ETSI TS 123 125 V6.3.0 (2004-12)

Technical Specification

Universal Mobile Telecommunications System (UMTS); Overall high level functionality and architecture impacts of flow based charging; Stage 2 (3GPP TS 23.125 version 6.3.0 Release 6)

Reference
DTS/TSGS-0223125v630

Keywords
UMTS

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2004.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 5
1 Scope 6
2 References 6
3 Definitions, symbols and abbreviations 6
3.1 Definitions 6
3.2 Symbols 7
3.3 Abbreviations 7
4 General Requirements 8
4.1 General 8
4.2 Backwards compatibility 8
4.3 Charging models 9
4.3.1 General 9
4.3.2 Examples of Service Data Flow Charging 9
5 Flow Based Charging Concepts 10
5.1 Overview 10
5.2 Charging rules 10
5.3 Service data flow filters and counting 12
5.4 Reporting 13
5.5 Credit management 13
5.6 Termination Action 14
5.7 Re-authorisation and Event Triggers 14
5.8 Policy functions provided by FBC architecture 15
5.8.1 General 15
5.8.2 Charging correlation 15
5.8.3 Gating 15
5.8.4 QoS control 16
5.8.5 Bearer events 16
5.8.6 Session events 16
6 Architectural concepts 16
6.1 Architecture 16
6.1.1 Online service data flow based bearer charging architecture 16
6.1.2 Offline service data flow based bearer charging architecture 17
6.2 Functional Entities 18
6.2.1 Based Charging Rules Function 18
6.2.2 Service Data Flow Based Credit Control Function 18
6.2.3 Charging Collection Function 18
6.2.4 Traffic Plane Function 18
6.2.5 Application Function 20
6.2.6 Relationship between functional entities 20
6.3 Reference points 20
6.3.1 Gx reference point 20
6.3.1.1 Initialisation and Maintenance of Gx Connection 21
6.3.1.2 Request for Charging Rules (from TPF to CRF) 21
6.3.1.3 Provision of Charging Rules (from CRF to TPF) 21
6.3.1.4 Indication of Bearer Termination (from TPF to CRF) 22
6.3.2 Gy reference point 22
6.3.3 Gz reference point 22
6.3.4 Rx reference point 22
6.3.4.1 General 22
6.3.4.2 Initialisation and Maintenance of Rx Connection 22

6.3.5 Ry reference point 22

7 Message Flows 23
7.1 AF input to provision of charging rules..23
7.2 Bearer events 24
7.2.1 Bearer Service Establishment 24
7.2.2 Bearer Service Modification 25
7.2.2.1 General..25
7.2.2.2 Bearer Service Modification in case of offline charging..26
7.2.2.3 Void..27
7.2.2.4 Bearer Service Modification in case of online charging 27
7.2.3 Bearer Service Termination 28
7.3 Provision of Charging Rules triggered by other event to the CRF 30

Annex A (informative): Overall architectural impacts of IP flow based charging..........................31

A.1 GGSN in HPLMN..31

A.2 Comparison of S-CDR and G-CDR fields 31
A.2.1 S-CDR information missing from G-CDR..31
A.2.2 Served IMEI 31
A.2.3 MS Network Capability..32
A.2.4 LAC/RAC/CI at “record opening” 32
A.2.5 Access Point Name Operator Identifier..32
A.2.6 System Type..32
A.2.7 CAMEL information 33
A.2.8 RNC unsent data volume..33
A.2.9 Time zone of the user’s location 33

A.3 RADIUS attributes 34

Annex B (informative): IMS and Flow based charging 35

B.1 IMS SIP signalling 35

B.2 IMS media..35

B.3 FBC with IMS compared to rel5 IMS charging correlation..37

B.4 Rx/Gx functions and SBLP usage 37

Annex C (informative): WLAN and flow based charging 41

C.1 TPF usage for WLAN 41

Annex D (informative): Policy functions provided by FBC architecture..42

D.1 General 42

D.2 General architectural considerations 42
D.2.1 Charging correlation..42
D.2.2 Gating..43
D.2.3 QoS control 43
D.2.4 Bearer events..43
D.2.5 Session events 44

D.3 Summary and comparison..44

Annex E (informative): Change history 46

History 48

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 specifies the overall high level functionality and architecture impacts of Flow Based Charging.

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 41.001: "GSM Release specifications".

[2] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[3] 3GPP TS 32.200: "Charging Principles".

[4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem - Stage 2".

[5] 3GPP TS 23.002: "Network architecture".

[6] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[7] 3GPP TS 32.225: “Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)”.

[8] 3GPP TS 23.078: “Customised Applications for Mobile network Enhanced Logic (CAMEL); Stage 2”.

[9] Diameter Credit-Control Application, draft-ietf-aaa-diameter-cc-06.txt, work in progress

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[10] 3GPP TS 23.234: “3GPP system to Wireless Local Area Network (WLAN) Interworking”

[11] 3GPP TR 33.919: “Generic Authentication Architecture (GAA)”

[12] 3GPP TS 23.207: “End-to-end Quality of Service (QoS) concept and architecture”

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 21.905 [2] and in TS 32.225 [7] and the following apply:

Charging key: information used by the online and offline charging system for rating purposes.

Charging rule: a set of information including the service data flow filters, and the charging key, for a single service data flow (further details can be found in 5.2).

Dynamic charging rule: Charging rule where some of the data within the charging rule (e.g. service data flow filter information) is assigned via real-time analysis, which may use dynamic application derived criteria.

FBC Policy Functions: The charging rules may be configured in such a way to allow FBC for a certain usage that allows/disallows traffic to pass through the TPF (further details can be found in 5.8).

IP network connection: The unique UE association with an IP network (for GPRS, APN) and the allocated IP address at the TPF.

Packet flow: a specific user data flow carried through the TPF. A packet flow can be an IP flow.

Predefined charging rule: A charging rule which is predefined in the TPF. A predefined charging rule is either applicable for all bearers of all users or dynamically activated for an individual bearer.

Service identifier: An identifier for a service. The service identifier may designate an end user service, a part of an end user service or an arbitrarily formed group thereof. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow.

Service data flow: aggregate set of packet flows. In the case of GPRS, it shall be possible that a service data flow is more granular than a PDP context.

Service Data Flow Filter: a set of filter parameters used to identify one or more of the packet flows constituting a service data flow. At least the following means for the packet flow identification shall be supported: source and destination IP address+port, transport protocol, or application protocol.

TPF/CRF dialogue: A dialogue, between a TPF and a CRF, with a unique identity, There is one TPF/CRF dialogue per user and IP network connection.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Application Function
CCF	Charging Collection Function
CDR	Charging Data Records
CRF	Charging Rules Function
CSCF	Call Session Control Function
FBC	Flow Based Charging
FTP	File Transfer Protocol
G-CDR	GGSN generated CDR
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
gsmSCF	GSM Service Control Function
HPLMN	Home PLMN
HTTP	Hypertext Transfer Protocol
I-CSCF	Interrogating CSCF
IM	IP Multimedia
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identity
OCS	Online Charging System
P-CSCF	Proxy-CSCF
PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
QoS	Quality of Service
SAI	Service Area Identity
S-CDR	SGSN generated CDR
S-CSCF	Serving-CSCF
SBLP	Service Based Local Policy

SDF	Service Data Flow
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
TPF	Traffic Plane Function
UE	User Equipment
WAP	Wireless Application Protocol
WLAN	Wireless LAN

4 General Requirements

4.1 General

The current level of traffic differentiation and traffic-type awareness of the GPRS architecture shall be extended beyond APN and PDP Context level. It shall be possible to apply differentiated charging for the traffic flows belonging to different services (a.k.a. different service data flows) even if they use the same PDP Context.

In addition, it shall be possible to apply differentiated charging for the traffic flows belonging to different services carried by other IP Connectivity Access Networks (IP-CANs).

Charging and tariffing models described in this Technical Specification shall be possible to be applied to both prepaid and postpaid subscribers, i.e. to both online and offline charging.

Online and offline are not the same as prepaid and postpaid (see TS 32.225 [7]). For example it is worth highlighting that the operator can have postpaid subscribers on credit control by using on-line charging mechanisms.

The GPRS online charging solutions up to release 5 are built around CAMEL mechanisms that provide online access- and charging-control for GPRS - pertaining to PDP Contexts of an APN.

The flow based charging architecture developed in this Technical Specification shall use generic native IP charging mechanisms to the extent possible in order to enable the reuse of the same charging solution and infrastructure for different type of IP-Connectivity Networks.

Note: Providing differentiated service data flow based charging is a different function from providing differentiated traffic treatment on the IP-flow level. The operation of service data flow based charging shall not mandate the operation of service based local policy.

In addition charging based on specific application services or protocols shall be supported.

4.2 Backwards compatibility

The capabilities of the enhanced architecture introduced with flow based charging shall be backwards compatible with the release 5 charging capabilities. These new functions shall be compatible and coherent with the authentication, authorization, PDP context management, roaming and other functions provided by the release 5 architecture.

It shall be possible to collect data volumes per PDP context for use in billing and operational management systems.

Flow based charging is assumed to provide complete coverage of all traffic, but it shall be possible to collect statistics on data volumes, which were not subject to service data flow based charging.

In case of GPRS the data volumes may be charged according to the GPRS offline charging mechanisms.

In case of GPRS, when service data flow based online charging is applied in the GGSN, other GPRS online charging procedures need not be applied to packets counted by FBC.

4.3 Charging models

4.3.1 General

When developing the charging solutions, the following charging models should be considered, even though the full solution to support the models may not be within the scope of this TS.

Shared revenue services shall be supported. In this case settlement for all parties shall be supported, including the third parties that may have been involved providing the services.

The charging solution shall allow various charging models such as:

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

It shall be possible to apply different rates and charging models when a user is identified to be roaming from when the user is in the home network.

It shall be possible to restrict special rates to a specific service, e.g. allow the user to download a certain volume of data from one service for free, but this allowed volume is not transferable to other services. It shall be possible also to apply special rates based on the time of day.

It shall be possible to enforce per-service usage limits for a service data flow using online charging on a per user basis (may apply to pre-paid and postpaid users).

It shall be possible for online charging systems to check the amount of data used over some time period. The online charging systems can provide both volume credit and time indication. In case the TPF detects the counted volume reaches the volume credit or the counted time reaches the indicated period of time, the TPF shall send a request for credit to the OCS with the remaining time value and/or remaining credit volume.

In the case of online charging, it shall be possible to perform rating and allocate credit depending on the characteristics of the bearer resources allocated initially (in the GPRS case, the QoS of the PDP context).

The flow based bearer level charging can support dynamic selection of charging to apply. A number of different inputs can be used in the decision to identify the specific charging to apply. For example, a service data flow may be charged with different rates depending on what QoS is applicable. The charging rate may thus be modified when a bearer is created or removed, to change the QoS provided for a service data flow.

The charging rate or charging model applicable to a service data flow may also be changed as a result of events in the service (e.g. insertion of a paid advertisement within a user requested media stream). The charging model applicable to a service data flow may also change as a result of events identified by the OCS (e.g. after having spent a certain amount, the user gets to use some services for free). The charging rate or charging model applicable to a service data flow may also be changed as a result of having used the service data flow for a certain amount of time and/or volume.

In the case of online charging, it shall be possible to apply an online charging action upon TPF events (e.g. re-authorization upon QoS change).

It shall be possible to indicate to the TPF that interactions with the charging systems are not required for a charging rule, i.e. to perform neither accounting nor credit control for this service data flow.

4.3.2 Examples of Service Data Flow Charging

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

A network server provides an FTP service. The FTP server supports both the active (separate ports for control and data) and passive modes of operation. A charging rule is configured for the service data flows associated with the FTP server for the user. The charging rule uses a filter specification for the uplink that identifies packets sent to port 20 or 21 of the

IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 20 or 21 of the IP address of the server.

A network server provides a “web” service. A charging rule is configured for the service data flows associated with the HTTP server for the user. The charging rule uses a filter specification for the uplink that identifies packets sent to port 80 of the IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 80 of the IP address of the server.

The same server also provides a WAP service. The server has multiple IP addresses, and the IP address of the WAP server is different from the IP address of the web server. The charging rule uses the same filter specification as for the web server, except the IP address is different.

An operator offers a zero rating for network provided DNS service. A charging rule is established setting all DNS traffic to/from the operators DNS servers as offline charged. The data flow filter identifies the DNS port number, and the source/destination address within the subnet range allocated to the operators network nodes.

An operator has a specific charging rate for user-user VoIP traffic over the IMS. A charging rule is established for this service data flow. The filter information to identify the specific service data flow for the user-user traffic is provided by the P-CSCF.

An operator is implementing UICC based authentication mechanisms for HTTP based services utilizing the GAA Framework as defined in TR 33.919 [11] by e.g. using the Authentication Proxy. The Authentication Proxy may appear as an AF and provide information to the CRF for the purpose of selecting an appropriate Charging Rule.

5 Flow Based Charging Concepts

5.1 Overview

The following functions are provided by the network for service data flow based charging. This applies to both online and offline charging unless otherwise specified:

- Identification of the service data flows that need to be charged individually (e.g. at different rates), and those that can be handled as an aggregate;
- Provision and control of charging rules on service data flow level;
- In the GPRS case: Provision and control of charging rules on a per PDP context basis;
- Reporting of service data flow level byte counts (for volume based charging) and service data flow durations (for time based charging);
- Event indication according to on-line charging procedures (e.g. sending AAA Accounting Stop) and, optionally, following this particular event, taking appropriate actions on service data flow(s) according to the termination action.
- Event indication and event monitoring by the TPF and following this particular event, taking the appropriate on-line charging actions.
- In addition FBC Policy Functions may be achieved by activating/deactivating charging rules according to the policies of the operator.

5.2 Charging rules

Charging rules contain information that allow for filtering of traffic to identify the packets belonging to a particular service data flow, and allow for defining how the service data flow is to be charged. The following apply to charging rules:

- The charging rules for bearer charging are defined by the operator.
- These charging rules are made available to the TPF for both offline and online charging.

- Multiple charging rules are supported simultaneously per user.
- Filtering information within a charging rule is applied through filtering functionality at the TPF to identify the packets belonging to a particular service data flow.
- Charging rules with dynamically provisioned filtering information (i.e. made available to the TPF) are supported in order to cover IP service scenarios where the filtering information is dynamically negotiated (e.g. negotiated on the application level (e.g. IMS)).
- Predefined charging rules stored in the TPF are supported. The charging rule identifiers of the predefined charging rules shall be different from the charging rule identifiers allocated by the CRF.
- Predefined filters that are part of the predefined charging rules may support extended capabilities, including enhanced capabilities to identify packets associated with application protocols.
- There may be overlap between the service data flow filter information of charging rules that are applicable. Overlap can occur between:
    - multiple predefined charging rules in the TPF;
    - multiple charging rules from the CRF;
    - charging rules predefined in the TPF and rules from the CRF, which can overlay the predefined rules in the TPF.

  The precedence identified with each charging rule shall resolve all overlap between the charging rules. When overlap occurs between a dynamically allocated charging rule and a predefined charging rule at the TPF, and they both share the same precedence, then the dynamically allocated charging rule shall be used.

Note: It's operators' responsibility to ensure that overlap between the predefined charging rules can be resolved based on precedence of each predefined charging rule in the TPF. It's CRF's responsibility to ensure that overlap between the dynamically allocated charging rules can be resolved based on precedence of each dynamically allocated charging rule.

- Charging rules contain information on:
    - How a particular service data flow is to be charged: online, offline or neither;
    - In case of offline charging whether to record volume- or time-based charging information or both;
    - Charging key;
    - Service data flow filter(s);
    - Service identifier;
    - Precedence (used at the TPF to determine the order in which charging rules shall be applied to a service data flow);
    - Charging rule identifier (used between CRF and TPF for referencing charging rules);
    - Application Function Record Information;
    - Service identifier level reporting: mandated or not required.
- Event triggers associated with all the charging rules of an IP network connection.
- A CCF and/or OCS address may be associated with an IP network connection.
- The charging rule identifiers allocated by the CRF shall be unique within a TPF/CRF dialogue.
- The Application Function Record information (e.g. ICID and flow ID(s)) is included in the charging rule, and in subsequently generated charging information generated as a result of the rule, if it is provided by an AF and the rule filters are based on the AF provided information. It should be noted that, in order to associate a single Application Function Record with specific counts/credits, it is necessary that new counts/credits be generated for the user by the TPF each time the AF generates new Application Function Record information.

- Once the charging rule is determined it is applied to the service data flow at the TPF and packets are counted and categorised per the rule set in the charging rule.

- Separate charging rules can be provided for downlink and uplink.

- Charging rules can be configured for both user initiated and network initiated flows.

- The charging key value and, optionally, the service identifier value of the charging rule identifies the service data flow.

- Charging rules that were provided by the CRF and established for a bearer can be modified by the CRF later on, e.g. for a previously established PDP context in the GPRS case, based on specific events (e.g. IM domain events or GPRS domain events, credit control events). Apart from the charging rule identifier and the charging method (online, offline, neither) all parts of a charging rule may be modified. Modification of a charging rule shall trigger the same TPF behaviour as the simultaneous removal of the old and instalment of the new (modified) charging rule.

- Different charging rules can be applied for different users.

- The same charging rule can be applied for multiple users.

- Different charging rules can be applied based on the location of the user (e.g. based on identity of the roamed to network).

- - Charging rule assignment can occur at bearer service establishment, modification and termination. For GPRS, charging rule assignment can occur at PDP context activation, modification and deactivation.

- For GPRS at PDP context activation, modification and deactivation a CRF may decide to align the set of charging rules for any other active PDP context. The CRF considers in such a case this as an Internal Trigger Event as described in 7.3 for the interaction with the TPF.

- For GPRS, the charging rules can be dependent on the APN used.

5.3 Service data flow filters and counting

This section refers to the filtering that identifies the service data flows that need to be charged individually (e.g. at different rates). Basic example: look for packets of one service, e.g. to and from a server A.

- Separate filtering and counting can be applied for downlink and uplink. The service data flow filters are specified separately for the uplink and downlink direction.

Note: A charging rule may provide information for a service data flow for one direction, or for both directions.

- Different granularity for service data flow filters identifying the service data flow is possible e.g.
  - Filters based on the IP 5 tuple (source IP address, destination IP address, source port number, destination port number, protocol ID of the protocol above IP). Port numbers and protocol ID may be wildcarded. IP addresses may be wildcarded or masked by a prefix mask.
  - Special filters which look further into the packet, or require other complex operation (e.g. maintaining state) may be predefined in the TPF and activated by the CRF using standardised means. Such filters may be used to support filtering with respect to a service data flow based on the transport and application protocols used above IP. This shall be possible for HTTP and WAP. This includes the ability to differentiate between TCP, Wireless-TCP according to WAP 2.0, WDP, etc, in addition to differentiation at the application level. Filtering for further application protocols and services may also be supported.

- In the case of GPRS, the TPF supports simultaneous independent filtering on service data flows associated with each individual active PDP context.

- In case of no applicable filters for a service data flow for that particular bearer (PDP context in the case of GPRS), the TPF shall discard the packets for this service data flow. To avoid the TPF automatically discarding packets due to no applicable charging rules, the operator may define generic charging rules (with wild-carded packet filters) to allow for default charging for the packets that don’t match any other charging rule.

- The service data flow filters and counting are applied by the TPF (the GGSN in the case of GPRS).

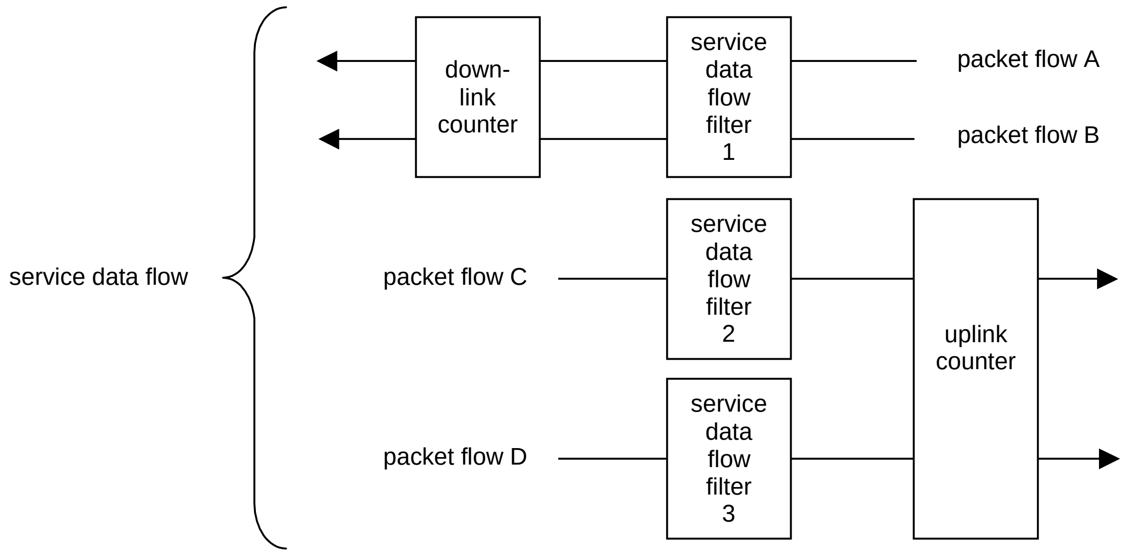


Figure 5.1 – Relationship of service data flow, packet flow and service data flow filter

5.4 Reporting

This refers to the differentiated charging information being reported to the online or offline charging functions. Note that reporting usage to the online charging function is distinct from requesting quotas for online credit control. Basic example: those 20 packets were in rating category A, include this in your global charging information.

- The TPF shall report bearer charging information for online charging;
- The TPF shall report bearer charging information for offline charging;
- Charging information is reported based on the application of the bearer charging rules in the TPF (service data flow related charging information), and in the case of GPRS, as specified in [3] (per PDP context);
- The TPF shall report triggered Events of an existing charging rule for both offline and on-line charging;
- The TPF shall report triggered re-authorisation of existing charging keys for on-line charging;
- The TPF shall report charging information for each bearer and charging key value;
- Depending on the configuration of a charging rule the TPF may report charging information for each charging key/service identifier;
- A report may contain multiple containers, each container associated with a charging key/service identifier;
- It shall be possible to associate per PDP context charging information with the corresponding service data flow based charging information.

5.5 Credit management

Online charging credits shall operate on a per charging key basis. This implies that where independent credit control is required for an individual service data flow, then the charging rule applying to that flow must have a unique charging key value. The TPF shall support credit management on a per bearer basis.

In case of online charging, it shall be possible for the OCS to apply re-authorisation of credit in case of particular events as described in section 5.7.

In case of online charging, credit can be pooled for multiple (one or more) charging keys applied at the Traffic Plane Function with the objective of avoiding credit fragmentation. A pool of credit applying to a single charging key is equivalent to an individual credit limit for that charging key. Multiple pools of credit shall be allowed per bearer.

The OCS shall strictly control the rating decisions. The OCS shall also control the credit pooling decisions. The OCS shall, when credit provision is sought, either provide a new pool of credit, together with a new credit limit, or a reference to a pool of credit that already exists at the TPF.

The grouping of charging keys into pools in this way shall not restrict the ability of the OCS to do credit authorisation and provide termination action individually for each charging key of the pool.

Note: 'credit' as used here does not imply actual monetary credit, but an abstract measure of resources available to the user. The relationship between this abstract measure, actual money, and actual network resources or data transfer, is controlled by the OCS.

It shall be possible for the OCS to group service data flows charged at different rates or in different units (e.g. time/volume) into the same pool.

5.6 Termination Action

The termination action applies only in case of online charging. The termination action indicates the action, which the TPF should perform when no more credit is granted. A packet that matches a charging rule, indicating a charging key for which no credit has been granted, is subject to a termination action.

The defined termination actions include:

- Allowing the packets, subject to the termination action, to pass through;
- Dropping the packets, subject to the termination action;
- The TPF Default Termination Action;
- The re-direction of packets, subject to the termination action, to an application server (e.g., defined in the termination action).

Note: such a re-direction may cause an application protocol specific asynchronous close event and application protocol specific procedures may be required in the UE and/or AF in order to recover, e.g., as specified in RFC 2616 for HTTP.

The Default Termination Action for all charging keys , for which no more credit is granted and there is no specific termination action shall be pre-configured in the TPF according to operator's policy. For instance, the default behaviour may consist of allowing packets of any terminated service data flow to pass through the TPF.

The OCS may provide a termination action for each charging key over the Gy interface. Any previously provided termination action may be overwritten by the OCS.

Note: A termination action remains valid and shall be applied by the TPF until all the corresponding charging rules of that charging key are removed or the corresponding bearer is removed (for GPRS the PDP context).

The OCS shall provide the termination action to the TPF before denying credit; otherwise the TPF default termination action will be performed.

The termination action may trigger other procedures, e.g. the deactivation of a PDP context or the termination of a WLAN session.

5.7 Re-authorisation and Event Triggers

Re-authorisation applies to online charging. For each charging key, the TPF receives re-authorisation trigger information from the OCS, which determines when the TPF shall perform a re-authorisation. The re-authorisation trigger detection will cause the TPF to request re-authorisation of the credit in the OCS. It shall be possible for the OCS to apply re-authorisation of credit in case of the following events:

- credit authorisation lifetime expiry;
- idle timeout;

- charging key is changed;
- SGSN change;
- PLMN change;
- QoS changes;
- RAT type change.

Event triggers apply to both offline and online charging. The event triggers are provided by the CRF to the TPF using Provision Charging Rule procedure. Event triggers are associated with all charging rules of an IP network connection. Event triggers determine when the TPF shall signal to the CRF that a bearer has been modified or a specific event has been detected.

Event triggers include the following events

- SGSN change;
- PLMN change;
- QoS change;
- RAT type change;
- TFT change.

Event triggers apply after bearer establishment.

Bearer modifications, which do not match an event trigger shall cause no action at the TPF.

5.8 Policy functions provided by FBC architecture

5.8.1 General

Service Based Local Policy (SBLP) specified in 3GPP TS 23.207[12] provides policy control functions for PS traffic. Some of these policy control functions are also provided by the FBC architecture to a certain extent, as described in the following sub-clauses. Note that there is no intention to duplicate the same SBLP functionalities with FBC, instead an overall description of the FBC Policy Functions is given.

5.8.2 Charging correlation

SBLP provides means to correlate bearer charging and application level charging by passing Charging Identifiers on the Go interface.

The FBC architecture passes the charging key applicable for the AF media flow to the OCS/CCF which is the input to the rating logic. Hence, AF media flows will be rated accordingly, but this provides no direct charging correlation between an AF session and the IP-CAN bearer its media flows use.

FBC provides the capability for charging correlation through the usage of Application Function Record information.

5.8.3 Gating

The Gating functionality of SBLP provides the ability to control blocking or allowing packets of a service flow to pass through. FBC achieves this functionality by discarding the packets for the service data flow in case of there is no other applicable filter available in the TPF for this service data flow.

For peer-to-peer traffic, special rates may apply. The gate could therefore be either closed for this traffic before the applicable filters are available, or the gate could be opened with a more generic charging rule, which does not allow for this special rate to apply yet.

The AF controls the point of time where Rx input is given to the CRF, which then sends this information down to the TPF, allowing for the filters for this peer-to-peer traffic to form a new charging rule. This allows the AF and CRF to control whether flows can pass through a particular bearer (PDP Context in case of GPRS):

- If the bearer has a charging rule installed that matches the flow, the flow is allowed to pass through on the bearer;
- If the bearer does not have a charging rule installed that matches the flow, the flow is not allowed to pass through on the bearer. If none of the bearers have a charging rule installed matching the flow, the flow is not allowed to pass through on any of the bearers.

5.8.4 QoS control

The QoS control functionality of SBLP provides control and authorization of the QoS parameters of the bearer that carries the service flow.

FBC provides means to control what bearer a service flow is allowed to be carried on. This implicitly allows the CRF to control what type of bearer (to the extent of QoS parameters) a service flow is allowed to use. A charging rule may apply to one or more particular bearer(s) (to a particular PDP Context in case of GPRS). Hence, the QoS the service flow is allowed to use is restricted to the QoS of a particular bearer(s).

5.8.5 Bearer events

SBLP provides means for the Policy Enforcement Function to indicate certain bearer events (e.g. loss of bearer connection) to the Application Function via the Go and Gq interfaces.

In the FBC architecture charging rules are downloaded to the TPF upon bearer events, see clause 7.2 for details. A charging rule either only applies to that particular bearer, or may apply to two or more bearers of a UE IP address:

- In case a charging rule for an AF service flow applies to a particular bearer, it is possible for the CRF to inform the AF about events related to that bearer. Hence, it is possible for the AF to initiate AF session actions accordingly.
- In case a charging rule for an AF service flow applies to more than one bearer of a UE IP address, the CRF informs the AF when all these bearers of a UE IP address have been removed. Hence, when a Charging Rule for a particular service is allowed for multiple bearers, the AF is not aware of the removal of individual bearers.

5.8.6 Session events

SBLP provides means to enforce bearer release upon certain AF session events (e.g. session hold or release).

The FBC architecture provides means to disable the service flows of the AF session upon AF session events (e.g. session hold or release). This is achieved by the AF providing new Rx input to the CRF, which then removes the charging rules of the service flows of the AF session from the TPF. Hence, traffic of the service flow will be blocked in case there is no other applicable filter available in the TPF for this service data flow i.e. the CRF has not allowed this traffic to pass through the network.

6 Architectural concepts

6.1 Architecture

6.1.1 Online service data flow based bearer charging architecture

Figure 6.1 below presents the overall architecture for service data flow based online bearer charging.

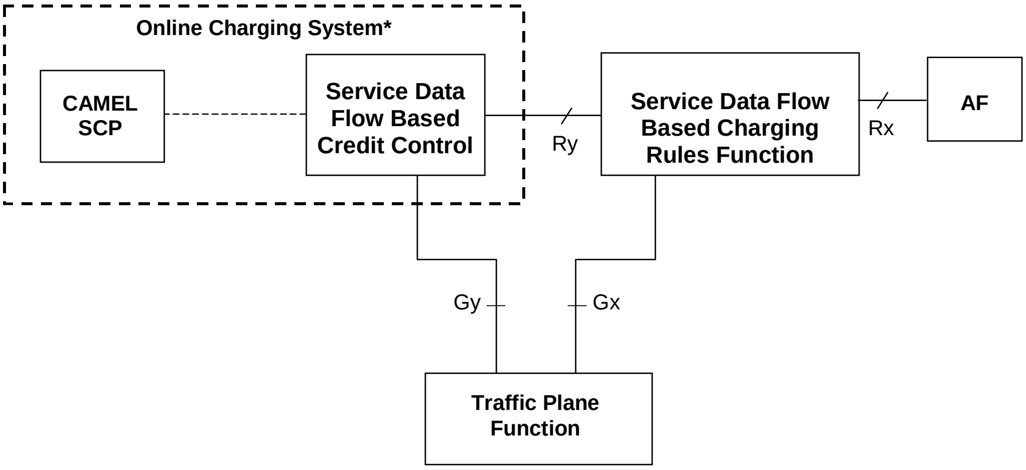


Figure 6.1: Overall architecture for service data flow based online bearer charging

Note(*): The detailed functional entities of the Online Charging System are not shown in this figure. The details of the OCS are specified in [3].
The CAMEL-SCP depicted on the figure above performs the functions as defined in [8].

6.1.2 Offline service data flow based bearer charging architecture

Figure 6.2 below presents the overall architecture for service data flow based offline bearer charging.

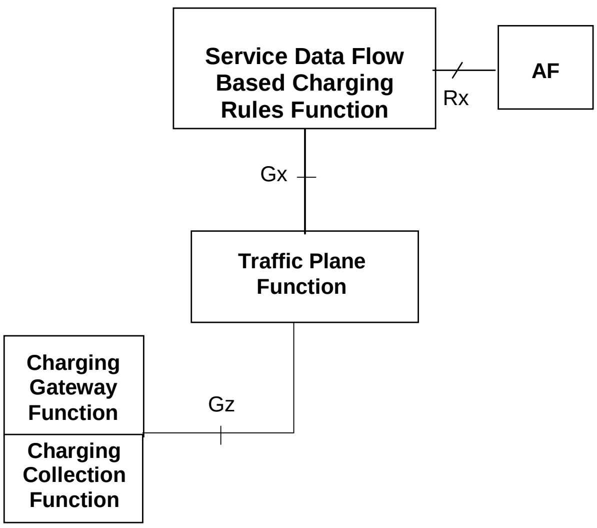


Figure 6.2: Overall architecture for service data flow based offline bearer charging

Note: The CCF depicted on the figure above performs the functions as defined in [3].

6.2 Functional Entities

6.2.1 Based Charging Rules Function

The CRF provides service data flow level charging rules. This functionality is required for both offline and online charging. The CRF accesses information stored in the service data flow based charging rules data repository. An external interface to the charging rules data repository may be used for management of the charging rules within the data repository. Specification of interfaces to the data repository is out of scope of this TS.

The CRF supports both dynamic activation of predefined charging rules in the TPF and dynamic charging rules that are downloaded to the TPF.

The CRF determines what charging rules (including precedence) to apply for a user. The applicable charging rules are determined based on information available to the CRF including that received from the TPF, i.e. information about the user, the bearer characteristics, and the network related information. When a further request for charging rules from the TPF or information from an AF arrives the CRF shall be able to identify whether new charging rules need to be transferred to the TPF and respond accordingly.

The CRF will receive information from the AF that allows a service data flow to be identified, and this information may be used within the charging rule (i.e. protocol, IP addresses and port numbers). Other information that is received by the CRF (i.e. application identifier, type of stream) may be used in order to select the charging rule to be applied.

For a specific AF, the CRF shall apply the AF input to the charging rule completion and selection to all charging rules of the user.

A CRF node may serve multiple TPFs.

6.2.2 Service Data Flow Based Credit Control Function

The Service Data Flow Based Credit Control Function performs online credit control functions together with the Online Charging System. It provides a new function within the Online Charging System.

The Online Charging System is specified in 3GPP TS 32.200 [3]. The Service Data Flow Based Credit Control Function is considered as a new functional entity for release 6 within the Online Charging System.

The OCS can interact with the CRF, by using the Ry interface. This allows the OCS to provide input to the CRF for charging rules selection.

There may be several OCSs in a PLMN. To allow for this case, OCS addresses (i.e. the primary address and secondary address) may be passed once per IP network connection from the CRF to the TPF. This information shall be locally pre-configured within the TPF for all users. The addresses provided by the CRF have higher priority than the pre-configured ones.

6.2.3 Charging Collection Function

The Charging Collection Function is specified in 3GPP TS 32.200 [3].

There may be several CCFs in a PLMN. To allow for this case, CCF addresses (i.e. the primary address and secondary address) may be passed once per IP network connection from the CRF to the TPF. This information shall be locally pre-configured within the TPF for all users. The addresses provided by the CRF have higher priority than the pre-configured ones.

6.2.4 Traffic Plane Function

The TPF shall be capable of differentiating user data traffic belonging to different service data flows for the purpose of collecting offline charging data and performing online credit control.

The TPF shall support predefined charging rules, and predefined filters. See subclause 5.3 for further filtering and counting requirements.

In the case of online charging, the TPF shall not allow traffic unless network resource usage has been granted by the OCS.

For online charging, the TPF shall be capable of managing a pool of credit used for some or all of the service data flows of a user. The TPF shall also be capable of managing the credit of each individual service data flow of the user.

A TPF may be served by one or more CRF nodes. For GPRS, the TPF shall contact the appropriate CRF based on the APN , which is the primary mechanism. Optionally, the IMSI or MSISDN may in addition to the APN be used as input for selection of the appropriate CRF. For other IP-CANs the TPF shall contact the appropriate CRF based on the access point connected to and, optionally, a UE identity information that is applicable in that kind of IP-CAN.

Note: For GPRS the CRF address(es) are configured in the TPF (GGSN) per APN.

For GPRS, it shall be possible to provide flow based charging functions for different service data flows even if they are carried in the same PDP Context. For GPRS, the TPF is a logical function allocated to the GGSN.

For GPRS, the TPF/GGSN applies charging rules on a per PDP context basis.

For each PDP context, the TPF shall accept information during bearer establishment and modification relating to:

- The user and terminal (e.g. MSISDN, IMEISV)
- Bearer characteristics (e.g. QoS negotiated, APN, IM CN Subsystem signaling flag)
- Network related information (e.g. MCC and MNC)

The operators may apply different charging rules and rates depending on different PLMN. The TPF shall be able to provide MCC and MNC of the serving network (i.e. SGSN) to the CRF, which may be used by the CRF in order to select the charging rule to be applied.

The TPF may use this information in the OCS request/reporting or request for charging rules.

For each PDP context, there shall be a separate OCS request/CCF reporting, so this allows the OCS and offline charging system to apply different rating depending on the PDP context.

The TPF shall identify packets that are charged according to service data flow based charging. The TPF shall report the data volume(s) charged according to service data flow based charging. In case of GPRS, the TPF shall report the service data flow based charging data for each charging rule on a per PDP context basis.

At initial bearer establishment the TPF shall request charging rules applicable for this bearer from the CRF. As part of the request, the TPF provides the relevant information to the CRF. The TPF shall use the charging rules received in the response from the CRF. In addition, the TPF shall use any applicable predefined charging rules. Predefined charging rules may apply for all bearers of all users or may be dynamically activated (or deactivated) by the CRF for a specific bearer.

If the bearer is modified, by changing the bearer characteristics, the TPF shall first use the event triggers to determine whether to request the charging rules for the new bearer characteristics from the CRF. Afterwards, the TPF shall use the re-authorisation triggers in order to determine whether to require re-authorisation for the charging rules that were either unaffected or modified.

If the TPF receives an unsolicited update of the charging rules from the CRF, the new charging rules shall be used.

If another bearer is established by the same user (e.g. for GPRS the Secondary PDP Context Activation procedure), the same procedures shall be applied by the TPF as described for the initial bearer. For a bearer, the TPF shall only apply the charging rules that are activated/associated with this bearer. Hence a charging rule is installed, modified and removed on a per PDP context basis. If multiple PDP contexts are active for a UE the CRF may decide that a charging rule is to be activated/associated with more than one PDP context.

The TPF shall evaluate received packets against the service data flow filters in the order according to the precedence for the charging rules. When a packet is matched against a SDF filter, the packet matching process for that packet is complete, and the charging rule for that SDF filter shall be applied. If there is no match against any SDF filter established for that bearer the packet shall be discarded.

6.2.5 Application Function

The AF provides information to the service data flow based CRF, which can then be used for selecting the appropriate charging rule, and also used for configuring some of the parameters for the charging rule. The operator configures the charging rules in the service data flow based CRF, and decides what data from the AF shall be used in the charging rule selection algorithm.

An AF may communicate with multiple CRFs. The AF shall contact the appropriate CRF based on either:-

- the end user IP Address;

Note: By using the end user IP address, an AF is not required to acquire any UE identity in order to provide information, for a specific user, to the CRF.

- the end user IP address and any other UE identity information the AF is aware of.

The AF shall provide information to allow the service data flow to be identified. The AF shall also provide some other information that may be used in the charging rule selection process.

The information provided by the AF is as follows:

Information to identify the service data flow: refer to subclause 5.3.
The AF may use wildcards to identify an aggregate set of IP flows.

- Optional Application Function Record information that would be included in charging data generated by the AF and by the TPF and could be used to associate the records for post processing.
- Information to support charging rule selection:
  - Application identifier;
  - Application event identifier;
  - Type of Stream (e.g. audio, video) (optional);
  - Data rate of stream (optional);
  - User information (such as user identity).

The “Application Identifier” is an identifier associated with each service that an AF provides for an operator (e.g. a packet streaming service AF would have one application identifier for the service).

The “Application event identifier” is an identifier within an Application identifier. It is used to notify the Service Data Flow Based CRF of such a change within a service session that affects the charging rules, e.g. triggers the generation of a new charging rule.

6.2.6 Relationship between functional entities

The AF and the CRF need not exist within the same operator’s network. The Rx interface may be intra- or inter-domain and shall support the relevant protection mechanisms for an inter-operator or third party interface. The TPF and the CRF exist within the same operator’s network.

6.3 Reference points

6.3.1 Gx reference point

The Gx reference point enables the use of service data flow based charging rules such as counting number of packets belonging to a rate category in the IP-Connectivity Network. This functionality is required for both offline and online charging.

Note: The reuse of existing protocols over the Gi reference point for Gx shall be evaluated in stage 3.

The Gx reference point supports the following functions:

1. Initialisation and maintenance of Gx connection
2. Request for Charging Rules (from TPF to CRF)
3. Provision of Charging Rules (from CRF to TPF)
4. Indication of Bearer Service Termination (from TPF to CRF)

6.3.1.1 Initialisation and Maintenance of Gx Connection

The TPF shall ensure the establishment of a single Gx connection to each CRF. The connection can be direct, or established via a relay/proxy node. A connection may be redirected to an alternate CRF.

Note: The set of CRFs, to which the TPF must establish a Gx connection, depends on the configuration.

At a failover, commands which have not been successfully received shall be forwarded to an alternate CRF.

Only CRFs responsible for the same IP network (for GRPS, APN) and UE identity information may be selected as alternate CRF.

The detailed specification of the connection establishment and maintenance is for specification in stage 3.

6.3.1.2 Request for Charging Rules (from TPF to CRF)

The TPF requests the charging rules to be applied:

- At bearer service establishment (PDP context establishment for GPRS) or,
- At bearer service modification (PDP context modification for GPRS) if the Event trigger is met, or
- At bearer service termination (PDP context deactivation for GPRS).

The request from the TPF to the CRF must identify whether it is an initial request from the UE (for GPRS the PDP Context Activation procedure [6]), or a subsequent request (i.e. for GPRS, a new PDP context is activated with the Secondary PDP Context Activation procedure [6], or a PDP context is modified with any of the PDP Context Modification procedures [6]). For an initial request for GPRS, the request from the TPF to the CRF shall include at a minimum APN, PDP address information, values MCC and MNC of the serving network (i.e. SGSN), and at least one of IMSI or MSISDN.

An identifier is required to allow the specific instance in the TPF/CRF to be identified for subsequent data exchange. The identifier for the communication must be provided.

The request must provide further information used for the charging rule selection. The request shall include an identifier for the bearer, the QoS information, and flow identifier information allocated to the bearer. For GPRS, this information would include the traffic class, IM CN Subsystem Signalling Flag (if present in the downlink), and the TFT.

6.3.1.3 Provision of Charging Rules (from CRF to TPF)

The CRF identifies the charging rules that are applicable to the TPF. The CRF then sends the charging rule information to the TPF.

The charging rule information represents the set of charging rules to be installed (or activated) by the TPF, which can be one or a combination of the following:

- charging rules,
- identifiers for pre-defined charging rules,
- a single identifier for a set of pre-defined charging rules.

The provisioning may be a response to a Request for Charging Rules, or it may be unsolicited.

Provision of Charging Rule shall support cases where charging rules are to be installed, removed or modified in the TPF as well as cases where charging rules are neither installed nor removed nor modified in the TPF (only relevant in the response to a request for charging rules).

Note: Predefined charging rules cannot be modified.

The Provision of Charging Rules shall include information about the instance it relates to (i.e. identifier for the relevant TPF/CRF instance), in addition, the Provision of Charging Rules may include charging rules and the associated action indications (install, modify, remove).

6.3.1.4 Indication of Bearer Termination (from TPF to CRF)

The TPF indicates to the CRF that a bearer is terminated.

The bearer termination indication includes information to identify the instance it relates to (i.e. an identifier for the relevant TPF/CRF instance), and an indication of the bearer being removed (the PDP context in the case of GPRS). The termination also indicates if this is the last bearer for that TPF/CRF instance.

6.3.2 Gy reference point

The Gy reference point allows credit control for service data flow based online charging. The functionalities required across the Gy reference point use existing functionalities and mechanisms for example based on [9].

6.3.3 Gz reference point

The Gz reference point enables transport of service data flow based offline charging information.

For GPRS the relationship of the Gz reference point and the existing Ga interface is subject to investigation in SA5.

The Ga interface is specified by TS 32.200 [3].

6.3.4 Rx reference point

6.3.4.1 General

The Rx reference point enables transport of information (e.g. dynamic media stream information) from the AF to the CRF. An example of such information would be filter information to identify the service data flow. The AF and the CRF, which may reside in the same or different security domain, shall have a trust relationship. Hence the information exchanged between an AF and a CRF shall be protected with adequate security.

6.3.4.2 Initialisation and Maintenance of Rx Connection

The AF node shall ensure the establishment of a single Rx connection to each CRF. The connection can be direct, or established via a relay/proxy node. A connection may be redirected to an alternate CRF.

Note: The set of CRFs, to which the AF must establish a Rx connection, depends on the configuration.

At a failover, commands which have not been successfully received shall be forwarded to an alternate CRF.

Only CRFs responsible for the same IP network (for GPRS, APN) and UE identity information may be selected as alternate CRF. Furthermore, the maintenance mechanism for Rx shall ensure that the same alternate CRF is selected as the one selected by the Gx maintenance mechanism.

The detailed specification of the connection establishment and maintenance is for specification in stage 3.

6.3.5 Ry reference point

The Ry reference point enables transport of information (e.g. charging rules selection information) from the OCS to the CRF. The functionality supported over the Ry reference point should be the same as for the Rx reference point and a common interface specification is expected.

7 Message Flows

7.1 AF input to provision of charging rules

The AF may provide the CRF with application/service data flow charging information as described in 6.2.5. This information is used by the CRF to determine and complete the appropriate charging rules to send to the TPF. It is an AF decision when to send this information and the CRF takes the AF input into account from the point that it receives the AF information. The AF input may trigger an unsolicited provision of charging rules by the CRF as described in 7.3.

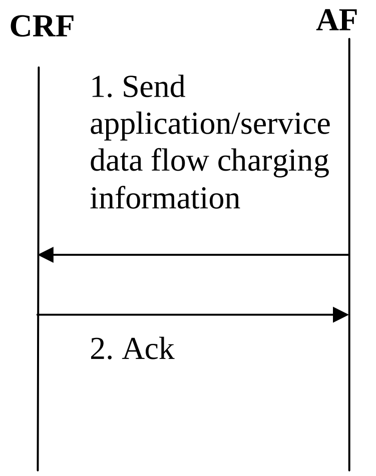


Figure 7.0a: AF input to provision of charging rules

1. The AF sends application/service data flow charging information. The AF may include IMSI/MSISDN in addition to the IP Address of the UE
2. If the AF only provides the IP Address of the UE the CRF acknowledges the AF input. If the AF in addition to the IP Address of the UE also provides the IMSI/MSISDN the CRF performs, based on the operator configuration, a check of the UE identities provided by the AF against the UE identities provided by the TPF. After the identity matching procedures the CRF informs the AF about the result. For GPRS the CRF receives the IMSI and MSISDN from the TPF at bearer establishment.

7.1a OCS input to provision of charging rulesThe OCS may provide the CRF with OCS related charging information. It is an OCS decision when to send this information and the CRF takes the OCS input into account from the point that it receives the OCS information. The OCS input may trigger an unsolicited provision of charging rules by the CRF as described in 7.3.

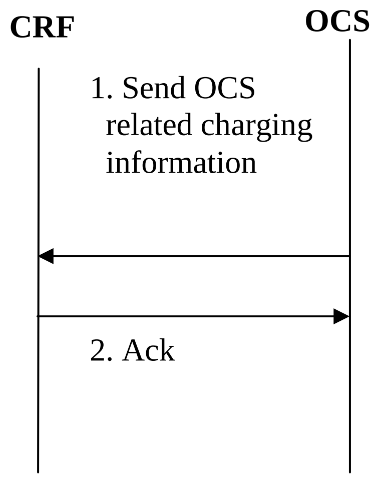


Figure 7.0b: OCS input to provision of charging rules

1. The OCS sends OCS related charging information

2. The CRF acknowledges the OCS input.

7.2 Bearer events

7.2.1 Bearer Service Establishment

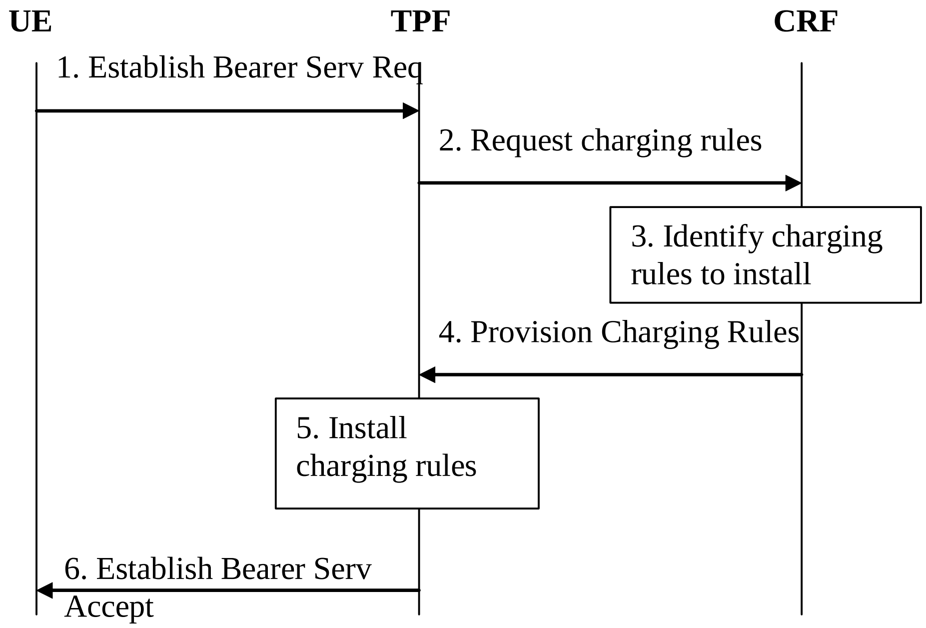


Figure 7.1: Bearer Service Establishment in case of offline charging

1 The TPF receives a request to establish a bearer service. For GPRS, it is the GGSN that receives a Create PDP context request from the SGSN.

2 The TPF requests the applicable charging rules, and provides relevant input information for the charging rule selection.

3 The CRF determines the charging rules to be provisioned, based on information available to the CRF (e.g. information may be available from the AF as described in 7.1 and the new information received from the TPF). Charging rules may need to be installed. In addition, the CRF also determines which event triggers shall be monitored by the TPF.

4 The CRF provides the to the TPF. For the first bearer service of an IP network connection the CRF may additionally provide and associated event triggers, CCF and OCS addresses to the TPF. This message is flagged as the response to the TPF request.

5 The TPF performs charging rule actions as indicated, i.e. installing charging rules. During establishment of the bearer service the TPF also installs any predefined charging rules.

6 The TPF continues with the bearer service establishment procedure.

The TPF shall wait for the charging rules installation before accepting the Bearer establishment as shown in figure 7.1.

In case of online charging, in order to allow for Bearer establishment control upon credit check, the TPF shall wait for the credit control information before accepting the Bearer establishment as shown in figure 7.2.

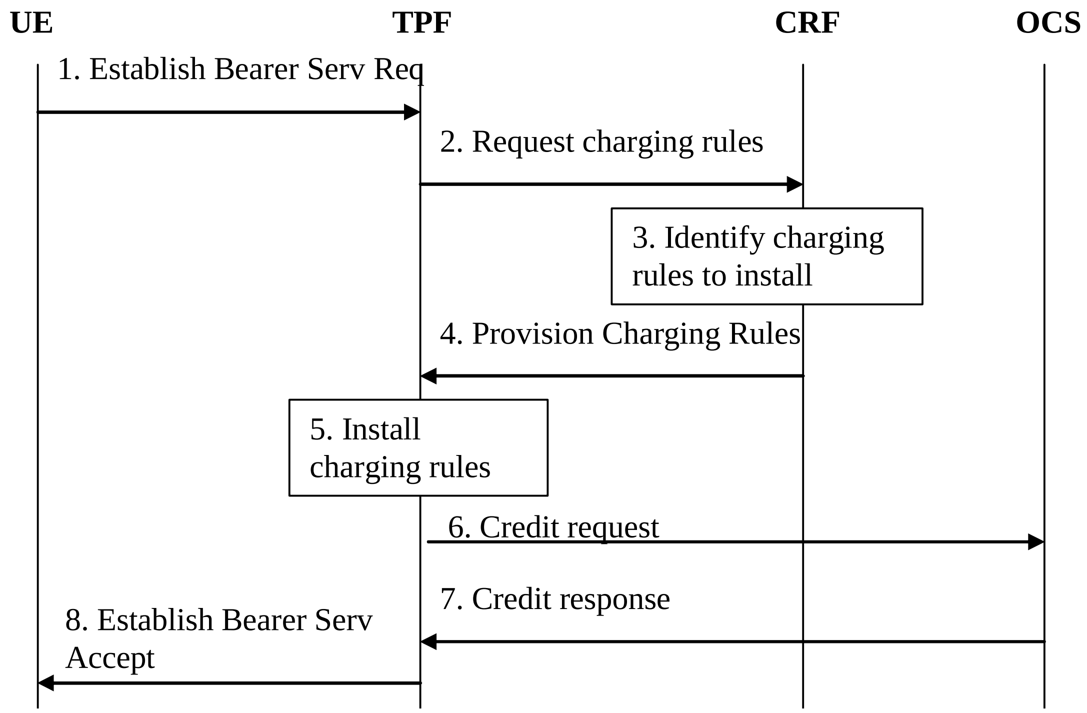


Figure 7.2: Bearer Service Establishment in case of online charging

1. The TPF receives a request to establish a bearer service. For GPRS, it is the GGSN that receives a Create PDP context request from the SGSN.

2. The TPF requests the applicable charging rules, and provides relevant input information for the charging rule decision.

3. The CRF determines the charging rules to be provisioned, based on information available to the CRF (e.g. information may be available from the AF as described in 7.1 and the new information received from the TPF). Charging rules may need to be installed. In addition, the CRF also determines which event triggers shall be monitored by the TPF.

4. The CRF provides the charging rules to the TPF. For the first bearer service of an IP network connection the CRF may additionally provide event triggers, CCF and OCS addresses to the TPF. This message is flagged as the response to the TPF request.

5. The TPF performs charging rule actions as indicated, i.e. installing charging rules. During establishment of the bearer service the TPF also installs any predefined charging rules.

6. The TPF requests credit for any charging key of the established charging rules (either predefined or newly installed) from the OCS, and provides relevant input information for the OCS decision.

7. The OCS provides the credit information to the TPF and may provide re-authorisation triggers for each of the credits.

8. If credit is available at least for one charging key, the TPF accepts the bearer service establishment. If no credit is available, the TPF rejects the bearer service establishment.

Note: Further details of the credit control mechanism are expected to be specified by Stage 3.

7.2.2 Bearer Service Modification

7.2.2.1 General

According to the Event triggers and Re-authorisation triggers, Bearer Service Modification may trigger the TPF to signal the CRF that a bearer has been modified and/or trigger the TPF to request re-authorisation (for online).

7.2.2.2 Bearer Service Modification in case of offline charging

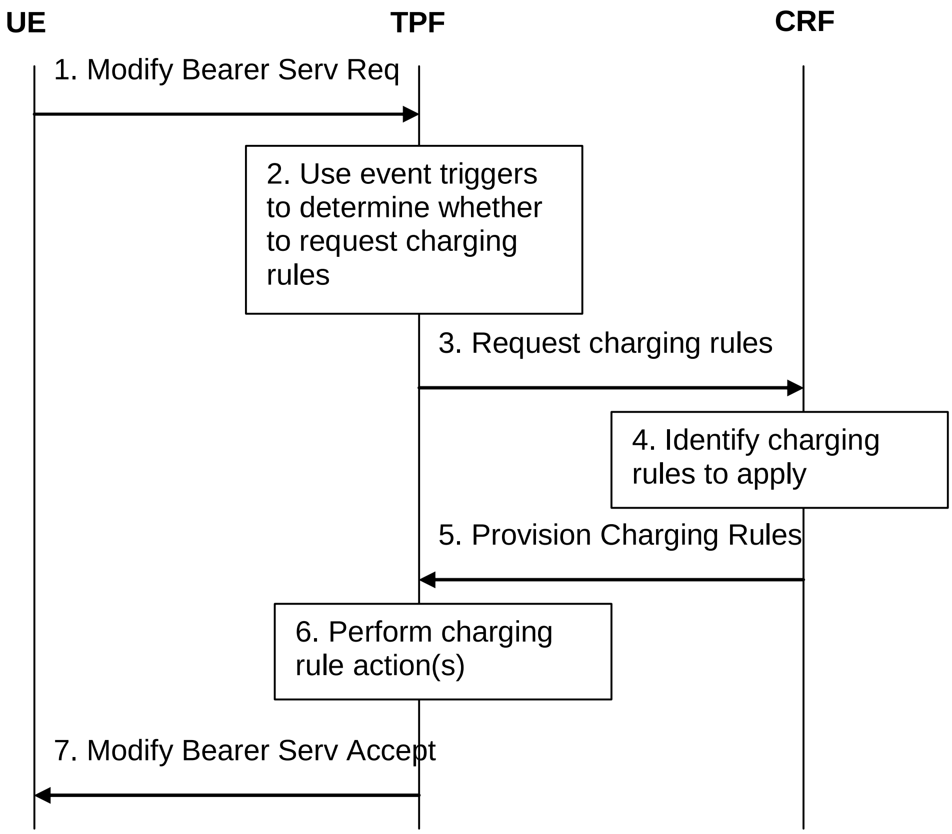


Figure 7.2a: Bearer Service Modification triggered Charging Rule Request

1. The TPF receives a request to modify a bearer service. For GPRS, the GGSN receives an Update PDP context request.
2. The TPF uses the event triggers in order to determine whether a request for charging rules is required
3. The TPF requests the applicable charging rules indicating a bearer modification, and provides relevant input information for the charging rule selection.
4. The CRF determines the charging rules to be provisioned, based on information available to the CRF (e.g. information may be available from the AF as described in 7.1 and the new information received from the TPF). Charging rules may need to be installed, and/or removed, and/or modified.
5. The CRF provides the charging rule information to the TPF. This message is flagged as the response to the TPF request.
6. The TPF performs charging rule actions as indicated, i.e. installing, modifying or removing charging rules.
7. The TPF continues with the bearer service modification procedure.

Note-i: In the case of GPRS, the modification of the bearer service may also be initiated by other nodes such as the SGSN.

Note-ii: The TPF shall wait for the charging rules installation before accepting the Bearer modification, as shown in figure 7.1.

7.2.2.3 Void

7.2.2.4 Bearer Service Modification in case of online charging

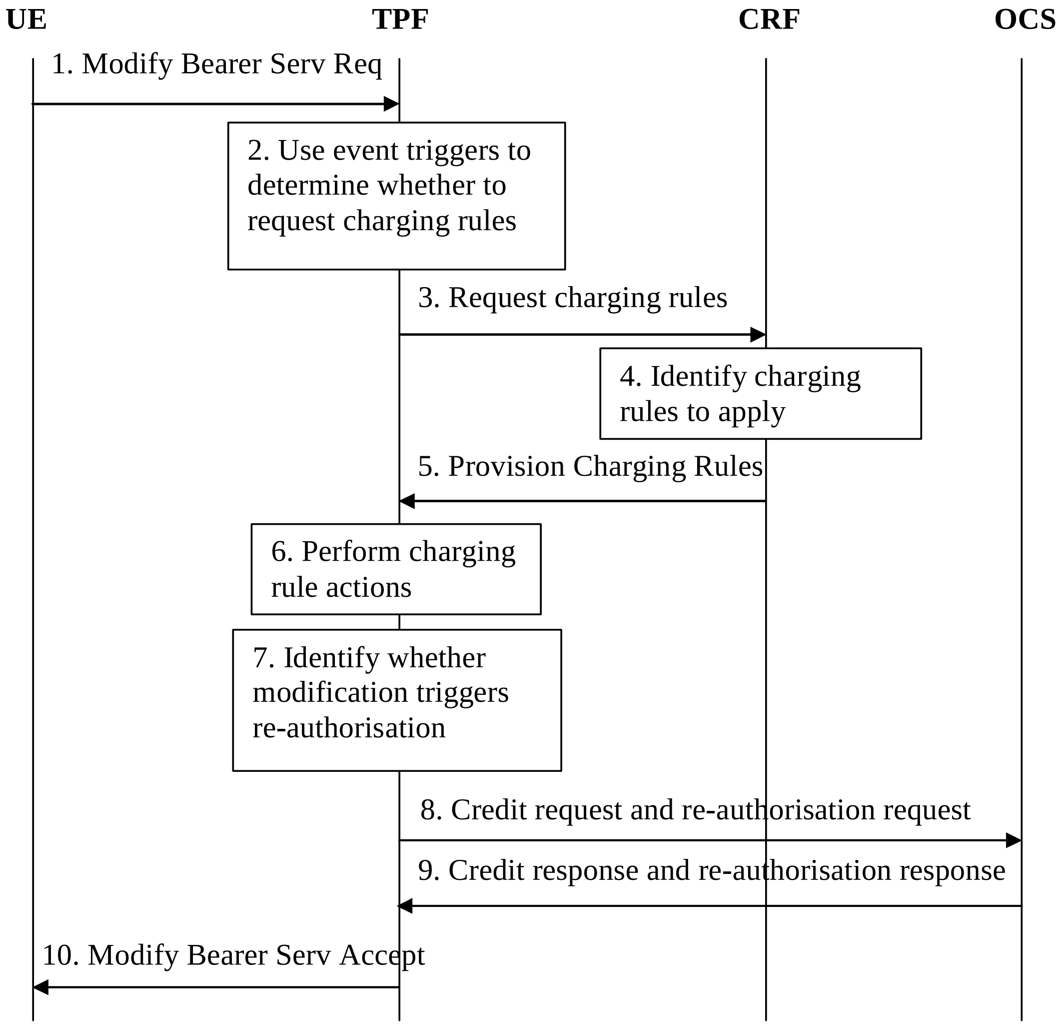


Figure 7.2c: Bearer Service Modification in case of online charging

1. The TPF receives a request to modify a bearer service. For GPRS, the GGSN receives an Update PDP context request.
2. The TPF uses the event triggers in order to determine whether a request for charging rules is required.
3. The TPF requests the applicable charging rules indicating a bearer modification, and provides relevant input information for the charging rule selection.
4. The CRF determines the charging rules to be provisioned, based on information available to the CRF (e.g. information may be available from the AF as described in 7.1 and the new information received from the TPF) Charging rules may need to be installed, and/or removed, and/or modified.
5. The CRF provides the charging rule information to the TPF. This message is flagged as the response to the TPF request.
6. The TPF performs charging rule actions as indicated, i.e. installing, modifying or removing charging rules.
7. The TPF identifies whether the bearer modification matches the re-authorisation trigger(s) of any charging key, which belongs to charging rules that have neither been installed nor removed in step 6.

8. The TPF interacts with the OCS if the set of charging keys has changed or if the bearer modification matches re-authorisation trigger(s) of any charging key in the step 7. The TPF requests credit for any new charging key, and provides relevant input information for the OCS decision. The TPF returns the remaining credit of any charging key for which the last charging rule has been removed (i.e. there is no longer a charging rule with this charging key). The TPF returns the unused credit(s) for any charging key (s) applicable for re-authorisation and requests re-authorisation of their credits.

9. The OCS answers to the TPF providing credits.

10. If credit is available at least for one charging rule, the TPF accepts the bearer modification.

Note: In the case of GPRS, the modification of the bearer service may also be initiated by other nodes such as the SGSN.

7.2.3 Bearer Service Termination

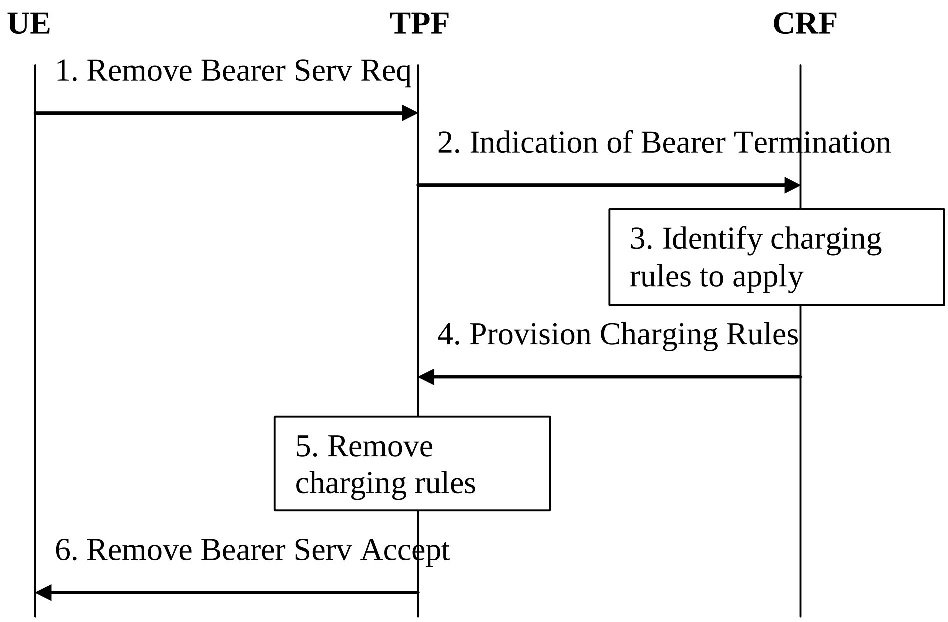


Figure 7.3: Bearer Service Termination in case of offline charging

1 The TPF receives a request to remove a bearer service. For GPRS, this is the GGSN that receives a delete PDP context request.

2 The TPF indicates that a bearer service (for GPRS, a PDP context) is being removed and provides relevant information for the CRF.

3 The CRF applies the indication of the bearer service termination to determine whether charging rules need to be provisioned for any other bearer service of the same IP network connection (using an unsolicited provision of charging rules by the CRF as described in 7.3). Charging rules may need to be removed for the terminated bearer service. However, there is no need for the CRF to remove charging rules explicitly.

4 The CRF provides the charging rule information to the TPF. This message is flagged as the response to the TPF request.

5 The TPF performs charging rule actions as indicated, i.e. removing charging rules.

6 The TPF continues with the bearer service removal procedure.

Note: In the case of GPRS, the bearer service termination procedure may also be initiated by other nodes such as the SGSN.

Note: The bearer service removal procedure can proceed in parallel with the indication of bearer service termination.

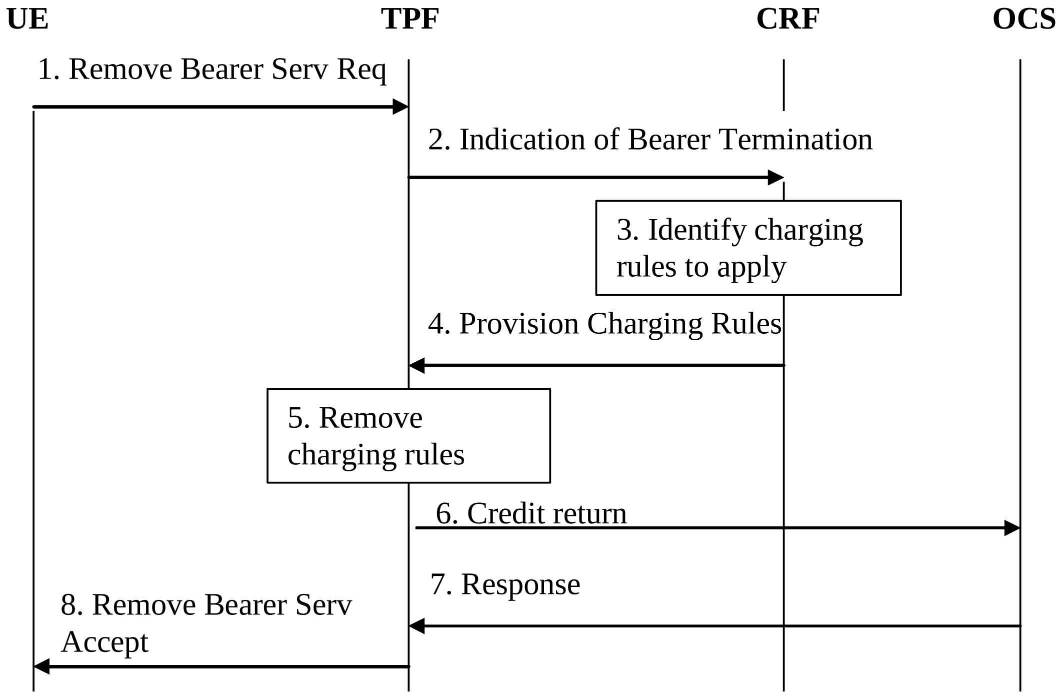


Figure 7.3a: Bearer Service Termination in case of online charging

1. The TPF receives a request to remove a bearer service. For GPRS, this is the GGSN that receives a delete PDP context request.

2. The TPF indicates that a bearer service (for GPRS, a PDP context) is being removed and provides relevant information for the CRF.

3. The CRF applies the indication of the bearer service termination to determine whether charging rules need to be provisioned for any other bearer service of the same IP network connection (using an unsolicited provision of charging rules by the CRF as described in 7.3). Charging rules may need to be removed for the terminated bearer service. However, there is no need for the CRF to remove charging rules explicitly.

4. The CRF provides the charging rule information to the TPF. This message is flagged as the response to the TPF request.

5. The TPF performs charging rule actions as indicated, i.e. removing charging rules.

6. The TPF returns the remaining credit of every charging key to the OCS.

7. The OCS acknowledges the report to the TPF.

8. The TPF continues with the bearer service removal procedure.

Note: The bearer service termination indication can proceed in parallel with the final usage reporting and the bearer service removal procedure.

Note: Further details of the credit control mechanism are expected to be specified by Stage 3.

7.3 Provision of Charging Rules triggered by other event to the CRF

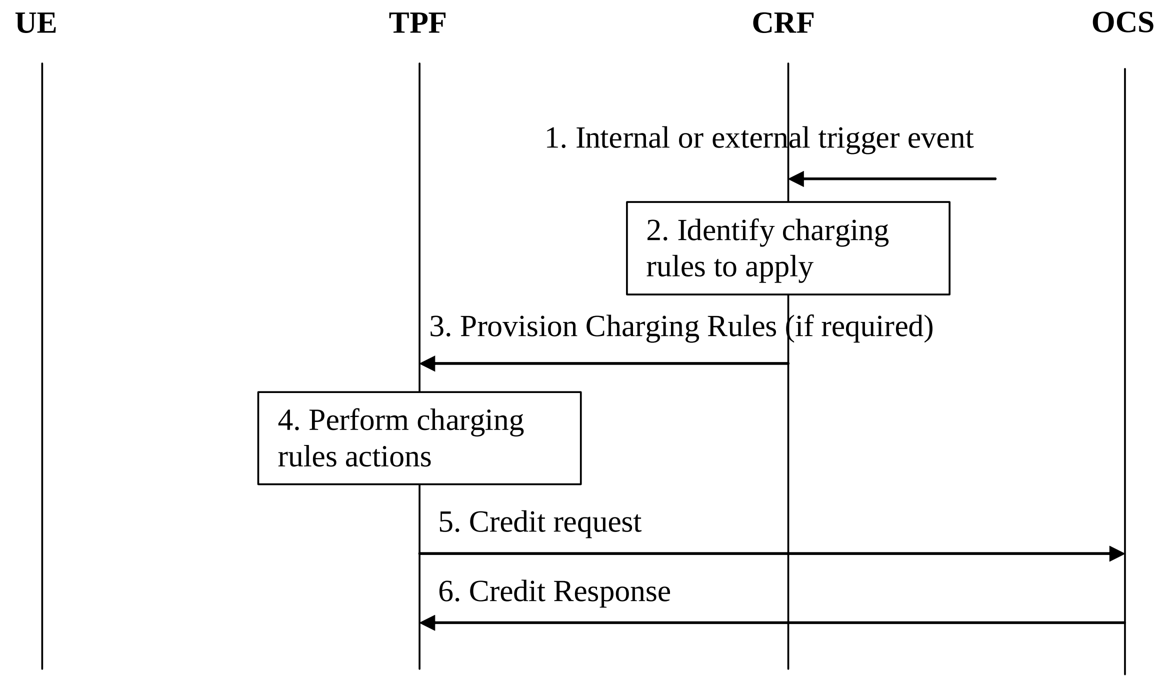


Figure 7.4: Provision of Charging Rules due to external or internal Trigger Event

1 The CRF receives a trigger event, with relevant information related to the event. One example event is an AF interaction as described in 7.1.

2 The CRF determines the charging rules to be provisioned, based on information available to the CRF (e.g. information may be available from the AF as described in 7.1 and the new information received from the trigger). Charging rules may need to be installed, and/or removed, and/or modified.

3 If required, the CRF provisions the charging rules to the TPF.

4 The TPF performs charging rule actions as indicated, i.e. installing, modifying or removing charging rules.

5 In case of online charging, the TPF requests credit for any new charging key from the OCS, and provides relevant input information for the OCS decision. The TPF returns the remaining credit of any charging key for which the last charging rule has been removed (i.e. there is no longer a charging rule with this charging key).

6 In case of online charging, the OCS provides the credit information to the TPF and may provide re-authorisation triggers for each of the credits.

Annex A (informative): Overall architectural impacts of IP flow based charging

A.1 GGSN in HPLMN

One of the underlying drivers for the IP flow charging work is to permit greater flexibility in PS domain charging, and, to control this flexibility in the HPLMN. This is a fairly fundamental change from the concepts that lead to development of the CAMEL 3 standards (which provide the capability for pre-pay charging on the SGSN) and some aspects of the IMS architecture (e.g. P-CSCF and I-CSCF).

This movement towards charging in the “GGSN arena” rather than “charging at the SGSN” leads to a few questions:

a) is all the information that the SGSN places on the S-CDR available at the GGSN? If not, what is missing, is it important, and, can GTP be upgraded to provide it to the GGSN?

b) when this information is passed to the GGSN, can it then be made available as extra Radius parameters?

c) does this information need to be sent on the Gx and/or Gy and/or Gz interfaces?

A.2 Comparison of S-CDR and G-CDR fields

A.2.1 S-CDR information missing from G-CDR

The following fields are present in the S-CDR but absent from the G-CDR

- Served IMEI;
- MS Network Capability;
- LAC/RAC/CI at “record opening”;
- Access Point Name Operator Identifier;
- System Type;
- CAMEL information;
- RNC unsent data volume;
- Time zone of the user's location.

These parameters are analysed further in the following subsections.

A.2.2 Served IMEI

This information is useful for many operational/statistical purposes within the HPLMN. Examples might include checking whether the SIM-IMEI combination “is correct”; which brands of mobile generate what proportion of revenue streams and/or access particular types of services; etc.

Hence it is recommended to provide the IMEISV to the GGSN for transparent transfer within the GGSN to the G-CDR and/or Radius attribute. This means the addition of an optional parameter to the Create PDP Context Request message.

Note that the IMEISV should be provided rather than just the IMEI because the SV information has some value, and, IMEISV is as equally easy for the SGSN to obtain as the IMEI.

A.2.3 MS Network Capability

This is the "core network" part of the mobile's classmark. Review of 24.008 shows that most of the really interesting information for the HPLMN is contained within the Radio Classmark information and not within the MS Network Capability. However, the Radio Classmark information is not included on the S-CDR.

Hence statistical information gathering (such as, what proportion of UK data traffic is carried by mobiles that support the PCS 1900 spectrum) has to be gathered from analysis of IMEIs rather than analysis of the Classmark field.

Hence, provided IMEISV is sent to the GGSN, this field need not be sent to the GGSN.

A.2.4 LAC/RAC/CI at "record opening"

Various tariffs can be imagined that use cell ID information (e.g. a home cell tariff, whereby, if the context is opened in your home cell, a certain volume of data is charged at a lower rate). Statistical information gathering is also performed on a per cell basis.

Hence knowledge of the "full" cell ID at the GGSN would be useful.

Note that the "full" cell ID includes the MNC and MCC – but these fields have recently been added to R'97 and R'99 GTP. During the debate on this topic, it might have been argued that the 3G-SGSN did not know the Service Area Code where the mobile was activating the PDP context. However, this seems to be incorrect, because study of RANAP shows that the RNC is required to add the mobile's current SAI to every Direct Transfer message sent to the SGSN,

There may be some concerns about sending cell-ID information between networks, however, it may well already be sent in the inter-operator TAP records! Also, as a "ball park figure", 90% of subscribers are in their home network and 10% are roaming abroad, and the main usage of this field would be for the 90% of subscribers in their HPLMN.

So, it seems useful to add CGI/SAI information into the GTP signalling.

Further complexity arises however from the phrase "at record opening". In both SGSN and GGSN, it is possible to raise partial CDRs. A "partial CDR" is potentially generated every 15 minutes and reduces the fraud risks associated with only generating a full CDR after many mega bytes have been sent on a PDP context that has been open for several days. From reading 32.215 it seems that the Cell ID needs to be inserted into the S-CDR every time a partial CDR is opened.

Full support of the Cell ID in Partial G-CDRs appears difficult, however, a useful compromise would seem to be to add CGI/SAI information to all GTP messages that can be sent by the SGSN as a result of receiving a RANAP Direct Transfer message. When the mobile is using the Gb interface, the SGSN should add the CGI to these messages.

Hence it is recommended to add CGI/SAI as an optional parameters in the following GTP messages:

- Create PDP Context Request;
- Update PDP Context Request.

Whether or not the CGI/SAI is included by the SGSN should be controlled by the SGSN operator according to the PLMN-ID of the GGSN.

A.2.5 Access Point Name Operator Identifier

Section 14.13 of 3GPP TS 23.060 states that this field is part of the APN and that the APN is used to identify the GGSN. As such, it is logical that this field is included on the S-CDR.

However, there appears to be absolutely no need to transfer this field to the GGSN.

A.2.6 System Type

On the S-CDR, this indicates whether the SGSN serves 2G or 3G cells. There is no code point for a combined 2G/3G SGSN, and no indication as to whether or not the combined SGSN has separate 2G and 3G Routeing Areas!

It is recommended to add an "SGSN type" information element to the following GTP messages:

- Create PDP Context Request;
- Update PDP Context Request.

The contents of the “SGSN type” information element should be able to encode the following information, and permit future backwards compatible extension:

- 2G only SGSN;
- 3G only SGSN;
- Combined 2G/3G SGSN with all 2G cells in separate Routeing Areas to 3G cells;
- Combined 2G/3G SGSN with some 2G and 3G cells in the same Routeing Area.

Future additions might be needed to add in UMTS FDD/TDD differentiation, or if new Radio Access Technologies are adopted in the future.

Note that this “SGSN type” is different to the current “System type” field on the S-CDR. Whether or not the “System type” field on the S-CDR should be updated is FFS.

A.2.7 CAMEL information

Some CAMEL functionality relates to SGSN based on-line charging. When using SGSN based on-line charging, GGSN based on-line charging is unlikely to also be used. However, other CAMEL functionality relates to APN ID manipulation; SGSN resource utilisation, and the provision for the gsmSCF to write a “free format field” to the main CDR. This information appears to be useful to transfer to the GGSN.

Overall it appears simplest to transfer all the S-CDR CAMEL Information as one parameter from the SGSN to the GGSN. The format and encoding of this information element should be constructed in an extensible manner, hopefully by just referencing the encoding already used within 3GPP TS 32.215.

This information element should be included in the Create PDP Context Request and Update PDP Context Request messages.

A.2.8 RNC unsent data volume

If this information is useful to an SGSN, then it should be passed to the GGSN. In doing so it needs to be supplemented by the “2G SGSN unsent data volume”. Probably the unsent data volume could be accumulated by the new SGSN and sent to the GGSN at PDP context release. Providing this information to the new SGSN at inter SGSN change may require new GTP messages. Obtaining the information from the RNC may require additional use of existing RANAP signalling procedures.

However, as the value of sending this information from the RNC to the SGSN is as yet unclear, so far it is not agreed to add this information into the GTP signalling.

A.2.9 Time zone of the user’s location

Tariffs for different service flows may be time dependent, i.e. a tariff is different based on the time of the day, week or year (for example off-peak tariff for weekends, special holidays and/or night-times, on-peak tariff at day-time). Currently the time is reported at where the usage is measured. However the tariff may depend on the time at where the user is located. The time at the user’s location may be different than the time at the GGSN due different time zones and daylight saving time settings. Each SGSN should know the area and the corresponding time zone the user is within, and indicate that to the GGSN. Otherwise tariffs based on the time at user’s location may not be used.

Hence it is recommended to add “User Location Time Zone” as a parameter to the following GTP messages:

- Create PDP Context Request;
- Update PDP Context Request .in case of a SRNC relocation.

This parameter should indicate the offset from the GMT and the Daylight Saving Time period at the user's location. The GGSN adds it to the charging information (either to CDRs or to online credit requests).

NOTE 1; It should be noted that a SGSN may cover an area expanding over several time-zones. This adds complexity when user moves from a time-zone to another during an open PDP context.

NOTE 2; A solution applying user's location based on SGSN address, MNC, MCC or LAC/RAC/CI may not be elegant since it requires to keep information of each location a home users may roam.

A.3 RADIUS attributes

With the provision of the above information to the GGSN, then if RADIUS accounting is applied in the operator's network then it is recommended that the following RADIUS attributes are added to the appropriate RADIUS messages:

- IMEISV;
- CGI/SAI;
- SGSN type;
- CAMEL information.

Annex B (informative): IMS and Flow based charging

Flow Based Charging could be used to provide IMS Bearer Charging in addition to IMS Session Charging which is done at the S-CSCF or IMS Event Charging which is done at the AF. This requires the transfer of information about the IMS session.

Considering this, we need to study the usage of Flow Based Charging for IMS Bearer Charging in relation to IMS Session Charging or IMS Event Charging.

The following needs to be studied:

1. Flow Based Charging needs to provide a solution to the issues solved by Rel5 IMS charging correlation, considering issues such as backwards compatibility.

2. It needs to be clarified whether having multiple filters provided to the GGSN (over Go and Gx) is an issue (and if it is, it needs to be resolved).

3. How charging rules can be applied to the SIP signalling used for IMS session control

B.1 IMS SIP signalling

This section studies how flow based charging can be applied to the IMS signalling used for IMS session control.

It is to be noted though that the SIP signalling itself could carry different type of information that may be charged differently (e.g. SIP Session Invites, IMS messaging, etc.).

Possible ways to charge SIP with Flow Based Charging could consist of:

- Applying pre-configured static rules in the TPF;

- Obtaining charging rules from the CRF;

- Updating charging for the IMS signalling charging rules based on specific triggers (e.g. time of day, modification of the session parameters, etc.) for a given user.

Note: the usage of the signalling indication needs to be further studied with respect to Flow Based Charging.

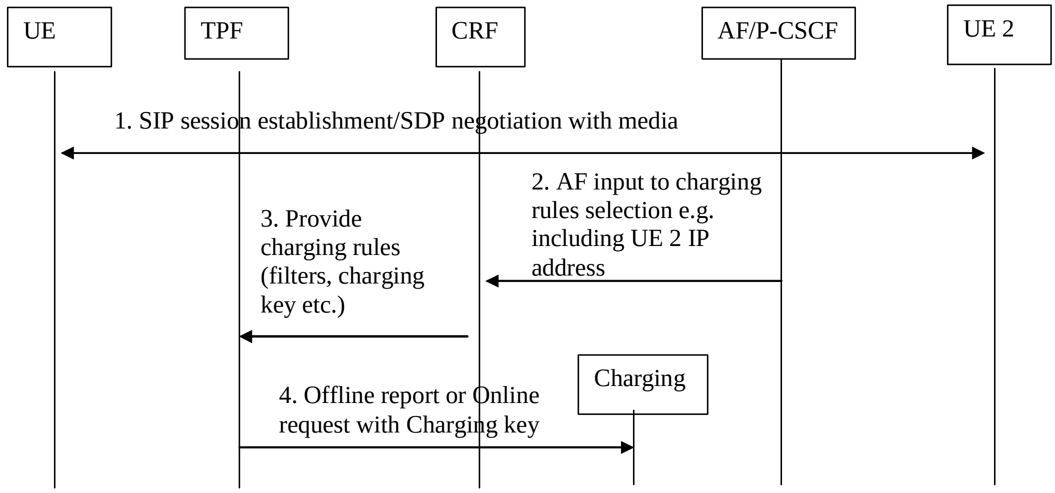
Since IMS SIP signalling may be compressed and encrypted, the TPF needs to be able to filter signalling based on other means than SIP application protocol identification. Therefore filters defined for IMS SIP signalling need to be based on IP 5-tuple. This also allows to charge SIP packets destined to the P-CSCF differently from other non IMS SIP packets.

B.2 IMS media

This section studies how flow based charging can be applied to the media associated with IMS sessions.

IMS media flows can be of two categories:

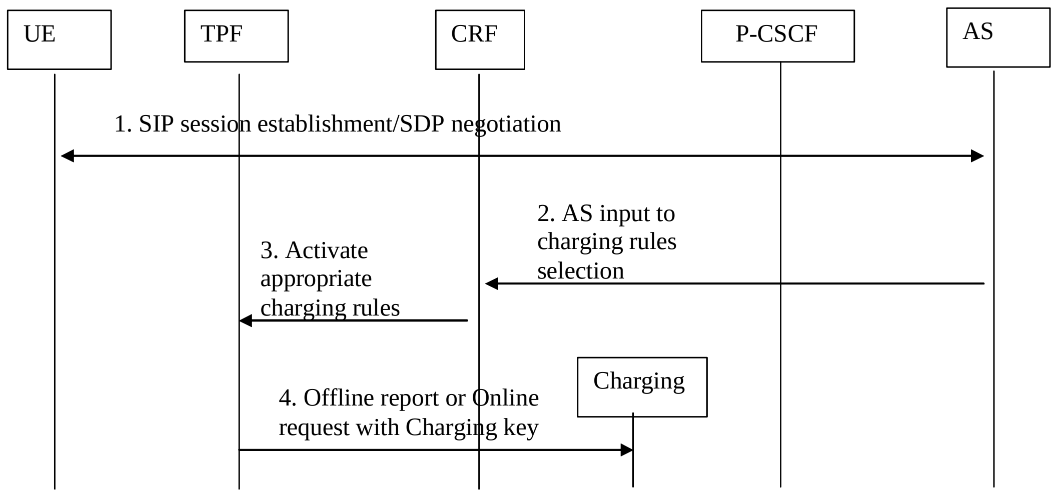
A. Peer-to-peer IMS media flows. Filters for these flows may need to be dynamically defined as the session control occurs for that particular peer-to-peer session. The details of the filters (e.g. destination address) may need to be dynamically provided to the TPF via the CRF (Rx and Gx interfaces).



1. IMS SIP session establishment occurs between UE1 and UE2, via a P-CSCF
2. The P-CSCF sends Rx input to the CRF for charging rules selection. This may include high level information such as identifying the IMS application. In the case of peer-to-peer, the information may include the IP address of the destination UE in order for the applicable filters to be applied by the CRF and TPF.
3. The CRF uses the input from the P-CSCF to complete the appropriate charging rules. The CRF provides the TPF with an appropriate charging key.
4. The charging key is used as an input to the rating logic in the offline or online charging system.

Note that session based messaging falls into this category, but immediate messaging doesn't (see IMS SIP signalling section).

B. Client/Server IMS media flows. Filters for these flows need to be identified dynamically when the session control is established to the server, but can reference well known IP 5-tuple for the client/server services used.



1. IMS SIP session establishment occurs between UE1 and AS, via a P-CSCF
2. The AS sends Rx input to the CRF for charging rules selection. This may include high level information such as identifying the IMS application.
3. The CRF uses the input from the AS to activate the appropriate charging rules. The CRF provides the TPF with an appropriate charging key.
4. The charging key is used as an input to the rating logic in the offline or online charging system.

The following issues are FFS:

- * AF input to the CRF in Step 2 above must include some identifier for the UE, so that the correct TPF can be identified.

* The CRF must determine which of the user's PDP Context(s) the new charging rule needs to be applied to. This could be based on analysis of the Traffic Flow Templates against the IP flow definitions in the new charging rule. Then the OCS may enforce that the IMS charging keys are only used on bearers with the right QoS by only providing quotas at the 'IMS rates' if the QoS matches that which is authorised for that special IMS charging key.

B.3 FBC with IMS compared to rel5 IMS charging correlation

The principles followed in B.1 and B.2 is that the charging key input to the rating logic allows the Offline or Online Charging System to determine the appropriate rate for the IMS session.

In rel5 where a correlation mechanism is used, the Offline or Online Charging System determines the GPRS and IMS charging records that are related in order to apply special handling. One example of special handling is to zero rate the GPRS volume, and use time based charging for the IMS session. Logic for determination of IMS-specific charging policies is contained within the Offline or Online Charging System.

In rel6 with FBC, special handling of IMS traffic can be achieved by activating the appropriate charging rules. For example, filters for IMS media/GPRS data from UE1 to UE2 can be associated in the charging rule with a charging key that is zero rated. Alternatively, special charging keys can be defined for 'IMS voice media' etc. In this case, a large part of the logic which determines IMS-specific charging policies is required to determine the Charging Key to be selected. This logic needs to be executed within the Application Function or Charging Rules function.

Additionally, the Offline and Online Charging systems in rel6, which support the FBC architecture, need to be enhanced to support the concept of charging key and thus use a different charging logic from that user in rel5 with charging correlation.

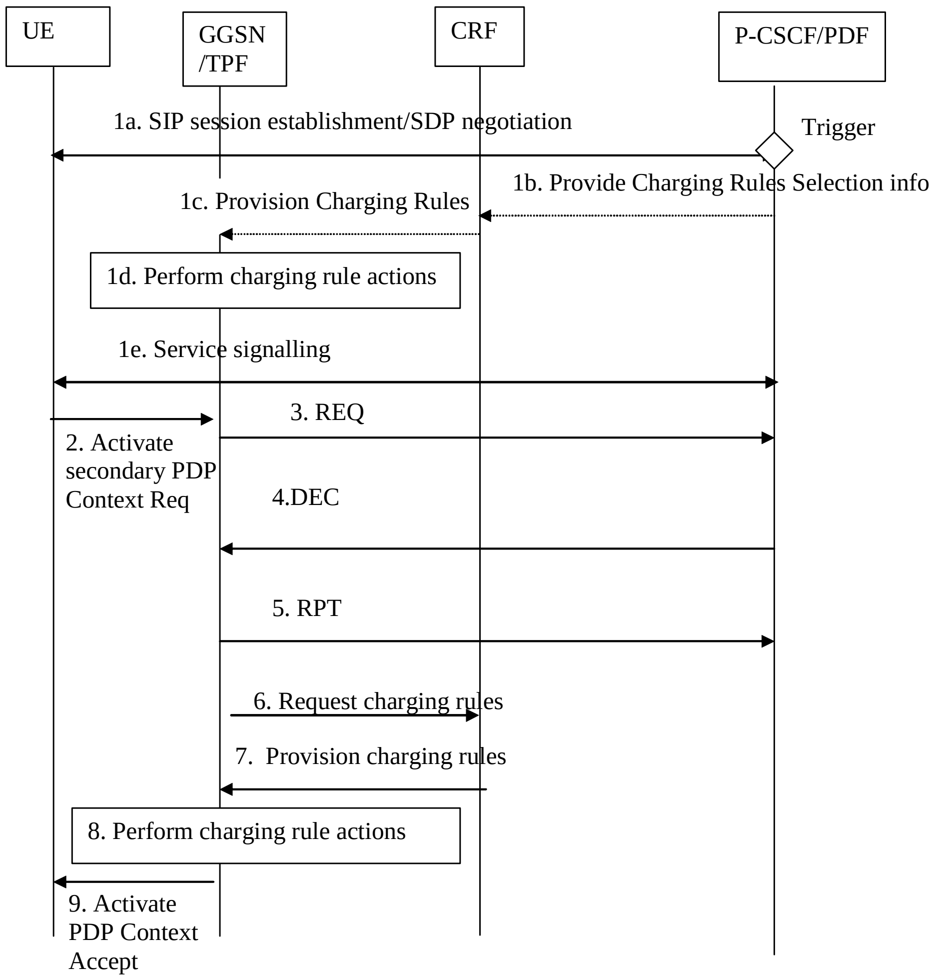
B.4 Rx/Gx functions and SBLP usage

Dynamic media stream filter information for QoS policy and charging correlation may be provided to the GGSN via the Gq and Go interfaces. This is described in TS 23.207 and TR 23.917.

Dynamic and static media stream filter information for charging (data for the charging rules) may be provided to the Traffic Plane Function (GGSN in the case of GPRS) via the Rx and Gx interfaces. This is described in this TS.

These two functions are independent and thus can be provided separately.

Mechanisms used for Rx/Gx functions and SBLP can be efficiently used for IMS bearer flow charging as the following description shows.



Scenario 1. PDF is co-located with P-CSCF

1a. The UE interacts with P-CSCF to establish a SIP session and negotiates the SDP parameters end to end.

1b. During SIP session establishment, P-CSCF may be triggered to provide charging rules selection info to CRF .

1c. If required, the CRF installs charging rules for the session's media components for the already active bearers (PDP Contexts) to the TPF.

1d. The TPF performs charging rule actions as indicated.

1e. The P-CSCF forwards the service signaling message containing the session description. The P-CSCF shall include the authorization token in this service signaling message.

2. UE sends activate secondary PDP Context request.

3. The GGSN sends a COPS REQ message with the Binding Information to the PDF in order to obtain relevant policy information.

4. The PDF sends a COPS DEC message back to the GGSN/TPF.

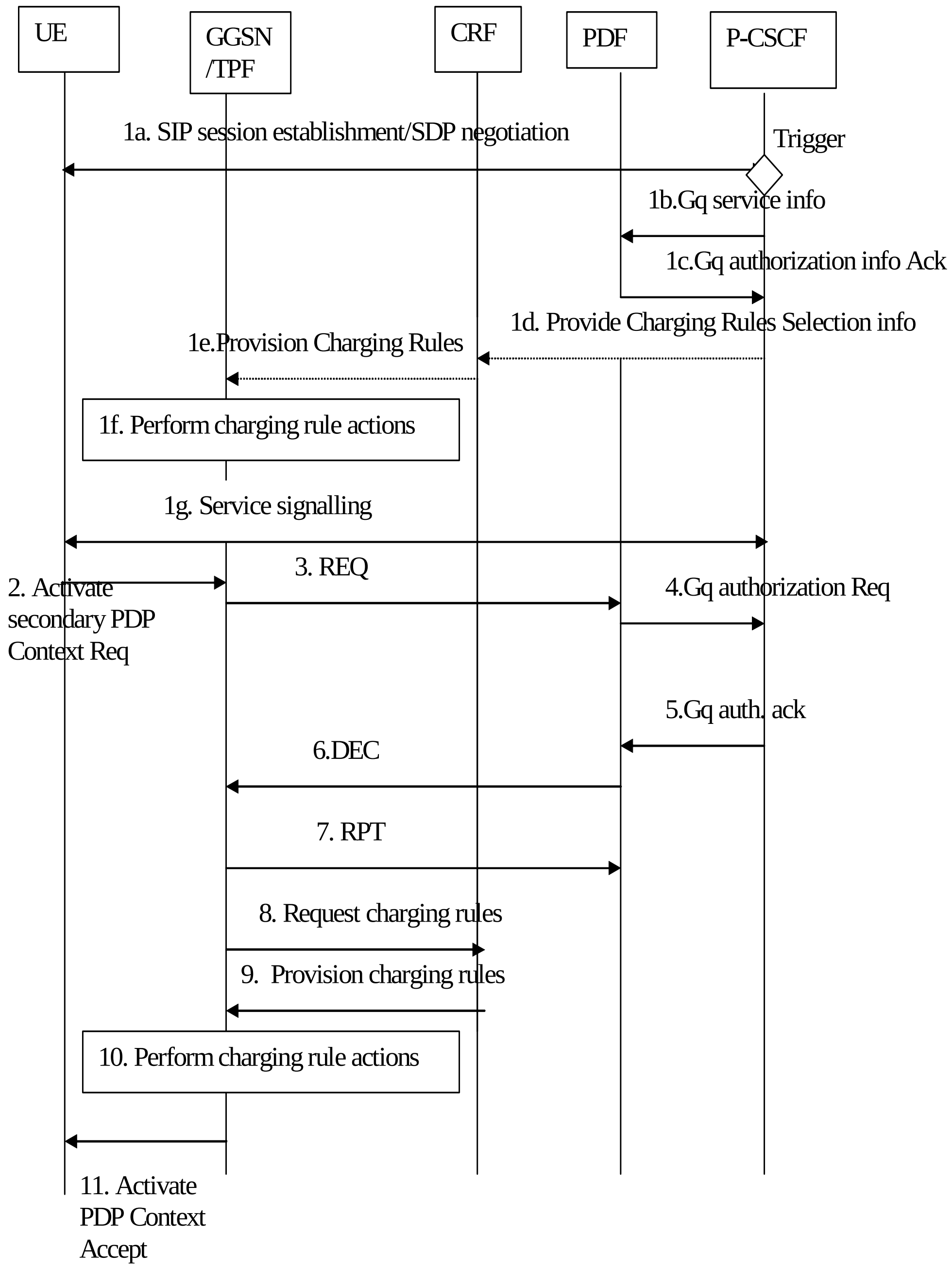
5. The GGSN sends a COPS RPT message back to the PDF.

6. GGSN/TPF requests charging rules from CRF.

7. CRF provides charging rules to GGSN/TPF.

8. The TPF performs charging rule actions as indicated.

9. GGSN sends activate PDP context accept to confirm that bearer service is ready.



Scenario 2. Gq interface is used

1a. The UE interacts with P-CSCF to establish a SIP session and negotiates the SDP parameters end to end.

1b~1c. During SIP session establishment, P-CSCF may be triggered to send a request for authorization token to the PDF with full service information, which includes session description information based on the session signaling.

1d. Based on SIP session information and local policy, P-CSCF may provide charging rules selection info to CRF immediately after Gq interface interaction.

1e. If required, the CRF installs charging rules for the session's media components for the already active bearers (PDP Contexts) to the TPF.

1f. The TPF performs charging rule actions as indicated.

1g. The P-CSCF forwards the service signaling message containing the session description. The P-CSCF shall include the authorization token in this service signaling message.

2. UE sends activate secondary PDP Context request.

3. The GGSN sends a COPS REQ message with the Binding Information to the PDF in order to obtain relevant policy information.

4. Further interaction between the P-CSCF and the PDF to provide the full service information is needed. PDF sends an authorisation request to P-CSCF.

5. P-CSCF responds to PDF's request.

Note: step 4,5 only happen when further interaction between PDF and P-CSCF is needed.

6. PDF sends a COPS DEC message back to the GGSN/TPF.

7. GGSN sends a COPS RPT message back to the PDF.

8. GGSN/TPF requests charging rules from CRF.

9. CRF provides charging rules to GGSN/TPF.

10. The TPF performs charging rule actions as indicated.

11. GGSN sends activate PDP context accept to confirm that bearer service is ready.

Annex C (informative): WLAN and flow based charging

C.1 TPF usage for WLAN

For WLAN, the TPF is a logical function allocated to the PDG.

NOTE: In case the PDG is implemented using the Gn' reference point, then the TPF is allocated to the GGSN-part of the PDG. For further details of. TS 23.234 [10].

Annex D (informative): Policy functions provided by FBC architecture

D.1 General

This Annex studies the possibilities and solutions for evolving FBC towards supporting policy control functions similar but not equivalent to what is provided by SBLP and Go. However, policy requirements in the context of FBC need to be clarified and could establish different needs than those of SBLP and Go. SBLP focuses on the control of bearer resources based on a binding mechanism that binds one or more service to a bearer. FBC evolution towards supporting policy control functions is mainly aiming for the policy control of the service itself.

Once the architecture and functionalities described in this Annex become stable, parts of the content are intended to be moved to the main body of this document. Some parts have been included in the body upon this release of the specifications, other parts may be included in the next release.

D.2 General architectural considerations

Considering the FBC development described in this specification, as well as the definition of new services e.g. IMS based services, which were not available in Release 5, it has been recognized that there is a need to introduce flexibility in the handling of the different services. It will be studied whether a CRF responsible for Charging Rules and Policy control may be considered. This could facilitate the possibility to minimize the number of nodes to maintain as well as for Stage 3 defined interfaces i.e. from a Stage 3 point of view interfaces may be re-used.

Media flows for an AF (e.g. IMS) can be divided into two categories:

- Peer-to-peer where the AF (e.g. P-CSCF) may provide information to the CRF for Charging Rule selection;
- Client/Server media flows where the AF (e.g. AS) sends input to the CRF for Charging Rule selection. The handling of the Charging Rule procedures as defined in Annex B is to be performed dynamically.

The handling of Charging Rules and the procedures related to selecting charging rules is specified in this technical specification. Below, the procedures for possible handling of policy control within the FBC framework are described.

It shall be possible to have multiple flows over the same PDP context.

It shall be possible to support generic IP flow policies.

The CRF shall take the responsibility for all applications, which means that conflicts between policies are alleviated facilitating easier and faster provisioning of services. The CRF shall be responsible for the precedences of the policies. An AS may provide information to the CRF whether the subscriber is allowed to access the service or not as an input to the decision function for filter definition.

The evolved FBC architecture including not only charging rules but also policy control shall implement policies for both IMS and non-IMS services, as SBLP has also been generalized in Rel6 to support both IMS and non-IMS services.

The CRF not only provides dynamic filters but also references to pre-configured filters.

The following subclauses provide a list and corresponding analysis of policy functions considered to be provided by the FBC architecture.

D.2.1 Charging correlation

The FBC architecture provides an alternative bearer charging mechanism. The charging key passed to the OCS/CCF is the only input to the rating logic (along with any AF/CSCF input about type of sessions, start/stop time of session etc. that may have come from Ro/Rf).

FBC provides the capability for charging correlation through the usage of Application Function Record information. In case of IMS the Application Function Record information should include the ICID and the flow ID(s).

Since the charging systems may need to be upgraded in this release to support FBC, we could use the FBC model and logic based on the charging key, instead of adding any correlation identifier (ICID) to Gx/Gy.

This function is part of this release.

D.2.2 Gating

This refers to the ability to block or allow traffic to flow. This can be achieved by the TPF in the FBC architecture which discards the packets for the service data flow in case of no applicable filters for this service data flow. However, it is only possible to implicitly block a specific service data flow, i.e. in case there are no other charging rules matching the service data flow for any bearer.

For peer-to-peer traffic, special rates may apply. The gate could therefore be either closed for this traffic before the applicable filters are available, or the gate could be opened with a more generic charging rule which doesn't allow for this special rate to apply yet.

The AF (e.g. P-CSCF) could wait until answer to give Rx input to the CRF which then sends this information down to the TPF, allowing for the filters for this peer-to-peer traffic to form a new charging rule. This allows waiting until the final SDP and the actual answer to allow the special rate to apply (and possibly the traffic to flow if no other filters were applicable before). As soon as the rules are sent down to the TPF then they are active at the TPF.

Compared to Gq/Go gating functionality the FBC ability of blocking traffic provides for further flexibility in combining the charging and policy models, because Go/Gq do not provide for a model where different rates can be applied in combination with different gating rules. However, FBC is able to prevent the usage of a specific PDP context as Gq/Go gating functionality does as long as there is no other matching charging rule established for this PDP context.

The functionality for allowing and implicit blocking of service data flows is part of this release.

Editor's note: It is FFS if and how the explicit blocking (i.e. blocking of a specific service data flow that also matches a generic charging rule) can be provided by FBC.

D.2.3 QoS control

This refers to the ability to authorize different QoS for different applications (even peer-to-peer session) and to the ability to control the bandwidth usage once the traffic has been allowed to flow.

Requirements need to be identified for QoS control in the context of FBC, which could be different needs than those of SBLP and Go. FBC provides means to control what bearer a service flow is allowed to be carried on. This implicitly allows the CRF to control the QoS parameters of the bearer a service flow is allowed to use. A charging rule may only apply to one or more particular bearer(s) (to a particular PDP Context in case of GPRS). Hence, the QoS the service flow is allowed to use is restricted to the QoS of a particular bearer(s).

To evolve the FBC architecture towards complete QoS control for the service data flow as well as the bearer enhancements and extensions are probably required. The binding concept could be replaced by TFT interpretation to some extent but for the uplink similar information would be required. The control of the bitrate of a PDP context is only possible in case the charging rules apply only to a particular bearer. Otherwise one does not know on which bearer and at which time the service data flows occur.

The functionality for limiting the maximum QoS class of a service data flow is part of this release.

Editor's note: It is FFS how complete QoS control can be provided by FBC

D.2.4 Bearer events

Indication of bearer events could allow for communication between the GGSN and the AF (P-CSCF in IMS).

In case a charging rule for an AF service flow applies only to a particular bearer, it is possible for the CRF to inform the AF about events related to that bearer. However, this bearer event indication functionality of FBC only works if there is no matching charging rule installed for any other bearer.

In case a charging rule for an AF service flow applies to more than one bearer of a UE IP address or more than one matching charging rule is applied, it is only possible for the CRF to inform the AF in case of the removal of all these bearers of a UE IP address (i.e. the AF is not aware of the removal of individual bearers). Because due to the missing binding concept it is difficult to predict if a service data flow would use another PDP context instead once the previously used PDP context was deleted. Therefore, it may not be necessary or even wrong to inform the AF. Furthermore, the knowledge which service data flows are currently active may need to be extended to the CRF because an AF is only interested in such information if the corresponding service data flow is currently active.

The functionality for informing the CRF about the removal the last bearer for a specific IP address and APN is part of this release. Based on the applied charging rules, the CRF may also be able to inform the AF about events related to a particular bearer.

Editor's note: There is a need to confirm whether this functionality is required in the case that the service data flow used for the AF session can be found on multiple bearers.

D.2.5 Session events

This refers to the ability to react on AF session modification or AF session release, e.g. upon IMS session release. This can be provided by the Rx input which allows the AF to tell the CRF that e.g. no charging rule exists for a traffic flow any more, meaning the traffic will no longer be allowed at the TPF. The same applies if, over the Gy reference point, the OCS indicates to abort the session (Abort Session Request in Diameter Credit Control).

While the FBC architecture supports an update of charging rules in the TPF due to a session modification, it is only to some extent possible to enforce a bearer modification or removal. It is possible to disable the service data flow belonging to the AF session as long as there are no other matching charging rules. However the actual bearer release or modification cannot be enforced in general.

The functionality for updating the charging rules in the TPF due to a session modification is part of this release.

Editor's note: It is FFS if and when the TPF could release the entire bearer (e.g. GGSN PDP context deletion).

D.3 Summary and comparison

Go/Gq procedure	**Provides for**	**FBC equivalent in this release**	**FBC equivalent not in this release**
Authorize QoS Resources, AF session establishment	QoS control, charging correlation	Transfer of charging correlation information Or relies on charging key for rating instead of charging correlation QoS control is limited to maximum QoS class for a service data flow (in case no other matching charging rule is in place)	Complete QoS control for service data flow and the bearer is FFS
Authorize QoS Resources, bearer establishment	QoS control, charging correlation	Transfer of charging correlation information Or relies on charging key for rating instead of charging correlation QoS control is limited to maximum QoS class for a service data flow (in case no other matching charging rule is in place)	Complete QoS control for service data flow and the bearer is FFS

Enable Media procedure	Gating (open)	Provide charging rules over Gx for the traffic flow Provide credit over Gy for the traffic flow Service data flow can be enabled and usage of bearer controlled (in case no other matching charging rule is in place)	Control of bearer usage in case of existing other matching charging rules is FFS
Disable Media procedure	Gating (close)	Provide no charging rule over Gx for the traffic flow Provide no credit over Gy for the traffic flow Service data flow can be disabled and usage of bearer controlled (in case no other matching charging rule is in place)	Control of bearer usage and explicit disabling in case of existing other matching charging rules is FFS
Revoke Authorization for GPRS and IP Resources	Session events	AF input to provision of charging rules over Rx followed by Provision of Charging Rules triggered by other event to the CRF, Or OCS Abort Session Request	Complete QoS control for service data flow and the bearer is FFS
Indication of PDP Context Release	Bearer events	Bearer service termination over Gx and Gy Rx in case a charging rule applies only to this bearer and no other matching charging rules are used on any other bearer	Rx in the general case is FFS
Authorization of PDP Context Modification	QoS control	Bearer service modification over Gx Rx in case a charging rule applies only to this bearer and no other matching charging rules are used on any other bearer	Complete QoS control for service data flow and the bearer is FFS Rx in the general case is FFS
Indication of PDP Context Modification	Bearer events	Bearer service modification over Gx Rx in case a charging rule applies only to this bearer and no other matching charging rules are used on any other bearer	Rx in the general case is FFS
Update Authorization procedure	QoS control	AF input to provision of charging rules over Rx followed by Provision of Charging Rules triggered by other event to the TPF, Or OCS initiated re-authorisation	Complete QoS control for service data flow and the bearer is FFS

Annex E (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-01					Initial base		0.0.1
2004-01					Moved text from TR 23.825 v 1.4.0, editorial changes	0.0.1	0.1.0
2004-02					Updated with approved contributions from SA2#38 (Atlanta): S2-040695, S2-040696, S2-040700, S2-040701, S2-040702, S2-040703, S2-040705, S2-040706, S2-040707, S2-040708, S2-040963, S2-040964, S2-040965, S2-041027	0.1.0	0.2.0
2004-02					Editorial changes in chapter 7.1 and annex D	0.2.0	0.2.1
2004-03	SA #23	SP-040050			Presentation to SA #23 plenary for approval	0.2.1	2.0.0
2004-03	SA #23	SP-040050			Raised to v.6.0.0 after approval at SA#23 (same content as previous version)	2.0.0	6.0.0
2004-06	SA #24	SP-040314	002	1	Introduction of charging rule identifier	6.0.0	6.1.0
2004-06	SA #24	SP-040314	004	1	Add some use cases to the Flow Based Charging	6.0.0	6.1.0
2004-06	SA #24	SP-040314	006	2	Time based charging tariffs	6.0.0	6.1.0
2004-06	SA #24	SP-040314	008	2	FBC and IMS	6.0.0	6.1.0
2004-06	SA #24	SP-040314	009		RAT Type as possible re-authorisation trigger	6.0.0	6.1.0
2004-06	SA #24	SP-040314	011	1	Ro reference removal	6.0.0	6.1.0
2004-06	SA #24	SP-040314	013	2	Traffic flow at TPF	6.0.0	6.1.0
2004-06	SA #24	SP-040314	016	1	Time and volume allocation in online charging	6.0.0	6.1.0
2004-06	SA #24	SP-040314	018		General Corrections	6.0.0	6.1.0
2004-06	SA #24	SP-040314	019		Gx connection maintenance	6.0.0	6.1.0
2004-06	SA #24	SP-040314	020		Rx connection maintenance	6.0.0	6.1.0
2004-06	SA #24	SP-040314	021	2	FBC online charging	6.0.0	6.1.0
2004-06	SA #24	SP-040314	024	1	Message flow for input to provision of charging rules in Ry interface	6.0.0	6.1.0
2004-06	SA #24	SP-040314	025	2	Correction to the Termination Action	6.0.0	6.1.0
2004-06	SA #24	SP-040314	027		Clarification to the charging rule	6.0.0	6.1.0
2004-06	SA #24	SP-040314	028	1	Information to support charging rule selection	6.0.0	6.1.0
2004-06	SA #24	SP-040314	033	1	Re-authorization in case of charging rule change	6.0.0	6.1.0
2004-06	SA #24	SP-040314	035	1	Applying charging rules input from AF	6.0.0	6.1.0
2004-06	SA #24	SP-040314	036	1	Set of charging rules	6.0.0	6.1.0
2004-06	SA #24	SP-040314	037	3	Policy functions provided by FBC	6.0.0	6.1.0
2004-06	SA #24	SP-040314	043	1	TPF in the GGSN for WLAN access	6.0.0	6.1.0
2004-06	SA #24	SP-040314	045	2	FBC and GAA	6.0.0	6.1.0
2004-06	SA #24	SP-040314	046	2	Limitations of FBC for IMS	6.0.0	6.1.0
2004-06	SA #24	SP-040458	047		Combined CR for CR#3, CR#12, CR#14	6.0.0	6.1.0
2004-09	SA #25	SP-040518	048	2	Add CCF and/or OCS address to charging rule	6.1.0	6.2.0
2004-09	SA #25	SP-040518	051	1	Add a definition of TPF/CRF instance	6.1.0	6.2.0
2004-09	SA #25	SP-040518	055		Allowing specific charging rule selection for dedicated IMS signalling PDP contexts	6.1.0	6.2.0
2004-09	SA #25	SP-040518	056	2	Application Function Tag	6.1.0	6.2.0
2004-09	SA #25	SP-040518	059	2	Clarification on precedence of charging rules	6.1.0	6.2.0
2004-09	SA #25	SP-040518	060	2	Rx/Gx functions and SBLP usage in IMS Charging	6.1.0	6.2.0
2004-09	SA #25	SP-040518	061	2	Policy control functions provided by FBC	6.1.0	6.2.0
2004-09	SA #25	SP-040518	063	2	Clarification of pre-defined charging rules	6.1.0	6.2.0
2004-09	SA #25	SP-040518	064		Clarification on charging rules	6.1.0	6.2.0
2004-09	SA #25	SP-040518	065	2	Traffic plane function behaviour	6.1.0	6.2.0
2004-09	SA #25	SP-040518	066	2	Termination action	6.1.0	6.2.0
2004-09	SA #25	SP-040518	067		Re-authorization triggers	6.1.0	6.2.0
2004-09	SA #25	SP-040518	068	1	Gx reference point functions	6.1.0	6.2.0
2004-09	SA #25	SP-040518	069	2	Clarifications in message flows	6.1.0	6.2.0
2004-09	SA #25	SP-040518	070	2	Bearer service modification in case of online charging	6.1.0	6.2.0
2004-09	SA #25	SP-040518	071	2	Policy functions of FBC – update of Annex D	6.1.0	6.2.0
2004-09	SA #25	SP-040518	072	1	Removal of superfluous FFS notes	6.1.0	6.2.0
2004-09	SA #25	SP-040518	074	2	FBC Control	6.1.0	6.2.0
2004-09	SA #25	SP-040518	075	1	TPF performing no charging	6.1.0	6.2.0
2004-12	SA #26	SP-040753	078	3	CCF/OCS address clarifications	6.2.0	6.3.0
2004-12	SA #26	SP-040753	079	1	Connection maintenance	6.2.0	6.3.0
2004-12	SA #26	SP-040753	080	1	Modification of charging rules	6.2.0	6.3.0
2004-12	SA #26	SP-040753	083	2	Clarify that SGSN event is MCC/MNC related	6.2.0	6.3.0
2004-12	SA #26	SP-040753	085	2	Clarify the handling of PDP contexts	6.2.0	6.3.0
2004-12	SA #26	SP-040753	086	2	Clarify that Charging Rules apply on a per PDP context basis	6.2.0	6.3.0
2004-12	SA #26	SP-040753	088	1	CRF addressing	6.2.0	6.3.0
2004-12	SA #26	SP-040753	089	1	Removal of FFS notes	6.2.0	6.3.0
2004-12	SA #26	SP-040753	091	2	Clarify the terminology related to instances	6.2.0	6.3.0

2004-12	SA #26	SP-040753	092	1	Clarification of credit pooling	6.2.0	6.3.0
2004-12	SA #26	SP-040753	093		Clarify that CRF is responsible for policy control functions in FBC	6.2.0	6.3.0
2004-12	SA #26	SP-040753	094	3	Selecting the charging rule	6.2.0	6.3.0
2004-12	SA #26	SP-040753	095	1	Security considerations between CRF and AF	6.2.0	6.3.0
2004-12	SA #26	SP-040753	096	1	Selection of the appropriate CRF by a TPF for a user in GPRS.	6.2.0	6.3.0
2004-12	SA #26	SP-040753	098	1	Clarification of volume and time based charging	6.2.0	6.3.0
2004-12	SA #26	SP-040753	099	2	Clarification of online charging procedure	6.2.0	6.3.0
2004-12	SA #26	SP-040753	101		Update of bearer termination message flow	6.2.0	6.3.0
2004-12	SA #26	SP-040882	102	1	Reporting and credit management granularity	6.2.0	6.3.0
2004-12	SA #26	SP-040753	103	2	Updates to Rx handling	6.2.0	6.3.0

History

Document history		
V6.3.0	December 2004	Publication