(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2012 (06.12.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/163405 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 28/16* (2009.01)
H04W 12/08 (2009.01)

(21) International Application Number:
PCT/EP2011/058928

(22) International Filing Date:
31 May 2011 (31.05.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **HELLGREN, Vesa, Pauli** [FI/FI]; Hakaniemenranta 26 A 12, FI-00530 Helsinki (FI).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: COMMUNICATION CONTROL IN COMMUNICATION NETWORKS

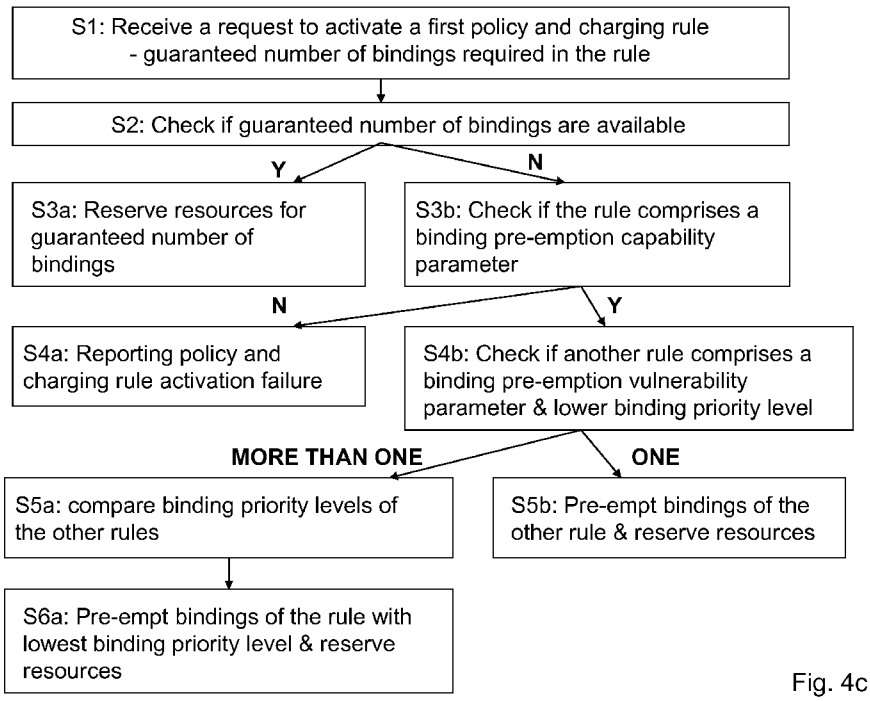


Fig. 4c

(57) **Abstract**: A method is provided for controlling firewall or network address translation function comprising receiving a request to activate a first communication control rule, said rule comprising at least one communication control rule parameter wherein said communication control rule is associated with controlling firewall or a network address translation function policy.

WO 2012/163405 A1

Description

Title

Communication control in communication networks

FIELD OF THE INVENTION

The present invention relates to communication control in communication systems. In particular, the present invention relates to a method, apparatuses, a system and a computer program product for controlling network address translator and firewall policies in a telecommunication network.

BACKGROUND ART

There are currently several Internet Protocol (IP) version 4 (IPv4) address sharing mechanisms such as network address translator (NAT), e.g. NAT44, because of shortage of IPv4 addresses. When an IP flow is initiated from a user side and its source IPv4 address is replaced by a shared IPv4 address at a NAT44 device, the source transmission control protocol / user datagram protocol (TCP/UDP) port in the IPv4 packet is also replaced by one dynamically allocated by the NAT44 device, most likely from a single port pool, and as such, the IP flow can be uniquely identified end-to-end. A NAT44 device usually randomizes the port selection, and this practice helps enhance the security in the network. However, such practice increases the translation logging task on a NAT44 device. Each NAT44 translation log entry corresponds to a unique IP flow and typically includes the destination address and port, translated source address (the shared IPv4 address), translated source port (the one allocated by the NAT44 device), original source address and port, etc. It requires large volume of storage and also processing capacity on a NAT44 device for such operation.

Firewalls are deployed in the third generation of mobile phone standards (3G) and beyond networks at various places for protection against attacks and for access control to define which host is permitted to use certain services or applications. Some examples of possible locations for firewalls are:

- at the changeover point between radio access networks and an IP-based packet core
- inside the packet core network to make attacks more difficult (detection of distributed attacks)
- at administrative borders between two operators
- at the entry point of an IP Multimedia Subsystem (IMS) and
- towards the public internet

The most common type of firewall is a packet filter that permits traffic flow identified by the so called IP-5tuple: source address and port number, destination address and port number, and the higher-layer protocol (usually TCP or UDP). Such packet filters are implemented in a Gateway General Packet Radio Service (GPRS) Support Node (GGSN) of today's 2.5G and 3G networks, they are used for filtering based on traffic flow templates (TFT, see e.g. section 15.3. of 3GPP TS 23.060, version 10.3.0) or service-based local policy (SBLP, see e.g. section 4 of 3GPP TS 29.207, version 6.5.0).

For policy control in IMS, a Policy Decision Function (PDF) entity has been specified; the corresponding Policy Enforcement Function (PEF) is located in the GGSN. Lately, this PEF has been changed to a Policy and Charging Control (PCC) architecture which will unify the previously separate systems for policy and charging control. In this new architecture, the tasks of a PDF are carried out by a Policy and Charging Rules Function (PRCF), whereas the PEF is included in a Policy and Charging Enforcement Function (PCEF), which is still

located inside the GGSN or a packet data network (PDN) gateway (P-GW).

The general 3GPP IMS architecture is specified in 3GPP TS 23.228 (see e.g. version 11.0.0). Annex G defines the reference architecture for the case where NAT and/or firewall is invoked between a user equipment (UE) and the IMS domain, as illustrated in Figure 1. This architecture maps to the basic PCC architecture, where a Proxy Call Session Control function (P-CSCF) is an Application Function (AF). NAT and firewall function may be co-located with PCEF in one gateway node, see Figure 2.

The basic PCC rule procedures are specified in section 4 of 3GPP TS 29.212 (see e.g. version 11.0.1) and illustrated in Figure 3. When a PDN connection is activated in a PCEF, the PCEF sends information about the PDN connection to PCRF (including e.g. International Mobile Subscriber Identity (IMSI), Mobile Station International Integrated Services Digital Network (ISDN) Number (MSISDN), etc.) in a Credit Control Request (CCR) Diameter message and the PCRF returns PCC rule(s) in a Credit Control Answer (CCA) Diameter message. PCEF then activates the PCC rule for the activated PDN connection.

NAT function requires maintaining state information about the active NAT bindings. Stateful firewalls are similar to NAT in that sense that they also maintain state information about the active traffic flows, so that they are able to allow or block traffic if the flow is initiated from a wrong source direction or there are too many active flows. For example, firewall may allow uplink packet from a user equipment (UE) to pass to any Hypertext Transfer protocol (HTTP) server, but traffic from a HTTP server is not allowed if the UE has never sent any traffic to it (in this way the firewall can prevent e.g. billing attacks). The term “binding” is used for the resource usage related to single traffic flow, where NAT and/or firewall function is enabled.

3GPP has not defined how the NAT/firewall policies are to be managed if the NAT/firewall function is implemented as part of GGSN or P-GW. In particular, there are no methods for defining how to control the resource usage related to active bindings. Gateway nodes do not have infinite resources, so there is a limit for active bindings.

SUMMARY

It is therefore an object of this invention to address some of the above mentioned problems by providing a method, apparatuses, a system and a computer program product for communication control, e.g. controlling NAT and firewall policies, in mobile telecommunication systems.

The present invention aims to define NAT and firewall policies in a policy control server and to enforce those policies in the gateway product(s) which implement NAT and/or firewall function. The main focus is in the 3GPP architecture, where policy control is implemented in PCRF and policy enforcement is implemented in GGSN or P-GW nodes.

According to a first aspect of the invention, there is provided a method for controlling firewall or network address translation function comprising receiving at a policy and charging enforcement function a request to activate a first communication control rule, for example a policy and charging rule, the rule comprising at least one communication control rule parameter, wherein the communication control rule is associated with controlling firewall or network address translation function policy.

According to some embodiments, the at least one communication control rule parameter comprises a maximum number of firewall or network address translation function bindings for an application, a guaranteed number of firewall or network address translation function bindings for an application, a binding

pre-emption capability of the communication control rule, a binding pre-emption vulnerability of the communication control rule, or a binding priority level of the communication control rule.

According to further embodiments, the method further comprises storing the first communication control rule. In some embodiments, the first communication control rule is stored as a part of local policy and charging rules at the policy and charging enforcement function.

According to further embodiments, the method further comprises receiving the first communication control rule from a policy and charging rules function. In some embodiments, the first communication control rule is received in an attribute value pair via Gx interface. In some embodiments, the first communication control rule is received in a diameter credit control answer message.

According to further embodiments, the first communication control rule comprises a guaranteed number of firewall or network address translation function bindings parameter and the method further comprises checking whether at least the guaranteed number of firewall or network address translation function bindings are available.

According to further embodiments, the method further comprises reserving resources for the guaranteed number of firewall or network address translation function bindings as part of the first communication control rule activation in case at least the guaranteed number of firewall or network address translation function bindings are available.

According to further embodiments, the method further comprises checking whether the first communication control rule comprises a binding pre-emption capability parameter in case at

least the guaranteed number of firewall or network address translation function bindings are not available.

According to further embodiments, the method further comprises reporting communication control rule activation failure in case the first communication control rule does not comprise a binding pre-emption capability parameter.

According to further embodiments, the method further comprises checking whether at least one second activated communication control rule, for example a policy and charging rule, comprises a binding pre-emption vulnerability parameter and whether the at least one second activated communication control rule comprises a lower binding priority level than the first communication control rule in case the first communication control rule comprises a binding pre-emption capability parameter.

In some embodiments, one second activated communication control rule comprises a binding pre-emption vulnerability parameter and a lower binding priority level than the first communication control rule and the method further comprises pre-empting (S5) at least one firewall or network address translation function binding associated with the one second activated communication control rule, and reserving resources for the guaranteed number of firewall or network address translation function bindings as part of the first communication control rule activation.

In some embodiments, at least two second activated communication control rules comprise a binding pre-emption vulnerability parameter and a lower binding priority level than the first communication control rule and the method further comprises comparing binding priority levels of the at least two second activated communication control rules.

According to further embodiments, the method further comprises pre-empting at least one firewall or network address translation function binding associated with a second activated communication control rule with lowest priority level, and reserving resources for the guaranteed number of firewall or network address translation function bindings for activating the first communication control rule.

According to further embodiments, the method further comprises pre-empting firewall or network address translation function bindings associated with a second activated communication control rule such that the guaranteed number of firewall or network address translation function bindings comprised in the first communication control rule are available.

According to some embodiments the first communication control rule comprises a policy and charging rule. According to some embodiments the second communication control rule comprises a policy and charging rule. According to some embodiments the communication control parameter rule comprises a policy and charging rule parameter.

According to a second aspect of the invention, there is provided an apparatus comprising an input configured to receive a request to activate a first communication control rule, for example a policy and charging rule, the rule comprising at least one communication control rule parameter, wherein the communication control rule is associated with controlling firewall or network address translation function policy.

According to some embodiments, the at least one communication control rule parameter comprises a maximum number of firewall or network address translation function bindings for an application, a guaranteed number of firewall or network address translation function bindings for an application, a binding pre-emption capability of the communication control rule, a binding pre-emption vulnerability of the communication con-

trol rule, or a binding priority level of the communication control rule.

According to some embodiments, the apparatus further comprises a memory configured to store the first communication control rule. In some embodiments, the memory is further configured to store the first communication control rule as a part of local policy and charging rules.

According to some embodiments, the input is further configured to receive the first communication control rule from a policy and charging rules function. In some embodiments, the input is further configured to receive the first communication control rule in an attribute value pair via Gx interface. In some embodiments, the input is further configured to receive the first communication control rule in a diameter credit control answer message.

According to further embodiments, the first communication control rule comprises a guaranteed number of firewall or network address translation function bindings parameter and the apparatus further comprises a processor configured to check whether at least the guaranteed number of firewall or network address translation function bindings are available.

According to further embodiments, the processor is further configured to reserve resources for the guaranteed number of firewall or network address translation function bindings as part of the first communication control rule activation in case at least the guaranteed number of firewall or network address translation function bindings are available.

According to further embodiments, the processor is further configured to check whether the first communication control rule comprises a binding pre-emption capability parameter in case at least the guaranteed number of firewall or network address translation function bindings are not available.

According to further embodiments, the apparatus further comprises an output configured to report communication control rule activation failure in case the first communication control rule does not comprise a binding pre-emption capability parameter.

According to some embodiments, the processor is further configured to check whether at least one second activated communication control rule, for example a policy and charging rule, comprises a binding pre-emption vulnerability parameter and whether the at least one second activated communication control rule comprises a lower binding priority level than the first communication control rule in case the first communication control rule comprises a binding pre-emption capability parameter.

In some embodiments, one second activated communication control rule comprises a binding pre-emption vulnerability parameter and a lower binding priority level than the first communication control rule, and the processor is further configured to pre-empt at least one firewall or network address translation function binding associated with the one second activated communication control rule, and to reserve resources for the guaranteed number of firewall or network address translation function bindings as part of the first communication control rule activation.

In some embodiments, at least two second activated communication control rules comprise a binding pre-emption vulnerability parameter and a lower binding priority level than the first communication control rule and the processor is further configured to compare binding priority levels of the at least two second activated communication control rules.

According to further embodiments, the processor is further configured to pre-empt at least one firewall or network ad-

dress translation function binding associated with a second activated communication control rule with lowest priority level, and to reserve resources for the guaranteed number of firewall or network address translation function bindings as part of the first communication control rule activation.

In some embodiments, the processor is further configured to pre-empt firewall or network address translation function bindings associated with a second activated communication control rule such that the guaranteed number of firewall or network address translation function bindings comprised in the first communication control rule are available.

In some embodiments, the apparatus comprises a policy and charging enforcement function. In some embodiments, the apparatus is located in a gateway general packet radio service support node or in a packet data network gateway.

According to some embodiments the first communication control rule comprises a policy and charging rule. According to some embodiments the second communication control rule comprises a policy and charging rule. According to some embodiments the communication control parameter rule comprises a policy and charging rule parameter.

According to a third aspect of the invention, there is provided an apparatus comprising an output configured to send a first communication control rule, for example a policy and charging rule, to a policy and charging enforcement function, the rule comprising at least one communication control rule parameter, wherein the communication control rule is associated with controlling firewall or network address translation function policy.

According to some embodiments, the at least one communication control rule parameter comprises a maximum number of firewall or network address translation function bindings for an application, a guaranteed number of firewall or network address translation function bindings for an application, a binding pre-emption capability of the communication control rule, a binding pre-emption vulnerability of the communication control rule, or a binding priority level of the communication control rule.

In some embodiments, the apparatus comprises a policy and charging rules function.

According to some embodiments the first communication control rule comprises a policy and charging rule. According to some embodiments the second communication control rule comprises a policy and charging rule. According to some embodiments the communication control parameter rule comprises a policy and charging rule parameter.

According to a fourth aspect of the invention, there is provided a system comprising an apparatus of any of claims 18-36 and an apparatus of any of claims 37-40.

According to a fifth aspect of the invention, there is provided a computer program product comprising code means adapted to perform all the steps of any of claims 1 to 17 when the program is run on a processor.

Embodiments of the present invention may have one or more of following advantages:

- defining a new NAT/firewall policy architecture in 3GPP
- simple support for NAT/firewall policies
- enabling prioritized resource management

BRIEF DESCRIPTION OF DRAWINGS

Embodiments of the present invention are described below with reference to the accompanying drawings, which are not necessarily drawn to scale, wherein:

Figure 1 illustrates a reference architecture for a case where NAT and/or firewall is invoked between a user equipment (UE) and the IMS domain, according to 3GPP TS 23.228.

Figure 2 illustrates a basic PCC reference architecture.

Figure 3 illustrates a basic PCC rule procedure according to 3GPP TS 29.212.

Figures 4a, 4b and 4c illustrate a method according to an exemplary embodiment of the invention.

Figures 5a and 5b illustrate an apparatus according to an exemplary embodiment of the invention.

Figure 6 illustrates an apparatus according to an exemplary embodiment of the invention.

Figure 7 illustrates a signaling flow when a default bearer is activated in a P-GW according to an exemplary embodiment of the invention.

Figure 8 illustrates a signaling flow related to an IMS voice call according to an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF SOME EMBODIMENTS

Some applications consume lots of NAT/firewall resources even though those applications may be of low priority. This may lead to a situation where e.g. low priority file transfer using a file-sharing application (e.g. BitTorrent) consumes all the bindings in a gateway node and thus the gateway cannot forward traffic related to some other, more critical, application(s). Even if a subscriber has some guaranteed resources available for NAT/firewall, subscriber may have concurrently open multiple applications where a low priority application is using all the resources, even though some of those resources should be given to the higher priority application.

The present invention defines policies depending on the applications and not just on the subscribers or PDN connections. In addition, the defined policies may allow pre-empting the already allocated resources, so that when e.g. resources are allocated to a low priority best-effort application, a high priority application having guaranteed resource may pre-empt some of the resources already given to the best-effort application. In summary, there are following problems, at least some of which this invention aims to solve:

- missing NAT/firewall policy architecture in 3GPP
- no way to define maximum and particularly guaranteed number of bindings per application
- no way to define priority levels for the binding reservations, and no way to define which bindings should be released if there is need to allocate a new binding and all the binding resources have been already consumed

The present invention is described herein with reference to particular non-limiting examples. Exemplary embodiments of the present invention will be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the invention are shown. It is generally to be noted that, according to certain needs and constraints, all of the described alternatives may be provided alone or in any conceivable combination (also including combinations of individual features of the various alternatives). A person skilled in the art will appreciate that the invention is not limited to these examples, and may be more broadly applied.

In particular, the present invention and its embodiments are mainly described in relation to 3GPP specifications being used as non-limiting examples for network configurations. As such, the description of the embodiments given herein specifically refers to terminology which is directly related thereto. Such terminology is only used in the context of the presented non-limiting examples, and does naturally not limit the invention in any way. Rather, any other network configuration or implementation may also be utilized as long as compliant with the features described herein.

The invention is generic for all NAT variants, so the same invention can be applied for e.g. NAT44 and NAT64.

The firewall/policy architecture according to the invention may comprise the following nodes:

- PCRF 200, which defines the NAT/firewall policies for 3GPP nodes in addition to other policy control.
- PCEF 100, which implements the enforcement of NAT/firewall policies and other policies given by PCRF

200. PCEF 100 is one of the functions of a user plane gateway 300, e.g. GGSN or P-GW.

Actual NAT/firewall rules may be defined as extensions to the existing PCC rules of the 3GPP PCC architecture. Particularly, the following new parameters may be added to the existing PCC rule(s):

- Maximum number of NAT/firewall bindings
- Guaranteed number of NAT/firewall bindings
- Binding Pre-emption Capability (BPC) of PCC rule
- Binding Pre-emption Vulnerability (BPV) of PCC rule
- Binding Priority Level (BPL) of PCC rule

These new PCC rule parameters may be passed to the PCEF 100 from the PCRF 200 as a part of the new Gx interface application attribute-value-pairs (AVPs) when a PCC rule is installed or modified by the PCRF 200, as in Figure 3. These new PCC rule parameters may also be defined in local PCC rules, which are activated based on the rulebases installed by the PCRF 200. When the initial PCC rulebase or PCC rules are installed as part of the PDN connection activation, PCRF 200 may also enable/disable NAT, and depending on this information, the binding policies in the PCC rule may be applied to NAT or firewall function in the PCEF 100.

Alternatively, these NAT/firewall rules may be defined as separate NAT/firewall rules, instead of as extensions to the existing PCC rules. The invented method applies also in this case. For the sake of simplicity, in the following, the terms “PCC rule” and “PCC rule parameter” is used, but according to the invention they may as well be replaced with the terms “NAT/firewall rule” and “NAT/firewall rule parameter”.

The invention defines a new NAT/firewall policy architecture, where NAT/firewall policies are controlled by the PCRF 200, which handles all the Quality of Service (QoS) and charging policies in the 3GPP architecture. The benefit of this approach is that support for NAT/firewall policies may be done

by adding a few new AVPs in the Gx interface. If local PCC rules are used, then only the PCC rule configuration in the PCEF 100 requires changes. Having common node for handling all policies allows having synergies when making the policy decisions.

Middlebox Communication working group (MIDCOM) defined architecture may also deployed. PCRF 200 may install NAT/firewall policies to the PCEF 100, which may then use the MIDCOM protocol to define the actual NAT/firewall rules for the user plane function where NAT or firewall function is implemented.

Invention defines maximum and guaranteed number of bindings per PCC rule. This may allow more granular resource management than the prior art solutions, which allocated bindings per subscriber or per PDN connection. It may be possible to define that e.g. subscriber may have one guaranteed binding per for e-mail traffic, while the HTTP traffic may have maximum 16 concurrent bindings active without any guaranteed number of bindings.

For a guaranteed number of bindings, the defined number of bindings may be reserved when the PCC rule is activated (see below). When a new binding is required, then maximum number of bindings of the PCC rule defines whether a new binding can be reserved.

Figures 4a, 4b and 4c illustrate some examples of the method according to the invention. In one embodiment, the PCEF 100 may receive (step S1) a request to activate a PCC rule, where the rule may comprise at least one PCC rule parameter. In further embodiments, the PCEF 100 may check whether the PCC rule requires guaranteed number of bindings, (step S2). If guaranteed bindings are required, then PCEF 100 may reserve (step S3a) them when the PCC rule is activated. If there are not enough bindings available, PCEF 100 may check the binding pre-emption capability (BPC) value of the PCC rule (step S3b). If BPC is not defined, then the PCC rule activation may

fail. If BPC is defined, the PCEF 100 may check if there are any binding reservations done by other PCC rules where the binding pre-emption vulnerability (BPV) value indicates that its bindings can be pre-empted and if those PCC rules have lower priority (BPL) than the new PCC rule (step S4b). If that is not the case, then the PCC rule activation may fail and the PCEF 100 may report PCC rule activation failure (step S4a). Otherwise the binding(s) reserved by the other PCC rule may be released and allocated to the new PCC rule (step S5b). If pre-emption is possible for multiple PCC rules, then BPL may be used to select the PCC rule with the lowest priority (steps S5a and S6a). Pre-empting the other PCC rule may release enough resource allocations done as part of the activation of the other PCC rule for the "first" PCC rule. In one example, the other already activated PCC rule has 1000 bindings. In addition, there are currently 100 unallocated resources for bindings. If the new PCC requires 1000 guaranteed bindings, then pre-emption may release resources reserved for 900 bindings of the other PCC rule and the rest is taken from the unallocated resources.

If PCC rule activation fails at any point of the method, the PCEF 100 may report this to the PCRF 200 according to the section 4.5.12 of 3GPP TS 29.212 (e.g. version 11.0.1): If the installation/activation of one or more PCC rules fails using a PULL mode (i.e. the PCRF 200 installs/activates a rule using a CCA command) the PCEF 100 may send the PCRF 200 a new CCR command and include the Rule-Failure-Code AVP.

The same pre-emption method is applied also when a new binding needs to be activated for the PCC rule, i.e. there are no free guaranteed level bindings available in the PCC rule, but the number of bindings does not exceed the maximum number of bindings of the PCC rule. The main difference is that if the new binding cannot be reserved, then the PCC rule may remain active.

The PCEF 100, as illustrated in Figures 5a and 5b, may comprise an input 101 configured to receive a request to acti-

vate a PCC rule. The PCEF may further comprise a memory 102 configured to store the PCC rule, a processor 103 configured to check whether a guaranteed number of firewall or network address translation function bindings are available, and an output 104 configured to report PCC rule activation failure in case the PCC rule cannot be activated. The PCEF 100 may be located in a user plane gateway 300, e.g. in a GGSN or in a PDN-GW.

The PCRF, as illustrated in Figure 6, may comprise an output 201 configured to send a PCC rule to a PCEF 100. The PCRF 200 may further comprise an input configured to receive a failure report from the PCEF 100.

The processor 103 may comprise a central processing unit (CPU) or any other means for processing. The input 101 may comprise a receiver or any other means for receiving. The output 104, 201 may comprise a transceiver or any other means for transmitting. The processor 103, the memory 102, the input 101, and the output 104 may exchange information over an internal interface of the PCEF 100.

The input 101 and the output 104 of the PCEF 100 may be functionalities running on the processor 103 of the PCEF 100 or may alternatively be separate functional entities or means. The input 101 and the output 104, 201 may also be implemented as integral transceivers or may be implemented e.g. as physical transmitters/receivers for transceiving via the air interface, as routing entities for sending/receiving data packets in a PS (packet switched) network, or as any suitable combination thereof.

The processor 103 may be configured to process various data inputs and to control input 101 and the output 104. The apparatus 100, 200 may further comprise a memory that may serve for storing code means for carrying out e.g. the methods according to the examples of the present invention, e.g. when run e.g. on the processor 103.

According to all example embodiments, the PCC rule requested to be activated may be associated with controlling firewall or network address translation function policy and comprise at least one policy and charging rule parameter. The parameter may be e.g. a maximum number of firewall or network address translation function bindings for an application, a guaranteed number of firewall or network address translation function bindings for an application, a binding pre-emption capability of the policy and charging rule, a binding pre-emption vulnerability of the policy and charging rule, or a binding priority level of the policy and charging rule.

An example of a signaling flow when a default bearer is activated in a P-GW 300 according to the invention is shown in Figure 7. A serving gateway (S-GW) 400 may request a new default bearer in the P-GW 300. The P-GW 300 may then send an initial CCR message to the PCRF 200 in order to receive policies, including the NAT/firewall policies. The CCA message returned from the PCRF 200 may include PCC rules or PCC rule-bases which define the policies. The P-GW 300 may then activate the PCC rules for the default bearer and make binding reservations according to the NAT/firewall policies. Default bearer activation may be completed when the P-GW 300 returns create session response to the S-GW 400.

Figure 8 shows an example of a signaling flow related to an IMS voice call. The IMS system, which corresponds to an AF 500 in the PCC architecture, may send a request to a PCRF 200 indicating that an IMS voice call is required. The PCRF 200 may send a Re-Auth-Request (RAR) message to a P-GW 300, containing a PCC rule which conventionally triggers dedicated bearer activation. If NAT is enabled for the PDN connection, this PCC rule may have additional NAT policies, which typically define guaranteed NAT bindings for the voice media and BPC enabled to indicate that the voice call may pre-empt other less important NAT bindings. If NAT is not enabled, but firewall is enabled, the PCC rule may define firewall policies for the voice call. The P-GW 300 may create a new dedi-

cated bearer for the voice call and it may also make the required binding reservations.

One having ordinary skill in the art will readily understand that the invention as discussed above may be practiced with steps in a different order, and/or with hardware elements in configurations which are different than those which are disclosed. Therefore, although the invention has been described based upon these preferred embodiments, it would be apparent to those of skill in the art that certain modifications, variations, and alternative constructions would be apparent, while remaining within the scope of the invention.

Claims

1. A method for controlling firewall or network address translation function comprising:

receiving (S1) at a policy and charging enforcement function a request to activate a first communication control rule, said rule comprising at least one communication control rule parameter;

wherein said communication control rule is associated with controlling firewall or network address translation function policy.

2. The method of claim 1, wherein said at least one communication control rule parameter comprises

- a maximum number of firewall or network address translation function bindings for an application,
- a guaranteed number of firewall or network address translation function bindings for an application,
- a binding pre-emption capability of said communication control rule,
- a binding pre-emption vulnerability of said communication control rule, or
- a binding priority level of said communication control rule.

3. The method of claim 1 or 2, further comprising:

storing said first communication control rule.

4. The method of any of preceding claims, further comprising:
receiving (S1) said first communication control rule from a policy and charging rules function.

5. The method of any of preceding claims, wherein said first communication control rule comprises a guaranteed number of firewall or network address translation function bindings parameter and the method further comprises:

checking (S2) whether at least said guaranteed number of firewall or network address translation function bindings are available.

6. The method of claim 5, further comprising:

reserving (S3a) resources for said guaranteed number of firewall or network address translation function bindings as part of said first communication control rule activation in case at least said guaranteed number of firewall or network address translation function bindings are available.

7. The method of claim 5, further comprising:

checking (S3b) whether said first communication control rule comprises a binding pre-emption capability parameter in case at least said guaranteed number of firewall or network address translation function bindings are not available.

8. The method of claim 7, further comprising:

reporting (S4a) communication control rule activation failure in case said first communication control rule does not comprise a binding pre-emption capability parameter.

9. The method of claim 7, further comprising:

checking (S4b) whether at least one second activated communication control rule comprises a binding pre-emption vulnerability parameter and whether said at least one second activated communication control rule comprises a lower binding priority level than said first communication control rule in case said first communication control rule comprises a binding pre-emption capability parameter.

10. The method of claim 9, wherein one second activated communication control rule comprises a binding pre-emption vulnerability parameter and a lower binding priority level than said first communication control rule and the method further comprises:

pre-empting (S5b) at least one firewall or network address translation function binding associated with said one second activated communication control rule, and

reserving resources for said guaranteed number of firewall or network address translation function bindings as part of said first communication control rule activation.

11. The method of claim 9, wherein at least two second activated communication control rules comprise a binding pre-emption vulnerability parameter and a lower binding priority level than said first communication control rule and the method further comprises:

comparing (S5a) binding priority levels of said at least two second activated communication control rules.

12. The method of claim 11, further comprising:

pre-empting (S6a) at least one firewall or network address translation function binding associated with a second activated communication control rule with lowest priority level, and

reserving resources for said guaranteed number of firewall or network address translation function bindings for activating said first communication control rule.

13. The method of claim 10 or 12, further comprising:

pre-empting firewall or network address translation function bindings associated with a second activated communication control rule such that said guaranteed number of firewall or network address translation function bindings com-

prised in said first communication control rule are available.

14. The method of any of preceding claims, wherein the communication control rule comprises a policy and charging rule or a firewall or network address translation function rule.

15. An apparatus (100) comprising:

an input (101) configured to receive a request to activate a first communication control rule, said rule comprising at least one communication control rule parameter;

wherein said communication control rule is associated with controlling firewall or network address translation function policy.

16. The apparatus (100) of claim 15, wherein said at least one communication control rule parameter comprises

- a maximum number of firewall or network address translation function bindings for an application,
- a guaranteed number of firewall or network address translation function bindings for an application,
- a binding pre-emption capability of said communication control rule,
- a binding pre-emption vulnerability of said communication control rule, or
- a binding priority level of said communication control rule.

17. The apparatus (100) of claim 15 or 16, further comprising:

a memory (102) configured to store said first communication control rule.

18. The apparatus (100) of any of claims 15 to 17, wherein said input (101) is further configured to receive said first communication control rule from a policy and charging rules function (200).

19. The apparatus (100) of any of preceding claims, wherein said first communication control rule comprises a guaranteed number of firewall or network address translation function bindings parameter and the apparatus (100) further comprises:

a processor (103) configured to check whether at least said guaranteed number of firewall or network address translation function bindings are available.

20. The apparatus (100) of claim 19, wherein said processor (103) is further configured to reserve resources for said guaranteed number of firewall or network address translation function bindings as part of said first communication control rule activation in case at least said guaranteed number of firewall or network address translation function bindings are available.

21. The apparatus (100) of claim 19, wherein said processor (103) is further configured to check whether said first communication control rule comprises a binding pre-emption capability parameter in case at least said guaranteed number of firewall or network address translation function bindings are not available.

22. The apparatus (100) of claim 21, further comprising:

an output (104) configured to report communication control rule activation failure in case said first communication control rule does not comprise a binding pre-emption capability parameter.

23. The apparatus (100) of claim 21, wherein said processor (103) is further configured to check whether at least one

second activated communication control rule comprises a binding pre-emption vulnerability parameter and whether said at least one second activated communication control rule comprises a lower binding priority level than said first communication control rule in case said first communication control rule comprises a binding pre-emption capability parameter.

24. The apparatus (100) of claim 23, wherein one second activated communication control rule comprises a binding pre-emption vulnerability parameter and a lower binding priority level than said first communication control rule, and the processor (103) is further configured

to pre-empt at least one firewall or network address translation function binding associated with said one second activated communication control rule, and

to reserve resources for said guaranteed number of firewall or network address translation function bindings as part of said first communication control rule activation.

25. The apparatus (100) of claim 23, wherein at least two second activated communication control rules comprise a binding pre-emption vulnerability parameter and a lower binding priority level than said first communication control rule and the processor (103) is further configured to compare binding priority levels of said at least two second activated communication control rules.

26. The apparatus (100) of claim 25, wherein the processor (103) is further configured

to pre-empt at least one firewall or network address translation function binding associated with a second activated communication control rule with lowest priority level, and

to reserve resources for said guaranteed number of firewall or network address translation function bindings as part of said first communication control rule activation.

27. The apparatus (100) of claim 24 or 26, wherein the processor (103) is further configured to pre-empt firewall or network address translation function bindings associated with a second activated communication control rule such that said guaranteed number of firewall or network address translation function bindings comprised in said first communication control rule are available.

28. The apparatus (100) of any of claims 15-27, wherein the communication control rule comprises a policy and charging rule or a firewall or network address translation function rule.

29. An apparatus (200) comprising:

an output (201) configured to send first communication control rule to a policy and charging enforcement function (100), said rule comprising at least one communication control rule parameter;

wherein said communication control rule is associated with controlling firewall or network address translation function policy.

30. The apparatus (200) of claim 29, wherein said at least one communication control rule parameter comprises

- a maximum number of firewall or network address translation function bindings for an application,
- a guaranteed number of firewall or network address translation function bindings for an application,
- a binding pre-emption capability of said communication control rule,
- a binding pre-emption vulnerability of said communication control rule, or
- a binding priority level of said communication control rule.

31. The apparatus (200) of claim 29 or 30, wherein the communication control rule comprises a policy and charging rule or a firewall or network address translation function rule.

32. A system comprising an apparatus (100) according to any of claims 15 to 28 and an apparatus (200) according to any of claims 29 to 31.

33. A computer program product comprising code means adapted to perform all the steps of any of claims 1 to 14 when the program is run on a processor.

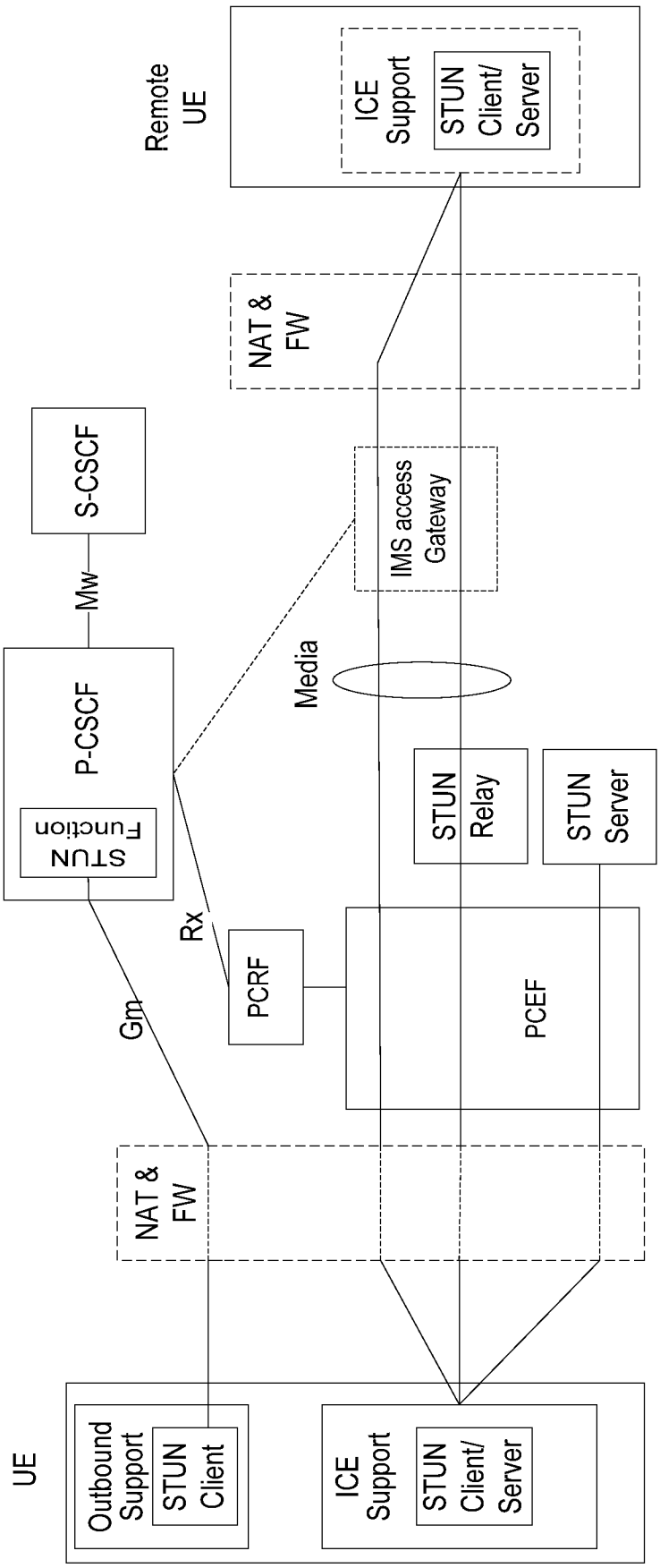

Remote UE
ICE Support
STUN Client/ Server
NAT & FW
S-CSCF
IMS access Gateway
Mw
P-CSCF
STUN Function
Media
STUN Relay
STUN Server
Rx
PCRF
PCEF
Gm
NAT & FW
UE
Outbound Support
STUN Client
ICE Support
STUN Client/ Server

Fig. 1

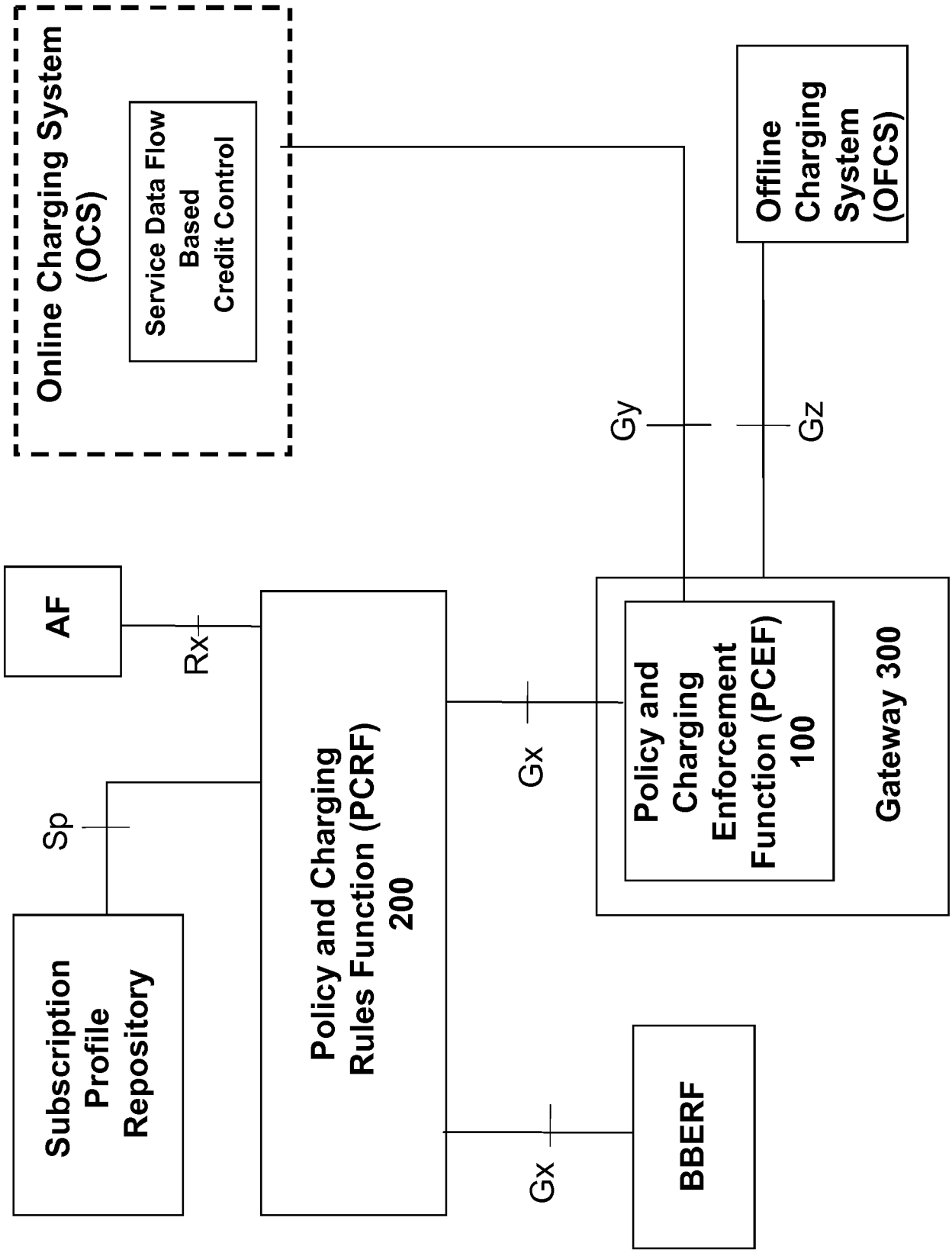

Online Charging System (OCS)
Service Data Flow Based Credit Control
Offline Charging System (OFCS)
Gy
Gz
AF
Rx
Policy and Charging Rules Function (PCRF) 200
Gx
Policy and Charging Enforcement Function (PCEF) 100
Gateway 300
Sp
Subscription Profile Repository
Gx
BBERF

Fig. 2

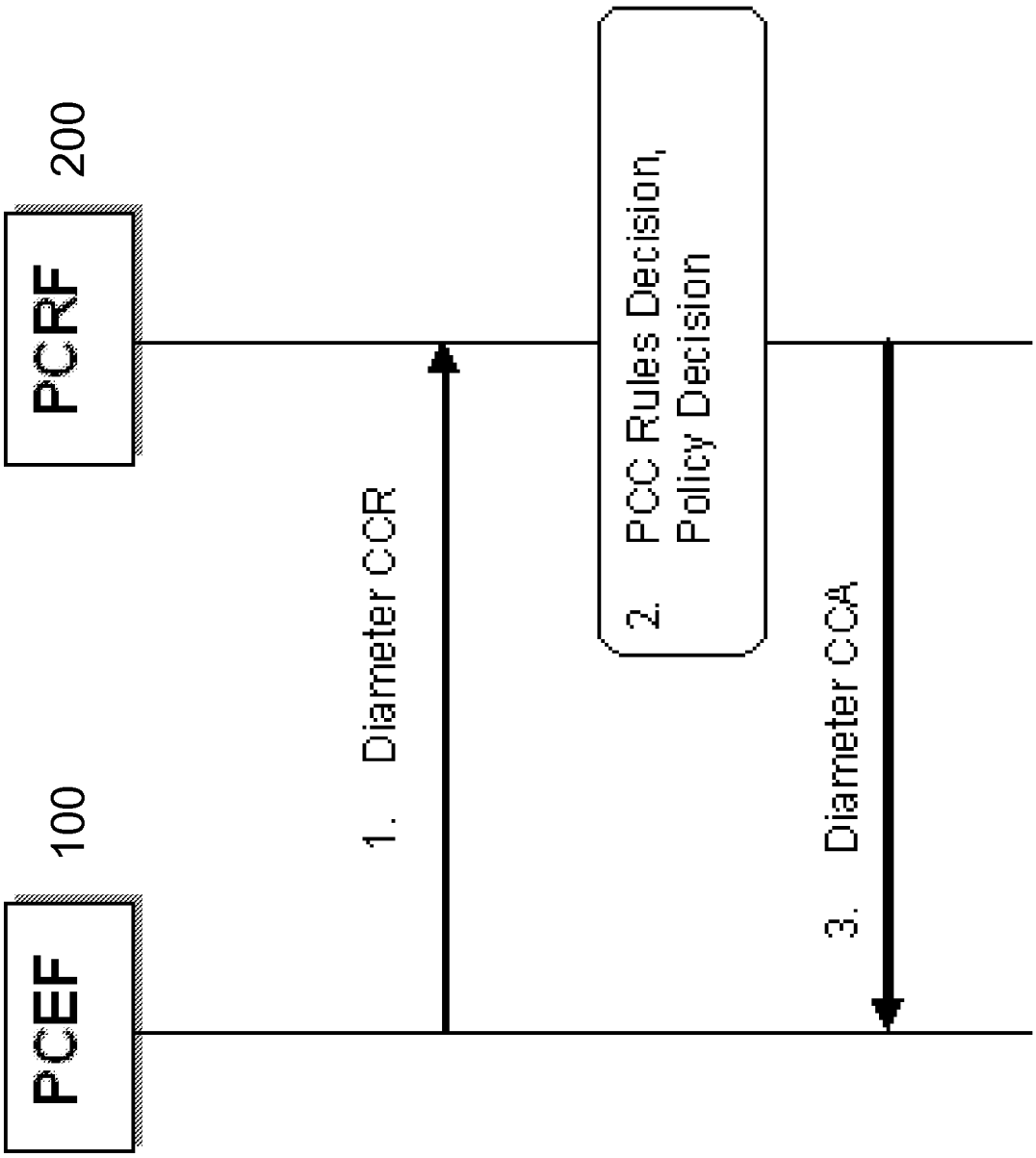

PCRF
200
PCEF
100
1. Diameter CCR
2. PCC Rules Decision, Policy Decision
3. Diameter CCA

Fig. 3

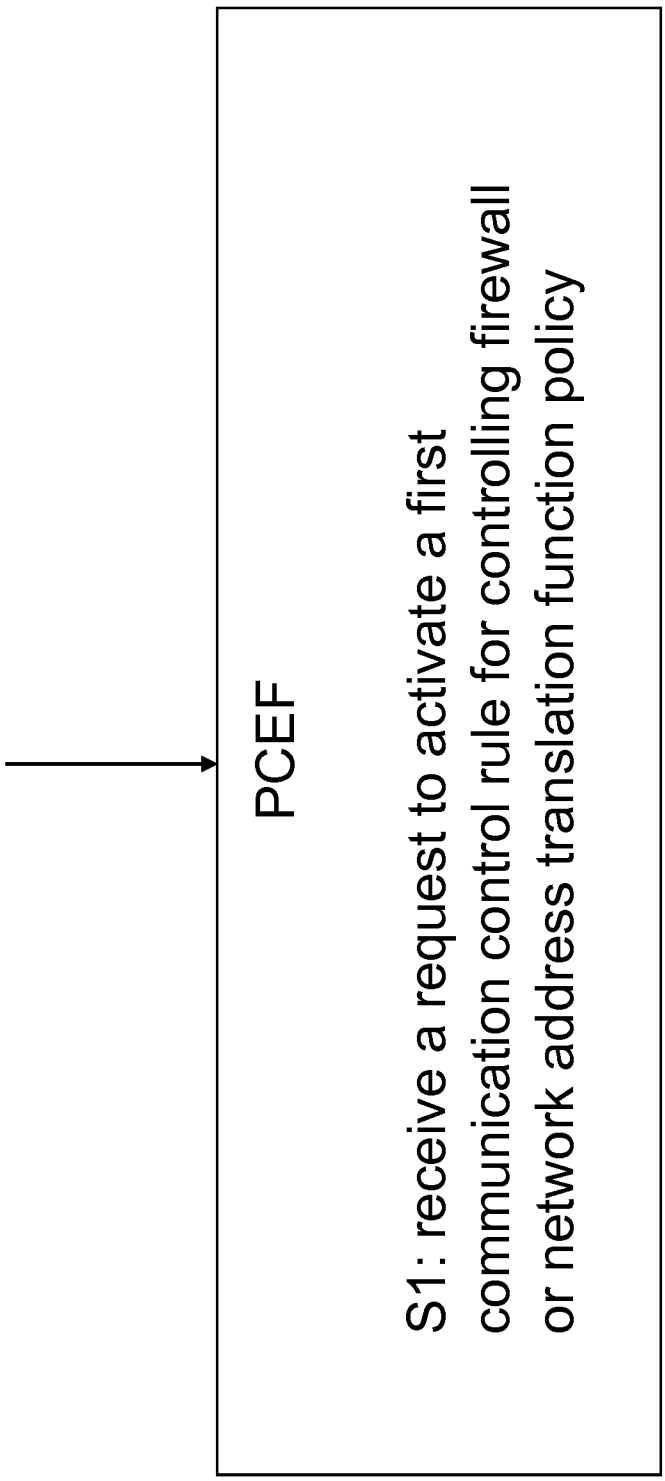

PCEF
S1: receive a request to activate a first communication control rule for controlling firewall or network address translation function policy

Fig. 4a

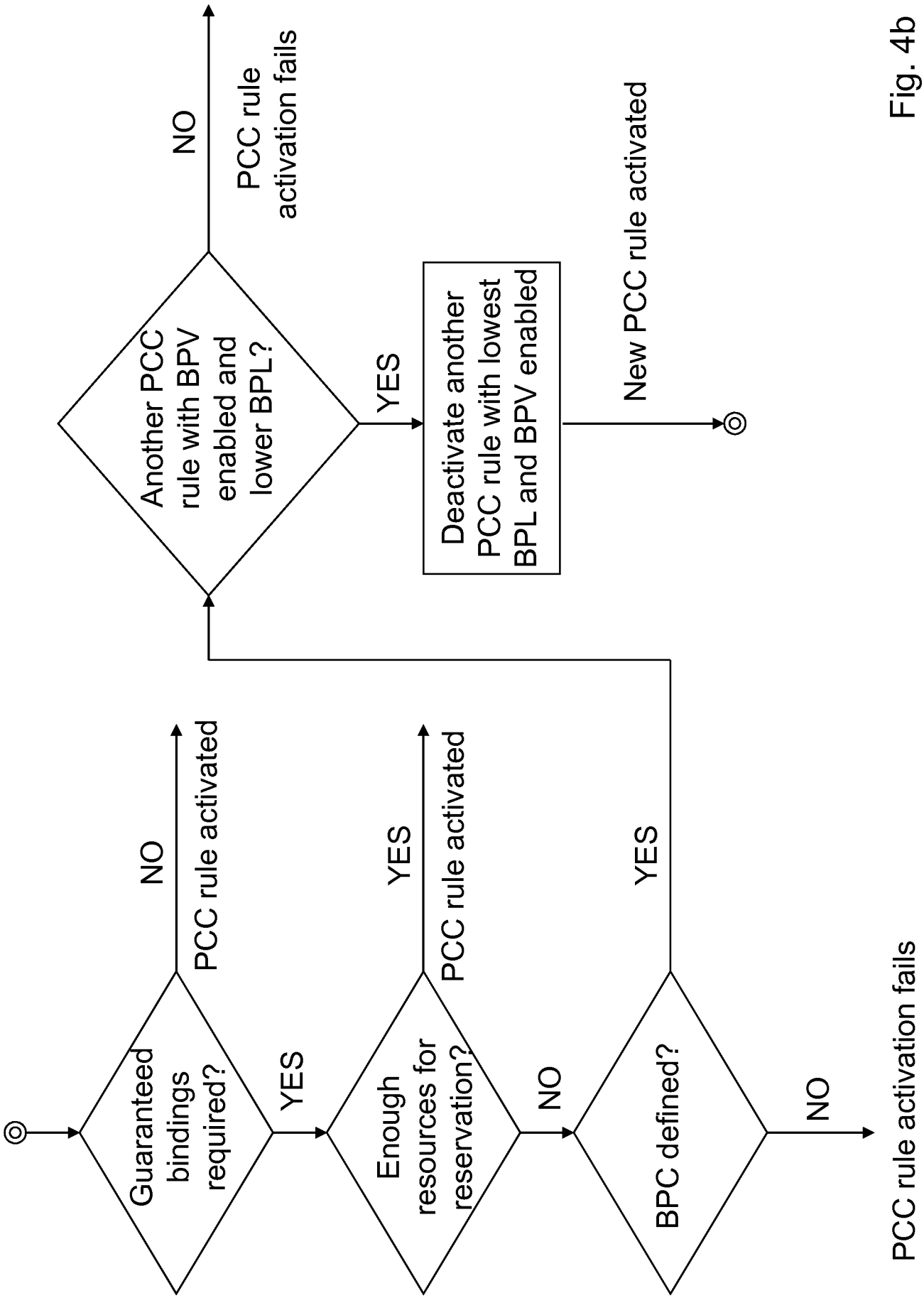

Guaranteed bindings required?
NO
PCC rule activated
YES
Enough resources for reservation?
YES
PCC rule activated
NO
BPC defined?
YES
NO
PCC rule activation fails
Another PCC rule with BPV enabled and lower BPL?
NO
PCC rule activation fails
YES
Deactivate another PCC rule with lowest BPL and BPV enabled
New PCC rule activated

Fig. 4b

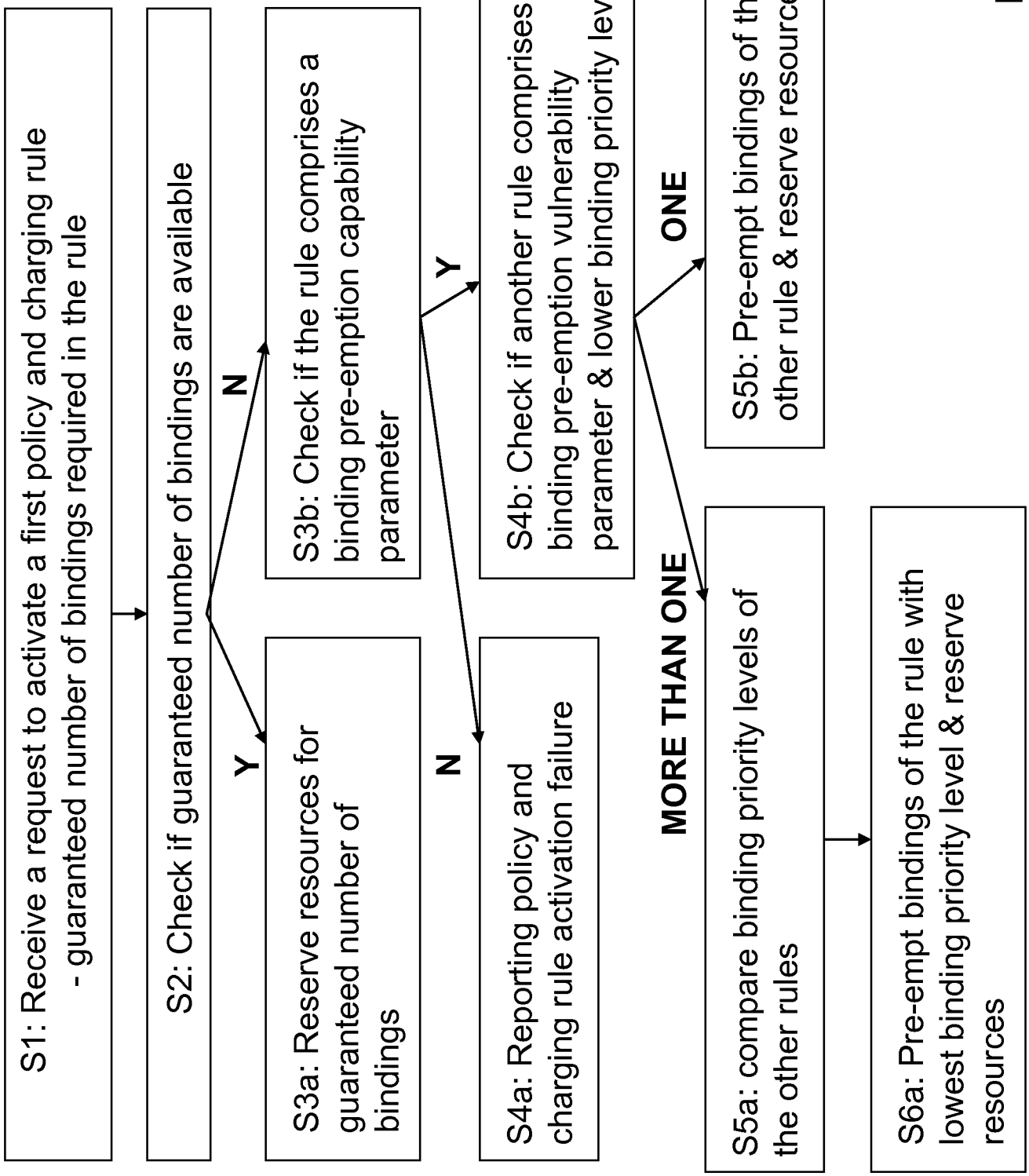

S1: Receive a request to activate a first policy and charging rule - guaranteed number of bindings required in the rule
S2: Check if guaranteed number of bindings are available
N
Y
S3b: Check if the rule comprises a binding pre-emption capability parameter
Y
N
S4b: Check if another rule comprises a binding pre-emption vulnerability parameter & lower binding priority level
ONE
S5b: Pre-empt bindings of the other rule & reserve resources
S3a: Reserve resources for guaranteed number of bindings
S4a: Reporting policy and charging rule activation failure
MORE THAN ONE
S5a: compare binding priority levels of the other rules
S6a: Pre-empt bindings of the rule with lowest binding priority level & reserve resources

Fig. 4c

Fig. 5a

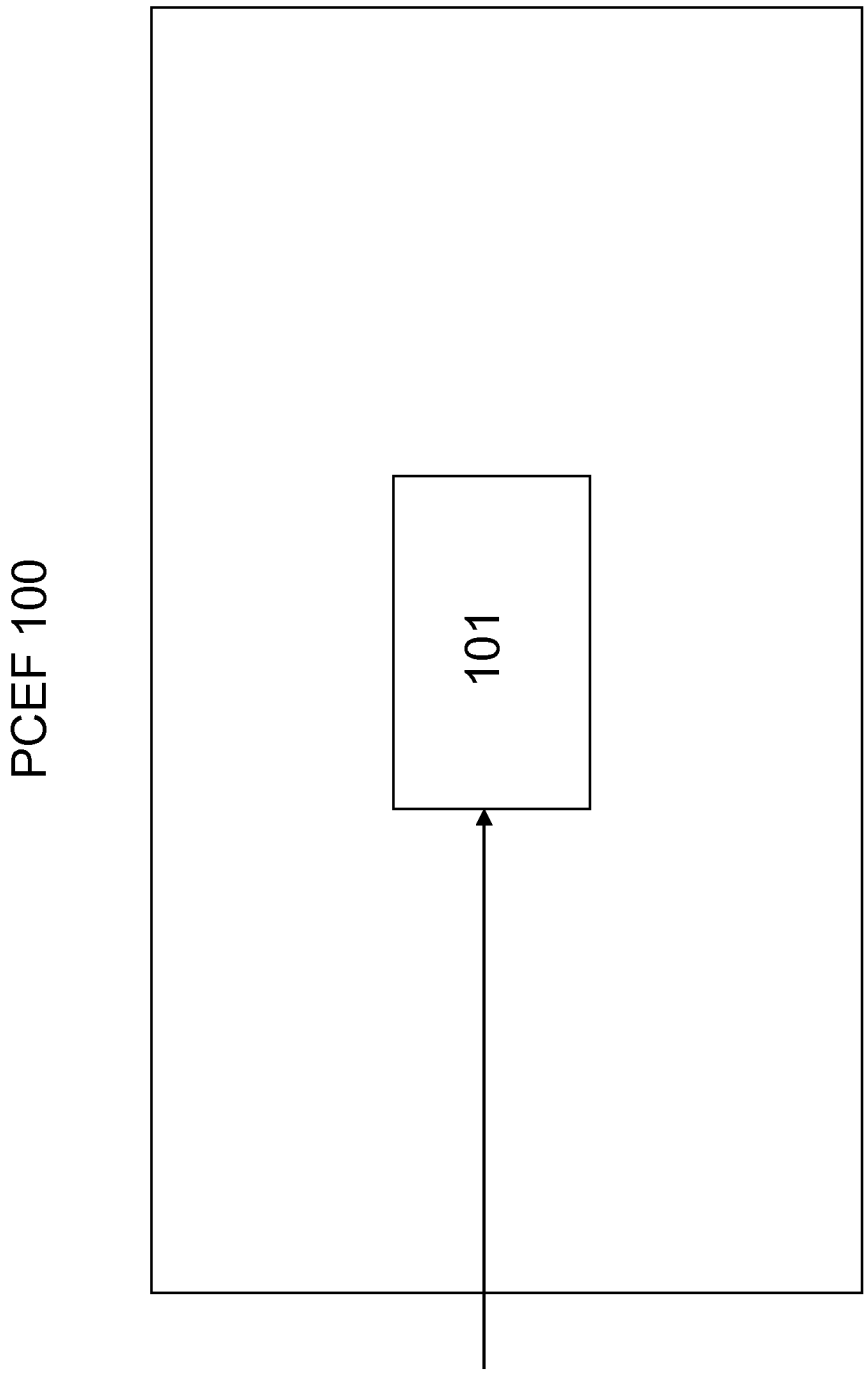


Fig. 5b

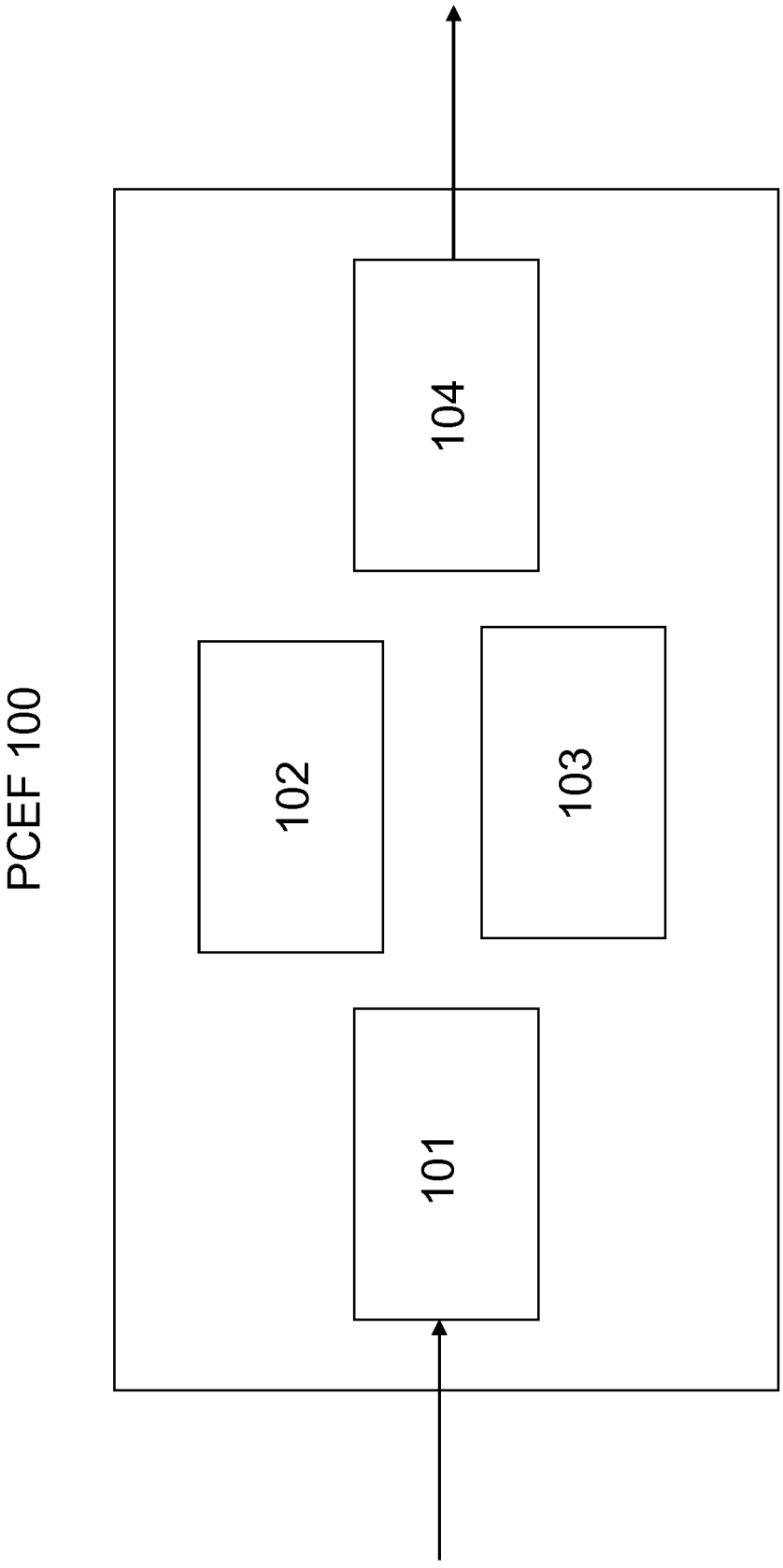
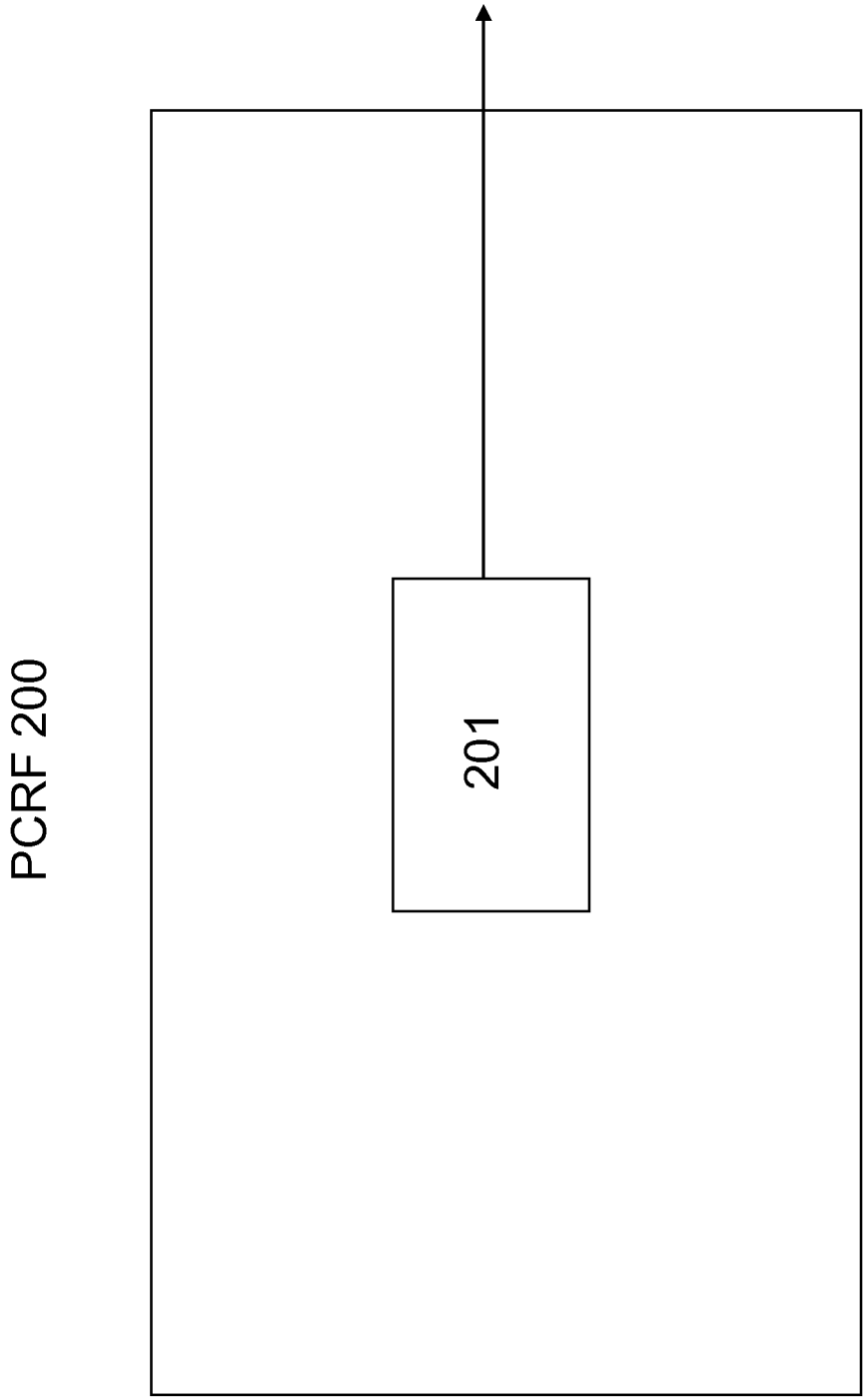


Fig. 6



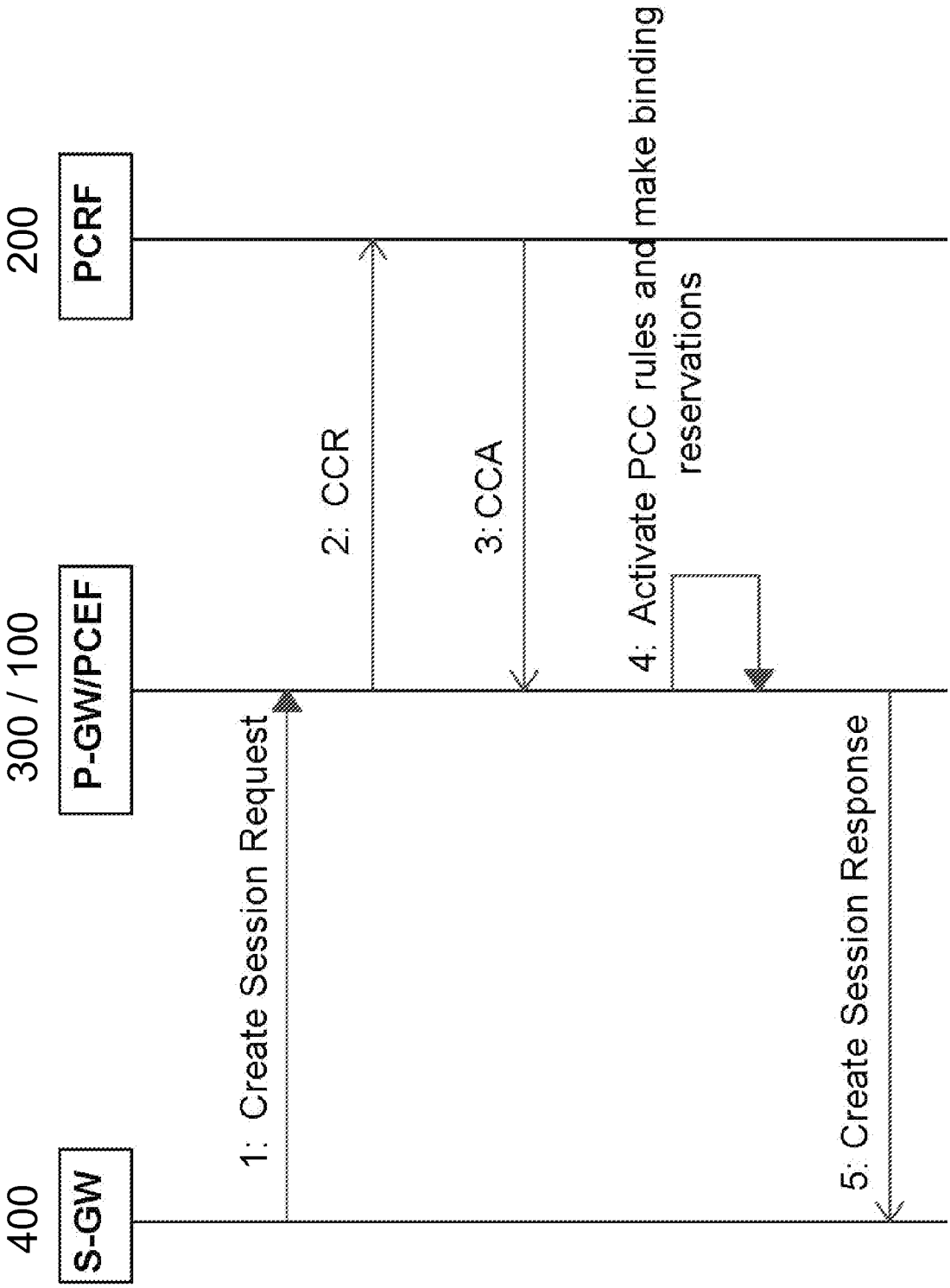

200
PCRF
300 / 100
P-GW/PCEF
400
S-GW
1: Create Session Request
2: CCR
3: CCA
4: Activate PCC rules and make binding reservations
5: Create Session Response

Fig. 7

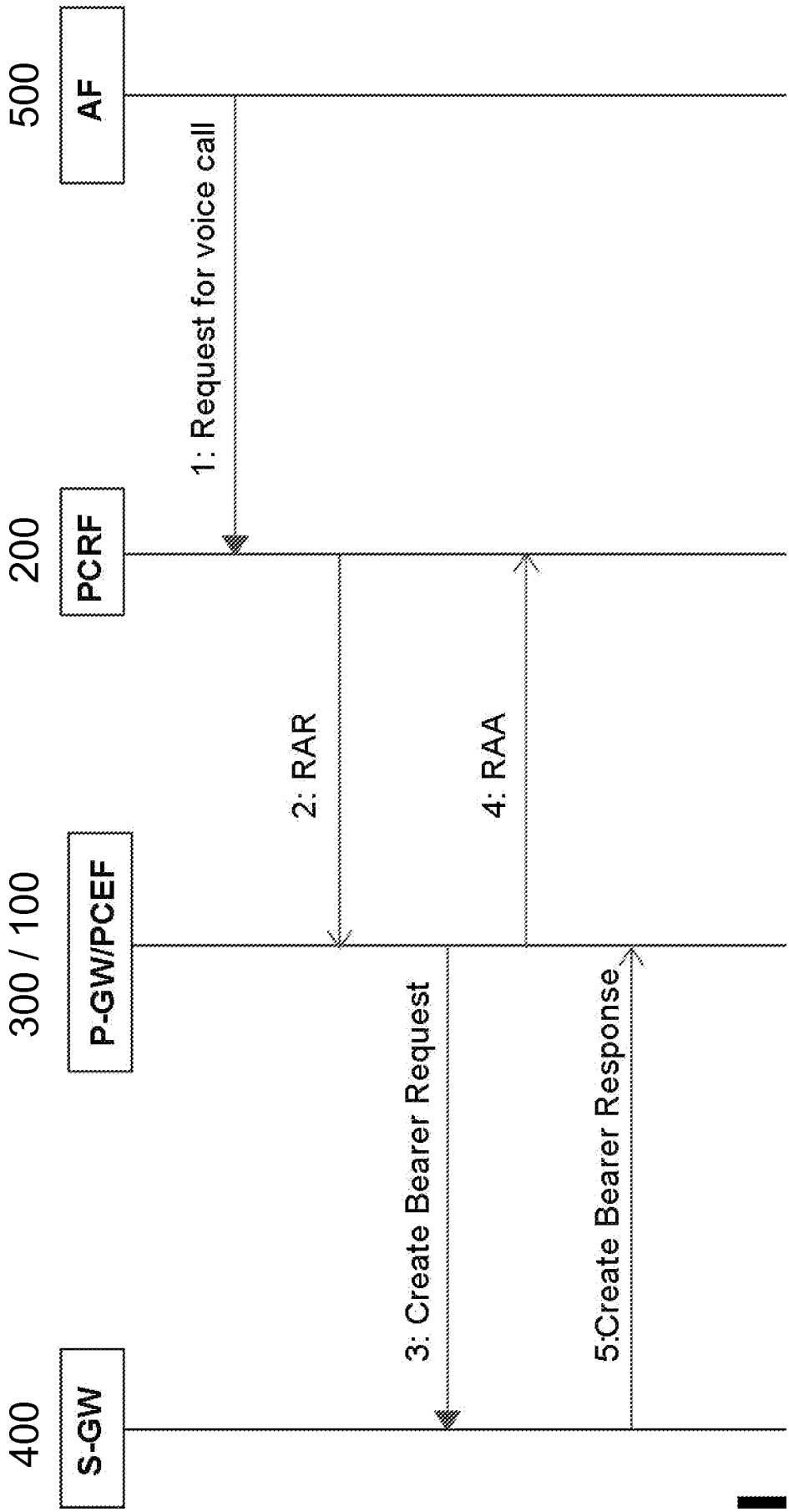

500
AF
1: Request for voice call
200
PCRF
2: RAR
4: RAA
300 / 100
P-GW/PCEF
3: Create Bearer Request
5:Create Bearer Response
400
S-GW

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/058928

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. H04W12/08 H04W28/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping (3GPP TS 29.213 version 10.1.0 Release 10)", TECHNICAL SPECIFICATION, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS ; FRANCE, vol. 3GPP CT 3, no. V10.1.0, 1 April 2011 (2011-04-01), XP014065089, page 8 - page 10 page 24 - page 27 page 44 - page 45 page 54 - page 57 page 66 - page 68 page 94 -/--	1-33

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 February 2012	16/02/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kopp, Klaus

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 128	

X	"Protocol at the interface between the policy decision physical entity (PD-PE) and the policy enforcement physical entity (PE-PE) (Rw interface): Diameter; Q.3303.3 (05/08)", ITU-T STANDARD, INTERNATIONAL TELECOMMUNICATION UNION, GENEVA ; CH, no. Q.3303.3 (05/08), 22 May 2008 (2008-05-22), pages 1-58, XP017466787, [retrieved on 2009-02-16]	1,3,4, 15,17, 18,29, 31-33
A	page 5 - page 17 page 26 - page 27 page 40 - page 45	2,5-14, 16, 19-28,30

X	"3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)", 3GPP STANDARD; 3GPP TS 29.212, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. V7.11.0, 18 December 2009 (2009-12-18) , pages 1-47, XP050401204, [retrieved on 2009-12-18] cited in the application page 7 - page 24 page 43 - page 45	1,15,29, 32,33

X	"Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN); NAT Traversal feasibility study report; Draft ETSI TR 187 008", IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, no. V0.0.16, 1 December 2007 (2007-12-01), XP014040980, ISSN: 0000-0001 page 8 - page 11 page 16 - page 17 page 19 - page 25	1,15,29, 32,33

1