

ETSI TS 123 503 V16.12.0 (2022-07)



**5G;
Policy and charging control framework
for the 5G System (5GS);
Stage 2
(3GPP TS 23.503 version 16.12.0 Release 16)**

<https://standards.iteh.ai/catalog/standards/sist/62ef3dba-1f6d-4922-955f-99d5046c1cc8/etsi-ts-123-503-v16-12-0-2022-07>



Reference

RTS/TSGS-0223503vgc0

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://standards.iteh.ai> <https://portal.etsi.org/People/CommitteeSupportStaff.aspx> f-99d5046efcc8@etsi-

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

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 2022.
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 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

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	6
Introduction	6
1 Scope	7
2 References	7
3 Definitions and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations	10
4 High level architectural requirements	11
4.1 General requirements	11
4.2 Non-session management related policy control requirements	11
4.2.1 Access and mobility related policy control requirements	11
4.2.2 UE policy control requirements	12
4.2.3 Network analytics information requirements	12
4.2.4 Management of packet flow descriptions	12
4.2.5 SMF selection management related policy control requirements	12
4.2.6 Support for non-session management related network capability exposure	12
4.3 Session management related policy control requirements	13
4.3.1 General requirements	13
4.3.2 Charging related requirements	14
4.3.2.1 General	14
4.3.2.2 Charging models	14
4.3.2.3 Charging requirements	14
4.3.2.4 Examples of Service Data Flow Charging	14
4.3.3 Policy control requirements	15
4.3.3.1 Gating control requirements	15
4.3.3.2 QoS control requirements	15
4.3.3.2.1 QoS control at service data flow level	15
4.3.3.2.2 QoS control at QoS Flow level	15
4.3.3.2.3 QoS control at PDU Session level	16
4.3.3.3 Subscriber spending limits requirements	16
4.3.4 Usage monitoring control requirements	16
4.3.5 Application detection and control requirements	16
4.3.6 Support for session management related network capability exposure	17
4.3.7 Traffic steering control	17
5 Architecture model and reference points	17
5.1 General	17
5.2 Reference architecture	17
5.2.1 Non-roaming architecture	17
5.2.2 Roaming architecture	18
5.2.3 Void	20
5.3 Service-based interfaces and reference points	21
5.3.1 Interactions between PCF and AF	21
5.3.2 Interactions between PCF and SMF	21
5.3.3 Interactions between PCF and AMF	21
5.3.4 Interactions between V-PCF and H-PCF	22
5.3.5 Interactions between PCF and UDR	22
5.3.6 Interactions between SMF and CHF	22
5.3.7 Void	22
5.3.8 Interactions between PCF and CHF	23

5.3.9	Interactions between SMF and NEF	23
5.3.10	Interactions between NEF and PCF	23
5.3.11	Interactions between NWDAF and PCF	23
6	Functional description	24
6.1	Overall description	24
6.1.1	General	24
6.1.1.1	PCF Discovery and Selection	24
6.1.1.2	Binding an AF request targeting an UE address to the relevant PCF	24
6.1.1.2.1	General	24
6.1.1.2.2	The Binding Support Function (BSF)	25
6.1.1.3	Policy decisions based on network analytics	26
6.1.2	Non-session management related policy control	26
6.1.2.1	Access and mobility related policy control	26
6.1.2.2	UE policy control	27
6.1.2.2.1	General	27
6.1.2.2.2	Distribution of the policies to UE	29
6.1.2.3	Management of packet flow descriptions	31
6.1.2.3.1	PFD management	31
6.1.2.3.2	Packet Flow Description	33
6.1.2.4	Negotiation for future background data transfer	33
6.1.2.5	Policy Control Request Triggers relevant for AMF	35
6.1.3	Session management related policy control	37
6.1.3.1	General	37
6.1.3.2	Binding mechanism	37
6.1.3.2.1	General	37
6.1.3.2.2	Session binding	37
6.1.3.2.3	PCC rule authorization	38
6.1.3.2.4	QoS Flow binding	38
6.1.3.3	Reporting	39
6.1.3.4	Credit management	40
6.1.3.5	Policy Control Request Triggers relevant for SMF	40
6.1.3.6	Policy control	49
6.1.3.7	Service (data flow) prioritization and conflict handling	49
6.1.3.8	Termination action	50
6.1.3.9	Handling of packet filters provided to the UE by SMF	50
6.1.3.10	IMS emergency session support	50
6.1.3.11	Multimedia Priority Service support	51
6.1.3.12	Redirection	52
6.1.3.13	Resource sharing for different AF sessions	52
6.1.3.14	Traffic steering control	53
6.1.3.15	Resource reservation for services sharing priority	53
6.1.3.16	3GPP PS Data Off	54
6.1.3.17	Policy decisions based on spending limits	55
6.1.3.18	Event reporting from the PCF	56
6.1.3.19	Mission Critical Services support	59
6.1.3.20	Access Traffic Steering, Switching and Splitting	59
6.1.3.21	QoS Monitoring to assist URLLC Service	60
6.1.3.22	AF session with required QoS	61
6.1.3.23	Support of integration with Time Sensitive Networking	62
6.1.3.24	Policy control for redundant PDU Sessions	62
6.2	Network functions and entities	63
6.2.1	Policy Control Function (PCF)	63
6.2.1.1	General	63
6.2.1.1.1	Session management related functionality	63
6.2.1.1.2	Non-session management related functionality	64
6.2.1.2	Input for PCC decisions	64
6.2.1.3	Policy control subscription information management	67
6.2.1.4	V-PCF	70
6.2.1.5	H-PCF	70
6.2.1.6	Application specific policy information management	71
6.2.1.7	Usage monitoring	71

6.2.1.8	Sponsored data connectivity.....	72
6.2.2	Session Management Function (SMF).....	72
6.2.2.1	General	72
6.2.2.2	Service data flow detection	74
6.2.2.3	Measurement.....	75
6.2.2.4	QoS control	76
6.2.2.5	Application detection	77
6.2.2.6	Traffic steering	77
6.2.2.7	Access Traffic Steering, Switching and Splitting.....	77
6.2.3	Application Function (AF).....	77
6.2.4	Unified Data Repository (UDR)	78
6.2.5	Charging Function (CHF).....	78
6.2.6	Void	78
6.2.7	Network Exposure Function (NEF)	78
6.2.8	Access and Mobility Management Function (AMF)	79
6.2.9	Network Data Analytics Function (NWDAF)	79
6.3	Policy and charging control rule.....	79
6.3.1	General.....	79
6.3.2	Policy and charging control rule operations	91
6.4	PDU Session related policy information	92
6.5	Access and mobility related policy information.....	98
6.6	UE policy information.....	99
6.6.1	Access Network Discovery & Selection Policy Information.....	99
6.6.1.1	General	99
6.6.1.2	UE selecting a WLANSP rule.....	99
6.6.1.3	UE procedure for selecting a WLAN access based on WLANSP rules.....	100
6.6.2	UE Route Selection Policy information.....	100
6.6.2.1	Structure Description	100
6.6.2.2	Configuration and Provision of URSP	104
6.6.2.3	UE procedure for associating applications to PDU Sessions based on URSP	104
6.6.3	V2X Policy information.....	105
Annex A (informative):	URSP rules example	106
Annex B (informative):	Deployment option to support of BSF and DRA coexistence due to network migration	110
Annex C (Normative):	Support for Application Functions supporting Rx interface	111
Annex D (informative):	PCC usage for sponsored data connectivity	113
D.1	General	113
D.2	Reporting for sponsored data connectivity.....	114
Annex E (informative):	Change history	115
History	121

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.

Introduction

For references to TS 23.203 [4] made in this document,

- the IP-CAN session of TS 23.203 [4] maps to the PDU Session in 5GC.
- the APN of TS 23.203 [4] maps to DNN in 5GC.
- the IP-CAN bearer of TS 23.203 [4] maps to the QoS Flow in 5GC.
- The PCRF of TS 23.203 [4] maps to the PCF in 5GC.
- The PCEF of TS 23.203 [4] maps to the combination of SMF and UPF in 5GC.
- The BBF shall be considered as being located in the PCEF.
- TDF related description does not apply.
- NBIFOM related description does not apply.

1 Scope

The present document defines the Stage 2 policy and charging control framework for the 5G System specified in TS 23.501 [2] and TS 23.502 [3].

The policy and charging control framework encompasses the following high level functions:

- Flow Based Charging for network usage, including charging control and online credit control, for service data flows;
- Policy control for session management and service data flows (e.g. gating control, QoS control, etc.);
- Management for access and mobility related policies;
- Management of UE policy information.

Interworking with E-UTRAN connected to EPC is described in TS 23.501 [2].

TS 23.502 [3] contains the stage 2 procedures and flows for the policy and charging control framework and it is a companion specification to this specification.

TS 32.255 [21] contains the functional description of the converged offline and online charging functionality for the 5G System.

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: "Technical Specification Group Services and System Aspects; System Architecture for the 5G System".
- [3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".
- [4] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".
- [5] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [6] 3GPP TS 23.179: "Functional architecture and information flows to support mission-critical communication service; Stage 2".
- [7] Void.
- [8] 3GPP TS 32.240: "Charging management; Charging architecture and principles".
- [9] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".
- [10] 3GPP TS 23.161: "Network-Based IP Flow Mobility (NBIFOM); Stage 2".
- [11] 3GPP TS 23.261: "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2".

- [12] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS) emergency sessions".
- [13] 3GPP TS 29.507: "Access and Mobility Policy Control Service; Stage 3".
- [14] Void.
- [15] 3GPP TS 22.011: "Service Accessibility".
- [16] 3GPP TS 23.221: "Architectural requirements".
- [17] 3GPP TS 29.551: "5G System; Packet Flow Description Management Service; Stage 3".
- [18] 3GPP TS 32.421: "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements".
- [19] 3GPP TS 24.526: "UE Equipment (UE) policies for 5G System (5GS); Stage 3".
- [20] 3GPP TS 32.291: "Charging management; 5G system, Charging service; stage 3".
- [21] 3GPP TS 32.255: "Telecommunication management; Charging management; 5G Data connectivity domain charging; Stage 2".
- [22] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".
- [23] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".
- [24] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".
- [25] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".
- [26] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2".
- [27] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".
- [28] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".
- [29] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- [30] 3GPP TS 24.237: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".
- [31] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".
- [32] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 23.501 [2], TS 23.502 [3] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Application detection filter: A logic used to detect packets generated by an application based on extended inspection of these packets, e.g. header and/or payload information, as well as dynamics of packet flows. The logic is entirely internal to a UPF, and is out of scope of this specification.

Application identifier: An identifier referring to a specific application detection filter.

Application service provider: A business entity responsible for the application that is being / will be used by a UE, which may be either an AF operator or has an association with the AF operator.

Authorised QoS: The maximum QoS that is authorised for a service data flow. In the case of an aggregation of multiple service data flows within one QoS Flow, the combination of the "Authorised QoS" information of the individual service data flows is the "Authorised QoS" for the QoS Flow. It contains the 5QI and the data rate.

Binding: The association between a service data flow and the QoS Flow transporting that service data flow.

Binding mechanism: The method for creating, modifying and deleting bindings.

Charging control: The process of associating packets, belonging to a service data flow, to a charging key and applying online charging and/or offline charging, as appropriate.

Charging key: information used by the CHF for rating purposes.

Detected application traffic: An aggregate set of packet flows that are generated by a given application and detected by an application detection filter.

Dynamic PCC Rule: a PCC rule, for which the definition is provided to the SMF by the PCF.

Gating control: The process of blocking or allowing packets, belonging to a service data flow / detected application's traffic, to pass through to the UPF.

Monitoring key: information used by the SMF and PCF for usage monitoring control purposes as a reference to a given set of service data flows or application (s), that all share a common allowed usage on a per UE and DNN basis.

Non-3GPP access network selection information: It consists of ePDG identifier configuration, N3IWF identification and non-3GPP access network selection information, as defined in clause 6.3.6.1 in TS 23.501 [2].

Non-Seamless Offload: A capability of the UE to access the data networks via non-3GPP access (e.g. WLAN radio access) outside of a PDU Session.

Operator-controlled service: A service for which complete PCC rule information, including service data flow filter information, is available in the PCF through configuration and/or dynamic interaction with an AF.

Operating System (OS): Collection of UE software that provides common services for applications.

Operating System Identifier (OSId): An identifier identifying the operating system.

OS specific Application Identifier (OSAppId): An identifier associated with a given application and uniquely identifying the application within the UE for a given operating system.

Packet flow: A specific user data flow from and/or to the UE.

Packet Flow Description (PFD): A set of information enabling the detection of application traffic provided by a 3rd party service provider.

PCC decision: A PCF decision for policy and charging control provided to the SMF (consisting of PCC rules and PDU Session related attributes), a PCF decision for access and mobility related control provided to the AMF, a PCF decision for UE policy information provided to the UE or a PCF decision for background data transfer policy provided to the AF.

PCC rule: A set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control and/or other control or support information. The possible information is described in clause 6.3.1.

Policy control: The process whereby the PCF indicates to the SMF how to control the QoS Flow. Policy control includes QoS control and/or gating control.

Policy Control Request trigger report: a notification, possibly containing additional information, of an event which occurs that corresponds with a Policy Control Request trigger.

Policy Control Request trigger: defines a condition when the SMF shall interact again with the PCF.

Policy counter: A mechanism within the CHF to track spending applicable to a subscriber.

Policy counter identifier: A reference to a policy counter in the CHF for a subscriber.

Policy counter status: A label whose values are not standardized and that is associated with a policy counter's value relative to the spending limit(s) (the number of possible policy counter status values for a policy counter is one greater than the number of thresholds associated with that policy counter, i.e. policy counter status values describe the status around the thresholds). This is used to convey information relating to subscriber spending from CHF to PCF. Specific labels are configured jointly in CHF and PCF.

Policy Section: A Policy Section is identified by a Policy Section Identifier and consists of one or multiple URSP rule(s) or one or multiple WLANSP rule(s) or non-3GPP access network selection information or a combination of WLANSP rule(s) and non-3GPP access network selection information.

Predefined PCC Rule: a PCC rule that has been provisioned directly into the SMF by the operator.

Redirection: Redirect the detected service traffic to an application server (e.g. redirect to a top-up / service provisioning page).

Service data flow: An aggregate set of packet flows carried through the UPF that matches a service data flow template.

Service data flow filter: A set of packet flow header parameter values/ranges used to identify one or more of the packet flows in the UPF. The possible service data flow filters are defined in clause 6.2.2.2.

Service data flow filter identifier: A scalar that is unique for a specific service data flow (SDF) filter within a PDU Session.

Service data flow template: The set of service data flow filters in a PCC Rule or an application identifier in a PCC rule referring to an application detection filter in the SMF or in the UPF, required for defining a service data flow.

Service identifier: An identifier for a service. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow. A concrete instance of a service may be identified if additional AF information is available (further details to be found in clause 6.3.1).

Session based service: An end user service requiring application level signalling, which is separated from service rendering.

Spending limit: A spending limit is the usage limit of a policy counter (e.g. monetary, volume, duration) that a subscriber is allowed to consume.

Spending limit report: a notification, containing the current policy counter status generated from the CHF to the PCF.

Subscribed guaranteed bandwidth QoS: The per subscriber, authorized cumulative guaranteed bandwidth QoS which is provided by the UDR to the PCF.

Subscriber category: is a means to group the subscribers into different classes, e.g. gold user, silver user and bronze user.

UE Local Configuration: Information about the association of an application to either a PDU Session or to non-seamless Offload is configured in the Mobile Termination (MT) and in the Terminal Equipment (TE). For example, UE Local Configuration can include operator specific configuration (e.g. operator provided S-NSSAI(s)), or application specific parameters to set up a PDU Session or end user configuration for specific applications.

UE policy information: Policy information preconfigured in the UE and/or provisioned to the UE for access selection (i.e. ANDSP), PDU Session selection (i.e. URSP) and/or V2X communications (i.e. V2XP).

Uplink binding verification: The network enforcement of terminal compliance with the negotiated uplink traffic mapping to QoS Flows.

User Preferences On Non-3GPP Access Selection: The list of configuration parameters provided by a layer (e.g. application) above NAS and used by the UE for access network discovery and selection.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [2], TS 23.502 [3], TS 23.316 [27] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AMBR	Aggregated Maximum Bitrate
------	----------------------------

ANDSP	Access Network Discovery & Selection Policy
ARP	Allocation and Retention Priority
ASP	Application Service Provider
BDT	Background Data Transfer
BSF	Binding Support Function
CHF	CHarging Function
H-PCF	A PCF in the HPLMN
H-UDR	A UDR in the HPLMN
MPS	Multimedia Priority Service
NBIFOM	Network-based IP flow mobility
NSWO	Non-Seamless WLAN Offload
NWDAF	Network Data Analytics Function
OAM	Operation Administration and Maintenance
OCS	Online Charging System
PCC	Policy and Charging Control
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
PRA	Presence Reporting Area
RAN	Radio Access Network
URSP	UE Route Selection Policy
V2XP	V2X Policy
V-PCF	A PCF in the VPLMN
V-UDR	A UDR in the VPLMN
vSRVCC	video Single Radio Voice Call Continuity
WLANSF	WLAN Selection Policy

4 High level architectural requirements

4.1 General requirements

It shall be possible to apply policy and charging control to any kind of 3GPP and non-3GPP accesses defined in TS 23.501 [2].

The policy and charging control framework shall support the roaming scenarios defined in TS 23.501 [2].

The policy and charging control shall be enabled on a per slice instance, per DNN, or per both slice instance and DNN basis.

NOTE: In single PCF deployment, the PCF will provide all mobility, UE access selection and PDU Session related policies that it is responsible for. In deployments where different PCFs support N15 and N7 respectively, no standardized interface between them is required in this release to support policy alignment.

The policy and charging control framework shall fulfil non-session management related requirements as defined in clause 4.2 and session management related requirements as defined in clause 4.3.

4.2 Non-session management related policy control requirements

4.2.1 Access and mobility related policy control requirements

The policy framework shall provide following functionality for the access and mobility enforcement:

- Policy Control Function (PCF) shall support interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces.
- The PCF shall be able to provide Access and Mobility Management related policies to the AMF.
- The PCF shall be able to evaluate operator policies that are triggered by events received from the AMF.

4.2.2 UE policy control requirements

The 5GC shall be able to provide policy information from the PCF to the UE. Such UE policy information includes:

- Access Network Discovery & Selection Policy (ANDSP): It is used by the UE for selecting non-3GPP accesses network.
- UE Route Selection Policy (URSP): This policy is used by the UE to determine how to route outgoing traffic. Traffic can be routed to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session.
- V2X Policy (V2XP): This policy provides configuration parameters to the UE for V2X communication over PC5 reference point or over Uu reference point or both. V2X Policies are defined in TS 23.287 [28].

4.2.3 Network analytics information requirements

The PCF shall be able to collect directly network analytic information from the NWDAF. The NWDAF provides network data analytics (e.g. load level information on a network slice level) to PCF. The PCF shall be able to use those data in its policy decisions. The details are defined in clause 6.1.1.3.

4.2.4 Management of packet flow descriptions

Management of Packet Flow Descriptions (PFDs) refers to the capability to create, update or remove PFDs in the NEF (PFDF) and the distribution from the NEF (PFDF) to the SMF and finally to the UPF. This feature may be used when the UPF is configured to detect a particular application provided by an ASP.

NOTE 1: A possible scenario for the management of PFDs in the SMF is when an application, identified by an application detection filter in the UPF, deploys a new server or a reconfiguration occurs in the ASP network which impacts the application detection filters of that particular application.

NOTE 2: The management of application detection filters in the SMF can still be performed by using operation and maintenance procedures.

NOTE 3: This feature aims for both: to enable accurate application detection at the UPF and to minimize storage requirements for the UPF and the SMF.

The management of PFDs is supported in non-roaming and home-routed scenarios for those ASPs that have a business relation with the home operator.

4.2.5 SMF selection management related policy control requirements

The policy framework may provide following functionality for the SMF selection management for a PDU Session:

- The Policy Control Function (PCF) may support interactions with the SMF selection functionality in the AMF and the PCF may provide SMF selection management related policies to the AMF;
- The PCF may provide a policy to the AMF to contact PCF for performing DNN replacement of specific DNNs;
- The PCF may provide a policy to the AMF to contact PCF for performing DNN replacement for an unsupported DNN.

4.2.6 Support for non-session management related network capability exposure

Support for network capability exposure enables an AF (e.g. an external ASP) to request the following non-session management related policy control functionality from the NEF:

- Management of PFDs as defined in clause 4.2.4 and in clause 4.18 of TS 23.502 [3];
- Negotiations for future background data transfer as defined in clause 6.1.2.4 and in clause 4.16.7 of TS 23.502 [3];

- Applying a previously negotiated background data transfer policy to a UE or group of UEs as defined in clause 6.1.2.4 and in clause 4.15.6.8 of TS 23.502 [3];
- Traffic steering control for AF influenced traffic diversion, as defined in clause 4.3.7 and in clause 5.6.7 of TS 23.501 [2];
- Service specific parameter provisioning for V2X communication (see clause 5.20 of TS 23.501 [2] and clause 4.15.6.7 of TS 23.502 [3]);
- 5G VN group management (see clause 5.29 of TS 23.501 [2] and clause 4.15.6 of TS 23.502 [3]).

4.3 Session management related policy control requirements

4.3.1 General requirements

It shall be possible for the PCC framework to base decisions upon subscription information, Access Type and the RAT Type.

The PCC framework shall perform Gating Control and discard packets that don't match any service data flow of the active PCC rules. It shall also be possible for the operator to define PCC rules, with wild-carded service data flow filters, to allow sending or receiving packets that do not match any service data flow template of any other active PCC rules.

The PCC framework shall allow the charging control to be applied on a per service data flow and on a per application basis, independent of the policy control.

The PCC framework shall have a binding method that allows the unique association between service data flows and specific QoS Flow.

A single service data flow detection shall suffice for the purpose of both policy control and flow based charging.

A PCC rule may be predefined or dynamically provisioned at establishment and during the lifetime of a PDU Session. The latter is referred to as a dynamic PCC rule.

It shall be possible to take a PCC rule into service, and out of service, at a specific time of day, without any PCC interaction at that point in time.

It shall be possible to take DNN-related policy information into service, and out of service, once validity conditions specified as part of the DNN-related policy information are fulfilled or not fulfilled anymore, respectively, without any PCC interaction at that point in time.

PCC shall be enabled on a per DNN basis at the SMF. It shall be possible for the operator to configure the PCC framework to perform charging control, policy control or both for a DNN access.

The PCC framework shall allow the resolution of conflicts which would otherwise cause a subscriber's Subscribed Guaranteed Bandwidth QoS to be exceeded.

It should be possible to use PCC framework for handling IMS-based emergency service.

It shall be possible with the PCC framework, in real-time, to monitor the overall amount of resources that are consumed by a user and to control usage independently from charging mechanisms, the so-called usage monitoring control.

It shall be possible for the PCC framework to provide application awareness even when there is no explicit service level signalling.

The PCC framework shall support making policy decisions based on subscriber spending limits.

The PCC framework shall support making policy decisions for N6 traffic steering.

4.3.2 Charging related requirements

4.3.2.1 General

In order to allow for charging control on service data flow, the information in the PCC rule identifies the service data flow and specifies the parameters for charging control.

For the purpose of charging correlation between service data flow level and application level (e.g. IMS) as well as on-line charging support at the application level, applicable charging identifiers and Access Type identifiers shall be passed from the PCF to the AF, if such identifiers are available.

4.3.2.2 Charging models

The PCC charging shall support the following charging models for charging performed by SMF:

- Volume based charging;
- Time based charging;
- Volume and time based charging;
- Event based charging;
- No charging.

NOTE: The charging model - "No charging" implies that charging control is not applicable, and no charging records are generated.

4.3.2.3 Charging requirements

It shall be possible to apply different rates and charging models depending on a UE's roaming status.

It shall be possible to apply different rates based on the location of a UE.

It shall be possible to apply different rates for specific part of a service, e.g. allow the UE to download a certain volume for one rate, and after this volume has been reached continue with a different rate.

It shall be possible to apply different rates based on the time of day.

It shall be possible to enforce per service data flow, identified by PCC Rule, usage limits on a per UE basis.

It shall be possible to apply different rates depending on the access used to carry a Service Data Flow

It shall be possible to apply an online charging action upon Application Start/Stop events.

It shall be possible to indicate to the SMF that interactions with the CHF are not required for a PCC rule, i.e. to not perform accounting, credit control or recording of usage for the service data flow, in this case no charging information is generated.

4.3.2.4 Examples of Service Data Flow Charging

There are many different services that may be used within a network, including both user-user and user-network services. Service data flows from these services may be identified and charged in many different ways. A number of examples of configuring PCC rules for different service data flows are described below.

EXAMPLE 1: A network server provides an FTP service. The FTP server supports both the active (separate ports for control and data) and passive modes of operation. A PCC rule is configured for the service data flows associated with the FTP server for the user. The PCC rule uses a filter specification for the uplink that identifies packets sent to port 20 or 21 of the IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 20 or 21 of the IP address of the server.