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

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

Reference
RTS/TSGC-0329507vf90

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

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 at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

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

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

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

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

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

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

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

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[15] void.

[16] void.

[17] 3GPP TS 29.519: "5G System; Usage of the Unified Data Repository service for Policy Data, Application Data and Structured Data for Exposure; Stage 3".

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

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

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

4 Access and Mobility Policy Control Service

4.1 Service Description

4.1.1 Overview

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

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

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

- deletion of the policy context for a UE.

4.1.2 Service Architecture

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

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

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

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

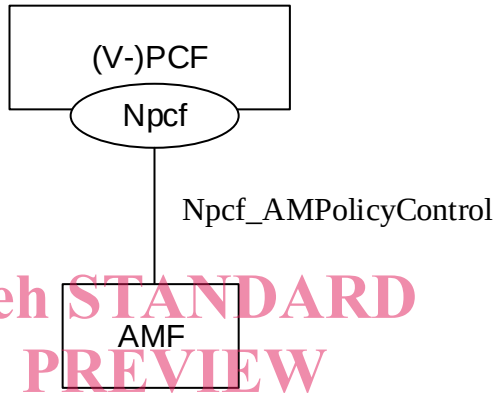

Figure 4.1.2-1: Reference Architecture for the Npcf_AMPolicyControl Service; SBI representation

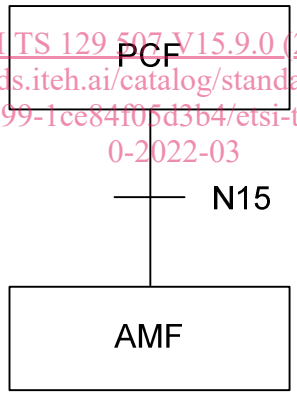

Figure 4.1.2-2: Non-roaming Reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

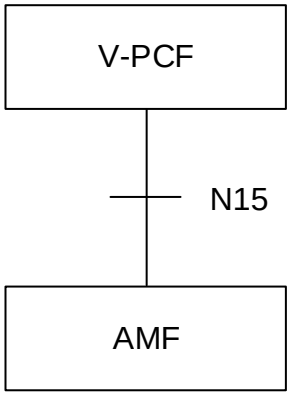

Figure 4.1.3-2: Roaming reference Architecture for the Npcf_AMPolicyControl Service; reference point representation

4.1.3 Network Functions

4.1.3.1 Policy Control Function (PCF)

The Policy Control Function (PCF):

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

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

4.1.3.2 NF Service Consumers

The Access and Mobility Management function (AMF) provides:

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

4.2 Service Operations

4.2.1 Introduction

Table 4.2.1-1: Operations of the Npcf_AMPolicyControl Service

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

4.2.2 Npcf_AMPolicyControl_Create Service Operation

4.2.2.1 General

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

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

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

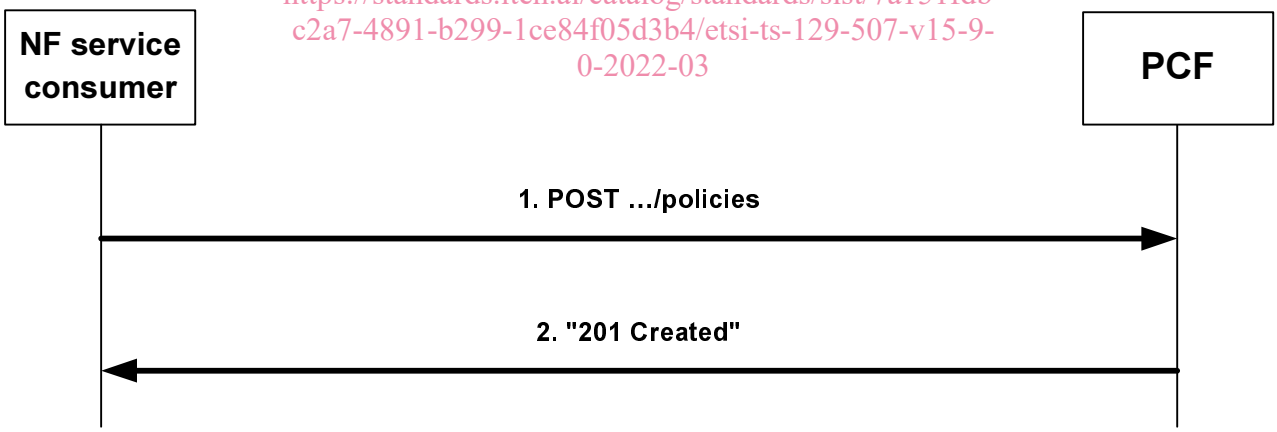

Figure 4.2.2.1-1: Creation of a policy association

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

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

- Notification URI encoded as "notificationUri" attribute; and

- SUPI encoded as "supi" attribute,

and that shall include when available:

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

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

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

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

and the the PolicyAssociation data type as body including:

- conditionally AMF Access and Mobility Policy (see subclause 4.2.2.3), i.e.:
  a) if the PCF received the "servAreaRes" in the request, Service Area Restrictions encoded as "servAreaRes" attribute; and/or
  b) if the PCF received the "rfsp" attributes in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute;
- optionally one or several of the following Policy Control Request Trigger(s) encoded as "triggers" attribute (see subclause 4.2.3.2):
  a) Location change (tracking area); and
  b) Change of UE presence in PRA; and

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

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

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

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

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

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

4.2.2.2 Void

4.2.2.2.0 Void

4.2.2.2.1 Void

4.2.2.2.2 Void

4.2.2.3 AMF Access and Mobility Policy

4.2.2.3.1 Service Area Restriction

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

- a limited allowed area represented as:

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

  b) both of:

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

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

  c) both a) and b) above;

- or a limited allowed area represented as:

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

  b) all of:

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

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