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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 December 2016 (22.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/202406 A1

(51) International Patent Classification:
H04W 48/18 (2009.01) *H04W 76/02* (2009.01)
H04W 88/16 (2009.01) *H04W 76/04* (2009.01)

(21) International Application Number:
PCT/EP2015/063851

(22) International Filing Date:
19 June 2015 (19.06.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA SOLUTIONS AND NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors: **UNGVARI, Gabor**; Rigo u. 29/2, H-2360 Gyal (HU). **WOLFNER, Gyorgy Tamas**; Szeru utca 33, H-1163 Budapest (HU). **MUSTAJARVI, Jari Pekka**; Seitsemäs Järvikuja 6, FI-02730 Espoo (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

WO 2016/202406 A1

(54) Title: EPDG HOME REDIRECT

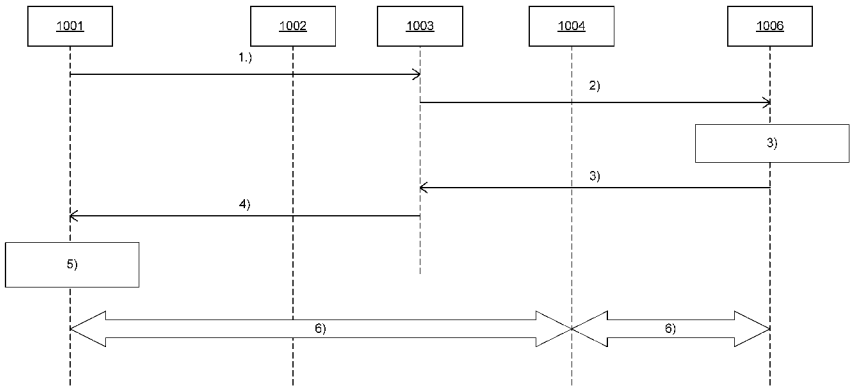


Fig. 1

(57) Abstract: It is provided a method, comprising deciding (3) if a terminal (1001) using an identity is to be redirected from a first gateway device (1003) to a second gateway device (1004) comprised in a set of one or more gateway devices, wherein the identity is received in an identity request from the first gateway device (1003) for at least one of an authentication and an authorization of the identity, wherein at least one of the one or more gateway devices (1004) of the set is different from the first gateway device; providing, if the terminal (1001) is to be redirected, an address of the set.

ePDG home redirect

Field of the invention

The present invention relates to an apparatus, a method, and a computer program product related to non-3GPP access. More particularly, the present invention relates to an apparatus, a method, and a computer program product related to ePDG home redirect.

Abbreviations

3GPP	3rd Generation Partnership Project
AA	Authentication, Authorization
AAA	Authentication, Authorization, Accounting
ANDSF	Access Network Discovery and Selection Function
DNS	Domain Name Server
EDGE	Enhanced Datarate for GSM Evolution
EPC	Evolved Packet Core
ePDG	Evolved PDG
FQDN	Fully Qualified Domain Name
GPRS	Generic Packet Radio Service
GSM	Global System for Mobile Communication
HPLMN	Home PLMN
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IKEv2	Internet Key Exchange version 2, RFC 5996
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
LTE	Long Term Evolution
LTE-A	LTE Advanced
PDG	Packet Data Gateway
PDN	Packet Data Network
PDN-GW	PDN Gateway
PLMN	Public Land Mobile Network
RFC	Request for Comments

SA	System Architecture
TS	Technical Specification
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
VPLMN	Visited PLMN
WiFi	Wireless Fidelity, also named WLAN
WLAN	Wireless LAN

Background of the invention

3GPP specifies two types of non-3GPP access to the EPC: trusted and untrusted (see details in 3GPP TS 23.402). Whether a non-3GPP access network (such as a WLAN network) is trusted or untrusted is not a characteristic of the non-3GPP access network but decided by the respective 3GPP operator. I.e., a non-3GPP network may be trusted for one 3GPP operator and untrusted for another 3GPP operator.

The PDN-GW is the user plane anchor for mobility between 3GPP access and trusted non-3GPP access. On the other hand, in case of untrusted non-3GPP access, ePDG serves as a tunnel endpoint for the Swu interface to the UE via an IPSec tunnel through the untrusted non-3GPP network. i.e., the UE may establish an IPSec tunnel to an ePDG in order to access EPC via a WLAN. Besides, ePDG may be responsible for handling the local and remote IP addresses, routing of packets from/to PDN GW to/from UE, as e.g. according to 3GPP TS 23.402. ePDG belongs to the domain of a 3GPP operator, which may be the operator of the HPLMN or an operator of a another 3GPP network (VPLMN).

3GPP TS 23.402 defines two options for ePDG selection by the UE: static and dynamic. In case of static configuration, the home operator may configure the UE to select an ePDG in the HPLMN. This is not a flexible solution as in this case the UE always selects an ePDG in the HPLMN. E.g., it is not possible to configure that the UE selects ePDG in the HPLMN only when it roams in specific VPLMNs. When dynamic ePDG selection is applied then the UE first tries to find an ePDG in the VPLMN. It only selects an ePDG in the HPLMN if no ePDG has been found in the VPLMN. Therefore, when the UE is roaming, currently it is not possible for the home operator to dynamically set preference for the UE to select and connect to an ePDG in the home network.

3GPP SA2 and CT1 working groups received a request to enable the home operator to set preference for roaming UE to connect to an ePDG in the HPLMN instead of connecting to an ePDG in the VPLMN. This request was related to the Voice over Wifi profile definition.

There were proposals (C1-151142, C1-151174, C1-151175, C1-151176, C1-151202, C1-151286, C1-151287) during the 3GPP CT1#91 meeting regarding the issue. The proposals are based on ANDSF. Where the home operator can set preference in the ANDSF provisioned to the UE to connect to the home network ePDG during roaming scenario.

There was a proposal (S2-150821) in 3GPP SA2#108 meeting that the network sends an indication to the UE whether ePDG in the home or visited network is preferred. The means how this indication is sent to the UE was not clarified.

Summary of the invention

It is an object of the present invention to improve the prior art.

According to a first aspect of the invention, there is provided an apparatus, comprising deciding means adapted to decide if a terminal using an identity is to be redirected from a first gateway device to a second gateway device comprised in a set of one or more gateway devices, wherein the identity is received in an identity request from the first gateway device for at least one of an authentication and an authorization of the identity, wherein at least one of the one or more gateway devices of the set is different from the first gateway device; providing means adapted to provide, if the terminal is to be redirected, an address of the set.

The providing means may be adapted to provide the address of the set to the first gateway device.

The providing means may be adapted to provide the address of the set to the terminal in a challenge request, and the challenge request may belongs to a procedure for the respective at least one of the authentication and the authorization of the identity.

The apparatus may further comprise monitoring means adapted to monitor if the first gateway device belongs to a home network to which the apparatus belongs; inhibiting means adapted to inhibit the deciding means from deciding that the terminal is to be redirected if the first gateway device belongs to the home network.

The deciding means may be adapted to decide based on at least one of a predetermined policy, an identification of the first gateway device, the identity, subscription data related to the identity, a timing of the first request, a location of the terminal, a load on the second gateway device, a load on the first gateway device, and an emergency indication received in the identity request.

The apparatus may further comprise indicating means adapted to indicate if the terminal should store that it is to be redirected from the first gateway device to the second gateway device.

The set may consist of the second gateway device and the address of the set may be the address of the second gateway device.

According to a second aspect of the invention, there is provided an apparatus, comprising checking means adapted to check if a response comprises an address of a set of one or more gateway devices, wherein the response is received in response to an identity request for at least one of an authentication and an authorization of an identity, and the identity is used to identify a terminal in a received tunnel request to set up a tunnel to the terminal; redirecting means adapted to redirect the terminal to request setting up the tunnel to one gateway device of the set of gateway devices if the address is received.

The redirecting means may be adapted to redirect the terminal using a redirect mechanism of internet key exchange version 2.

The apparatus may further comprise emergency monitoring means adapted to monitor if the tunnel request comprises an emergency indication indicating that the tunnel is for an emergency call; emergency forwarding means adapted to forward the emergency indication with the identity request.

The set may consist of the one gateway device and the address of the set may be the address of the one gateway device.

According to a third aspect of the invention, there is provided an apparatus, comprising monitoring means adapted to monitor if a tunnel request to set up a first tunnel between the apparatus and a first gateway device is redirected to a second gateway device different from

the first gateway device, wherein the second gateway device is comprised in a set of one or more gateway devices; storing means adapted to store a pair of an address of the set and an address of the first gateway device, if the tunnel request is redirected; supervising means adapted to supervise if a second tunnel between the apparatus and the first gateway device is intended to be set up; determining means adapted to determine, if the second tunnel is intended to be set up, whether the pair comprising the address of the first gateway device is stored by the storing means; retrieving means adapted to retrieve the address of the set from the pair if the address of the first gateway device is stored in the pair; tunnel requesting means adapted to request to set up the second tunnel between the apparatus and a third gateway device if the address of the first gateway device is stored in the pair, wherein the third gateway device is comprised in the set.

The apparatus may further comprise inhibiting means adapted to inhibit the tunnel requesting means from requesting to set up the second tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the pair stored by the storing means.

According to a fourth aspect of the invention, there is provided an apparatus, comprising checking means adapted to check, if a challenge request comprises an address of a set of one or more gateway devices, wherein the challenge request is received from a first gateway device after a tunnel request requesting to set up a first tunnel between the apparatus and the first gateway device was sent to the first gateway device, the apparatus is identified by an identity in the tunnel request, and the challenge request belongs to a procedure for at least one of an authentication and an authorization of the identity; requesting means adapted to request to set up a second tunnel between the apparatus and a second gateway device if the challenge request comprises the address, wherein the second gateway device belongs to the set.

The apparatus may further comprise abandoning means adapted to abandon the setting up of the first tunnel if the challenge request comprises the address.

The apparatus may further comprise storing means adapted to store a pair of the address of the set and an address of the first gateway device; determining means adapted to determine if an address of the first gateway device is comprised in the pair stored by the storing means; retrieving means adapted to retrieve the address of the set from the pair; tunnel requesting means adapted to request to set up a third tunnel between the apparatus and a third

gateway device if the address of the first gateway device is comprised in the pair stored by the storing means, wherein the third gateway device belongs to the set.

The apparatus may further comprise inhibiting means adapted to inhibit the tunnel requesting means from requesting to set up the third tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the pair stored by the storing means.

The apparatus may further comprise monitoring means adapted to monitor if the challenge request comprises a store indication; inhibiting means adapted to inhibit the storing means from storing the pair of the address of the set and the address of the first gateway device if the challenge request does not comprise the store indication.

In the apparatus according to any of the third and fourth aspects, the set may consist of the second gateway device and the address of the set may be the address of the second gateway device.

According to a fifth aspect of the invention, there is provided an apparatus, comprising deciding circuitry configured to decide if a terminal using an identity is to be redirected from a first gateway device to a second gateway device comprised in a set of one or more gateway devices, wherein the identity is received in an identity request from the first gateway device for at least one of an authentication and an authorization of the identity, wherein at least one of the one or more gateway devices of the set is different from the first gateway device; providing circuitry configured to provide, if the terminal is to be redirected, an address of the set.

The providing circuitry may be configured to provide the address of the set to the first gateway device.

The providing circuitry may be configured to provide the address of the set to the terminal in a challenge request, and the challenge request may belongs to a procedure for the respective at least one of the authentication and the authorization of the identity.

The apparatus may further comprise monitoring circuitry configured to monitor if the first gateway device belongs to a home network to which the apparatus belongs; inhibiting

circuitry configured to inhibit the deciding circuitry from deciding that the terminal is to be redirected if the first gateway device belongs to the home network.

The deciding circuitry may be configured to decide based on at least one of a predetermined policy, an identification of the first gateway device, the identity, subscription data related to the identity, a timing of the first request, a location of the terminal, a load on the second gateway device, a load on the first gateway device, and an emergency indication received in the identity request.

The apparatus may further comprise indicating circuitry configured to indicate if the terminal should store that it is to be redirected from the first gateway device to the second gateway device.

The set may consist of the second gateway device and the address of the set may be the address of the second gateway device.

According to a sixth aspect of the invention, there is provided an apparatus, comprising checking circuitry configured to check if a response comprises an address of a set of one or more gateway devices, wherein the response is received in response to an identity request for at least one of an authentication and an authorization of an identity, and the identity is used to identify a terminal in a received tunnel request to set up a tunnel to the terminal; redirecting circuitry configured to redirect the terminal to request setting up the tunnel to one gateway device of the set of gateway devices if the address is received.

The redirecting circuitry may be configured to redirect the terminal using a redirect mechanism of internet key exchange version 2.

The apparatus may further comprise emergency monitoring circuitry configured to monitor if the tunnel request comprises an emergency indication indicating that the tunnel is for an emergency call; emergency forwarding circuitry configured to forward the emergency indication with the identity request.

The set may consist of the one gateway device and the address of the set may be the address of the one gateway device.

According to a seventh aspect of the invention, there is provided an apparatus, comprising monitoring circuitry configured to monitor if a tunnel request to set up a first tunnel between the apparatus and a first gateway device is redirected to a second gateway device different from the first gateway device, wherein the second gateway device is comprised in a set of one or more gateway devices; storing circuitry configured to store a pair of an address of the set and an address of the first gateway device, if the tunnel request is redirected; supervising circuitry configured to supervise if a second tunnel between the apparatus and the first gateway device is intended to be set up; determining circuitry configured to determine, if the second tunnel is intended to be set up, whether the pair comprising the address of the first gateway device is stored by the storing circuitry; retrieving circuitry configured to retrieve the address of the set from the pair if the address of the first gateway device is stored in the pair; tunnel requesting circuitry configured to request to set up the second tunnel between the apparatus and a third gateway device if the address of the first gateway device is stored in the pair, wherein the third gateway device is comprised in the set.

The apparatus may further comprise inhibiting circuitry configured to inhibit the tunnel requesting circuitry from requesting to set up the second tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the pair stored by the storing circuitry.

According to a eighth aspect of the invention, there is provided an apparatus, comprising checking circuitry configured to check, if a challenge request comprises an address of a set of one or more gateway devices, wherein the challenge request is received from a first gateway device after a tunnel request requesting to set up a first tunnel between the apparatus and the first gateway device was sent to the first gateway device, the apparatus is identified by an identity in the tunnel request, and the challenge request belongs to a procedure for at least one of an authentication and an authorization of the identity; requesting circuitry configured to request to set up a second tunnel between the apparatus and a second gateway device if the challenge request comprises the address, wherein the second gateway device belongs to the set.

The apparatus may further comprise abandoning circuitry configured to abandon the setting up of the first tunnel if the challenge request comprises the address.

The apparatus may further comprise storing circuitry configured to store a pair of the address of the set and an address of the first gateway device; determining circuitry configured to

determine if an address of the first gateway device is comprised in the pair stored by the storing circuitry; retrieving circuitry configured to retrieve the address of the set from the pair; tunnel requesting circuitry configured to request to set up a third tunnel between the apparatus and a third gateway device if the address of the first gateway device is comprised in the pair stored by the storing circuitry, wherein the third gateway device belongs to the set.

The apparatus may further comprise inhibiting circuitry configured to inhibit the tunnel requesting circuitry from requesting to set up the third tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the pair stored by the storing circuitry.

The apparatus may further comprise monitoring circuitry configured to monitor if the challenge request comprises a store indication; inhibiting circuitry configured to inhibit the storing circuitry from storing the pair of the address of the set and the address of the first gateway device if the challenge request does not comprise the store indication.

In the apparatus according to any of the seventh and eighth aspects, the set may consist of the second gateway device and the address of the set may be the address of the second gateway device.

According to a ninth aspect of the invention, there is provided a method, comprising deciding if a terminal using an identity is to be redirected from a first gateway device to a second gateway device comprised in a set of one or more gateway devices, wherein the identity is received in an identity request from the first gateway device for at least one of an authentication and an authorization of the identity, wherein at least one of the one or more gateway devices of the set is different from the first gateway device; providing, if the terminal is to be redirected, an address of the set.

The address of the set may be provided to the first gateway device.

The address of the set may be provided to the terminal in a challenge request, and the challenge request may belong to a procedure for the respective at least one of the authentication and the authorization of the identity.

The method may further comprise monitoring if the first gateway device belongs to a home network to which an apparatus performing the method belongs; inhibiting the deciding that the terminal is to be redirected if the first gateway device belongs to the home network.

The deciding may be based on at least one of a predetermined policy, an identification of the first gateway device, the identity, subscription data related to the identity, a timing of the first request, a location of the terminal, a load on the second gateway device, a load on the first gateway device, and an emergency indication received in the identity request.

The method may further comprise indicating if the terminal should store that it is to be redirected from the first gateway device to the second gateway device.

The set may consist of the second gateway device and the address of the set may be the address of the second gateway device.

According to a tenth aspect of the invention, there is provided a method, comprising checking if a response comprises an address of a set of one or more gateway devices, wherein the response is received in response to an identity request for at least one of an authentication and an authorization of an identity, and the identity is used to identify a terminal in a received tunnel request to set up a tunnel to the terminal; redirecting the terminal to request setting up the tunnel to one gateway device of the set of gateway devices if the address is received.

The redirecting of the terminal may use a redirect mechanism of internet key exchange version 2.

The method may further comprise monitoring if the tunnel request comprises an emergency indication indicating that the tunnel is for an emergency call; forwarding the emergency indication with the identity request.

The set may consist of the one gateway device and the address of the set may be the address of the one gateway device.

According to an eleventh aspect of the invention, there is provided a method, comprising monitoring if a tunnel request to set up a first tunnel between an apparatus performing the method and a first gateway device is redirected to a second gateway device different from the first gateway device, wherein the second gateway device is comprised in a set of one or

more gateway devices; storing a pair of an address of the set and an address of the first gateway device, if the tunnel request is redirected; supervising if a second tunnel between the apparatus and the first gateway device is intended to be set up; determining, if the second tunnel is intended to be set up, whether the pair comprising the address of the first gateway device is stored; retrieving the address of the set from the pair if the address of the first gateway device is stored in the pair; requesting to set up the second tunnel between the apparatus and a third gateway device if the address of the first gateway device is stored in the pair, wherein the third gateway device is comprised in the set.

The method may further comprise inhibiting the requesting to set up the second tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the stored pair.

According to a twelfth aspect of the invention, there is provided a method, comprising checking, if a challenge request comprises an address of a set of one or more gateway devices, wherein the challenge request is received from a first gateway device after a tunnel request requesting to set up a first tunnel between an apparatus performing the method and the first gateway device was sent to the first gateway device, the apparatus is identified by an identity in the tunnel request, and the challenge request belongs to a procedure for at least one of an authentication and an authorization of the identity; requesting to set up a second tunnel between the apparatus and a second gateway device if the challenge request comprises the address, wherein the second gateway device belongs to the set.

The method may further comprise abandoning the setting up of the first tunnel if the challenge request comprises the address.

The method may further comprise storing a pair of the address of the set and an address of the first gateway device; determining if an address of the first gateway device is comprised in the stored pair; retrieving the address of the set from the pair; requesting to set up a third tunnel between the apparatus and a third gateway device if the address of the first gateway device is comprised in the stored pair, wherein the third gateway device belongs to the set.

The method may further comprise inhibiting the requesting to set up the third tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the stored pair.

The method may further comprise monitoring if the challenge request comprises a store indication; inhibiting the storing of the pair of the address of the set and the address of the first gateway device if the challenge request does not comprise the store indication.

In the method according to any of the eleventh and twelfth aspects, the set may consist of the second gateway device and the address of the set may be the address of the second gateway device.

The method of any of the ninth to twelfth aspects may be a method of redirecting.

According to a thirteenth aspect of the invention, there is provided a computer program product comprising a set of instructions which, when executed on an apparatus, is configured to cause the apparatus to carry out the method according to any of the ninth to twelfth aspects. The computer program product may be embodied as a computer-readable medium or directly loadable into a computer.

According to some embodiments of the invention, at least one of the following advantages may be achieved:

- The HPLMN operator has full control of ePDG selection in a fully dynamic way.
- ANDSF support in the UE is not required.
- Existing IKEv2 extension is re-used, therefore an easy implementation in UEs and ePDGs is expected.
- Emergency calls are supported.
- Reduced signaling effort if UE stores decision on redirection.
- Risk of malicious redirection may be reduced.
- ePDG in VPLMN may not be affected, which may result in a simplified rollout.

It is to be understood that any of the above modifications can be applied singly or in combination to the respective aspects to which they refer, unless they are explicitly stated as excluding alternatives.

Brief description of the drawings

Further details, features, objects, and advantages are apparent from the following detailed description of the preferred embodiments of the present invention which is to be taken in conjunction with the appended drawings, wherein

Fig. 1 shows a message flow according to some embodiments of the invention;
Fig. 2 shows an apparatus according to an embodiment of the invention;
Fig. 3 shows a method according to an embodiment of the invention;
Fig. 4 shows an apparatus according to an embodiment of the invention;
Fig. 5 shows a method according to an embodiment of the invention;
Fig. 6 shows an apparatus according to an embodiment of the invention;
Fig. 7 shows a method according to an embodiment of the invention;
Fig. 8 shows an apparatus according to an embodiment of the invention;
Fig. 9 shows a method according to an embodiment of the invention; and
Fig. 10 shows an apparatus according to an embodiment of the invention.

Detailed description of certain embodiments

Herein below, certain embodiments of the present invention are described in detail with reference to the accompanying drawings, wherein the features of the embodiments can be freely combined with each other unless otherwise described. However, it is to be expressly understood that the description of certain embodiments is given by way of example only, and that it is by no way intended to be understood as limiting the invention to the disclosed details.

Moreover, it is to be understood that the apparatus is configured to perform the corresponding method, although in some cases only the apparatus or only the method are described.

According to some embodiments of the invention, if the operator of the HPLMN wants that a UE should use an ePDG in the HPLMN, the 3GPP AAA server, which is in the HPLMN, provides an FQDN or an IP address of ePDG(s) in the home network where the UE should be redirected during initial authentication and authorization procedure towards the ePDG in roaming network. The ePDG in the roaming network then redirects the UE using the IKEv2 redirect mechanism towards ePDG in the HPLMN using the IP address or FQDN received from the 3GPP AAA server.

The decision whether or not ePDG in HPLMN is to be used may depend on one or more of the following criteria: a local policy configured in the AAA server, a VPLMN identifier of the ePDG, a user identity, subscription data related to the user identity etc. Other potential

criteria may be the time of the day or the weekday (in low traffic times, ePDG in HPLMN may be preferred). Also, the AAA server may be made aware of the current load on the ePDGs of the HPLMN and decide on the current load whether ePDG in HPLMN or ePDG in VPLMN is to be used. Some or all of these criteria may be combined by logical OR and/or logical AND. E.g., the 3GPP AAA server may only redirect UEs to an ePDG in the HPLMN when they have IMS subscription and local break-out to IMS in the given VPLMN is not supported.

In some embodiments of the invention, in case of emergency sessions the UE indicates at the initial tunnel setup request that the session is for an emergency call. The ePDG forwards this indication to the 3GPP AAA server and thus, the 3GPP AAA server may take into account the emergency indication as a further criterion when it decides if ePDG in the visited or in the home network should be used. For example, 3GPP AAA server may decide not to redirect the UE to the ePDG in the HPLMN in case of an emergency call, regardless of all other criteria.

Furthermore, the 3GPP AAA server may also take into account the location of the UE (e.g. the 3GPP AAA server may know the current location of the UE in cellular access) during the redirection; i.e. the ePDG identifier sent to the UE may depend on the UE's location. Note that the redirection between ePDGs in the same PLMN is also possible in order to find the ePDG that is the most appropriate based on the UE's location.

Throughout this application, both expressions “redirecting a UE (terminal)” and “redirecting a request” and similar expressions are used. These expressions are substantially equivalent. Namely, “redirecting a UE” means, that a request from the UE to a first addressee is redirected to a second addressee different from the first addressee. More precisely, it may mean that the request to the first addressee is cancelled and, instead, a new, corresponding, request to the second addressee is issued. On the other hand, “redirecting a request” means that a request to the first addressee is now directed to the second addressee. More precisely, it may mean that the request to the first addressee is cancelled and, instead, a new, corresponding, request to the second addressee is issued. However, for both expressions, according to some embodiments of the invention, the request to the first addressee may not be cancelled and the request to the second addressee may be additionally issued.

Fig. 1 shows a message flow according to some embodiments of the invention. Fig. 1 shows an UE 1001, non-3GPP IP access 1002, a roaming ePDG 1003 (ePDG in VPLMN), a home

ePDG 1004 (ePDG in HPLMN), and a 3GPP AAA server 1006. The 3GPP AAA server may be combined with HSS or separated therefrom. The 3GPP AAA server 1006 is in the HPLMN of the UE 1001. Communication with the 3GPP AAA server 1006 may be performed via an AAA proxy (not shown) or directly with the 3GPP AAA server 1006.

The message flow is as follows:

1) UE 1001 contacts ePDG 1003 in the VPLMN by non-3GPP IP access 1002 (e.g. WLAN) to request setup of a tunnel (e.g. IPSec tunnel) through the non-3GPP IP access 1002. This step may be done according the ePDG selection mechanism as currently specified, or it may be done by a modified procedure. In the request to setup the tunnel, UE 1001 provides its identity (e.g. IMSI) to ePDG 1003.
2) ePDG 1003 performs an initial Authentication and Authorization procedure. Therefore, it contacts the 3GPP AAA server 1006 in the HPLMN of UE 1001. This step may be done according to the currently specified procedures or according to a modified procedure.
3) The 3GPP AAA server 1006 receiving the initial Authentication and Authorization request from the ePDG 1003 in the VPLMN may decide that the UE shall be redirected to ePDG 1004 in the HPLMN. This decision may be based on one or more of the criteria described above. If the 3GPP AAA server 1006 decides to redirect the UE 1001 to ePDG 1004 in the HPLMN, the 3GPP AAA server 1006 indicates to the ePDG 1003 in the VPLMN, in response to the request for authentication and authorization of message 2), that the UE 1001 shall be redirected to ePDG 1004 in the HPLMN and sends an address of the ePDG 1004 in the HPLMN (e.g. IP address or an FQDN) where the UE 1001 shall be redirected to. E.g. the providing of the address of the ePDG 1004 in the HPLMN may be considered as an implicit indication that the UE 1001 is to be redirected. In some embodiments of the invention, such as that shown in Fig. 1, the address of the ePDG 1004 in the HPLMN may be included in a portion of the response, which ePDG 1003 in the VPLMN is expected to evaluate.In detail, the ePDG 1003 in the VPLMN has to check whether the response from the 3GPP AAA server 1006 contains an address of the ePDG 1004 in the HPLMN. Depending on the implementation, the address of the ePDG 1004 in the HPLMN may be comprised in an additional field in the response from the 3GPP AAA server 1006, or an existing field in the response may be re-interpreted as comprising the address.
4) When the ePDG 1003 in the VPLMN receives the address of the ePDG 1004 in the HPLM in the response from the 3GPP AAA server 1006, the ePDG 1003 in the

VPLMN triggers redirection. For the redirection, it may use e.g. the IKEv2 REDIRECT mechanism as defined in the RFC 5685. For example, ePDG 1003 in the VPLMN may add REDIRECT payload in the IKE_AUTH response with the address of the ePDG 1004 in the HPLMN, Note that this IKEv2 mechanism may also be used if a PDN-GW is reallocated during attach procedure over S2c interface, as defined in 3GPP TS 23.402 and in 3GPP TS 24.303.

5) The UE 1001 contacts ePDG 1004 in the HPLMN based on the redirect information received from the ePDG 1003 in the VPLMN. That is, it requests to set up a tunnel through non-3PGG access to the ePDG 1004 in the HPLMN.
6) The UE 1001 performs authentication and authorization at 3GPP AAA server 1006, via ePDG 1004 in the HPLMN for setting up the tunnel between ePDG 1004 in the HPLMN and the UE 1001.

In some embodiments of the invention, the address of the ePDG in the HPLMN is included in a message to the UE which is encapsulated in the message from 3GPP AAA server and not evaluated by ePDG in VPLMN. For example, according to 3GPP TS 33.402, the 3GPP AAA Server may initiate an authentication challenge. 3GPP AAA server may include the address of the ePDG in the HPLMN in the EAP of the authentication challenge. Depending on the implementation, the address of the ePDG in the HPLMN may be comprised in an additional field in the EAP, or an existing field may be re-interpreted as comprising the address. The information may be ciphered and secured if it is included for example into the AT_ENCR_DATA attribute in EAP AKA authentication.

If UE receives the authentication challenge (challenge message) including the address of the ePDG in the HPLMN, it knows that it is to be redirected to the ePDG in the HPLMN and performs accordingly. For example, it will request to set up a tunnel to the ePDG in the HPLMN. In addition, typically, it may abandon the setup procedure of the tunnel to the ePDG in the VPLMN.

These embodiments of the invention have an advantage that ePDG in the VPLMN is not involved in the redirecting and that, thus, the UE can rely on the validity of the redirection, especially if information is secured by ciphering it. There is hardly any risk of a malicious redirection.

In some embodiments of the invention, UE may store indication whether it was redirected to a ePDG in HPLMN. In these cases, if the same ePDG in VPLMN is selected again, UE may

skip the attempt to set up a tunnel to this ePDG and immediately attempt to set up a tunnel to the ePDG in the HPLMN.

In some embodiments of the invention, 3GPP AAA server may indicate to UE, whether or not it should store the redirection. For example, if the decision depends on the timing of the request, UE should not remember the redirection, but if it depends on the VPLMN, it should remember the redirection.

In some embodiments of the invention, 3GPP AAA server, if it receives the request for authentication and authorization from ePDG, may check if the ePDG is in a foreign (roaming) network (VPLMN) or in the home network (HPLMN). If it is an ePDG in the home network, it may not decide on redirection but disrupt the method.

In some embodiments of the invention, 3GPP AAA server may decide if and where the redirection should take place, even if the request for authentication and authorization is received from an ePDG in the HPLMN. Thus, operator may further influence the traffic even in the home network. E.g., operator may improve load balancing among ePDGs of the home network. In these embodiments, 3GPP AAA server may not check if the requesting ePDG is in the roaming network, or the deciding may take place even if the result of the checking is that the requesting ePDG is in the HPLMN.

In some embodiments of the invention, ePDG may decide to redirect the terminal not to an ePDG in the HPLMN but to another ePDG in the same of another VPLMN. E.g., the home operator may have a corresponding agreement with an operator of another VPLMN which is geographically more suitable to provide the ePDG function than the ePDG(s) of the HPLMN. Or, the home operator may have an agreement with the visited operator that a certain ePDG in the VPLMN has to be used by all users of the home operator roaming in the VPLMN.

In some embodiments of the invention, the 3GPP AAA server redirects the UE from an ePDG in the HPLMN to an ePDG in the VPLMN. E.g. the home operator configures the UE with an identifier (IP address or FQDN) of an ePDG in the HPLMN and the 3GPP AAA server makes a redirection decision depending on the UE location or Registered PLMN (Registered PLMN is the PLMN that is used by the UE to access 3GPP RAN).

That is, depending on the configuration of the 3GPP AAA server, the 3GPP AAA server may redirect the terminal (directly or via the first ePDG, i.e. the ePDG to which the first request to

set up a tunnel is directed) from any ePDG ("first gateway device") in any network including the HPLMN to any ePDG ("second gateway device") in any network including the HPLMN, and the terms "home gateway device" and "roaming gateway device" are not necessarily restricted to an ePDG in the HPLMN and an ePDG in a VPLMN. In the example embodiment shown in Fig. 1, the ePDG in the VPLMN ("roaming ePDG") corresponds to the "first gateway device" and the ePDG in the HPLMN ("home ePDG") corresponds to the "second gateway device".

In some embodiments of the invention, the AAA server may provide a FQDN as a redirection address. In that case, the provided address (FQDN) may point to a set of ePDGs (e.g. ePDGs in the HPLMN). Then the UE may select one of the ePDGs whose IP address can be fetched from the DNS using the provided FQDN.

That is, the AAA server may provide either an address of a single ePDG or an address of a set of ePDGs. The address of the single ePDG may be considered as a special case of an address of a set, wherein the set consists of one ePDG.

Fig. 2 shows an apparatus according to an embodiment of the invention. The apparatus may be a server for authentication and/or authorization of a 3GPP network such as a 3GPP AAA server or an element thereof. Fig. 3 shows a method according to an embodiment of the invention. The apparatus according to Fig. 2 may perform the method of Fig. 3 but is not limited to this method. The method of Fig. 3 may be performed by the apparatus of Fig. 2 but is not limited to being performed by this apparatus.

The apparatus comprises deciding means 10 and providing means 20. The deciding means 10 and providing means 20 may be a deciding circuitry and a providing circuitry, respectively.

The deciding means 10 decides if a terminal using an identity is to be redirected from a first gateway device to a second gateway device (S10). The identity is received in an identity request from the first gateway device. The identity request is for at least one of an authentication and an authorization of the identity. E.g., throughout Figs. 2 to 9, the first gateway device may be a roaming gateway device (an ePDG in a VPLMN), and the second gateway device may be a home gateway device (an ePDG in the HPLMN). The second gateway device is comprised in a set of one or more gateway devices. If the set consists of the second gateway device (i.e., the second gateway device is the only member of the set), the second gateway device is different from the first gateway device. In this case, the

address of the set may be the address of the second gateway device. If the set comprises more than one gateway devices, at least one of these gateway devices is anyway different from the first gateway device. In some embodiments of the invention, each of the gateway devices of the set is different from the first gateway device.

If the terminal is to be redirected (S10 = "yes"), the providing means 20 provides an address of the set (S20). The providing means 20 may provide the address to the first gateway device and/or to the terminal. If it provides the address to the terminal it may be comprised in a challenge request belonging to a procedure for the respective at least one of the authentication and the authorization of the identity.

Fig. 4 shows an apparatus according to an embodiment of the invention. The apparatus may be a gateway (gateway device) to a 3GPP network such as an ePDG or an element thereof. Fig. 5 shows a method according to an embodiment of the invention. The apparatus according to Fig. 4 may perform the method of Fig. 5 but is not limited to this method. The method of Fig. 5 may be performed by the apparatus of Fig. 4 but is not limited to being performed by this apparatus.

The apparatus comprises checking means 110 and redirecting means 20. The checking means 110 and redirecting means 120 may be a checking circuitry and a redirecting circuitry, respectively.

The checking means 110 checks if a response comprises an address of a set of one or more gateway devices (S120). The response is received in response to an identity request for at least one of an authentication and an authorization of an identity. The identity is used to identify a terminal in a received tunnel request to set up a tunnel to the terminal.

If the address of the second gateway device is received (S110 = "yes"), the redirecting means 120 redirects the terminal to request setting up the tunnel to one of the gateway devices of the set of gateway devices (S120).

Fig. 6 shows an apparatus according to an embodiment of the invention. The apparatus may be a terminal such as an UE or an element thereof. Fig. 7 shows a method according to an embodiment of the invention. The apparatus according to Fig. 6 may perform the method of Fig. 7 but is not limited to this method. The method of Fig. 7 may be performed by the apparatus of Fig. 6 but is not limited to being performed by this apparatus.

The apparatus comprises monitoring means 210, storing means 220, supervising means 230, determining means 240, retrieving means 250, and tunnel requesting means 260. The monitoring means 210, storing means 220, supervising means 230, determining means 240, retrieving means 250, and tunnel requesting means 260 may be a monitoring circuitry, storing circuitry, supervising circuitry, determining circuitry, retrieving circuitry, and tunnel requesting circuitry, respectively.

The monitoring means 210 monitors if a first tunnel request is redirected to a second gateway device different from the first gateway device (S210). By the first tunnel request, it is requested to set up a first tunnel between the apparatus and the first gateway device. The second gateway device is comprised in a set of one or more gateway devices.

If the first tunnel request is redirected (S210 = ”yes”), the storing means 220 stores a pair of an address of the set and an address of the first gateway device (S220); otherwise (S210 = “no”, not shown in Fig. 7), in some embodiments of the invention, the storing means 220 may not store the pair and the method is stopped.

The supervising means 230 supervises if it is intended to set up a second tunnel between the apparatus and the first gateway device (S230). E.g., such an intention may be based on conventional ePDG selection. For example, the request to set up a second tunnel may be issued some time before or after the first tunnel request was redirected.

If it is intended to set up a second tunnel between the apparatus and the first gateway device (S230 = “yes”), the determining means 240 determines if an address of the first gateway device is comprised in the pair stored by the storing means 220, i.e. as a member of the pair (S240). If the address of the first gateway device is stored in the pair (S240 = “yes”), the retrieving means 250 retrieves the address of the set from the pair (S250).

After the address of the second gateway device is retrieved from the pair, the tunnel requesting means (260) requests to set up the second tunnel between the apparatus and a third gateway device (S260). The third gateway device is comprised in the set. The third gateway device may be the same as the second gateway device or different from the second gateway device.

Fig. 8 shows an apparatus according to an embodiment of the invention. The apparatus may be a terminal such as an UE or an element thereof. Fig. 9 shows a method according to an embodiment of the invention. The apparatus according to Fig. 8 may perform the method of Fig. 9 but is not limited to this method. The method of Fig. 9 may be performed by the apparatus of Fig. 8 but is not limited to being performed by this apparatus.

The apparatus comprises checking means 310 and requesting means 320. The checking means 310 and requesting means 320 may be a checking circuitry and a requesting circuitry, respectively.

The checking means 310 checks if a challenge request comprises an address of a set of one or more gateway devices (S310). The challenge request is received from a first gateway device after a tunnel request was sent to the first gateway device. The tunnel request requests to set up a first tunnel between the apparatus and the first gateway device. The apparatus is identified by an identity in the tunnel request. The challenge request belongs to a procedure for at least one of an authentication and an authorization of the identity.

If the challenge request comprises the address (S310 = “yes”), the requesting means 320 requests to set up a second tunnel between the apparatus and a second gateway device (S320). The second gateway device belongs to the set of one or more gateway devices. In addition, in some embodiments of the invention, the first tunnel between the apparatus and the first gateway device is not set up.

Fig. 10 shows an apparatus according to an embodiment of the invention. The apparatus comprises at least one processor 410, at least one memory 420 including computer program code, and the at least one processor 410, with the at least one memory 420 and the computer program code, being arranged to cause the apparatus to at least perform at least one of the methods according to Figs. 3, 5, 7, and 9.

Some embodiments of the invention are described in detail, wherein the UE (via a respective ePDG) requests authentication and authorization from the 3GPP AAA server. However, according to some embodiments, the UE may request only authentication or only authorization from the 3GPP AAA server. Also, the AAA server may be replaced by an AA server, or it may be a server providing only one of an authentication function and an authorization function, as long as the function of the server corresponds to the request from UE (via ePDG).

Embodiments of the invention may be employed in a LTE-A network as 3GPP network. They may be employed also in other mobile networks such as CDMA, EDGE, LTE, UTRAN networks, etc. The non-3GPP network may be a WiFi, WLAN network, fixed broadband access or a network of another access technology or any combination thereof, e.g. WLAN connected via fixed broadband access.

A terminal may be a user equipment such as a mobile phone, a smart phone, a PDA, a laptop, a tablet PC, a wearable, a machine-to-machine device, or any other device which may be connected to the respective 3GPP network and non-3GPP network.

A gateway device may be a ePDG or a corresponding function in a network of another technology.

One piece of information may be transmitted in one or plural messages from one entity to another entity. Each of these messages may comprise further (different) pieces of information.

Names of network elements, protocols, and methods are based on current standards. In other versions or other technologies, the names of these network elements and/or protocols and/or methods may be different, as long as they provide a corresponding functionality.

If not otherwise stated or otherwise made clear from the context, the statement that two entities are different means that they perform different functions. It does not necessarily mean that they are based on different hardware. That is, each of the entities described in the present description may be based on a different hardware, or some or all of the entities may be based on the same hardware. It does not necessarily mean that they are based on different software. That is, each of the entities described in the present description may be based on different software, or some or all of the entities may be based on the same software.

According to the above description, it should thus be apparent that example embodiments of the present invention provide, for example a gateway such as a ePDG, or a component thereof, an apparatus embodying the same, a method for controlling and/or operating the same, and computer program(s) controlling and/or operating the same as well as mediums carrying such computer program(s) and forming computer program product(s). According to

the above description, it should thus be apparent that example embodiments of the present invention provide, for example an AA server or an AAA server, or a component thereof, an apparatus embodying the same, a method for controlling and/or operating the same, and computer program(s) controlling and/or operating the same as well as mediums carrying such computer program(s) and forming computer program product(s). According to the above description, it should thus be apparent that example embodiments of the present invention provide, for example a terminal such as a UE, or a component thereof, an apparatus embodying the same, a method for controlling and/or operating the same, and computer program(s) controlling and/or operating the same as well as mediums carrying such computer program(s) and forming computer program product(s).

Implementations of any of the above described blocks, apparatuses, systems, techniques or methods include, as non limiting examples, implementations as hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

It is to be understood that what is described above is what is presently considered the preferred embodiments of the present invention. However, it should be noted that the description of the preferred embodiments is given by way of example only and that various modifications may be made without departing from the scope of the invention as defined by the appended claims.

Claims

1. Apparatus, comprising

deciding means adapted to decide if a terminal using an identity is to be redirected from a first gateway device to a second gateway device comprised in a set of one or more gateway devices, wherein the identity is received in an identity request from the first gateway device for at least one of an authentication and an authorization of the identity, wherein at least one of the one or more gateway devices of the set is different from the first gateway device;

providing means adapted to provide, if the terminal is to be redirected, an address of the set.

2. The apparatus according to claim 1, wherein

the providing means is adapted to provide the address of the set to the first gateway device.

3. The apparatus according to any of claims 1 and 2, wherein

the providing means is adapted to provide the address of the set to the terminal in a challenge request, and the challenge request belongs to a procedure for the respective at least one of the authentication and the authorization of the identity.

4. The apparatus according to any of claims 1 to 3, further comprising

monitoring means adapted to monitor if the first gateway device belongs to a home network to which the apparatus belongs;

inhibiting means adapted to inhibit the deciding means from deciding that the terminal is to be redirected if the first gateway device belongs to the home network.

5. The apparatus according to any of claims 1 to 4, wherein

the deciding means is adapted to decide based on at least one of a predetermined policy, an identification of the first gateway device, the identity, subscription data related to the identity, a timing of the first request, a location of the terminal, a load on the second gateway device, a load on the first gateway device, and an emergency indication received in the identity request.

6. The apparatus according to any of claims 1 to 5, further comprising

indicating means adapted to indicate if the terminal should store that it is to be redirected from the first gateway device to the second gateway device.

7. The apparatus according to any of claims 1 to 6, wherein the set consists of the second gateway device and the address of the set is the address of the second gateway device.

8. Apparatus, comprising

checking means adapted to check if a response comprises an address of a set of one or more gateway devices, wherein the response is received in response to an identity request for at least one of an authentication and an authorization of an identity, and the identity is used to identify a terminal in a received tunnel request to set up a tunnel to the terminal;

redirecting means adapted to redirect the terminal to request setting up the tunnel to one gateway device of the set of gateway devices if the address is received.

9. The apparatus according to claim 8, wherein

the redirecting means is adapted to redirect the terminal using a redirect mechanism of internet key exchange version 2.

10. The apparatus according to any of claims 8 and 9, further comprising

emergency monitoring means adapted to monitor if the tunnel request comprises an emergency indication indicating that the tunnel is for an emergency call;

emergency forwarding means adapted to forward the emergency indication with the identity request.

11. The apparatus according to any of claims 8 to 10, wherein the set consists of the one gateway device and the address of the set is the address of the one gateway device.

12. Apparatus, comprising

monitoring means adapted to monitor if a tunnel request to set up a first tunnel between the apparatus and a first gateway device is redirected to a second gateway device different from the first gateway device, wherein the second gateway device is comprised in a set of one or more gateway devices;

storing means adapted to store a pair of an address of the set and an address of the first gateway device, if the tunnel request is redirected;

supervising means adapted to supervise if a second tunnel between the apparatus and the first gateway device is intended to be set up;

determining means adapted to determine, if the second tunnel is intended to be set up, whether the pair comprising the address of the first gateway device is stored by the storing means;

retrieving means adapted to retrieve the address of the set from the pair if the address of the first gateway device is stored in the pair;

tunnel requesting means adapted to request to set up the second tunnel between the apparatus and a third gateway device if the address of the first gateway device is stored in the pair, wherein the third gateway device is comprised in the set.

13. The apparatus according to claim 12, further comprising

inhibiting means adapted to inhibit the tunnel requesting means from requesting to set up the second tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the pair stored by the storing means.

14. Apparatus, comprising

checking means adapted to check, if a challenge request comprises an address of a set of one or more gateway devices, wherein the challenge request is received from a first gateway device after a tunnel request requesting to set up a first tunnel between the apparatus and the first gateway device was sent to the first gateway device, the apparatus is identified by an identity in the tunnel request, and the challenge request belongs to a procedure for at least one of an authentication and an authorization of the identity;

requesting means adapted to request to set up a second tunnel between the apparatus and a second gateway device if the challenge request comprises the address, wherein the second gateway device belongs to the set.

15. The apparatus according to claim 14, further comprising

abandoning means adapted to abandon the setting up of the first tunnel if the challenge request comprises the address.

16. The apparatus according to any of claims 14 and 15, further comprising

storing means adapted to store a pair of the address of the set and an address of the first gateway device;

determining means adapted to determine if an address of the first gateway device is comprised in the pair stored by the storing means;

retrieving means adapted to retrieve the address of the set from the pair;

tunnel requesting means adapted to request to set up a third tunnel between the apparatus and a third gateway device if the address of the first gateway device is comprised in the pair stored by the storing means, wherein the third gateway device belongs to the set.

17. The apparatus according to claim 16, further comprising

inhibiting means adapted to inhibit the tunnel requesting means from requesting to set up the third tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the pair stored by the storing means.

18. The apparatus according to any of claims 16 and 17, further comprising

monitoring means adapted to monitor if the challenge request comprises a store indication;

inhibiting means adapted to inhibit the storing means from storing the pair of the address of the set and the address of the first gateway device if the challenge request does not comprise the store indication.

19. The apparatus according to any of claims 12 to 18, wherein the set consists of the second gateway device and the address of the set is the address of the second gateway device.

20. Method, comprising

deciding if a terminal using an identity is to be redirected from a first gateway device to a second gateway device comprised in a set of one or more gateway devices, wherein the identity is received in an identity request from the first gateway device for at least one of an authentication and an authorization of the identity, wherein at least one of the one or more gateway devices of the set is different from the first gateway device;

providing, if the terminal is to be redirected, an address of the set.

21. The method according to claim 20, wherein

the address of the set is provided to the first gateway device.

22. The method according to any of claims 20 and 21, wherein

the address of the set is provided to the terminal in a challenge request, and the challenge request belongs to a procedure for the respective at least one of the authentication and the authorization of the identity.

23. The method according to any of claims 20 to 22, further comprising

monitoring if the first gateway device belongs to a home network to which an apparatus performing the method belongs;

inhibiting the deciding that the terminal is to be redirected if the first gateway device belongs to the home network.

24. The method according to any of claims 20 to 23, wherein

the deciding is based on at least one of a predetermined policy, an identification of the first gateway device, the identity, subscription data related to the identity, a timing of the first request, a location of the terminal, a load on the second gateway device, a load on the first gateway device, and an emergency indication received in the identity request.

25. The method according to any of claims 20 to 24, further comprising

indicating if the terminal should store that it is to be redirected from the first gateway device to the second gateway device.

26. The method according to any of claims 20 to 25, wherein the set consists of the second gateway device and the address of the set is the address of the second gateway device.

27. Method, comprising

checking if a response comprises an address of a set of one or more gateway devices, wherein the response is received in response to an identity request for at least one of an authentication and an authorization of an identity, and the identity is used to identify a terminal in a received tunnel request to set up a tunnel to the terminal;

redirecting the terminal to request setting up the tunnel to one gateway device of the set of gateway devices if the address is received.

28. The method according to claim 27, wherein

the redirecting of the terminal uses a redirect mechanism of internet key exchange version 2.

29. The method according to any of claims 27 and 28, further comprising

monitoring if the tunnel request comprises an emergency indication indicating that the tunnel is for an emergency call;

forwarding the emergency indication with the identity request.

30. The method according to any of claims 27 to 29, wherein the set consists of the one gateway device and the address of the set is the address of the one gateway device.

31. Method, comprising

monitoring if a tunnel request to set up a first tunnel between an apparatus performing the method and a first gateway device is redirected to a second gateway device different from the first gateway device, wherein the second gateway device is comprised in a set of one or more gateway devices;

storing a pair of an address of the set and an address of the first gateway device, if the tunnel request is redirected;

supervising if a second tunnel between the apparatus and the first gateway device is intended to be set up;

determining, if the second tunnel is intended to be set up, whether the pair comprising the address of the first gateway device is stored;

retrieving the address of the set from the pair if the address of the first gateway device is stored in the pair;

requesting to set up the second tunnel between the apparatus and a third gateway device if the address of the first gateway device is stored in the pair, wherein the third gateway device is comprised in the set.

32. The method according to claim 31, further comprising

inhibiting the requesting to set up the second tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the stored pair.

33. Method, comprising

checking, if a challenge request comprises an address of a set of one or more gateway devices, wherein the challenge request is received from a first gateway device after a tunnel request requesting to set up a first tunnel between an apparatus performing the method and the first gateway device was sent to the first gateway device, the apparatus is identified by an identity in the tunnel request, and the challenge request belongs to a procedure for at least one of an authentication and an authorization of the identity;

requesting to set up a second tunnel between the apparatus and a second gateway device if the challenge request comprises the address, wherein the second gateway device belongs to the set.

34. The method according to claim 33, further comprising

abandoning the setting up of the first tunnel if the challenge request comprises the address.

35. The method according to any of claims 33 and 34, further comprising

storing a pair of the address of the set and an address of the first gateway device;

determining if an address of the first gateway device is comprised in the stored pair;

retrieving the address of the set from the pair;

requesting to set up a third tunnel between the apparatus and a third gateway device if the address of the first gateway device is comprised in the stored pair, wherein the third gateway device belongs to the set.

36. The method according to claim 35, further comprising

inhibiting the requesting to set up the third tunnel between the apparatus and the first gateway device if the address of the first gateway device is comprised in the stored pair.

37. The method according to any of claims 35 and 36, further comprising

monitoring if the challenge request comprises a store indication;

inhibiting the storing of the pair of the address of the set and the address of the first gateway device if the challenge request does not comprise the store indication.

38. The method according to any of claims 31 to 37, wherein the set consists of the second gateway device and the address of the set is the address of the second gateway device.

39. A computer program product comprising a set of instructions which, when executed on an apparatus, is configured to cause the apparatus to carry out the method according to any of 20 to 38.

40. The computer program product according to claim 39, embodied as a computer-readable medium or directly loadable into a computer.

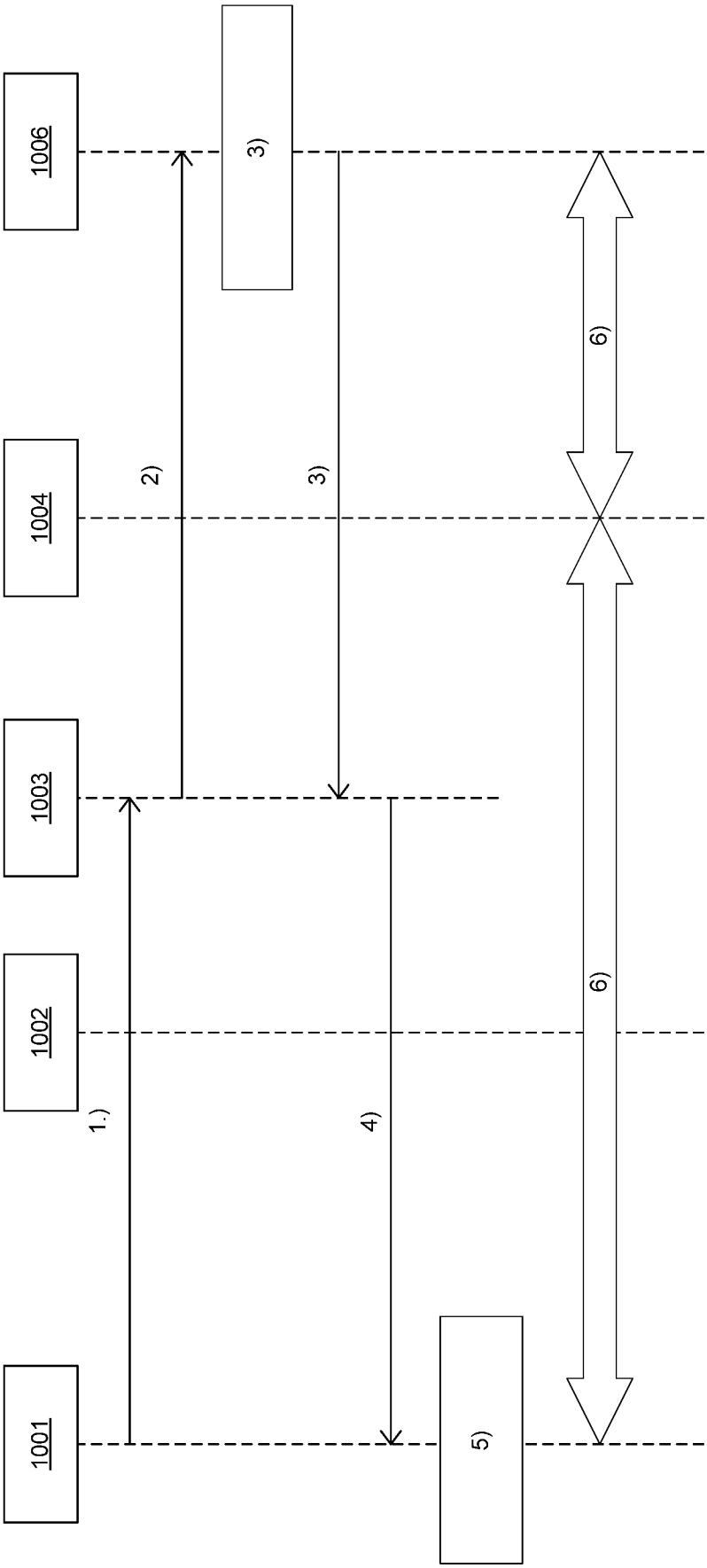


Fig. 1

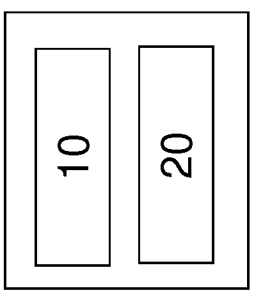


Fig. 2

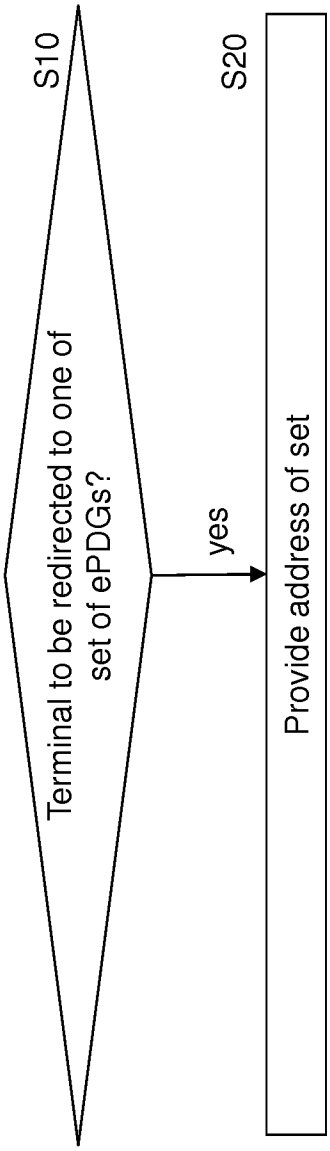


Fig. 3

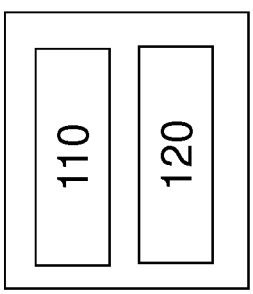


Fig. 4

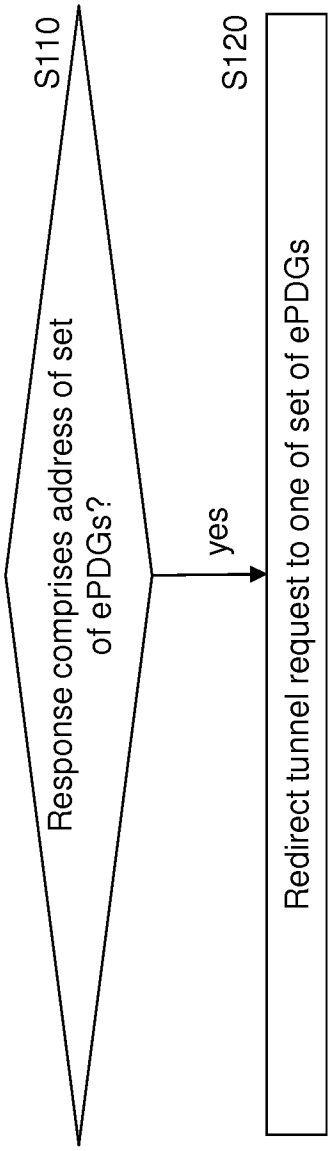


Fig. 5

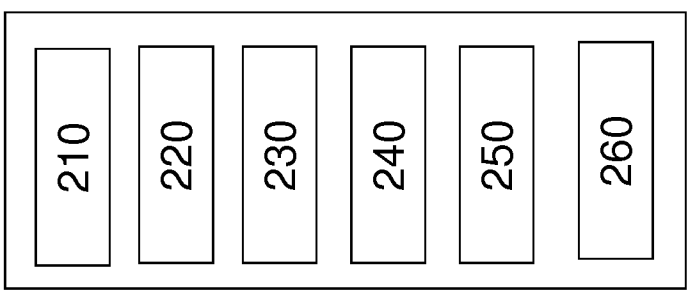

210
220
230
240
250
260

Fig. 6

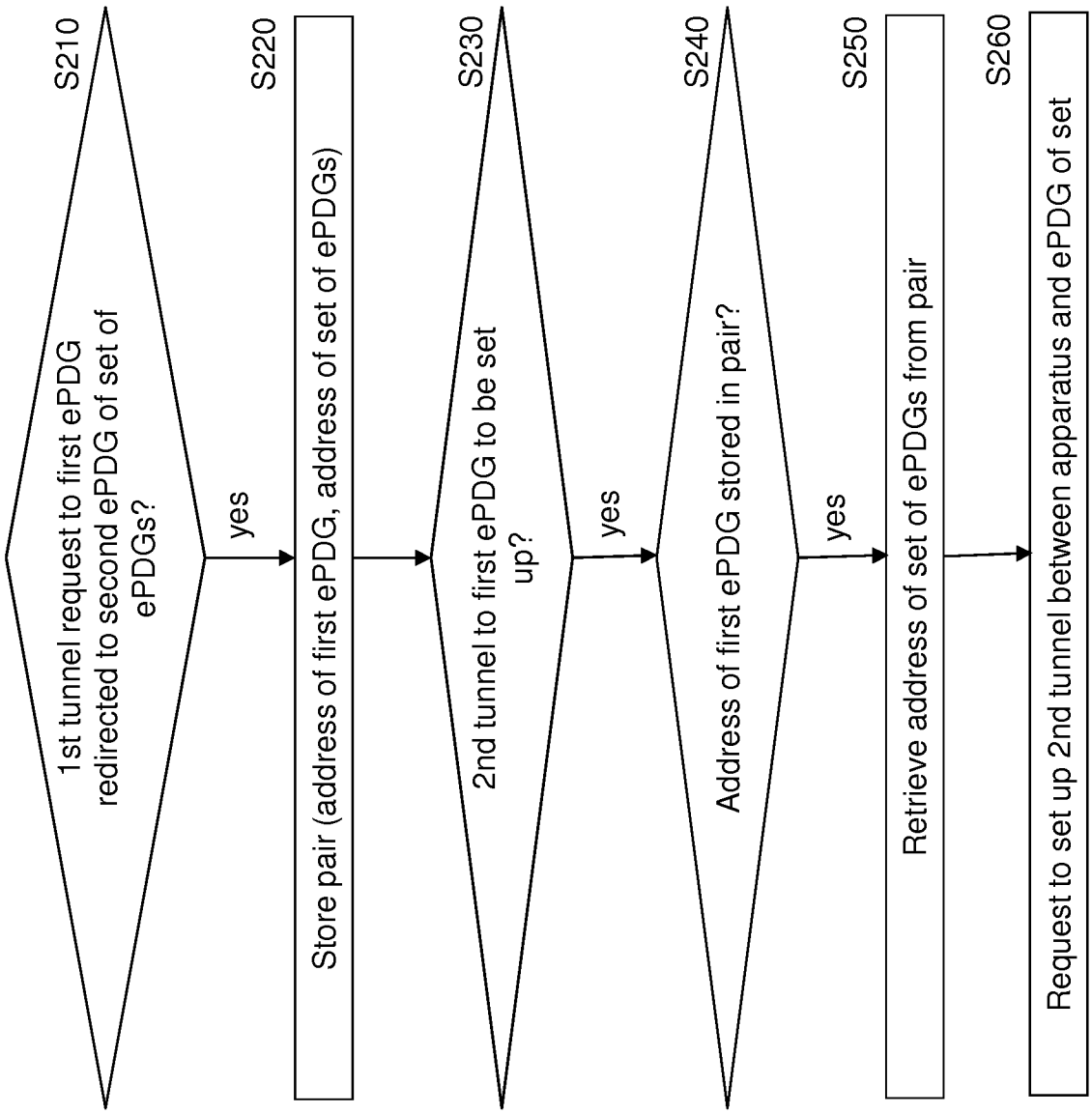

S210
1st tunnel request to first ePDG redirected to second ePDG of set of ePDGs?
yes
S220
Store pair (address of first ePDG, address of set of ePDGs)
S230
2nd tunnel to first ePDG to be set up?
yes
S240
Address of first ePDG stored in pair?
yes
S250
Retrieve address of set of ePDGs from pair
S260
Request to set up 2nd tunnel between apparatus and ePDG of set

Fig. 7

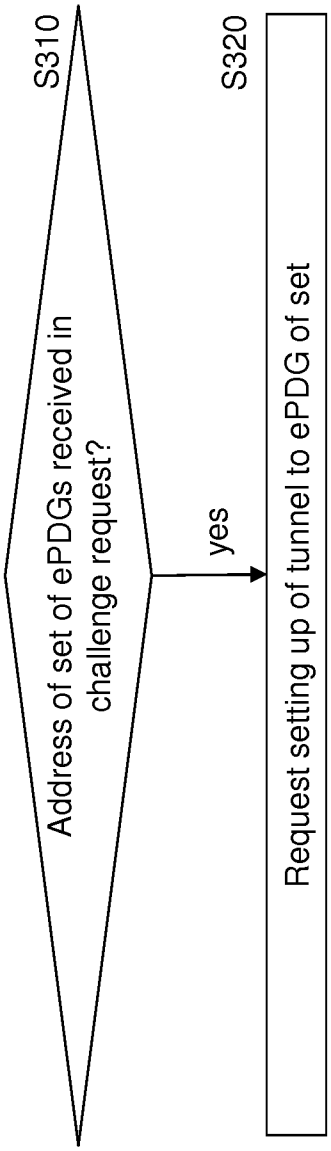


Fig. 9

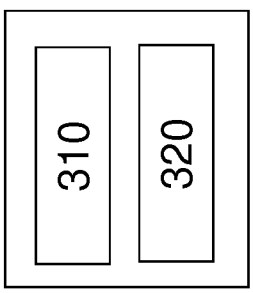


Fig. 8

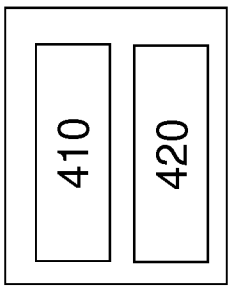


Fig. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/063851

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W48/18 H04W88/16
ADD. H04W76/02 H04W76/04

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)
H04W

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 practicable, 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	US 2010/054222 A1 (RUNE JOHAN [SE]) 4 March 2010 (2010-03-04) abstract figures 1a-6 paragraph [0004] - paragraph [0008] paragraph [0042] - paragraph [0047] paragraph [0069] - paragraph [0072] paragraph [0080] - paragraph [0082] paragraph [0086] - paragraph [0088] claims 36,48,55, 56,57 ----- -/--	1-40

[X] Further documents are listed in the continuation of Box C.

[X] 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 application or patent 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
23 February 2016	03/03/2016

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	Matt, Stefan

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.
X	ZTE: "3GPP AAA Server solution for ePDG selection", 3GPP DRAFT; S2-113370_EPDG REALLOCATION, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Naantali; 20110711, 5 July 2011 (2011-07-05), XP050548645, [retrieved on 2011-07-05] Reason for Change Summary of Change 4.5.4 ePDG Selection -----	1-40
X	EP 2 312 888 A1 (FRANCE TELECOM [FR]) 20 April 2011 (2011-04-20)	1,8,12, 14,20, 27,31, 33,39
A	abstract figure 4 paragraph [0054] - paragraph [0066] -----	2-7, 9-11,13, 15-19, 21-26, 28-30, 32, 34-38,40
A	NORTEL: "ePDG selection", 3GPP DRAFT; S2-071975 EPDG SELECTION, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Beijing; 20070418, 18 April 2007 (2007-04-18), XP050259709, [retrieved on 2007-04-18] 1 Discussion 5.4.2.2.3 Initial Attach procedure with PMIPv6 for roaming case with home routed traffic anchored by visited Serving GW figures 5.4.2.2.3-1 -----	1-40

-/--

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	NOKIA NETWORKS ET AL: "Enhancement of ePDG Selection", 3GPP DRAFT; S2-152245_(EPDG_SELECTION)_V3, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG2, no. Dubrovnik, Croatia; 20150706 - 20150710 6 July 2015 (2015-07-06), XP050987073, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/SA2/Docs [retrieved on 2015-07-07] the whole document -----	1-40

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/063851

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010054222 A1	04-03-2010	EP 2082546 A1	29-07-2009
		JP 5032582 B2	26-09-2012
		JP 2010510713 A	02-04-2010
		US 2010054222 A1	04-03-2010
		WO 2008060208 A1	22-05-2008
EP 2312888 A1	20-04-2011	EP 2312888 A1	20-04-2011
		WO 2011045407 A1	21-04-2011