established corresponding policy association towards the H-PCF, send as the NF service consumer towards the H-PCF a request for the deletion of that policy association as described in the present clause;
- send either an HTTP "204 No Content" response indicating the success of the deletion or an appropriate failure response, for the V-PCF as PCF taking into consideration a reply received for the possible policy association deletion request according to the previous bullet; and
- if errors occur when processing the HTTP DELETE request, apply error handling procedures as specified in subclause 5.7.

5 Npcf_UEPolicyControl API

5.1 Introduction

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

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

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

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [6].
- The {apiName} shall be "npcf-ue-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_UEPolicyControl 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".

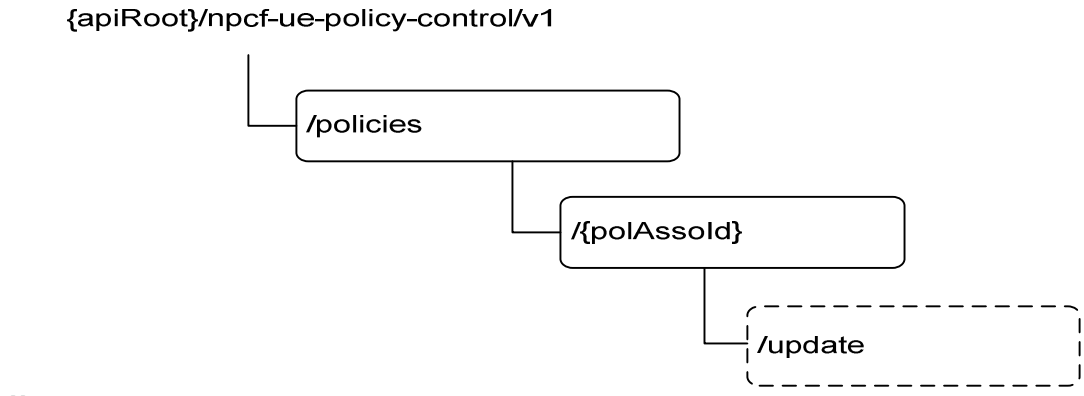
"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [21].

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



x

Figure 5.3.1-1: Resource URI structure of the Npcf_UEPolicyControl 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
UE Policy Associations	{apiRoot}/ npcf-ue-policy-control/ v1/policies/	POST	Create a new Individual UE policy association resource.
Individual UE Policy Association	{apiRoot} /npcf-ue-policy-control/ v1/policies/ {polAssoId}	GET	Read the Individual UE Policy Association resource.
		DELETE	Delete the Individual UE Policy Association resource.
	{apiRoot} /npcf-ue-policy-control/ v1/policies/ {polAssoId}/update	update (POST)	Report observed event trigger and obtain updated UE policies.

5.3.2 Resource:UE Policy Associations

5.3.2.1 Description

This resource represents a collection of UE policy associations.

5.3.2.2 Resource definition

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

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

Table 5.3.2.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See subclause 5.1

5.3.2.3 Resource Standard Methods

5.3.2.3.1 POST

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

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

Name	Data type	P	Cardinality	Description
n/a				

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

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

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

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

Data type	P	Cardinality	Response codes	Description
PolicyAssociation	M	1	201 Created	Policy association was created and policies are being provided.
NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

5.3.3 Resource: Individual UE Policy Association

5.3.3.1 Description

This resource represents an individual UE policy association.

5.3.3.2 Resource definition

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

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

Table 5.3.2.2-1: Resource URI variables for this resource

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

5.3.3.3 Resource Standard Methods

5.3.3.3.1 GET

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

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

Name	Data type	P	Cardinality	Description
n/a				

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

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

Data type	P	Cardinality	Description
n/a			

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

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

5.3.3.3.2 DELETE

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

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

Name	Data type	P	Cardinality	Description
n/a				

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

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

Data type	P	Cardinality	Description
n/a			

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

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

5.3.3.4 Resource Custom Operations

5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

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

5.3.3.4.2 Operation: Update

5.3.3.4.2.1 Description

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

5.3.3.4.2.2 Operation Definition

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

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

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

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

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

5.4 Custom Operations without associated resources

None.

5.5 Notifications

5.5.1 General

Table 5.5.1-1: Notifications

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

5.5.2 Policy Update Notification

5.5.2.1 Description

This notification is used by the H-PCF to provide updates of UE policies to the V-PCF as 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.
NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

5.5.3 Request for termination of the UE policy association

5.5.3.1 Description

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

5.5.3.2 Operation Definition

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

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

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

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

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

5.6 Data Model

5.6.1 General

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

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

Table 5.6.1-1: Npcf_UEPolicyControl specific Data Types

Data type	Section defined	Description	Applicability
PolicyAssociation	5.6.2.2	Description of a policy association that is returned by the PCF when a policy Association is created, updated, or read.	
PolicyAssociationReleaseCause	5.6.3.4	The cause why the PCF requests the termination of the policy association.	
PolicyAssociationRequest	5.6.2.3	Information that NF service consumer provides when requesting the creation of a policy association.	
PolicyAssociationUpdateRequest	5.6.2.4	Information that NF service consumer provides when requesting the update of a policy association.	
PolicyUpdate	5.6.2.5	Updated policies that the PCF provides in a notification or in the reply to an Update Request.	
RequestTrigger	5.6.3.3	Enumeration of possible Request Triggers.	
TerminationNotification	5.6.2.6	Request to terminate a policy Association that the PCF provides in a notification.	
UePolicy	5.6.3.2	UE Policies	
UePolicyDeliveryResult	5.6.3.2	UE Policy delivery Result	
UePolicyRequest	5.6.3.2	Request for UE Policies	

Table 5.6.1-2 specifies data types re-used by the Npcf_UEPolicyControl 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_UEPolicyControl service based interface.

Table 5.6.1-2: Npcf_UEPolicyControl re-used Data Types

Data type	Reference	Comments	Applicability
AccessType	3GPP TS 29.571 [11]		
Gpsi	3GPP TS 29.571 [11]	Generic Public Subscription Identifier	
GroupId	3GPP TS 29.571 [11]		
Guami	3GPP TS 29.571 [11]	Globally Unique AMF Identifier	
Ipv4Addr	3GPP TS 29.571 [11]		
Ipv6Addr	3GPP TS 29.571 [11]		
NetworkId	3GPP TS 29.571 [11]		
Pei	3GPP TS 29.571 [11]	Permanent Equipment Identifier	
PresenceInfo	3GPP TS 29.571 [11]	Presence reporting area information	
ProblemDetails	3GPP TS 29.571 [11]		
Uri	3GPP TS 29.571 [11]		
UserLocation	3GPP TS 29.571 [11]		
RatType	3GPP TS 29.571 [11]		
Supi	3GPP TS 29.571 [11]	Subscription Permanent Identifier	
SupportedFeatures	3GPP TS 29.571 [11]	Used to negotiate the applicability of the optional features defined in table 5.8-1.	
TimeZone	3GPP TS 29.571 [11]		

5.6.2 Structured data types

5.6.2.1 Introduction

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

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	
uePolicy	UePolicy	O	0..1	The UE policy as determined by the PCF.	
triggers	array(RequestTrigger)	O	1..N	Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH" are permitted.	
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 praStatus attribute within the PresenceInfo data type shall not be supplied.	
suppFeat	SupportedFeatures	M	1	Indicates the negotiated supported features.	

5.6.2.3 Type PolicyAssociationRequest

Table 5.6.2.3-1: Definition of type PolicyAssociationRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	M	1	Identifies the recipient of Notifications sent by the PCF.	
altNotifIpv4Addrs	array(Ipv4Addr)	O	1..N	Alternate or backup IPv4 Addess(es) where to send Notifications.	
altNotifIpv6Addrs	array(Ipv6Addr)	O	1..N	Alternate or backup IPv6 Addess(es) where to send Notifications.	
supi	Supi	C	0..1	Subscription Permanent Identifier. Shall be provided when available.	
gpsi	Gpsi	C	0..1	Generic Public Subscription Identifier. Shall be provided when available.	
accessType	AccessType	C	0..1	The Access Type where the served UE is camping. Shall be provided when available.	
pei	Pei	C	0..1	The Permanent Equipment Identifier of the served UE. Shall be provided when available.	
userLoc	UserLocation	C	0..1	The location of the served UE. Shall be provided when available.	
timeZone	TimeZone	C	0..1	The time zone where the served UE is camping. Shall be provided when available.	
servingPlmn	NetworkId	C	0..1	The serving PLMN where the served UE is camping. Shall be provided when available.	
ratType	RatType	C	0..1	The RAT Type where the served UE is camping. Shall be provided when available.	
groupId	GroupId	C	0..1	Internal Group Identifier of the served UE. Shall be provided when available.	
hPcfId	string	C	0..1	H-PCF Identifier. Shall be provided when available.	
uePolReq	UePolicyRequest	C	0..1	A request for UE Policies. Shall be provided when the AMF receives an "UPSI LIST TRANSPORT" message, as defined in Annex D.5.4 of 3GPP TS 24.501 [15] .	
guami	Guami	C	0..1	The Globally Unique AMF Identifier (GUAMI) shall be provided by an AMF as service consumer.	
serviceName	string	O	0..1	If the NF service consumer is an AMF, it should provide the name of a service produced by the AMF that makes use of information received within the Npcf_UEPolicyControl_UpdateNotify service operation.	
suppFeat	SupportedFeatures	M	1	Indicates the features supported by the service consumer.	

5.6.2.4 Type PolicyAssociationUpdateRequest

Table 5.6.2.4-1: Definition of type PolicyAssociationUpdateRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	O	0..1	Identifies the recipient of Notifications sent by the PCF.	
altNotifIpv4Addrs	array(Ipv4Addr)	O	1..N	Alternate or backup IPv4 Address(es) where to send Notifications.	
altNotifIpv6Addrs	array(Ipv6Addr)	O	1..N	Alternate or backup IPv6 Address(es) where to send Notifications.	
triggers	array(RequestTrigger)	C	1..N	Request Triggers that the NF service consumer observes.	
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 praStatus attribute within the PresenceInfo data type shall be supplied.	
userLoc	UserLocation	C	0..1	The location of the served UE shall be provided for trigger "LOC_CH".	
uePolDelResult	UePolicyDeliveryResult	C	0..1	UE Policy Delivery Result. Shall be provided together with trigger "UE_POLICY" when a "MANAGE UE POLICY COMPLETE" message or a "MANAGE UE POLICY COMMAND REJECT" message, as defined in Annex D.5 of 3GPP TS 24.501 [15], has been received by the AMF and is being forwarded .	

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	C	0..1	The resource URI of the individual UE policy association related to the notification. Shall be included when policy is supplied as part of the Npcf_UEPolicyControl_UpdateNotify Service Operation.	
uePolicy	UePolicy	O	0..1	The UE policy as determined by the PCF.	
triggers	array(RequestTrigger)	O	1..N	Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH" are permitted.	
pras	map(PresenceInfo)	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 presenceStatus attribute within the PresenceInfo data type shall not be supplied.	

5.6.2.6 Type TerminationNotification

Table 5.6.2.6-1: Definition of type TerminationNotification

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

5.6.3 Simple data types and enumerations

5.6.3.1 Introduction

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

5.6.3.2 Simple data types

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

Table 5.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
UePolicy	Bytes	"MANAGE UE POLICY COMMAND" message content, as defined in Table D.5.1.1.1 of 3GPP TS 24.501 [15]	
UePolicyDeliveryResult	Bytes	"MANAGE UE POLICY COMPLETE" message content, as defined in Table D.5.2.1.1 of 3GPP TS 24.501 [15], or "MANAGE UE POLICY COMMAND REJECT" message content, as defined in Table D.5.3.1.1 of 3GPP TS 24.501 [15]	
UePolicyRequest	Bytes	"UPSI LIST TRANSPORT" message content, as defined in Table D.5.4.1.1 of 3GPP TS 24.501 [15]	

5.6.3.3 Enumeration: RequestTrigger

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

Table 5.6.3.3-1: Enumeration RequestTrigger

Enumeration value	Description	Applicability
LOC_CH	Location change (tracking area): the tracking area of the UE has changed.	
PRA_CH	Change of UE presence in PRA: the UE is entering/leaving a Presence Reporting Area.	
UE_POLICY	A "MANAGE UE POLICY COMPLETE" message or a "MANAGE UE POLICY COMMAND REJECT" message, as defined in Annex D.5 of 3GPP TS 24.501 [15], has been received by the AMF and is being forwarded.	

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_UEPolicyControl API, HTTP error responses shall be supported as specified in subclause 4.8 of 3GPP TS 29.501 [6]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [5] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [5].

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

5.7.2 Protocol Errors

No specific protocol errorsfor the Npcf_UEPolicyControl API are specified.

5.7.3 Application Errors

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

Table 5.7.3-1: Application errors

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

5.8 Feature negotiation

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

Table 5.8-1: Supported Features

Feature number	Feature Name	Description

5.9 Security

As indicated in 3GPP TS 33.501 [19] and 3GPP TS 29.500 [5], the access to the Npcf_UEPolicyControl 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_UEPolicyControl 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_UEPolicyControl service.

The Npcf_UEPolicyControl API defines a single scope "npcf-ue-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_UEPolicyControl API.

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

A.2 Npcf_UEPolicyControl API

```
openapi: 3.0.0
info:
  description: UE Policy Control Service API
  version: "1.0.0"
  title: Npcf_UEPolicyControl
externalDocs:
  description: 3GPP TS 29.525 V15.0.0; 5G System; UE Policy Control Service.
  url: 'http://www.3gpp.org/ftp/Specs/archive/29_series/29.525/'
servers:
  - url: '{apiRoot}/npcf-ue-policy-control/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in subclause subclause 4.4 of 3GPP TS 29.501
security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-ue-policy-control
paths:
  /policies:
    post:
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PolicyAssociationRequest'
      responses:
        '201':
          description: Created
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PolicyAssociation'
          headers:
            Location:
              description: 'Contains the URI of the newly created resource, according to the
structure: {apiRoot}/npcf-ue-policy-control/v1/policies/{polAssoId}'
              required: true
              schema:
                type: string
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
```

```
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
    callbacks:
      policyUpdateNotification:
        '{$request.body#/notificationUri}/update':
          post:
            requestBody:
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/PolicyUpdate'
            responses:
              '204':
                description: No Content, Notification was succesfull
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29571_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29571_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      policyAssocitionTerminationRequestNotification:
        '{$request.body#/notificationUri}/terminate':
          post:
            requestBody:
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/TerminationNotification'
            responses:
              '204':
                description: No Content, Notification was succesfull
              '307':
                description: temporary redirect
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29571_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29571_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /policies/{polAssoId}:
    get:
```

```
    parameters:
      - name: polAssoId
        in: path
        description: Identifier of a policy association
        required: true
        schema:
          type: string
    responses:
      '200':
        description: OK. Resource representation is returned
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PolicyAssociation'
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29571_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29571_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'
      '406':
        $ref: 'TS29571_CommonData.yaml#/components/responses/406'
      '429':
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  delete:
    parameters:
      - name: polAssoId
        in: path
        description: Identifier of a policy association
        required: true
        schema:
          type: string
    responses:
      '204':
        description: No Content. Resource was succesfully deleted
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29571_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29571_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'
      '429':
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
/policies/{polAssoId}/update:
  post:
    requestBody:
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/PolicyAssociationUpdateRequest'
    parameters:
      - name: polAssoId
        in: path
        description: Identifier of a policy association
        required: true
        schema:
          type: string
    responses:
      '200':
        description: OK. Updated policies are returned
        content:
```

```
            application/json:
              schema:
                $ref: '#/components/schemas/PolicyUpdate'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            npcf-ue-policy-control: Access to the Npcf_AMPolicyControl API
  schemas:
    PolicyAssociation:
      type: object
      properties:
        request:
          $ref: '#/components/schemas/PolicyAssociationRequest'
        uePolicy:
          $ref: '#/components/schemas/UePolicy'
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 1
          description: Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH"
are permitted.
        pras:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - suppFeat
    PolicyAssociationRequest:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        altNotifIpv4Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
          minItems: 1
          description: Alternate or backup IPv4 Address(es) where to send Notifications.
        altNotifIpv6Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
          minItems: 1
          description: Alternate or backup IPv6 Address(es) where to send Notifications.
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        gpsi:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        userLoc:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        timeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        servingPlmn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        groupId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
        hPcfId:
          type: string
          description: H-PCF Identifier. Shall be provided when available.
        uePolReq:
          $ref: '#/components/schemas/UePolicyRequest'
        guami:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Guami'
        serviveName:
          type: string
          description: If the NF service consumer is an AMF, it should provide the name of a service
produced by the AMF that makes use of information received within the
Npcf_UEPolicyControl_UpdateNotify service operation.
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - notificationUri
        - suppFeat
    PolicyAssociationUpdateRequest:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        altNotifIpv4Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
          minItems: 1
          description: Alternate or backup IPv4 Address(es) where to send Notifications.
        altNotifIpv6Addrs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
          minItems: 1
          description: Alternate or backup IPv6 Address(es) where to send Notifications.
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 1
          description: Request Triggers that the NF service consumer observes.
        praStatuses:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          description: Map of PRA status information.
          minProperties: 1
        userLoc:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        uePolDelResult:
          $ref: '#/components/schemas/UePolicyDeliveryResult'
    PolicyUpdate:
      type: object
      properties:
        resourceUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        uePolicy:
          $ref: '#/components/schemas/UePolicy'
        triggers:
          type: array
          items:
            $ref: '#/components/schemas/RequestTrigger'
          minItems: 1
          nullable: true
```

```
          description: Request Triggers that the PCF subscribes. Only values "LOC_CH" and "PRA_CH"
are permitted.
        pras:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          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
    UePolicy:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'
    UePolicyDeliveryResult:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'
    UePolicyRequest:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Bytes'
    RequestTrigger:
      anyOf:
      - type: string
        enum:
          - LOC_CH
          - PRA_CH
          - UE_POLICY
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - LOC_CH: Location change (tracking area). The tracking area of the UE has changed.
        - PRA_CH: Change of UE presence in PRA. The UE is entering/leaving a Presence Reporting
Area.
        - UE_POLICY: A MANAGE UE POLICY COMPLETE message or a MANAGE UE POLICY COMMAND REJECT
message, as defined in Annex D.5 of 3GPP TS 24.501, has been received by the AMF and is being
forwarded.
    PolicyAssociationReleaseCause:
      anyOf:
      - type: string
        enum:
          - UNSPECIFIED
          - UE_SUBSCRIPTION
          - INSUFFICIENT_RES
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - UNSPECIFIED: This value is used for unspecified reasons.
        - UE_SUBSCRIPTION: This value is used to indicate that the session needs to be terminated
because the subscription of UE has changed (e.g. was removed).
        - INSUFFICIENT_RES: This value is used to indicate that the server is overloaded and needs
to abort the session.
```

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New**
2018-10	CT3#98-Bis	C3-186282				First TS version created based on suitable parts of TS 29.507v15.1.0	0.1.0
2018-12	CT3#99	C3-187094				API Version	0.2.0
2018-12	CT3#99	C3-187532				ExternalDocs OpenAPI field	0.2.0
2018-12	CT3#99	C3-187096				Location header field in OpenAPI	0.2.0
2018-12	CT3#99	C3-187533				Security	0.2.0
2018-12	CT3#99	C3-187098				supported content types	0.2.0
2018-12	CT3#99	C3-187534				HTTP Error responses	0.2.0
2018-12	CT3#99	C3-187673				Alternate IP address in Npcf_UEPolicyControl_Update	0.2.0
2018-12	CT3#99	C3-187673				Corrections on Protocol and Application errors	0.2.0
2018-12	CP#82	CP-183130				TS sent to plenary for information and approval	1.0.0
2018-12	CP#82	CP-183175				PCR 29.xyz Corrections of Cardinality in OpenAPI	1.1.0
2018-12	CP#82	CP-183250				TS number assigned for approval at plenary	1.1.0
2018-12	CP#82	CP-183252				TS approved by plenary	15.0.0

History

Document history		
V15.0.0	April 2019	Publication