

ETSI TS 129 514 V15.17.0 (2026-03)



TECHNICAL SPECIFICATION

**5G;
5G System;
Policy Authorization Service;
Stage 3
(3GPP TS 29.514 version 15.17.0 Release 15)**

Sample Document



Reference

RTS/TSGC-0329514vfh0

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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 at [3GPP to ETSI numbering cross-referencing](#).

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

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	7
1 Scope	8
2 References	8
3 Definitions and abbreviations.....	9
3.1 Definitions	9
3.2 Abbreviations	9
4 Npcf_PolicyAuthorization Service.....	10
4.1 Service Description	10
4.1.1 Overview	10
4.1.2 Service Architecture	10
4.1.3 Network Functions.....	11
4.1.3.1 Policy Control Function (PCF)	11
4.1.3.2 NF Service Consumers.....	11
4.2 Service Operations	12
4.2.1 Introduction.....	12
4.2.2 Npcf_PolicyAuthorization_Create service operation.....	12
4.2.2.1 General.....	12
4.2.2.2 Initial provisioning of service information.....	13
4.2.2.3 Gate control.....	16
4.2.2.4 Initial Background Data Transfer policy indication.....	16
4.2.2.5 Initial provisioning of sponsored connectivity information	16
4.2.2.6 Subscriptions to Service Data Flow QoS notification control	17
4.2.2.7 Subscription to Service Data Flow Deactivation.....	17
4.2.2.8 Initial provisioning of traffic routing information.....	18
4.2.2.9 Void.....	19
4.2.2.10 Subscription to resources allocation outcome	19
4.2.2.11 Void.....	19
4.2.2.12 Invocation of Multimedia Priority Services	19
4.2.2.13 Support of content versioning	20
4.2.3 Npcf_PolicyAuthorization_Update service operation	20
4.2.3.1 General	20
4.2.3.2 Modification of service information.....	20
4.2.3.3 Gate control.....	22
4.2.3.4 Background Data Transfer policy indication at policy authorization update	23
4.2.3.5 Modification of sponsored connectivity information	23
4.2.3.6 Modification of Subscription to Service Data Flow QoS notification control	24
4.2.3.7 Modification of Subscription to Service Data Flow Deactivation.....	24
4.2.3.8 Update of traffic routing information.....	25
4.2.3.9 Void.....	25
4.2.3.10 Modification of subscription to resources allocation outcome.....	25
4.2.3.11 Void.....	25
4.2.3.12 Modification of Multimedia Priority Services	25
4.2.3.13 Support of content versioning	26
4.2.4 Npcf_PolicyAuthorization_Delete service operation	26
4.2.4.1 General	26
4.2.4.2 AF application session context termination	26
4.2.4.3 Reporting usage for sponsored data connectivity.....	27
4.2.4.4 Void.....	27
4.2.4.5 Termination of Multimedia Priority Services	27
4.2.5 Npcf_PolicyAuthorization_Notify service operation	28
4.2.5.1 General	28

4.2.5.2	Notification about application session context event	28
4.2.5.3	Notification about application session context termination	29
4.2.5.4	Notification about Service Data Flow QoS notification control	30
4.2.5.5	Notification about Service Data Flow Deactivation.....	30
4.2.5.6	Reporting usage for sponsored data connectivity.....	31
4.2.5.7	Void.....	31
4.2.5.8	Notification about resources allocation outcome	31
4.2.5.9	Void.....	32
4.2.6	Npcf_PolicyAuthorization_Subscribe service operation	32
4.2.6.1	General	32
4.2.6.2	Handling of subscription to events for the existing application session context	32
4.2.6.3	Initial subscription to events without provisioning of service information	34
4.2.6.4	Subscription to usage monitoring of sponsored data connectivity	35
4.2.6.5	Void.....	36
4.2.7	Npcf_PolicyAuthorization_Unsubscribe service operation	36
4.2.7.1	General	36
4.2.7.2	Unsubscription to events	36
5	Npcf_PolicyAuthorization Service API	37
5.1	Introduction	37
5.2	Usage of HTTP.....	37
5.2.1	General.....	37
5.2.2	HTTP standard headers.....	37
5.2.2.1	General	37
5.2.2.2	Content type	37
5.2.3	HTTP custom headers.....	37
5.3	Resources	38
5.3.1	Resource Structure	38
5.3.2	Resource: Application Sessions (Collection).....	39
5.3.2.1	Description.....	39
5.3.2.2	Resource definition	39
5.3.2.3	Resource Standard Methods.....	39
5.3.2.3.1	POST	39
5.3.2.4	Resource Custom Operations	40
5.3.3	Resource: Individual Application Session Context (Document)	40
5.3.3.1	Description	40
5.3.3.2	Resource definition	40
5.3.3.3	Resource Standard Methods.....	40
5.3.3.3.1	GET	40
5.3.3.3.2	PATCH.....	40
5.3.3.4	Resource Custom Operations	41
5.3.3.4.1	Overview	41
5.3.3.4.2	Operation: delete	41
5.3.4	Resource: Events Subscription (Document)	42
5.3.4.1	Description	42
5.3.4.2	Resource definition	42
5.3.4.3	Resource Standard Methods.....	42
5.3.4.3.1	PUT	42
5.3.4.3.2	DELETE.....	43
5.3.4.4	Resource Custom Operations	44
5.4	Custom Operations without associated resources.....	44
5.5	Notifications	44
5.5.1	General.....	44
5.5.2	Event Notification.....	44
5.5.2.1	Description	44
5.5.2.2	Target URI	44
5.5.2.3	Standard Methods	44
5.5.2.3.1	POST	44
5.5.3	Termination Request.....	45
5.5.3.1	Description	45
5.5.3.2	Target URI	45
5.5.3.3	Standard Methods	45

5.5.3.3.1	POST	45
5.6	Data Model	46
5.6.1	General	46
5.6.2	Structured data types	50
5.6.2.1	Introduction	50
5.6.2.2	Type AppSessionContext	51
5.6.2.3	Type AppSessionContextReqData	52
5.6.2.4	Type AppSessionContextRespData	53
5.6.2.5	Type AppSessionContextUpdateData	53
5.6.2.6	Type EventsSubscReqData	53
5.6.2.7	Type MediaComponent	54
5.6.2.8	Type MediaSubComponent	55
5.6.2.9	Type EventsNotification	55
5.6.2.10	Type AfEventSubscription	56
5.6.2.11	Type AfEventNotification	56
5.6.2.12	Type TerminationInfo	56
5.6.2.13	Type AfRoutingRequirement	56
5.6.2.14	Type ResourcesAllocationInfo	57
5.6.2.15	Type QosNotificationControlInfo	57
5.6.2.16	Type SpatialValidity	57
5.6.2.17	Type EthFlowDescription	58
5.6.2.18	Void	59
5.6.2.19	Void	59
5.6.2.20	Type AnGwAddress	59
5.6.2.21	Type Flows	59
5.6.2.22	Type TemporalValidity	59
5.6.2.23	Void	59
5.6.2.24	Type AfRoutingRequirementRm	59
5.6.2.25	Type EventsSubscReqDataRm	60
5.6.2.26	Type MediaComponentRm	60
5.6.2.27	Type MediaSubComponentRm	61
5.6.2.28	Type SpatialValidityRm	62
5.6.2.29	Void	62
5.6.2.30	Void	62
5.6.2.31	Void	62
5.6.2.32	Void	62
5.6.2.33	Void	62
5.6.2.34	Void	62
5.6.2.35	Void	62
5.6.2.36	Void	62
5.6.2.37	Void	62
5.6.2.38	Void	62
5.6.2.39	Void	62
5.6.2.40	Void	62
5.6.2.41	Void	62
5.6.2.42	Type EventsSubscPutData	62
5.6.2.43	Type AppSessionContextUpdateDataPatch	63
5.6.3	Simple data types and enumerations	63
5.6.3.1	Introduction	63
5.6.3.2	Simple data types	63
5.6.3.3	Enumeration: MediaType	63
5.6.3.4	Enumeration: ReservPriority	64
5.6.3.5	Enumeration: ServAuthInfo	64
5.6.3.6	Enumeration: SponsoringStatus	64
5.6.3.7	Enumeration: AfEvent	65
5.6.3.8	Enumeration: AfNotifMethod	65
5.6.3.9	Enumeration: QosNotifType	65
5.6.3.10	Enumeration: TerminationCause	65
5.6.3.11	Void	66
5.6.3.12	Enumeration: FlowStatus	66
5.6.3.13	Enumeration: MediaComponentResourcesStatus	66
5.6.3.14	Enumeration: FlowUsage	66

5.7	Error handling	67
5.7.1	General.....	67
5.7.2	Protocol Errors.....	67
5.7.3	Application Errors	67
5.8	Feature negotiation	67
5.9	Security	68
Annex A (normative): OpenAPI specification		69
A.1	General	69
A.2	Npcf_PolicyAuthorization API	69
Annex B (informative): Change history		85
History		89

Sample Document

get full document from standards.iteh.ai

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.

Sample Document

get full document from standards.iteh.ai

1 Scope

The present specification provides the stage 3 definition of the Policy Authorization Service of the 5G System.

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The stage 2 definition and related procedures for the Npcf Policy Authorization Service are specified in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

The 5G System 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 are specified in 3GPP TS 29.500 [5] and 3GPP TS 29.501 [6].

The Policy Authorization Service is provided by the Policy Control Function (PCF). This service creates policies as requested by the authorised AF for the PDU Session to which the AF session is bound.

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] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".
- [9] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".
- [10] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".
- [11] OpenAPI: "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.
- [12] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".
- [13] 3GPP TS 29.508: "5G System; Session Management Event Exposure Service; Stage 3".
- [14] 3GPP TS 29.554: "5G System; Background Data Transfer Policy Control Service; Stage 3".
- [15] 3GPP TS 29.122: "T8 reference point for Northbound APIs".
- [16] IEEE 802.3-2015: "IEEE Standard for Ethernet".
- [17] IEEE 802.1Q-2014: "Bridges and Bridged Networks".

- [18] IETF RFC 7042: "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters".
- [19] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".
- [20] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".
- [21] IETF RFC 7396: "JSON Merge Patch".
- [22] Void.
- [23] 3GPP TS 22.153: "5G System; "Multimedia Priority Service".
- [24] IETF RFC 7807: "Problem Details for HTTP APIs".
- [25] 3GPP TS 33.501: "Security architecture and procedures for 5G system".
- [26] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".
- [27] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".
- [28] 3GPP TR 21.900: "Technical Specification Group working methods".
- [29] IETF RFC 6733: "Diameter Base Protocol".
- [30] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification".

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].

Application Function (AF): Element offering application(s) that use PDU session resources.

AF application session context: Application level session context established by an application level signalling protocol offered by the AF that requires a session context set-up with explicit session context description before the use of the service.

MPS session: A session for which priority treatment is applied for allocating and maintaining radio and network resources to support the Multimedia Priority Service (MPS). MPS is defined in 3GPP TS 22.153 [23].

PCC rule: Set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control.

Service information: Set of information conveyed from the AF/NEF to the PCF by the Npcf_PolicyAuthorization service to be used as a basis for PCC decisions at the PCF, including information about the AF/NEF application session context (e.g. application identifier, type of media, bandwidth, IP address and port number).

Service data flow: An aggregate set of packet flows.

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].

AF	Application Function
DEI	Drop Eligible Indicator
DNAI	DN Access Identifier

DNN	Data Network Name
E-UTRA	Evolved Universal Terrestrial Radio Access
H-PCF	PCF in the HPLMN
JSON	JavaScript Object Notation
MPS	Multimedia Priority Service
NEF	Network Exposure Function
NR	New Radio
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
PCC	Policy and Charging Control
PCF	Policy Control Function
PCP	Priority Code Point
PRA	Presence Reporting Area
QoS	Quality of Service
RFSP	RAT Frequency Selection Priority
RTCP	Real Time Control Protocol
SDF	Service Data Flow
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SUPI	Subscription Permanent Identifier
UDR	Unified Data Repository
UPF	User Plane Function
URSP	UE Route Selection Policy
VID	VLAN Identifier
VLAN	Virtual Local Area Network
V-PCF	PCF in the VPLMN

4 Npcf_PolicyAuthorization Service

4.1 Service Description

4.1.1 Overview

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

The Npcf_PolicyAuthorization service authorises an AF request and creates policies as requested by the authorised NF service consumer for the PDU session to which the AF session is bound to. This service allows the NF service consumer to subscribe/unsubscribe to the notification of events (e.g. Access Type and RAT type, PLMN identifier, usage report).

4.1.2 Service Architecture

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The Policy and Charging control related 5G architecture is also described in 3GPP TS 23.503 [4] and 3GPP TS 29.513 [7].

The only known NF service consumers of the Npcf_PolicyAuthorization service are the Application Function (AF) and the Network Exposure Function (NEF).

The Npcf_PolicyAuthorization service is provided by the PCF and consumed by the AF and the NEF, as shown in figure 4.1.2-1 for the SBI representation model and in figure 4.1.2-2 for the reference point representation model.

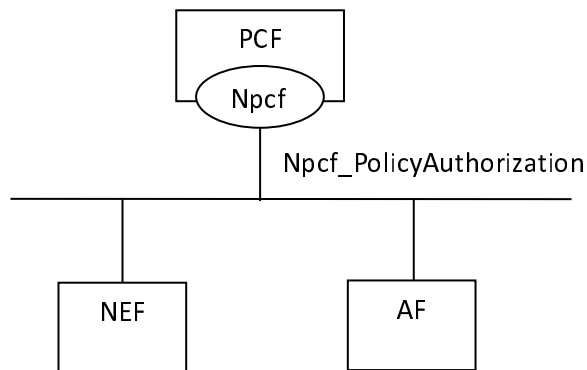


Figure 4.1.2-1: Npcf_PolicyAuthorization service Architecture, SBI representation

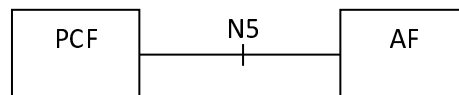


Figure 4.1.2-2: Npcf_PolicyAuthorization service Architecture, reference point representation

The NEF can act as an AF using N5 reference point.

4.1.3 Network Functions

4.1.3.1 Policy Control Function (PCF)

The PCF (Policy Control Function) is a functional element that encompasses policy control decision and flow based charging control functionalities, access and mobility policy decisions for the control of the UE Service Area Restrictions and RAT/RFSP control, and UE Policy for the Access network discovery and selection policy and UE Route Selection Policy (URSP).

The policy control decision and flow based charging control functionalities enable the PCF to provide network control regarding the service data flow detection, gating, QoS and flow based charging (except credit management) towards the SMF/UPF.

The PCF receives session and media related information from the Npcf_PolicyAuthorization service consumers and notifies them of subscribed traffic plane events.

The PCF checks that the service information provided by the NF service consumer is consistent with the operator defined policy rules before storing the service information.

The PCF uses the received service information and the subscription information when it applies as basis for the policy and charging control decisions.

The PCF derives PCC rules and provisions them to the SMF via the Npcf_SMPolicyControl service and subscribes to traffic plane events via policy control request triggers as described in 3GPP TS 29.512 [8].

4.1.3.2 NF Service Consumers

The known NF service consumers are the AF and the NEF, as defined in 3GPP TS 23.502 [3].

The AF is an element offering applications that require the Policy and Charging Control of traffic plane resources. The AF uses the Npcf_PolicyAuthorization service to provide service information to the PCF.

The AFs can be deployed by the same operator offering the access services or can be provided by external third-party service provider. If the AF is not allowed by the operator to access directly the PCF, the AF uses the external exposure framework via NEF to interact with the PCF, as described in subclause 5.20 of 3GPP TS 23.501 [2].

The Network Exposure Function (NEF) supports external exposure of capabilities of network functions.

4.2 Service Operations

4.2.1 Introduction

Service operations defined for the Npcf_PolicyAuthorization Service are shown in table 4.2.1-1.

Table 4.2.1-1: Npcf_PolicyAuthorization Service Operations

Service Operation Name	Description	Initiated by
Npcf_PolicyAuthorization_Create	Determines and installs the policy according to the service information provided by an authorized NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Update	Determines and updates the policy according to the modified service information provided by an authorized NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Delete	Provides means to delete the application session context of the NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Notify	Notifies NF service consumer of the subscribed events.	PCF
Npcf_PolicyAuthorization_Subscribe	Allows NF service consumers to subscribe to the notification of events.	AF, NEF
Npcf_PolicyAuthorization_Unsubscribe	Allows NF service consumers to unsubscribe to the notification of events.	AF, NEF

NOTE: The NEF and the AF use the Npcf_PolicyAuthorization service in the same way. To improve the readability of the service procedures, only the AF is mentioned in the following subclauses.

4.2.2 Npcf_PolicyAuthorization_Create service operation

4.2.2.1 General

The Npcf_PolicyAuthorization_Create service operation authorizes the request from the NF service consumer, and optionally communicates with Npcf_SMPolicyControl service to determine and install the policy according to the information provided by the NF service consumer.

The Npcf_PolicyAuthorization_Create service operation creates an application session context in the PCF.

The following procedures using the Npcf_PolicyAuthorization_Create service operation are supported:

- Initial provisioning of service information.
- Gate control.
- Initial Background Data Transfer policy indication.
- Initial provisioning of sponsored connectivity information.
- Subscription to Service Data Flow QoS notification control.
- Subscription to Service Data Flow Deactivation.
- Initial provisioning of traffic routing information.

- Subscription to resources allocation outcome.
- Invocation of Multimedia Priority Services.
- Support of content versioning.

4.2.2.2 Initial provisioning of service information

This procedure is used to set up an AF application session context for the service as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.2.2-1 illustrates the initial provisioning of service information.

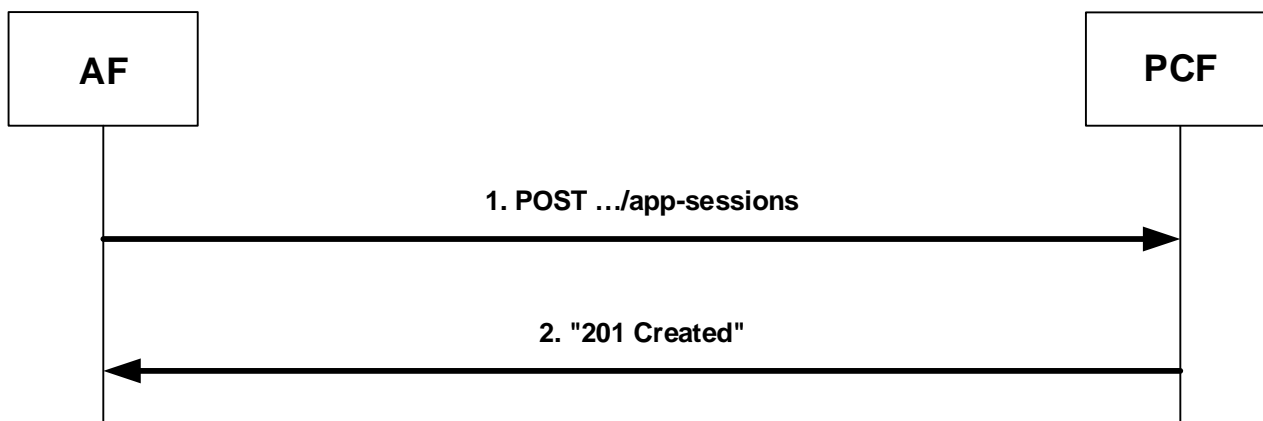


Figure 4.2.2.2-1: Initial provisioning of service information

When a new AF application session context is being established and media information for this application session context is available at the AF and the related media requires PCC control, the AF shall invoke the `Npcf_PolicyAuthorization_Create` service operation by sending the HTTP POST request to the resource URI representing the "Application Sessions" collection resource of the PCF, as shown in figure 4.2.2.2-1, step 1.

The AF shall include in the "AppSessionContext" data type in the payload body of the HTTP POST request a partial representation of the "Individual Application Session Context" resource by providing the "AppSessionContextReqData" data type. The "Individual Application Session Context" resource and the "Events Subscription" sub-resource are created as described below.

The AF shall provide in the body of the HTTP POST request:

- for IP type PDU sessions, the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute; and
- for Ethernet type PDU sessions, the MAC address of the UE in the "ueMac" attribute.

The AF shall provide the corresponding service information in the "medComponents" attribute if available. The AF shall indicate to the PCF as part of the "medComponents" attribute whether the service data flow(s) (IP or Ethernet) should be enabled or disabled with the "fStatus" attribute.

The AF may include the AF application identifier in the "afAppId" attribute into the body of the HTTP POST request in order to indicate the particular service that the AF session belongs to.

The AF application identifier may be provided at both "AppSessionContextReqData" data type level, and "MediaComponent" data type level. When provided at both levels, the AF application identifier provided at "MediaComponent" data type level shall have precedence.

The AF application identifier at the "AppSessionContextReqData" data type level may be used to trigger the PCF to indicate to the SMF/UPF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.512 [8].

The AF may also include the "evSubsc" attribute of "EventsSubscReqData" data type to request the notification of certain user plane events. The AF shall include the events to subscribe to in the "events" attribute, and the notification

URI where to address the Npcf_PolicyAuthorization_Notify service operation in the "notifUri" attribute. The events subscription is provisioned in the "Events Subscription" sub-resource.

The AF shall also include the "notifUri" attribute in the "AppSessionContextReqData" data type to indicate the URI where the PCF can request to the AF the deletion of the "Individual Application Session Context" resource.

If the PCF cannot successfully fulfil the received HTTP POST request due to the internal PCF error or due to the error in the HTTP POST request, the PCF shall send the HTTP error response as specified in subclause 5.7.

Otherwise, when the PCF receives the HTTP POST request from the AF, the PCF shall apply session binding as described in 3GPP TS 29.513 [7]. To allow the PCF to identify the PDU session for which the HTTP POST request applies, the AF shall provide in the body of the HTTP POST request:

- for IP type PDU session, either the "ueIpv4" attribute or "ueIpv6" attribute containing the IPv4 or the IPv6 address applicable to an IP flow or IP flows towards the UE; and
- for Ethernet type PDU session, the "ueMac" attribute containing the UE MAC address applicable to an Ethernet flow or Ethernet flows towards the UE.

The AF may provide DNN in the "dnn" attribute, SUPI in the "supi" attribute, GPSI in the "gpsi" attribute, the S-NSSAI in the "sliceInfo" attribute if available for session binding. The AF may also provide the domain identity in the "ipDomain" attribute.

NOTE 1: The "ipDomain" attribute is helpful in the following scenario: Within a network slice instance, there are several separate IP address domains, with SMF/UPF(s) that allocate IPv4 IP addresses out of the same private address range to UE PDU Sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPF(s) in different address domains. If one PCF controls several SMF/UPF(s) in different IP address domains, the UE IP address is thus not sufficient for the session binding. An AF can serve UEs in different IP address domains, either by having direct IP interfaces to those domains, or by having interconnections via NATs in the user plane between the UPF and the AF. If a NAT is used, the AF obtains the IP address allocated to the UE PDU session via application level signalling and supplies it for the session binding to the PCF in the "ueIpv4" attribute. The AF supplies an "ipDomain" attribute denoting the IP address domain behind the NAT in addition. The AF can derive the appropriate value from the source address (allocated by the NAT) of incoming user plane packets. The value provided in the "ipDomain" attribute is operator configurable.

NOTE 2: The "sliceInfo" attribute is helpful in the scenario where multiple network slice instances are deployed in the same DNN, and the same IPv4 address may be allocated to UE PDU sessions in different network slice instances. If one PCF controls several network slices, the UE IP address is not sufficient for the session binding. The AF supplies "sliceInfo" attribute denoting the network slice instance that allocated the IPv4 address of the UE PDU session. How the AF derives S-NSSAI is out of the scope of this specification.

If the PCF fails in executing session binding, the PCF shall reject the Npcf_PolicyAuthorization_Create service operation with an HTTP "500 Internal Server Error" response including the "cause" attribute set to "PDU_SESSION_NOT_AVAILABLE".

If the request contains the "medComponents" attribute the PCF shall store the received service information. The PCF shall process the received service information according to the operator policy and may decide whether the request is accepted or not. The PCF may take the priority information within the "resPrio" attribute into account when making this decision.

If the service information provided in the body of the HTTP POST request is rejected (e.g. the subscribed guaranteed bandwidth for a particular user is exceeded), the PCF shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED". If the service information provided in the HTTP POST request is rejected due to a temporary condition in the network (e.g. the NWDAF reported the network slice selected for the PDU session is congested), the PCF may include in the "403 Forbidden" response the "cause" attribute set to "REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED". The PCF may also provide a retry interval within the "Retry-After" HTTP header field. When the AF receives the retry interval within the "Retry-After" HTTP header field, the AF shall not send the same service information to the PCF again (for the same application session context) until the retry interval has elapsed. The "Retry-After" HTTP header is described in 3GPP TS 29.500 [5] subclause 5.2.2.2.