

ETSI TS 123 503 V18.11.0 (2026-02)



TECHNICAL SPECIFICATION

5G;
Policy and charging control framework
for the 5G System (5GS);
Stage 2
(3GPP TS 23.503 version 18.11.0 Release 18)



Reference

RTS/TSGS-0223503v18

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
Introduction	7
1 Scope	8
2 References	8
3 Definitions and abbreviations.....	10
3.1 Definitions	10
3.2 Abbreviations	12
4 High level architectural requirements	13
4.1 General requirements	13
4.2 Non-session management related policy control requirements	14
4.2.1 Access and mobility related policy control requirements	14
4.2.2 UE policy control requirements	14
4.2.3 Network analytics information requirements.....	14
4.2.4 Management of packet flow descriptions	14
4.2.5 SMF selection management related policy control requirements	15
4.2.6 Support for non-session management related network capability exposure	15
4.2.7 Slice replacement related policy control requirements	15
4.3 Session management related policy control requirements.....	16
4.3.1 General requirements.....	16
4.3.2 Charging related requirements.....	16
4.3.2.1 General	16
4.3.2.2 Charging models	16
4.3.2.3 Charging requirements	17
4.3.2.4 Examples of Service Data Flow Charging	17
4.3.3 Policy control requirements	17
4.3.3.1 Gating control requirements.....	17
4.3.3.2 QoS control requirements	18
4.3.3.2.1 QoS control at service data flow level.....	18
4.3.3.2.2 QoS control at QoS Flow level.....	18
4.3.3.2.3 QoS control at PDU Session level.....	18
4.3.3.3 Subscriber spending limits requirements	18
4.3.4 Usage monitoring control requirements.....	19
4.3.5 Application detection and control requirements	19
4.3.6 Support for session management related network capability exposure	19
4.3.7 Traffic steering control	20
4.4 Network slice related policy control requirements.....	20
5 Architecture model and reference points.....	20
5.1 General	20
5.2 Reference architecture	20
5.2.1 Non-roaming architecture	20
5.2.2 Roaming architecture.....	22
5.2.3 Void	24
5.3 Service-based interfaces and reference points.....	24
5.3.1 Interactions between PCF and AF	24
5.3.2 Interactions between PCF and SMF	25
5.3.3 Interactions between PCF and AMF.....	25
5.3.4 Interactions between V-PCF and H-PCF	26
5.3.5 Interactions between PCF and UDR	26
5.3.6 Interactions between SMF and CHF.....	26

5.3.7	Void	26
5.3.8	Interactions between PCF and CHF	26
5.3.9	Interactions between SMF and NEF	27
5.3.10	Interactions between NEF and PCF	27
5.3.11	Interactions between NWDAF and PCF	27
5.3.12	Interactions between PCF for the UE and PCF for the PDU Session	27
5.3.13	Interactions between PCF and TSCTSF	27
5.3.14	Interactions between NWDAF and NEF (PFDF)	28
6	Functional description	28
6.1	Overall description	28
6.1.1	General	28
6.1.1.1	PCF Discovery and Selection	28
6.1.1.2	Binding an AF request targeting an UE address to the relevant PCF	28
6.1.1.2.1	General	28
6.1.1.2.2	The Binding Support Function (BSF)	29
6.1.1.2a	Binding an NF request targeting a UE to the relevant PCF for the UE	30
6.1.1.3	Policy decisions based on network analytics	31
6.1.1.4	Policy decisions based on spending limits	36
6.1.1.5	Policy control decisions based on awareness of URSP rule enforcement	37
6.1.1.5.1	General	37
6.1.1.5.2	Policy control decisions based on awareness of URSP rule enforcement with UE assistance	38
6.1.1.5.3	Policy control decisions based on awareness of URSP rule enforcement without UE assistance	38
6.1.2	Non-session management related policy control	38
6.1.2.1	Access and mobility related policy control	38
6.1.2.2	UE policy control	41
6.1.2.2.1	General	41
6.1.2.2.2	Distribution of the policies to UE	44
6.1.2.2.3	URSP rule provisioning in EPS	47
6.1.2.2.4	Distribution of VPLMN specific URSP rules to the UE	47
6.1.2.3	Management of packet flow descriptions	48
6.1.2.3.1	PFD management	48
6.1.2.3.2	Packet Flow Description	50
6.1.2.4	Negotiation for future background data transfer	51
6.1.2.5	Policy Control Request Triggers relevant for AMF	53
6.1.2.6	AF influence on Access and Mobility related policy control	57
6.1.2.6.0	General	57
6.1.2.6.1	AF request Access and Mobility related Policy Control for a UE	57
6.1.2.6.2	AF request to influence on Access and Mobility related Policy Control	57
6.1.2.7	Negotiation for planned data transfer with QoS requirements	58
6.1.3	Session management related policy control	59
6.1.3.1	General	59
6.1.3.2	Binding mechanism	60
6.1.3.2.1	General	60
6.1.3.2.2	Session binding	60
6.1.3.2.3	PCC rule authorization	60
6.1.3.2.4	QoS Flow binding	61
6.1.3.3	Reporting	63
6.1.3.4	Credit management	63
6.1.3.5	Policy Control Request Triggers relevant for SMF	64
6.1.3.6	Policy control	73
6.1.3.7	Service (data flow) prioritization and conflict handling	74
6.1.3.8	Termination action	74
6.1.3.9	Handling of packet filters provided to the UE by SMF	75
6.1.3.10	IMS emergency session support	75
6.1.3.11	Multimedia Priority Service support	76
6.1.3.12	Redirection	77
6.1.3.13	Resource sharing for different AF sessions	78
6.1.3.14	Traffic steering control	78
6.1.3.15	Resource reservation for services sharing priority	79
6.1.3.16	3GPP PS Data Off	79

6.1.3.17	Policy decisions based on spending limits	81
6.1.3.18	Event reporting from the PCF	81
6.1.3.19	Mission Critical Services support	87
6.1.3.20	Access Traffic Steering, Switching and Splitting	87
6.1.3.21	QoS Monitoring control	90
6.1.3.22	AF session with required QoS	92
6.1.3.23	Support of integration with Time Sensitive Networking	94
6.1.3.23a	Support of Time Sensitive Communication and Time Synchronization	95
6.1.3.23b	Support of IETF Deterministic Networking	95
6.1.3.24	Policy control for redundant PDU Sessions	97
6.1.3.25	User Plane Remote Provisioning of UE SNPN Credentials in Onboarding Network	97
6.1.3.26	Packet Delay Variation monitoring and reporting	98
6.1.3.27	Support of eXtended Reality and Interactive Media Services	98
6.1.3.27.1	Exposure of network information	98
6.1.3.27.2	UL/DL policy control based on round-trip latency requirement	99
6.1.3.27.3	Support for delivery of multi-modal services	99
6.1.3.27.4	PDU Set based handling	100
6.1.3.27.5	Data Burst Based Handling	100
6.1.3.27.6	Traffic Parameter Information and Traffic Parameter Measurement	100
6.1.3.28	AF requested QoS for a UE or group of UEs not identified by a UE address	100
6.1.3.29	Network Slice replacement for a PDU Session	101
6.1.4	Network slice related policy control	102
6.1.4.1	General	102
6.1.4.2	Limitation of data rate per network slice with assistance of the NWDAF	103
6.1.4.3	Limitation of data rate per network slice with PCF based monitoring	103
6.1.5	Group related policy control	103
6.1.6	Void	104
6.2	Network functions and entities	104
6.2.1	Policy Control Function (PCF)	104
6.2.1.1	General	104
6.2.1.1.1	Session management related functionality	104
6.2.1.1.2	Non-session management related functionality	106
6.2.1.1.3	Network slice related functionality	106
6.2.1.1.4	Group related functionality	106
6.2.1.2	Input for PCC decisions	106
6.2.1.3	Policy control subscription information management	110
6.2.1.4	V-PCF	115
6.2.1.5	H-PCF	115
6.2.1.6	Application specific policy information management	115
6.2.1.7	Usage monitoring	116
6.2.1.8	Sponsored data connectivity	117
6.2.1.9	Monitoring the data rate per Network Slice for a UE	117
6.2.1.10	Monitoring the data rate per Network Slice	117
6.2.1.10.1	General	117
6.2.1.10.2	Monitoring the data rate per Network Slice by using QoS parameters	118
6.2.1.11	Monitoring the data rate per Group	118
6.2.1.11.1	General	118
6.2.1.11.2	Monitoring the data rate per Group by using QoS parameters	118
6.2.1.12	VPLMN Specific Offloading Policy	119
6.2.2	Session Management Function (SMF)	119
6.2.2.1	General	119
6.2.2.2	Service data flow detection	121
6.2.2.3	Measurement	121
6.2.2.4	QoS control	122
6.2.2.5	Application detection	123
6.2.2.6	Traffic steering	124
6.2.2.7	Access Traffic Steering, Switching and Splitting	124
6.2.2.8	Network Slice Replacement	124
6.2.3	Application Function (AF)	124
6.2.4	Unified Data Repository (UDR)	125
6.2.5	Charging Function (CHF)	125
6.2.6	Void	125

6.2.7	Network Exposure Function (NEF)	125
6.2.8	Access and Mobility Management Function (AMF)	126
6.2.9	Network Data Analytics Function (NWDAF)	126
6.2.10	Void	126
6.2.11	Time Sensitive Communication and Time Synchronization Function (TSCTSF).....	126
6.3	Policy and charging control rule.....	126
6.3.1	General.....	126
6.3.2	Policy and charging control rule operations	141
6.4	PDU Session related policy information	142
6.5	Access and mobility related policy information.....	147
6.6	UE policy information.....	150
6.6.1	Access Network Discovery & Selection Policy Information.....	150
6.6.1.1	General	150
6.6.1.2	UE selecting a WLANSP rule.....	151
6.6.1.3	UE procedure for selecting a WLAN access based on WLANSP rules.....	152
6.6.2	UE Route Selection Policy information.....	152
6.6.2.1	Structure Description	152
6.6.2.2	Configuration and Provision of URSP	158
6.6.2.2.1	General	158
6.6.2.2.2	URSP rules for an SNPN-enabled UE.....	158
6.6.2.2.3	Void.....	159
6.6.2.3	UE procedure for associating applications to PDU Sessions based on URSP	159
6.6.2.4	Support of URSP rule enforcement reporting	162
6.6.3	V2X Policy information.....	163
6.6.4	ProSe Policy information.....	163
6.6.5	Ranging/Sidelink Positioning Policy information	163
6.6.6	A2X Policy information.....	163
6.6.7	UE Policy Association supplementary information	164
Annex A (informative): URSP rules example		165
Annex B (informative): Deployment option to support of BSF and DRA coexistence due to network migration		170
Annex C (Normative): Support for Application Functions supporting Rx interface.....		171
Annex D (informative): PCC usage for sponsored data connectivity		173
D.1	General	173
D.2	Reporting for sponsored data connectivity.....	174
Annex E (informative): Change history		175
History		187

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".
- [33] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".
- [34] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".
- [35] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".
- [36] 3GPP TS 29.514: "Policy Authorization Service; Stage 3".
- [37] IETF RFC 9633: "Deterministic Networking (DetNet) YANG Model".
- [38] IETF RFC 5279: "A Uniform Resource Name (URN) Namespace for the 3rd Generation Partnership Project (3GPP)".
- [39] GSMA PRD NG.141, Version 3.0: "Guidelines for URSP".
- [40] 3GPP TS 26.522: "5G Real-time Media Transport Protocol Configurations".

- [41] 3GPP TS 23.586: "Architectural Enhancements to support Ranging based services and Sidelink Positioning".
- [42] IETF RFC 8939: "Deterministic Networking (DetNet) Data Plane: IP".
- [43] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".
- [44] 3GPP TS 29.512: "Session Management Policy Control Service; 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].

AM Policy Association: Access and Mobility management Policy Association. An association between the AMF and the PCF (i.e. the PCF for the UE) for performing access and mobility related policy control for a UE.

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.

Flow Description: information describing the characteristics of a packet flow for the purpose of detection, e.g. the combination of protocol (Protocol ID of the protocol above IP), source and destination IP address, source and destination port number, and optionally, ToS (IPv4) or TC (IPv6) value.

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.

Multi-modal service: A multi-modal service is a communication service that consists of several data flows that relate to each other and are subject to application coordination. The data flows can transfer different types of data (for example audio, video, positioning, haptic data) and may come from different sources (e.g. a single UE, a single device or multiple devices connected to the single UE, or multiple UEs).

Non-3GPP access network selection information: It consists of ePDG identifier configuration, N3IWF identification and non-3GPP access node 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 policy control provided to the AMF, a PCF decision for UE policy information provided to the UE or a PCF decision for service related policy (e.g. 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.

PCF for the PDU Session: A PCF providing session management policy control for a PDU Session of a UE.

PCF for the UE: A PCF providing non-session management policy control for a UE, i.e. access and mobility related policy control and/or UE policy control.

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 WLANS rule(s) or non-3GPP access network selection information or a combination of WLANS 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.

SM Policy Association: Session Management Policy Association. An association between the SMF and the PCF (i.e. the PCF for the PDU Session) for performing session management policy control for a PDU Session of a UE.

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 Association: An association between the AMF and the PCF (i.e. the PCF for the UE) for providing UE policy information from the PCF to the UE.

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), V2X communications (i.e. V2XP), ProSe operations (i.e. ProSeP), A2X communications (i.e. A2XP) and/or Ranging/Sidelink Positioning operations (i.e. RSLPP).

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.

VPLMN specific URSP Rules: A VPLMN specific URSP Rule is applicable when the UE is registered in that VPLMN or its equivalent PLMNs. A VPLMN specific URSP Rule may be used to route traffic to the VPLMN, if the V-PCF provides a local DNN to the AMF, using the PCRT on SMF selection management. A VPLMN specific URSP Rule may be used to route traffic to the Home PLMN if the HPLMN operator wants to provide a different list of RSDs for the same Traffic Descriptor for a VPLMN and for the HPLMN. When provided, the Time and Location criteria in the RSD(s) contain values that are based on agreements with the VPLMN or service parameters that were received from the VPLMN.

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].

5G DDNMF	5G Direct Discovery Name Management Function
A2XP	A2X Policy
AMBR	Aggregate 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
DCCF	Data Collection Coordination Function
H-PCF	A PCF in the HPLMN
H-UDR	A UDR in the HPLMN
HR-SBO	Home Routed with Session Breakout in VPLMN
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
PDTQ	Planned Data Transfer with QoS
PDUID	ProSe Discovery UE ID
PDV	Packet Delay Variation
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
PRA	Presence Reporting Area
ProSe	Proximity based Services
ProSeP	ProSe Policy
RAN	Radio Access Network
RSLPP	Ranging/Sidelink Positioning Policy
SNPN	Stand-alone Non-Public 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
WLANSP	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, the standardized interface between them supports policy alignment and exchange of relevant information.

The policy and charging control framework shall fulfil non-session management related requirements as defined in clause 4.2, session management related requirements as defined in clause 4.3 and network slice related requirements as defined in clause 4.4.

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.
- The AF may influence Access and Mobility related policy control performed by the PCF.

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, can be routed via a ProSe Layer-3 UE-to-Network Relay 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].
- ProSe Policy (ProSeP): This policy provides configuration parameters to the UE for ProSe features as defined in clause 5.1 of TS 23.304 [34].
- Ranging/Sidelink Positioning Policy (RSLPP): This policy provides configuration parameters to the UE for Ranging/Sidelink Positioning control. Ranging/Sidelink Positioning Policies are defined in TS 23.586 [41].
- A2X Policy (A2XP): This policy provides configuration parameters to the UE for A2X communication over PC5 reference point or over Uu reference point or both. A2X Policies are defined in TS 23.256 [43].

4.2.3 Network analytics information requirements

The PCF shall be able to collect network analytic information from the NWDAF directly or via DCCF, if deployed. 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.