3GPP TSG CN Plenary Meeting #15 **NP-020078**
6th – 8th March 2002. Cheju, Korea.

Source:	**TSG CN WG3**
Title:	**TS 29.207 V1.0.0 - Policy control over Go interface**
Agenda item:	**9.8**
Document for:	**INFORMATION**

3GPP TS 29.207 V1.0.0 (2002-02)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network;
Policy control over Go interface
(Release 5)

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword 5

1 Scope 6

2 References 6

3 Definitions and abbreviations 6
3.1 Definitions 6
3.3 Abbreviations 7

4 Go interface 7
4.1 Overview 7
4.2 Go reference model 9
4.3 Functional elements and capabilities 10
4.3.1 GGSN 10
4.3.1.1 Service-based local policy enforcement point 10
4.3.1.1.1 QoS Information processing 11
4.3.1.2 Initialisation and maintenance 11
4.3.1.3 Gate function 11
4.3.1.4 DiffServ edge function 12
4.3.1.5 Binding mechanism handling 12
4.3.2 PCF 12
4.3.2.1 Service-based local policy decision point 12
4.3.2.2 Initialisation and maintenance 12
4.3.2.3 Binding mechanism handling 12

5 Policy control procedures 13
5.1 GGSN 13
5.1.1 PDP context activation/modification 13
5.1.2 User plane operation 14
5.2 PCF 14
5.2.1 SBLP policy decisions 14

6 Go protocol 14
6.1 Protocol support 14
6.1.1 TCP connection for COPS protocol 14
6.1.2 COPS protocol 15
6.2 Basic COPS events/messages 15
6.2.1 Type of messages 15
6.3 Go events/messages 16
6.3.1 Event descriptions 16
6.3.1.1 Common Header, Client Type 16
6.3.1.2 Context Object 16
6.3.1.3 Client Specific Information (ClientSI) for outsourcing Operation 17
6.3.1.4 Reporting of Device Capabilities and Device Limitations 17
6.3.1.5 Initial UMTS Policy Provisioning 17
6.3.2 Message description 17
6.4 Go data 18

Annex A (informative): Information to be incorporated into other specifications 20

A.1 Capabilities of UE (TS27.060) 20
A.1.1 Binding mechanism 20
A.1.2 DiffServ edge function 20
A.1.3 RSVP/IntServ function 20
A.1.4 Pre-conditions for SIP QoS assured sessions 20

Annex B (normative): UMTS-Go PIB **21**

Annex C (informative): Change history **23**

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides the stage 3 specification of the Go interface. The functional requirements and the stage 2 specifications of the Go interface are contained in 3GPP TS 23.002 [2] and 3GPP TS 23.207 [3]. The Go interface is the interface between the GGSN and the Policy Control Function (PCF).

The present document defines:

- the protocol to be used between PCF and GGSN over the Go interface

- the signalling interactions to be performed between PCF and GGSN over the Go interface

- the information to be exchanged between PCF and GGSN over the Go interface

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 23.002: "Network Architecture"

[3] 3GPP TS 23.207: "End-to-end QoS Concept and Architecture"

[4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – stage 2"

[5] IETF RFC 2475: "An Architecture for Differentiated Services (Diffserv)"

[6] IETF RFC 2753: "A Framework for Policy-based Admission Control"

[7] IETF RFC 2748: "Common Open Policy Service protocol (COPS)"

[8] IETF RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)"

[9] IETF RFC 3159: "Structure of Policy Provisioning Information (SPPI)"

[10] IETF RFC 2205: "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification"

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply:

COPS Common Open Policy Service – The COPS protocol [7] is a simple query and response protocol that can be used to exchange policy information between a policy server (Policy Decision Point) and its clients (Policy Enforcement Points).

DiffServ Differentiated Services [5] – Diffserv networks classify packets into one of a small number of aggregated flows or "classes", based on the DiffServ codepoint (DSCP) in the packet's IP header. This is known as behaviour aggregate (BA) classification. At each DiffServ router, packets are subjected to a "per-hop behaviour" (PHB), which is invoked by the DSCP.

IP BS Manager The IP Bearer Service Manager uses standard IP mechanisms to manage the IP Bearer Service. It resides in the GGSN and optionally in the UE.

Go Interface Interface between P-CSCF (PCF) and GGSN [2].

PCF The Policy Control Function is a logical policy decision element that uses standard IP mechanisms to implement policy in the IP media layer. The PCF makes decisions in regard to network based IP policy using policy rules, and communicates these decisions to the PEP in the GGSN.

P-CSCF The Proxy Call Session Control Function is a network element providing session management services (e.g. telephony call control).

PEP The Policy Enforcement Point is a logical entity that enforces policy decisions made by the PCF. It resides in the IP BS Manager of the GGSN.

PIB The data carried by COPS-PR is a set of policy data. The protocol assumes a named data structure, known as a Policy Information Base (PIB), to identify the type and purpose of solicited and unsolicited policy information that is sent from the Policy Decision Point to the Policy Enforcement Point for provisioning policy or sent from the Policy Enforcement Point to the Policy Decision Point as a notification.

RSVP Resource ReSerVation Protocol – The RSVP [10] is used by a host to request specific qualities of service from the network for particular application data streams or flows. The network responds by explicitly admitting or rejecting RSVP requests.

Translation/mapping function This function provides the inter-working between the mechanisms and parameters used within the UMTS Bearer Service and those used within the IP Bearer Service.

UMTS BS Manager The UMTS Bearer Service Manager handles resource reservation requests from the UE. It resides in the GGSN and the UE.

3.3 Abbreviations

For the purposes of the present document, the abbreviations as specified in 3GPP TR 21.905 [1] and the following abbreviations apply:

COPS Common Open Policy Service protocol
COPS-PR COPS for policy provisioning
DEC COPS Decision message
DRQ COPS Delete Request State message
DSCP DiffServ Code Point
IMS IP Multimedia Core Network Subsystem
IntServ Integrated Services
PCF Policy Control Function
PEP Policy Enforcement Point
PHB Per Hop Behaviour
PIB Policy Information Base
PRC Provisioning Class. A type of policy data.
PRI Provisioning Instance. An instance of a PRC.
PRID Provisioning Instance Identifier - uniquely identifies an instance of a PRC.
REQ COPS Request message
RPT COPS Report State message

4 Go interface

4.1 Overview

The Go interface allows service-based local policy and QoS inter-working information to be “pushed” to or requested by the Policy Enforcement Point (PEP) in the GGSN from a Policy Control Function (PCF). As defined in the stage 2 specifications [3], this information is used by the GGSN to

- GPRS bearer authorisation,
- QoS charging related function

- Control of service-based policy "gating" function in GGSN,
- Control of DiffServ inter-working,
- Control of RSVP admission control and inter-working,

The Go interface uses IP flow based policies.

The Common Open Policy Service (COPS) protocol has been developed as a protocol for use between a policy server and a network device, as described in [7].

In addition, COPS for Provisioning extensions have been developed as described in [8] with [9] describing a structure for specifying policy information that can then be transmitted to a network device for the purpose of configuring policy at that device. The model underlying this structure is one of well-defined provisioning classes and instances of these classes residing in a virtual information store called the Policy Information Base (PIB).

The Go-interface shall conform to the IETF COPS [7] and the extensions of COPS-PR [8]. For the purpose of exchanging the required specific UMTS information, a COPS-PR Policy Information Based (PIB) is defined in the present document.

COPS Usage for Policy Provisioning (COPS-PR) is independent of the type of policy being provisioned (QoS, Security, etc.). In this specification, COPS-PR is used to communicate service-based local policy information between PCF and GGSN. COPS-PR can be extended to provide per-flow policy control along with a UMTS Go interface Policy Information Base (PIB). The UMTS Go PIB may inherit part of the data object definitions from the framework PIB and the DiffServ PIB defined in the IETF.

The minimum functionalities that the Go interface shall cover are introduced below.

- Media Authorisation information from PDP context

  The GGSN receives the binding information during the activation of a (Secondary) PDP context by the UE. To authorise the PDP context activation, the GGSN shall send a media authorisation request to the PCF. This authorisation request shall include the following information:

  - Binding information

  The binding information is used by the GGSN to identify the correct PCF and subsequently request service-based local policy information from the PCF.

  The media authorisation information sent by the PCF to the GGSN, contains at a minimum the following information:

  - Decision on the binding information

  The PCF shall respond with an authorisation decision for the binding information. The authorisation decision shall identify whether the binding information is validated with an ongoing SIP session. If validated, the PCF shall also communicate the following media authorisation details to the GGSN;

  - Authorised QoS
  - Packet Classifier

  This information is used by the GGSN to authorise the media resources according to the service-based local policy and the requested bearer QoS.

  The authorised QoS for media flows signalled over the Go interface is based on the SDP requirements signalled and agreed previously within SIP signalling for this session.

  The packet classifier for media flows is based on the IP-address and port number information in the SDP and shall allow for all flows associated with the SDP media description.

  The authorised QoS specifies the maximum QoS that is authorised for the UE for that specific binding information. The authorised QoS contains the following information:

  - Diff Serv class

Editor's note: DiffServ class is selected for the time being, DSCP or PHB are FFS.

- Data rate

Editor's note: The exact detail of this information is FFS.

- Charging correlation

The GGSN shall send the GPRS charging identifier of the PDP Context and the GGSN address to the PCF.

Editor's note: The additional charging correlation ID may be required. FFS. The timing for charging information to be available is FFS.

- Approval of QoS Commit / Removal of QoS Commit / Revoke Authorisation for GPRS and IP resources

The PCF controls media flows and may revoke resources at any time. Approval of QoS Commit / Removal of QoS Commit / Revoke Authorisation for GPRS and IP resources is communicated by the PCF to the GGSN.

- Indication of PDP Context Release / Modification

The GGSN informs the PCF of bearer changes related to the authorised resources for the IMS session in the following cases;

- Loss of radio contact (modification to 0 kbit/s for conversational and streaming class)
- Deactivation of PDP context

- Session modification handling
  - Case1: Change of media components within the authorized QoS

    The PCF updates the authorized information.

    The PCF closes old gates and opens new gates.

    Editor's note: Update of binding information or TFT is FFS.
  - Case2: Change of media components and the authorized QoS

    The PCF updates the authorized information including the change of QoS.

    The GGSN receives the PDP context modification and authorizes it according to available/requested policy decision.

    The PCF closes old gates and opens new gates.

    Editor's note: Update of binding information or TFT is FFS.

Editor's note: Currently CN3's working assumption is that "Session modification handling" is classed lower priority than the other identified items in this section.

4.2 Go reference model

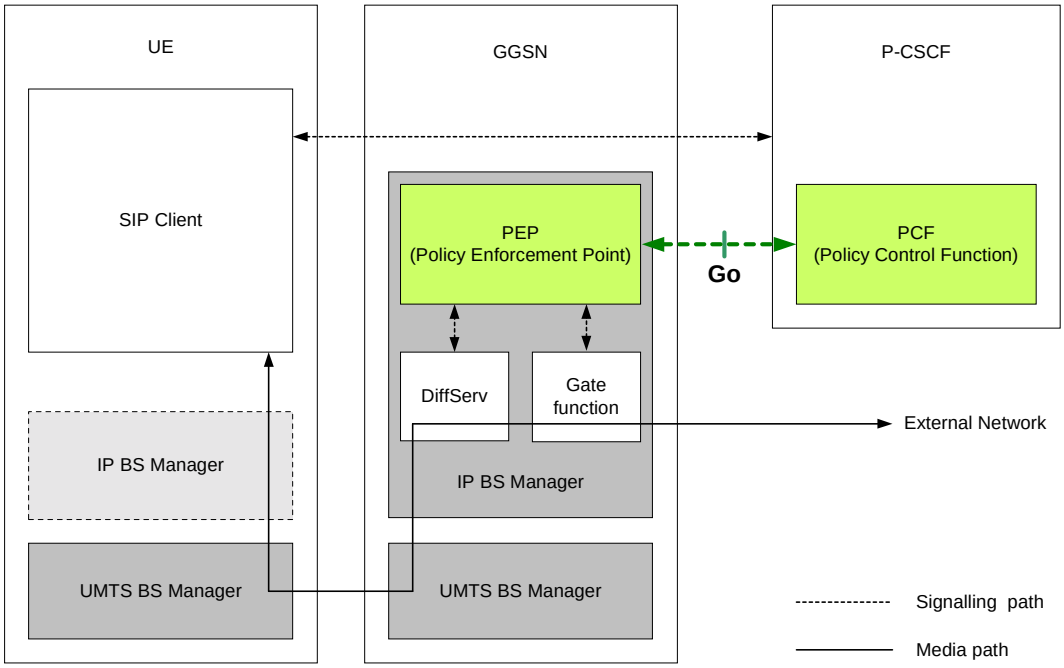
The Go interface is defined between the PCF and the GGSN [2].

The PCF is a logical entity of the P-CSCF (if the PCF is implemented in a separate physical node, the interface between the PCF and P-CSCF is not standardised).

The P-CSCF(PCF) is in the same PLMN as the GGSN.

Editor's note: The statement above is in line with TS 23.228 V 5.3.0, but not yet with 23.207 V 5.2.0.

The relationships between the different functional entities involved are depicted in Figure 4.2-1 below.



Editor's note: This figure has to be re-checked after all the texts in the other sections are provided. The necessity of inclusion of authorization function or charging boxes etc. has to be considered.

Note: For clarity in the diagram, network elements that are not involved in service-based local policy are not presented here (e.g. radio network elements, SGSN, etc).

Figure 4.2-1: Go interface architecture model

4.3 Functional elements and capabilities

4.3.1 GGSN

Editor's Note: This subclause provides the functional descriptions of capabilities of GGSN. It should be discussed whether the content of this subclause should be incorporated into 29.061 or 29.162, or should remain here.

4.3.1.1 Service-based local policy enforcement point

The Service-based Local Policy Enforcement Point (PEP) in the GGSN communicates with the PCF regarding Service-based local policy control. The PEP sends requests to and receives decisions from the PCF.

The PEP requests authorisation information from PCF for the media flows carried by a PDP context. The PEP enforces the PCF decisions related to the media flows carried by a PDP context. The PEP shall also report to the PCF its success or failure in carrying out the PCF decision.

The PEP includes policy-based admission control that is applied to the bearers associated with the media flows, and configures the policy based "gating" functionality in the user plane.

Policy-based admission control ensures that the GPRS bearer carrying media flows, which is activated in the GGSN, is authorised by the PCF decision.

Additionally, policy-based admission control ensures that the resources, which can be used by each particular media flow, are within the "authorised QoS" specified by the PCF. This information is mapped by the Translation/mapping function in the GGSN to give the authorised resources for GPRS bearer admission control.

Editor's note: the exact format for representing the "authorised QoS" is for further study

Policy based gating functionality represent the control of the PEP over the Gate Function in the user plane, i.e. the forwarding of IP packets associated with a media component. In the user plane, a “gate” is defined for each direction of a media component. The PCF provides the gate description and the commands to open or close the gate. The gate description is received from the PCF in the authorisation decision. The command to open or close the gate shall be sent either in the authorisation decision or in subsequent decisions from the PCF.

4.3.1.1.1 QoS Information processing

The PEP in the GGSN is responsible for the policy based admission control, i.e., to ensure that the requested QoS is in-line with the authorized QoS.

The PEP needs the authorised IP QoS information of the PDP context for the uplink as well as for the downlink direction. Therefore, the IP QoS information for the combination of all IP flows of each direction associated with the media component is used.

Editor’s note: The entity to perform the combination of IP flows is FFS.

Editor’s note: The rules for combination of QoS information is FFS. It may be documented in TS 29.208

In case of an aggregation of multiple media components within one PDP context the IP QoS information related to the combination of the authorized IP QoS information of the IP flows of the individual media components is used.

The GGSN shall perform the proper mapping between the IP QoS information and the UMTS QoS information. This mapping is performed by the Translation/mapping function which maps the authorised IP QoS information for the PDP context into authorised UMTS QoS information.

The UMTS BS Manager receives the authorised UMTS QoS information for the PDP context from the Translation/mapping function. If the requested QoS exceeds the authorised QoS it may either reject the activation/modification of the PDP context or downgrade the requested UMTS QoS information to the authorised UMTS QoS information.

4.3.1.2 Initialisation and maintenance

Editor’s note: This describes the initialisation and maintenance of the COPS protocol over Go interface. It may be simplified by referring to IETF RFC.

4.3.1.3 Gate function

The Gate Function represents a user plane function enabling or disabling the forwarding of IP packets. A gate is described by a set of packet classifiers that identify IP flows associated to the gate. The packet classifier includes the standard 5-tuple (source IP address, destination IP address, source port, destination port, protocol) explicitly describing a unidirectional IP flow. Wildcarding of fields shall be possible.

Editor’s note: The knowledge of the source IP address/port is FFS. Wildcarding is FFS.

Editor’s note: The impact of a packet classifier containing incomplete information are FFS (because SDP conveys only the destination IP address and port number).

The packet classifier is received from the PCF in an authorisation decision. The PEP installs the packet filter applying the packet classifier. After installation of the packet filter the gate shall be closed until the PEP receives a command to open the gate.

Editor’s note: The timing of the gating in relation with charging is for further study.

The commands to open or close the gate lead to the enabling or disabling of the passage for IP packets. If the gate is closed all packets of the related IP flows are dropped. If the gate is opened the packets of the related IP flows are allowed to be forwarded. The PCF may send these commands together with an authorisation decision or in subsequent decisions.

IP Packets of a PDP context not matching any packet classifier associated with this PDP context shall be dropped.

If the packet classifer is included as an additional IE in the authorisation information, the GGSN shall check for validity of the TFT in the Create PDP Context Request or Update PDP Context Request. If the TFT proposed will result in packets from the media flow being unable to pass through, the PDP context will be rejected with cause value indicating a semantic error in the TFT.

Editor's note: This issue should still be discussed in SA2.

4.3.1.4 DiffServ edge function

Editor's Note: This subclause describes the functionality of "DiffServ Edge Function" in GGSN.

4.3.1.5 Binding mechanism handling

The GGSN shall determine the IP address of the PCF from the PCF identifier received as part of the Authorization Token. This identifier shall be in the format of a fully qualified domain name.

The binding information associates a PDP context with one or more media components of an IMS session. The GGSN receives the binding information during an activation/modification/deletion of a (secondary) PDP context. The binding information consists of an authorisation token and a flow identifier. If there is more than one media component to be transported within the PDP context the binding information includes one flow identifier for each of the media components.

The PEP shall forward the binding information received from the UE to the PCF.

The PEP shall store the binding information and apply it to correlate events and actions between the PDP context and the service-based local policy.

4.3.2 PCF

Editor's Note: This subclause describes the overview of PCF.
For example, Policy Control Function (PCF) is a logical policy decision element which uses standard IP mechanisms to implement policy in the IP bearer layer…

4.3.2.1 Service-based local policy decision point

The PCF receives session and media related information from the P-CSCF. The P-CSCF forwards this information out of every SDP it receives together with an indication about the source of this SDP, i.e. originating or terminating side.

Note: The exact information (e.g. IP addresses, port numbers, media types, bandwidth information) is FFS.

All media components for which the PCF received information from both sides are authorised. That means, for each media component the authorised QoS and gate information of all associated IP flows is available.

Editor's note: Identification of associated IP flows is FFS.

Editor's note: The study of multiple codecs is still FFS.

4.3.2.2 Initialisation and maintenance

Editor's note: This describes the initialisation and maintenance of the COPS protocol over Go interface. It may be simplified by referring to IETF RFC.

4.3.2.3 Binding mechanism handling

The PCF shall allocate its PCF identifier as part of the Authorization Token. This identifier shall be in the format of a fully qualified domain name.

Editor's note: This will be updated depending on the CN1's decision.

The PCF receives the binding information and a Client Handle as part of a REQ from the GGSN. The PCF shall store the Client Handle for each media component identified by the binding information for subsequent message exchanges.

The binding information consists of an authorisation token and a flow identifier. The binding information can also include more than one flow identifier.

The authorisation token is applied by the PCF to identify the IMS session. If no IMS session can be found for an authorisation token, the GGSN is informed that the authorisation token is invalid.

For a valid authorisation token the flow identifier is used to select the available information on the media component of this IMS session. The PCF sends the available information on the media component back to the GGSN.

If the binding information consists of more than one flow identifier, the available information is selected and sent back to the GGSN for each of the media components.

5 Policy control procedures

Editor's Note: This clause is designated to provide all necessary specification for procedures with interaction with the Go interface.

5.1 GGSN

Editor's Note: This subclause describes the service-based local policy control procedures in the GGSN.

5.1.1 PDP context activation/modification

Editor's Note: This subclause describes the actions in the GGSN when a PDP context activation/modification occurs where there are SBLP operations. It is proposed that this should include the termination/modification to 0kb/s too, although this could possibly be placed into a separate chapter.

The GGSN receives binding information during the activation/modification of a (Secondary) PDP context by the UE. To authorise the PDP context activation/modification the GGSN shall send an authorisation request to the PCF including the binding information received from the UE.

To ensure charging correlation, the GGSN shall send the GPRS Charging ID and GGSN address information to the PCF.

Editor's note: The exact timing and COPS messages for transporting the GPRS Charging ID is for further study.

The GGSN authorisation request message to the PCF shall allow the Service-based Local Policy Enforcement Point to request policy information for authorisation of the media flows carried by a PDP context identified by binding information.

When the GGSN receives the PCF decision regarding authorisation of the media flows, the Service-based Local Policy Enforcement Point shall enforce the policy decision.

If the PCF decision information indicates that the binding information provided by the GGSN is associated with an ongoing SIP session at IMS level, the GGSN shall proceed with activation of the PDP context. The PEP in the GGSN shall map the authorized QoS resources into authorized resources for the bearer admission control.

When the PCF decision information indicates that the binding information provided by the GGSN is not associated with an ongoing SIP session at application layer, then the GGSN may reject the PDP context request.

Editor's note: the exact GGSN action when the binding information provided by the GGSN is not associated with an ongoing SIP session at application layer is for further study.

When revoke authorisation for GPRS and IP resources is performed, the GGSN receives a decision message from the PCF for disabling the use of the authorised QoS resources and deactivation of the PDP context associated with the binding information. The GGSN shall initiates deactivation of the PDP context used for carrying these media flows, if this has not occurred already.

The PEP in the GGSN is responsible for notifying the PCF when a procedure of PDP Context release or modification is performed. In case of indication of PDP context release, the PEP shall inform the PCF of bearer release related to the SIP session. In case of indication of PDP context modification, the PEP shall inform the PCF of the bearer changes, as

bandwidth modification to 0, and the PEP may inform the PCF of the bearer changes or if the modified QoS for the bearer is more than authorised QoS by the PCF.

Editor's note: This has dependency to offline discussion regarding the modification of PDP context.

5.1.2 User plane operation

Editor's Note: This subclause describes the actions in the GGSN to apply gating/filters received from the PCF to the received traffic.

The PEP shall enforce the configuration of the policy based "gating" functionality according to additional authorisation information received from the PCF.

Editor's note: the exact GGSN action if the "gating" parameters provided by the PCF are not identical with the parameters from the TFT in the PDP context request is for further study.

5.2 PCF

Editor's Note: This subclause describes the SBLP procedures in the P-CSCF/PCF.

5.2.1 SBLP policy decisions

Editor's Note: This subclause describes the operation in the PCF to receive data from the P-CSCF on which to base decisions, receive authorisation requests from the GGSN, and to send authorisation decisions to the GGSN. This may include the charging correlation aspects, or this may be a separate chapter.

The information needed for the PCF to perform media authorization is passed by the P-CSCF upon receiving a SIP message that contains SDP. The SDP contains sufficient information about the session, such as the end-points' IP address and port numbers and bandwidth requirements.

The P-CSCF shall send policy setup information to the PCF upon every SIP message that includes an SDP payload. This ensures that the PCF passes proper information to perform media authorization for all possible IMS session setup scenarios.

The media authorization information will be performed based on the SDP in PRACK in regular session setup; or based on the SDP in 183 in case that PRACK does not contain any; or based on the SDP in the 200 OK for PRACK if included.

Upon receiving the bearer authorization request from the GGSN, the PCF shall authorize the request according to the stored service based local policy information for the session identified by the binding information in the request.

The PCF may make a final decision to enable the allocated QoS resource for the authorized media stream. (Open the gate). This may be triggered by the receipt of the SIP 200 OK (to the INVITE request) in the P-CSCF. The QoS resources may also be enabled at the time they are authorized by the PCF.

6 Go protocol

Editor's Note: This subclause describes the information exchanged via Go interface

6.1 Protocol support

Editor's Note: This subclause describes the COPS protocol support for Go interface.

6.1.1 TCP connection for COPS protocol

To ensure the real-time characteristics of the Go interface, the COPS interactions shall be based on pre-established TCP/IP connections

6.1.2 COPS protocol

The Go interface allows service-based local policy and QoS inter-working information to be "pushed" to or requested by the GGSN from a Policy Control Function (PCF)

The Common Open Policy Service (COPS) protocol supports a client/server interface between the Policy Enforcement Point in the GGSN and Policy Control Function (PCF). The Go interface shall conform to the IETF COPS framework as a requirement and guideline for Stage 3 work.

The COPS protocol allows both push and pull operations. For the purpose of the initial authorisation of QoS resources the pull operation shall be used. Subsequently the interactions between the PCF and the GGSN may use either pull or push operations.

Policy decisions may be stored by the COPS client in a local policy decision point allowing the GGSN to make admission control decisions without requiring additional interaction with the PCF.

The COPS client (PEP) can request a policy decision from the PCF triggered by a QoS signalling request. One PEP request may be followed by one or more asynchronous PCF decisions. Each of the decisions will allow the PCF to notify the PEP in the GGSN whenever necessary to change earlier decisions, generate errors etc.

Protocol stack: IP, TCP and COPS

6.2 Basic COPS events/messages

Editor's Note: This sections describes the basic Go operation aspects eg initialisation messages. May use a sub-section for each event/message description.

The Go interface supports information passed between the GGSN and PCF. In order to allow effective communication between PCF and GGSN, all events associated with control functions are required:

- Coordination of events between the application layer and resource management in the IP bearer layer,

The specific events to the UMTS or IP bearer service are required in order to trigger the request from GGSN to PCF.

6.2.1 Type of messages

Editor's Note: This subclause describes the type of messages to be supported.
For example,
– Client-Open/Client-Accept/Client-Close,
– Request,
– Decision,
– Report State,
– Delete Request State,
– Keep Alive,
– Synchronize State Request/Synchronize State Complete.

The COPS protocol supports several messages between GGSN and PCF. The message content is dependent on the type of COPS operation (e.g. Client-Open/Client-Accept/Client-Close, Request, Decision and Delete Request State).

The Client Open, Client Accept, Client Close, Keep Alive, Synchronize State Request and Synchronize State Complete messages are used for setting up and maintaining the connection between the PCF and PEP [1].

The following messages supported by the COPS layer for Go interface are used for the policy control operations:

- **Request message (REQ)** from the GGSN to the PCF is used by the GGSN to request policy and QoS inter-working information for an IP flow identified by binding information. The binding information associates the policy and QoS inter-working information in the message with a PDP context including PCF address. The binding information includes an authorization token sent by the PCF to the UE during SIP signalling and may include one flow identifier used by the UE, GGSN and PCF to uniquely identify an IP media flow.

- **Decision (DEQ)** message from the PCF to the GGSN is a response to the Request message. The Decision message is used for "Authorize QoS/Revoke QoS authorization" for one or more IP flows, for

"Enable/Disable forwarding" for one or more IP flows and for asynchronous notification from PCF to the GGSN whenever necessary in order to change earlier decisions, generate errors, etc.

- **Report State (RPT)** message is from the GGSN to the PCF is used to communicate the success or failure of the GGSN in carrying out the PCF's decision indicated in the Decision message.

- **Delete Request State (DRQ)** message from the GGSN to the PCF indicates that the state identified by the client handle is no longer available/relevant and the corresponding state may be removed from the PCF.

6.3 Go events/messages

Editor's Note: This sections describes the Go events/messages which are specific for the Go interface. May use a sub-section for each event/message description.

The UMTS-specific information is carried in specific COPS-PR objects, as defined in the UMTS-Go PIB that is given in Annex B.

Editor's Note: The details of the UMTS specific objects in the UMTS-Go PIB are still under discussion in TSG CN3. The resulting work will be documented in annex B. Annex B will be the basis for the UMTS-Go PIB specification.

6.3.1 Event descriptions

Editor's note: The title of this section was originally "COPS-PR Usage for UMTS Go Interface & UMTS-specific Information in COPS-PR".

The Go Interface uses COPS-PR [8] schematics and the UMTS Go PIB. For COPS-PR to support the Outsourcing Model it is required to add a new UMTS Go PIB with objects to:

-Describe the Triggering Event Handling.

-Describe the Outsourcing Event.

-Describe the Decision for the Outsourced Event.

-Describe the Termination of the Outsourced Event.

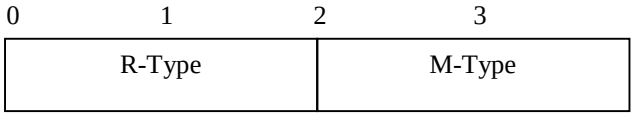
-Describe the resource used for the Outsourced Event.

6.3.1.1 Common Header, Client Type

Client-type is UMTS Go (Client type number to be assigned through IANA)

6.3.1.2 Context Object

C-Num = 2, C-Type = 1



R-Type (Request Type Flag)

M-Type (Message Type)

Editor's note: The required types of R-Type and M-Type have to be studied. M-type is dependent on the application which is defined above.

6.3.1.3 Client Specific Information (ClientSI) for outsourcing Operation

The Token and flow identifier(s) received in the incoming message at the GGSN is encapsulated inside the Client Specific Information object of the COPS request message sent from the GGSN to the PCF. The parameters describing the requested QoS may also be contained inside the Client SI object.

6.3.1.4 Reporting of Device Capabilities and Device Limitations

The functionality of reporting of device capabilities and device limitations is as described in RFC3084 [8]. In addition, the following shall apply:

The configuration request message serves as a request from the GGSN to the PCF and include provisioning client information to provide the PCF with client-specific configuration or capability information about the GGSN. This information from the client assists the server in deciding what types of policy the GGSN can install and enforce.

The PCF responds to the configuration request with an initial DEC message.

Editor's note: It has to be checked whether the device capabilities information exchanged by the initial messages shall be stored in the PCF.

Editor's note: Some texts are required to describe usage of data defined by the Go PIB.

Editor's note: The R-Type and M-Type is FFS.

6.3.1.5 Initial UMTS Policy Provisioning

The functionality of initial UMTS policy provisioning is as described in RFC3084 [8]. In addition, the following shall apply:

The DEC message is sent from the PCF to the GGSN in response to the REQ message received from the GGSN. The Client Handle shall be the same as that received in the corresponding REQ message.

The DEC message is sent as an immediate response to a configuration request with the solicited message flag set in the COPS message header. The PCF informs the GGSN of the capabilities that it supports.

Editor's Note: The R-Type and M-Type is FFS.

6.3.2 Message description

The Go interface uses the COPS-PR protocol. The following messages shall be supported:

Editor's Note – Require text providing a description of COPS protocol, or reference to IETF protocol.

Editor's Note – Require text to describe how to talk about our application events/messages (as compared to the protocol messages).

Editor's Note: The R-Type and M-Type is FFS.

The following events are available on the Go interface:

- Authorisation_Request

This event allows the GGSN to request authorisation details from the PCF. It contains the following information:

  - Client Handle
  - Binding Information
  - Charging Correlation Identifier

- Authorisation_Decision

This event provides the GGSN with the authorisation status, and relevant authorisation decision data if applicable. The event contains the following information:

  - Authorisation status
  - Authorised QoS
  - Packet classifier

- Start packet flow

This event indicates to the GGSN that the gate for a media component flow(s) shall be opened. The event contains the following information:

  - Client Handle

Editors note: Additional information required is FFS

Note: the opening of the gate may occur at the same time/be part of the authorisation decision event.

- Stop packet flow

This event indicates to the GGSN that the gate for a media component flow(s) shall be closed. The event contains the following information:

  - Client Handle

Editors note: Additional information required is FFS

Note: The closing of the gate may occur at the same time as the revoke authorisation decision event.

Editors note: This list is not complete and additional events are FFS

6.4 Go data

Editor's Note: This section describes relevant detailed structure and data format of each data element. May use a sub-section for each data element.

The detailed data description is provided in Annex B.

Editor's Note: This remainder of this chapter contains agreed detail message and data element format descriptions for the protocol prior to being defined in the PIB (Annex B). As the messages/data definitions are completed in the PIB, it shall be removed from here. Data shall not be removed from here until it is complete. Messages/data in the PIB which are not yet completed shall be clearly marked.

- Client Handle - a unique identifier for the authorisation request. The format of the Client Handle is FFS.
- Binding information - A data element from the PCF that identifies (at a minimum):
  - The PCF identity
  - The authorisation token for the session
  - The flow id(s) within the session

Editor's note: The format of the binding information is FFS.

- Authorisation Status – The authorisation status for the specified binding information. The status shall contain a valid/invalid indicator. The format of the authorisation status is FFS.
- Charging identifier – The charging identifier of the PDP context. The specific details of the charging identifier is FFS. Further information on the charging identifier is required from S2.
- Authorised QoS – The authorised QoS contains the maximum allowed class, and the bandwidth information.
  - Maximum allowed class – Format is FFS. Proposed to use a DSCP element from the DiffServ PIB.

  - Data rate - Format is FFS. Proposed to be based on qosTBParamRate from DiffServ PIB. The size and format of the element though shall be considered to ensure it is not unreasonable for use in 3GPP.

- Filter Specification – The information about the authorised IP end points addresses and ports. Format is FFS.

Annex A (informative): Information to be incorporated into other specifications

Editor's Note: The content of this annex will be incorporated into other specifications and deleted from here before publication.

A.1 Capabilities of UE (TS27.060)

Editor's Note: This clause describes the functional descriptions of capabilities of UE to be incorporated into e.g. TS27.060.

A.1.1 Binding mechanism

Editor's Note: This subclause describes the functionality of "Binding Mechanism" in UE.

A.1.2 DiffServ edge function

Editor's Note: This subclause describes the functionality of "DiffServ Edge Function" in UE.

A.1.3 RSVP/IntServ function

Editor's Note: This subclause describes the functionality of "RSVP/IntServ Function" in UE.

A.1.4 Pre-conditions for SIP QoS assured sessions

Editor's Note: This subclause describes the functionality of "Pre-conditions for SIP QoS Assured Sessions" in UE.

Annex B (normative): UMTS-Go PIB

Editor's Note: The content of this annex provides a skeleton for the definition of the UMTS Go PIB. The naming of each of the elements has to be revisited in order to include that they are related to Go interface. Rephrasing of UMTS to 3GPP has to be checked (can the name start with a digit?)

UMTS Go PIB PIB-DEFINITIONS

- IMPORTS
- uMTSGoPib MODULE-IDENTITY
- DESCRIPTION - "A PIB module containing the set of provisioning classes that are required for support of policies for UMTS subject-categories' Go interface."
- ORGANIZATION "3GPP CN3 WG"
- IANA.

The root OID for PRCs in the UMTS Go PIB

- uMTSCapabilityClasses
- uMTSEventPolicyClasses
- uMTSEventClasses
- uMTSConformance

UMTS Capability and Limitation Group

Capability and Limitation Policy Rule Classes

- To complete

UMTS Capability Base Table

- uMTSBaseCapsTable
- uMTSBaseCapsEntry "An instance of the uMTSBaseCaps class that identifies a specific PRC and associated attributes as supported by the device."

Component Limitations Table

- To complete - This table supports the ability to export information detailing provisioning class/attribute implementation limitations to the policy management system.

UMTS Event Group

UMTS Event Policy Classes

- To complete

UMTS Event Policy Base Table

- uMTSBaseEventPolicyTable
- uMTSBaseEventPolicyEntry "An instance of uMTSBaseEventPolicy identifying types of events to watch for and how to handle such events."

UMTS PDP Context Event Handler Provisioning Table

- uMTSPdpContextPolicyTable
- uMTSPdpContextPolicyEntry " An instance of the uMTSPdpContextPolicy describing how to handle a PDP Context Event."
- UMTSPdpContextPolicyEntry

RSVP Event Handler Provisioning Table

- To complete

UMTS Event Classes

- To complete

UMTS PDP Context Event Table

- uMTSPdpContextEventTable
- uMTSPdpContextEventEntry
- UMTSPdpContextEventEntry
    - uMTSPdpContextEventToken "The token associated with this PDP Context event."
    - uMTSPdpContextEventFlowIds "References the FlowIds associated with the Token indicated in this PDP Context event."

UMTS PDP Context FlowID Table

- uMTSPdpContextFlowIdTable
- uMTSPdpContextFlowIdEntry
- UMTSPdpContextFlowIdEntry
    - uMTSPdpContextFlowIdId "The FlowId itself."
    - uMTSPdpContextFlowIdsNext "References the next FlowId in the list associated with the same Token of a PDP Context event."

Conformance Section

Editor's Note: This is the section of the PIB to allow indication of the minimum requirements for conforming to this standard. More advanced features can be indicated in the PIB and they can be indicated as optional, while the basic features are required to conform to the standard and required for inter-operability. This section should be used, as a tool to achieve inter-operability while it does not limit the progress of technology.

Security considerations

The security mechanisms described in COPS [7] and COPS-PR [8] are re-used in 3GPP. No security concerns have been identified beyond those that the COPS base protocol security have already addressed and provide the necessary protection against security threats.

Annex C (informative): Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
10/07/01		N3-010284			Version 0.0.0 presented to CN3 #18 – Dresden	x.y.z	0.0.0
18/07/01		N3-010335			Tdocs N3-010286 and N3-010325 are agreed at CN3 #18 – Dresden, Germany and incorporated. Raised to Version 0.1.0.	0.0.0	0.1.0
18/10/01		N3-010480			Tdoc N3-010460 is agreed at CN3 #19 – Brighton, U.K. and incorporated. Deletion of section 5.4 is also agreed. Raised to Version 0.2.0.	0.1.0	0.2.0
29/11/01		N3-010577			Tdocs N3-010574, N3-010573, N3-010546, N3-010553, and N3-010525 are agreed with some modifications at CN3 #20 – Cancun, Mexico and incorporated. Raised to Version 0.3.0.	0.2.0	0.3.0
30/11/01		N3-010611			Tdoc N3-010547 is agreed at CN3 #20 – Cancun, Mexico and incorporated. Raised to Version 0.4.0.	0.3.0	0.4.0
30/11/01		N3-010614			The figure 4.2-1 is modified based on comments. Raised to Version 0.5.0.	0.4.0	0.5.0
01/02/02		N3-020120			Tdoc N3-020028 and N3-020109 are agreed at CN3 #21 – Sophia Antipolis, France and incorporated. Raised to Version 0.6.0.	0.5.0	0.6.0
25/02/02		N3-020157			Tdoc N3-020152, N3-020132, N3-020129, N3-020145, N3-020133, N3-020130, N3-020156, N3-020126, N3-020137, N2-020128, N3-020136 and N3-020138 are agreed with some modifications at Go drafting session in CN3 #21 Bis – Sophia Antipolis, France and incorporated. Raised to Version 0.7.0.	0.6.0	0.7.0
27/02/02		N3-020158			Tdoc N3-020151 (restructuring), N3-020160, and N3-020159 are agreed with some modifications at Go drafting session in CN3 #21 Bis – Sophia Antipolis, France and incorporated. Raised to Version 0.8.0.	0.7.0	0.8.0
27/02/02		N3-020166			Tdoc N3-020163 (additions to gate function) and N3-020161 (UMTS Go PIB) are agreed with some modifications at last day of CN3 #21 Bis – Sophia Antipolis, France and incorporated. Raised to Version 0.9.0.	0.8.0	0.9.0
27/02/02		N3-020168			Addition of security consideration regarding the UMTS Go PIB. Raised to Version 0.9.0.	0.9.0	0.10.0
2002-02					Some editorial cleaning - presented to NP#15 for information	0.10.0	1.0.0

Editor: Daisuke Yokota <yokota@lucent.com>