ETSI TS 123 503 V15.7.0 (2019-10)

5G;
Policy and charging control framework for the 5G System (5GS);
Stage 2
(3GPP TS 23.503 version 15.7.0 Release 15)

Reference

RTS/TSGS-0223503vf70

Keywords

5G

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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.

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 for UE access selection and PDU Session selection related policies.

It refers to the policy and charging control functionality specified in TS 23.203 [4] for policy and charging control for PDU Sessions, depicting the differences where those exist.

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.

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] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows; Stage 2".

[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".

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], TS 23.203 [4] 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].

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].

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.

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.

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 6.3.1.

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.

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.

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.

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.

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 23.203 [4] 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].

ANDSP Access Network Discovery & Selection Policy
BSF Binding Support Function
CHF CHarging Function
H-PCF A PCF in the HPLMN
H-UDR A UDR in the HPLMN
NWDAF Network Data Analytics Function
OCS Online Charging System
PFD Packet Flow Description
URSP UE Route Selection Policy
V-PCF A PCF in the VPLMN
V-UDR A UDR in the VPLMN
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, 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 access selection and PDU Session selection related policy (UE policy) control requirements

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

4.2.3 Network status analytics information requirements

The PCF shall be able to collect directly slice specific network status analytic information from NWDAF. NWDAF provides network data analytics (i.e. load level information) to PCF on a network slice level and the NWDAF is not required to be aware of the current subscribers using the slice. PCF shall be able to use that data in its policy decisions.

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.

4.3 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

The charging related requirements defined in clause 4.2 of TS 23.203 [4] apply.

4.3.3 Policy control requirements

4.3.3.1 Gating control requirements

Gating control shall be applied by the UPF on a per service data flow basis.

To enable the PCF gating control decisions, the AF shall report session events (e.g. session termination, modification) to the PCF. For example, session termination, in gating control, may trigger the blocking of packets or "closing the gate".

Gating Control applies for service data flows of IP type.

4.3.3.2 QoS control requirements

4.3.3.2.1 QoS control at service data flow level

It shall be possible to apply QoS control on a per service data flow basis in the SMF, applicable for service data flows of both IP type and Ethernet type.

QoS control per service data flow allows the PCC framework to provide the SMF with the authorized QoS to be enforced for each specific service data flow. Criteria such as the QoS subscription information may be used together with policy rules such as, service-based, subscription-based, or predefined PCF internal policies to derive the authorized QoS to be enforced for a service data flow.

It shall be possible to apply multiple PCC rules, without application provided information, using different authorised QoS within a single PDU Session and within the limits of the Subscribed QoS profile.

4.3.3.2.2 QoS control at QoS Flow level

It shall be possible for the PCC framework to support control of QoS reservation procedures (UE-initiated or network-initiated). It shall be possible to determine the QoS to be applied in QoS reservation procedures (QoS control) based on the authorised QoS of the service data flows that are applicable to the QoS Flow and on criteria such as the QoS subscription information, service based policies, and/or predefined PCF internal policies.

It shall be possible for the SMF to determine the authorized QoS of a QoS Flow using the PCC rules associated to the QoS Flow, and the SMF shall be able to notify the PCF if the QoS Flow is removed or the GFBR of a QoS Flow can no longer (or can again) be guaranteed.

It shall be possible for the PCC framework to support control of QoS for the packet traffic of the PDU Session.

The PCC framework shall be able to provide policy control in the presence of NAT devices. This may be accomplished by providing appropriate address and port information to the PCF.

The enforcement of the control for QoS reservation procedures for a QoS Flow shall allow for a downgrading or an upgrading of the requested QoS as part of a UE-initiated QoS Flow establishment and modification. The PCC framework shall be able to provide a mechanism to initiate QoS Flow establishment and modification as part of the QoS control.

The PCC framework shall be able to handle QoS Flows that require a guaranteed bitrate (GBR bearers) and QoS Flows for which there is no guaranteed bitrate (non-GBR bearers).

4.3.3.2.3 QoS control at PDU Session level

It shall be possible for the PCF to provide the authorized Session-AMBR values, default 5QI/ARP combination for PDU Session of IP type, Ethernet type and unstructured type unconditionally or conditionally, i.e. per PDU Session type and/or RAT type.

It shall be possible for the PCF to request a change of the unconditional or conditional authorized Session-AMBR value(s) at a specific point in time.

4.3.3.3 Subscriber spending limits requirements

It shall be possible to enforce policies based on subscriber spending limits. The CHF shall maintain policy counter(s) to track spending for a subscription. These policy counters must be available in the CHF prior to their use over the N28 interface.

NOTE: The mechanism for provisioning the policy counters in the CHF is out of scope of this document.

The PCF shall request information regarding the subscriber's spending from the CHF, to be used as input for dynamic policy decisions for the subscriber, using subscriptions to spending limit reports. The CHF shall make information regarding the subscriber's spending available to the PCF using spending limit reports.

4.3.4 Usage monitoring control requirements

The requirements to monitor, both volume and time usage, and report the accumulated usage of network resources described in clause 4.4 of TS 23.203 [4] apply for PDU Sessions of type IP and Ethernet.

It shall be possible to apply usage monitoring for the accumulated usage of network resources on a per Session and user basis. This capability is required for enforcing dynamic policy decisions based on the total network usage in real-time.

The PCF that uses usage monitoring for making dynamic policy decisions shall set and send the applicable thresholds to the SMF for monitoring. The usage monitoring thresholds shall be based either on time, or on volume. The PCF may send both thresholds to the SMF. The SMF shall notify the PCF when a threshold is reached and report the accumulated usage since the last report for usage monitoring. If both time and volume thresholds were provided to the SMF, the accumulated usage since last report shall be reported when either the time or the volume thresholds are reached.

NOTE: There are reasons other than reaching a threshold that can cause the SMF to report accumulated usage to the PCF as defined in clauses 6.2.2.3.

The usage monitoring capability shall be possible for an individual or a group of service data flow(s), or for all traffic of a PDU Session in the SMF. When usage monitoring for all traffic of a PDU Session is enabled, it shall be possible to exclude an individual SDF or a group of service data flow(s) from the usage monitoring for all traffic of this PDU Session. It shall be possible to activate usage monitoring both to service data flows associated with predefined PCC rules and dynamic PCC rules, including rules with deferred activation and/or deactivation times while those rules are active.