

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
18 November 2004 (18.11.2004)

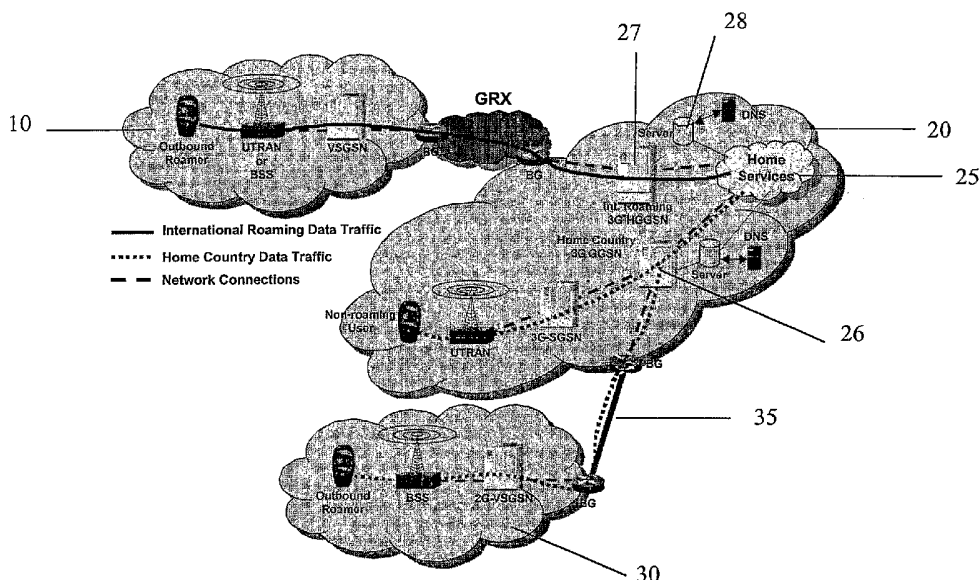
PCT

(10) International Publication Number
WO 2004/100595 A1

- (51) International Patent Classification⁷: **H04Q 7/38** (74) Agents: **BUTCHER, Ian, J.** et al.; A A Thornton & Co, 235 High Holborn, London WC1V 7LE (GB).
- (21) International Application Number:
PCT/GB2004/002020 (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (22) International Filing Date: 12 May 2004 (12.05.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
0310877.6 12 May 2003 (12.05.2003) GB
- (71) Applicant (for all designated States except US): **HUTCHINSON WHAMPOA THREE G IP (BAHAMAS) LIMITED** [BS/BS]; Offshore Group Chambers, PO Box CB-12751, Nassau, New Providence (BS).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **EL YAKHLIFI, Nadir** [FR/GB]; 23 Norreys Drive, Maidenhead, Berkshire SL6 4BJ (GB).
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SERVICE RESTRICTION IN MOBILE COMMUNICATION NETWORKS



Separating International & Home Country PS Traffic

(57) Abstract: This document describes solutions that enable 3G operators to identify the location of their subscribers (at a country level), the serving operator name and the access technology (i.e. 2.5G or 3G) supported by the serving network. This gives 3G operators the capability to control access to contents/services taking into account right and legal restrictions applicable outside the home country and the level of QoS provided by the serving network.



Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Service Restriction in Mobile Communication Networks

The present invention relates to mobile communications networks and methods of supplying services to users of such networks.

Background

Currently legacy mobile communications networks include (a) the GSM (Global System for Mobile Communications) mobile network (or second generation "2G" mobile network) which allows, for example, the exchange of voice calls, and (b) the GPRS (General Packet Radio Service) or 2.5G network which complements the GSM network and allows, to a limited extent, the access of data services using the same technology as the Internet.

The new mobile network, so called 3G, has increased capabilities and this, as well as offering services such as the exchange of voice calls, will enable users to communicate via video telephony. 3G networks also allow users to access additional data services currently not available on 2.5G networks, such as streamed (real time) video and advanced gaming. As for 2.5G networks, these data services will be offered using the same technology as the Internet. Licences to operate 3G networks have generally been granted by state governments and are restricted in terms of territory, usually to a particular country.

In the initial setting up of 3G communications it is likely that 3G coverage is not available throughout a particular country and 3G users roaming within one country may have to use a 2G/2.5G network to make up for gaps in the 3G network. Thus a Greenfield 3G operator, i.e. non-incumbent operator, will have one or more 2G/2.5G "national roaming" partners, i.e. operators of 2G/2.5G networks. In the case of incumbent operators implementing a 3G network, their existing 2G/2.5G network will be used to make up for gaps in their 3G network. For the access of Internet-like services, a 3G customer who has been transferred to the 2G/2.5G network will not be able to receive advanced 3G services with adequate quality of service.

3G customers travelling abroad will use a network of the visited country, which may or may not be 3G. Even if the visited network is 3G there may be restrictions on the services that can be offered to 3G customers abroad due to national laws. For example a visitor to Saudi Arabia will not be able legally to participate in gambling and some countries are more restrictive than others in terms of what adult material can be distributed.

In 2.5 and 3G mobile communications, customers are allocated one of a possible range of IP (Internet Protocol) addresses on requesting access to the Internet-like services from their mobile terminals, the IP addresses most of the time being allocated from the subscriber's home network regardless of the location of the customer.

Summary of the Invention

The present invention aims to solve two problems, namely the possibility of a 3G customer receiving poor service because he is registered with a 2G/2.5 G network and the possibility of a customer engaging in illegal activities using his mobile terminal via his home network.

The present invention provides a method of operating a mobile communications system, wherein traffic from mobile devices is routed via a serving support node and a gateway support node to one or more home network servers accessible only by those mobile devices, the home network having links to other networks whereby traffic to/from mobile devices located outside the home network is routed via another network from/to the home network, the method comprising (a) selecting at least one of the other networks to receive a restricted range of services from the home network server(s);
(b) determining whether mobile devices are communicating with the home network via a selected network; and

(c) barring the supply of certain services from the home network server(s) to mobile devices communicating with the home network via a selected network.

Previous system operating methods have not taken any account of the network(s) via which mobile devices are communicating with their home networks. Thus, hitherto, at least in terms of services to be received, all mobile devices identified as being associated with the home network (the subscribers) have been treated in the same way.

The “selected networks” might be national or foreign 2G/2.5 G networks, or foreign networks of countries with restrictive laws (2G/2.5G or 3G).

As will be explained in more detail below, the network(s) being used by a mobile device whether local or international can be identified from identification data included in control messages by those networks. From this the home server(s) may be able to determine the available access technology (2.5G or 3G) from stored data.

Alternatively, step (b) above might involve examining the QoS (Quality of Service) profile of incoming control messages, whereby certain services (e.g. real time content) might be denied to users on 2.5G.

In the preferred embodiment of the invention, instead of routing all traffic to the home network servers via the same gateway support nodes, as at present, more than one type of gateway support node are used. Thus, for example, all international roaming traffic can be segregated from “home” traffic. Then, if the “selected” networks are foreign networks, only traffic received via a gateway support node dedicated to international roaming traffic needs to be examined to determine which selected network it has arrived from. Other traffic can be handled in the usual way and is not slowed down.

Each gateway support node has its own IP address pool. Traffic can then be segregated simply by checking the IP address allocated to the user.

Brief Description of the Drawings

Embodiments of the invention will now be described by way of example only and with reference to the accompanying drawings in which:

Figure 1 is a schematic diagram showing an arrangement in which a dedicated gateway support node is used to separate traffic generated by customers roaming abroad from that generated by customers located in the country of the home network;

Figure 2 is a more detailed diagram showing the interaction required between the home network and the visited network to set up a session that makes use of a dedicated international roaming gateway support node;

Figure 3 is a diagram illustrating the call flow for session set up using a dedicated international roaming gateway support node;

Figure 4 shows information being transferred from an international roaming gateway support node to a RADIUS server, the information consisting of the IP address of the visited serving support node;

Figure 5 is a schematic diagram illustrating an alternative arrangement in which national and international roaming traffic uses a common gateway support node with home traffic;

Figure 6 shows information being transferred from the common gateway support node of Figure 5 to a server, the information consisting of the IP address of the serving support node;

Figure 7 is a decision tree for an arrangement in which the location of a mobile device is determined from the IP address of the serving support node, which was transferred from the common gateway support node to a server as shown in Figure 6;

Figure 8 shows information being transferred from a common gateway support node to a RADIUS server, the information consisting of the GTP version and part of the QoS profile (i.e. the “length” field);

Figure 9 shows a decision tree in which the type of network used by a mobile device is identified from the GTP (GPRS Tunnelling Protocol) version and the “length” field of the QoS profile, which were transferred from a common gateway support node to a server as shown in Figure 8;

Figure 10 shows information being transferred from the “home country” gateway support node to a server, the information consisting of the IP address of the serving support node;

Figure 11 shows a decision tree for an arrangement in which the type of network used by a mobile device is identified from the IP address of the serving support node, which was transferred from the “home country” gateway support node to a server as shown in Figure 10;

Figure 12 shows information being transferred from a common gateway support node to a server, the information consisting of the IP address of the serving support node; and

Figure 13 shows a decision tree for an arrangement in which the type of network used by a mobile device is identified from the IP address of the serving support node, which was transferred from a common gateway support node to a server as shown in Figure 12.

Description of the preferred embodiments of the present invention

1. High Level requirements:

The following describes a number of possibilities that enable a mobile communications operator to restrict services provided to customers based on their location and/or access technology of their serving network (3G or 2.5G).

The requirements for this service are:

1. To provide capability to filter content based on current access technology supported by the serving network. This applies to both home country based and international roaming PS (Packet Switched) traffic for home services access.
2. To consider scenarios where the access technology may change without dropping the session (i.e. PDP (Packet Data Protocol) Context).
3. To provide capability to filter content based on current country of subscriber. For this, two levels of granularity are possible:
 - All international roaming customers are treated in the same way, e.g. no gambling service outside the home country even if allowed in the visited country, and
 - Services/contents are restricted depending on the country the subscriber roamed to, e.g. no gambling service only in countries where it is forbidden by law, e.g. in Saudi Arabia.

In order to apply service/content restriction, only a coarse guide to the subscriber's location is necessary (e.g. MCC (Mobile Country Code) of roaming partner). The number of filters applicable to a particular

country is outside the scope of this document, but could impose a significant performance requirement on any solution.

4. Users located in the home country preferably should not be impacted by any solution to requirement 1, in terms of range of service availability or speed of response.

For access to home services, if the generated international and home country based PS traffic was routed through the same GGSNs (Gateway GPRS Support Node), every single request would have to be checked in order to determine whether or not the subscriber is allowed to access the desired service/content considering right or legal restrictions applicable outside the home country. The time taken by the application/service domain to process a request would considerably be affected therefore providing all subscribers (both roaming and non roaming) with a poor user experience. However this would be a possible short-term solution.

2. Service Restriction based on Subscriber's Location:

This section describes two solutions that enable operators to identify whether their subscribers are accessing home data services from abroad. Also these solutions enable operators to derive the location of their roaming subscribers (at a country level) from the Mobile Country Code (MCC) and the visited operator name from the Mobile Network Code (MNC). This gives operators the capability to control service access considering right and legal restrictions applicable outside the home country and, in some cases, applicable to a subset of countries only.

2.1 Solution 1:

This section depicts a solution that enables operators to:

- Segregate international PS traffic generated by outbound roamers accessing home data services from abroad, and
- Identify the country and visited operator serving their roaming subscribers.

2.1.1 Overview:

The idea is to use a dedicated GGSN for international PS traffic that is generated towards the home application/service domain. This is shown in Figure 1.

In Figure 1 the three clouds represent, respectively, a foreign network 10 which may be visited by a 3G subscriber, the home 3G subscriber network 20, and the network 30 of the national roaming partner (NRP). The home network and the foreign visited network are linked by a so-called GPRS roaming exchange, "GRX". The home network and that of the national roaming partner are linked by a leased line or other connection 35. Border gateways (BG) serve as the interfaces between individual networks and the GRX or leased line 35.

As shown in Figure 1 users on the national roaming network 30 and the home network 20 are directed to home services, indicated by reference 25 via a home country gateway support node 26. Ordinarily, users abroad would likewise be directed to this node. However, in this novel arrangement, a gateway support node 27 is dedicated to users abroad.

Now that the international PS traffic is routed through a dedicated GGSN, the visited SGSN (Serving GPRS Support Node) (VSGSN) IP address shall be transferred from this roaming GGSN to a server 28 (e.g. RADIUS server) in order to identify the country and visited operator serving the roaming subscribers.

Using this information in the application/service domain, the home operator can therefore apply some kind of filtering in order to restrict access to certain services/contents when customers are roaming abroad.

Figure 1 also shows Base Station Sub-systems (BSS) and UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Networks (UTRAN).

2.1.2 Architecture:

This section gives an overview of one example of how the home network operator can implement the routing of international PS traffic through a dedicated GGSN and identify the country and visited operator.

2.1.2.1 Use of a Dedicated Roaming GGSN:

In order for customers roaming abroad to access home services, all PS sessions (i.e. PDP Contexts) have to be established towards the same GGSN. To do so, the 'Operator.net' APN (Access Point Name) has to be resolved to the IP address of the GGSN.

The above APN is also used when customers located in the home country gain access to services. Therefore if the same DNS (Domain Name Server) is used to resolve the 'Operator.net' APN regardless of the subscriber's location then international roaming and home country based traffic will go through the same GGSNs.

Instead the use of a DNS dedicated to queries (for APN resolution) received from foreign networks enables the home operator to allocate a different GGSN for international roaming PS traffic only. This is possible since the content of the roaming DNS is independent of the information contained in the home country DNS. An overview of this architecture is given in Figure 2.

Note that the IP address of the roaming DNS must be specified to roaming partners.

The call flow given in Figure 3 shows how the session is set up towards the GGSN dedicated to international roaming PS traffic for access to home services.

When the subscriber requests access to Internet-like services, the "Operator.net" APN is sent to the VSGSN of the visited network (step 1). The VSGSN sends the APN to the visited network (VPLMN (Visited Public Land Mobile Network)) domain name server (DNS) 40 (step 2) for resolution. The DNS 40

identifies the APN and passes the query to the international roaming DNS 41 (step 3) located in the subscriber's home network. After resolving the APN, this DNS 41 returns the IP address of the international roaming GGSN to the VPLMN DNS (step 4), which passes it to the VSGSN (step 5) after which the VSGSN communicates directly with the dedicated international roaming HGGSN (Home GGSN) in order to complete the session set up. At this point the international roaming HGGSN allocates an IP address to the subscriber from a range of addresses reserved for international roaming traffic only.

It will be appreciated that the home services servers 25 do not then need to check every incoming request. All that is needed for traffic received via GGSN 26 to be handled differently from traffic received via GGSN 27. Traffic received via the home country GGSN 26 can be handled as previously.

The content of the roaming DNS (in Figure 2) shows that the 'Operator.net' APN is resolved to the IP address of the international roaming GGSN, which allows all PS sessions using that APN to be established towards this GGSN for customers abroad.

Note that roaming corporate subscribers' sessions will be established towards the usual corporate GGSN, i.e. there are no dedicated GGSN for roaming corporate PS traffic. In this example, as far as corporate services are concerned, it is left to network operators to deal with the problems with which this invention is concerned.

Also, Figure 2 shows that a dedicated IP address pool can be allocated to the international roaming GGSN. This would enable the application/service domain to identify that a subscriber is accessing data services from abroad simply by checking the IP address that was allocated during the session setup.

Figure 2 also shows User Equipment (UE).

2.1.2.2 Identifying the Country and Visited Operator:

For international roaming PS traffic, the roaming GGSN shall transfer the VSGSN IP address to a server (e.g. RADIUS server) (See Figure 1) upon reception of

the Create PDP Context Request message (as shown in Figure 4). The received VSGSN IP Address is used to derive the country and visited operator serving the roaming subscribers from respectively the MCC and MNC. To do so, the operator shall make use of a DNS (as shown in Figure 1) to store the MCC and MNC against the SGSN IP address of the corresponding roaming partner. The MCC/MNC information is retrieved through a reverse DNS query containing the VSGSN IP address that was received from the roaming GGSN.

The country and visited operator name are then derived and used by the application/service domain to apply service/content restriction where applicable.

2.2 Solution 2:

This section describes a “single GGSN” solution where the same GGSN is used for both home country based and international roaming PS traffic for access to home services. This is shown in Figure 5 with the single GGSN identified by reference 45.

Three scenarios can be identified:

- Subscribers on the home network, i.e. in the home country,
- Subscribers on the national roaming partner’s network, i.e. in the home country, and
- Subscribers on a foreign network, i.e. abroad.

Upon reception of the Create PDP Context Request message, the home operator’s GGSN shall transfer the SGSN IP address to a server (e.g. RADIUS server) (see Figure 5). This procedure is illustrated in Figure 6.

This will enable operators to:

- Differentiate between international, national and non-roaming subscribers, and
- Identify the country and operator serving their subscribers.

This is based on the assumption that UMTS (Universal Mobile Telecommunications System) to GPRS “Handover” towards the national roaming partner’s network is not implemented. The received SGSN IP Address can then be checked against a list including IP addresses of the home operator’s SGSNs and national roaming partner’s SGSNs. This will enable to identify whether the subscriber is an international, national or non-roamer, and therefore whether the subscriber is abroad or in the home country (see decision tree in Figure 7).

In addition to this, the received SGSN IP Address is used to derive the country and visited operator serving the operator’s subscribers from respectively the MCC and MNC. To do so, the operator shall make use of a DNS (as shown in Figure 5) to store the MCC and MNC against the SGSN IP address of the corresponding network operator.

The MCC/MNC information is retrieved through a reverse DNS query containing the SGSN IP address that was received from the home operator’s GGSN. The country and serving operator name are then derived and used by the application/service domain to apply service/content restriction where applicable.

3. Service Restriction based on Access Technology:

This section describes a number of solutions that enable 3G operators to identify the access technology, i.e. GPRS (2.5G) or UMTS (3G), supported by the network serving their customers when these are accessing home data services. This enables 3G operators to control service access considering the level of QoS provided by the serving network that can also be the home network.

3.1 Solution 1:

This section describes a solution where the home operator’s GGSN transfers the appropriate information to a server (e.g. a RADIUS server) (see Figure 1 & Figure

5) upon reception of a Create PDP Context Request or Update PDP Context Request message from an SGSN.

For 3GPP based networks, there are only three possible combinations of GTP version and QoS profile type in the Request messages sent to the home operator's GGSN:

R97/98 QoS sent over GTPv0, i.e. subscriber on 2.5G,

R97/98 QoS sent over GTPv1, i.e. subscriber on 2.5G, and

R99+R97/98 QoS sent over GTPv1, i.e. subscriber on 3G.

Therefore if:

The GTP version is 0, the subscriber is on 2.5G,

The GTP version is 1 and the QoS profile of R97/98, the subscriber is on 2.5G,

The GTP version is 1 and the QoS profile of R99+R97/98, the subscriber is on 3G.

3GPP TS 29.060 V3.7.0 – GPRS Tunnelling Protocol across the Gn and Gp Interface (1999-12) specifies that “a receiving end (in this case the home operator's GGSN) shall interpret the QoS profile Data field to be coded according to GSM 04.08 (i.e. according to the pre-Release '99 format) if the Length field value is 4”. This is to be taken into account when GTPv1 is used between the SGSN and GGSN. Therefore if, upon reception of a Create PDP Context Request or Update PDP Context Request message from an SGSN, the home operator's GGSN sends to a server (e.g. RADIUS server) the GTP version number, and the value of the length field in the QoS information element (only if GTP version is 1) then the access technology, supported by the network serving the subscriber, can be identified and passed onto the application/service domain to enable service access control.

In the case where the IETF RADIUS protocol (IETF RFC 2865 – Remote Authentication Dial In User Service (RADIUS) (2000-06)) is used between the GGSN and the server, the GGSN needs to make use of the Vendor-Specific attribute

(IETF RFC 2865 and IETF RFC 2866 – RADIUS Accounting (2000-06)) and Interim-Update message (IETF RFC 2866) defined for this protocol.

For this example, the transfer of information from the home operator's GGSN to the RADIUS server is illustrated in Figure 8.

In order to identify the access technology serving a given subscriber, the decision tree represented in Figure 9 is applied.

If the operator decides to implement this solution for international roaming PS traffic only, then it is important to note that the adoption of the "dedicated GGSN" architecture (section 2.1) will have the benefit of not affecting the home country based PS traffic.

3.2 Solution 2:

This section describes a short-term solution in the case where solution 1 (section 3.1) cannot be immediately implemented due to limitations of the GGSN. This solution is based on the "dedicated GGSN" architecture (section 2.1).

3.2.1 International Roaming PS Traffic:

Section 2.1 shows that international roaming PS traffic (for access to home services) can be separated from home country based PS traffic by making use of a dedicated GGSN. Also, in a short-term period, the following assumptions can be made:

All subscribers abroad will roam either onto 2.5G networks or onto 3G networks that do not support real time radio bearers for PS-based applications, and GRX (GPRS Roaming eXchange) networks will not support QoS for real time applications.

Therefore it can be considered that all roaming subscribers, being allocated an IP address through the "international roaming" GGSN, access services from a 2.5G or 2.5G like network. This illustrated in Figure 1.

3.2.2 Home Country Based PS Traffic:

For home country based traffic, two scenarios can be identified:

Subscribers on the home network, i.e. on 3G, and

Subscribers on the national roaming partner's network, i.e. on 2.5G.

Upon reception of the Create PDP Context Request message, the home operator's GGSN shall transfer the SGSN IP address to a server (e.g. RADIUS server) (see Figure 1) to enable to differentiate between national and non-roaming subscribers. This is illustrated in Figure 10. This is based on the assumption that UMTS to GPRS "Handover" towards the national roaming partner's network is not implemented. The received SGSN IP Address can then be checked against a list including IP addresses of the home operator's SGSNs and national roaming partner's SGSNs. This will enable to identify whether the subscriber is roaming nationally or not, and therefore whether the subscriber is on 2.5G or 3G (see decision tree in Figure 11).

It is important to note that the adoption of the "dedicated GGSN" architecture (section 2.1) will enable the operator to perform an SGSN IP address look up for the home country based traffic only.

3.3 Solution 3:

This section describes another short-term solution in the case where solution 1 (section 3.1) cannot be immediately implemented due to limitations of the GGSN. This solution is based on an architecture where the same GGSN is used for both home country based and international roaming PS traffic (section 2.2). The assumptions on international roaming PS traffic, listed in section 3.2.1, are also considered for this solution.

Therefore three scenarios can be identified:

- Subscribers on the home network, i.e. on 3G,
- Subscribers on the national roaming partner's network, i.e. on 2.5G,
and
- Subscribers on a foreign network, i.e. on 2.5G.

Upon reception of the Create PDP Context Request message, the home operator's GGSN shall transfer the SGSN IP address to a server (e.g. RADIUS server) (see Figure 5) to enable to differentiate between international, national and non-roaming subscribers. This is illustrated in Figure 12.

This is based on the assumption that UMTS to GPRS "Handover" towards the national roaming partner's network is not implemented.

The received SGSN IP Address can then be checked against a list including IP addresses of the home operator's SGSNs and national roaming partner's SGSNs. This will enable to identify whether the subscriber is an international, national or non-roaming user, and therefore whether the subscriber is on 2.5G or 3G (see decision tree in Figure 13).

Claims

1. A method of operating a mobile communications system, wherein traffic from mobile devices is routed via a serving support node and a gateway support node to one or more home network servers accessible only by those mobile devices, the home network having links to other networks whereby traffic to/from mobile devices located outside the home network is routed via another network from/to the home network, the method comprising
 - (a) selecting at least one of the other networks to receive a restricted range of services from the home network servers;
 - (b) determining whether mobile devices are communicating with the home network via a selected network; and
 - (c) barring the supply of certain services from the home network server(s) to mobile devices communicating with the home network via a selected network.
2. A method as claimed in claim 1 in which control messages received by the home network include data identifying the network via which the traffic has been routed, and in which step (b) comprises examining said network identifying data for each mobile device communicating with the home network server(s).
3. A method as claimed in claim 2 in which the home network has links to at least one network based in another state, and in which said identifying data allows to identify that state.
4. A method as claimed in claim 2 or 3 in which the home network has links to at least one network providing lower level of quality of service (QoS) than the home network, and in which the available level of QoS is determined from the data identifying the network.

5. A method as claimed in claim 1 in which the home network has links to at least one network providing lower level of QoS than the home network, control messages received by the home network include data identifying the available level of QoS of the network(s) via which traffic has been routed, and step (b) comprises examining said QoS identifying data for each mobile device communicating with the network.

6. A method as claimed in any preceding claim in which a separate gateway support node is provided for traffic routed to the home network server(s) via one of the other networks.

7. A method as claimed in claim 6, in which steps (b) and (c) include discriminating between types of traffic according to the gateway support node via which they are routed.

8. A method as claimed in claim 7, in which the home network has links to at least one network based in another state, and in which one or more separate gateway support nodes is/are provided for traffic routed to the home network server(s) via networks based in other states.

9. A method as claimed in claim 6, 7 or 8 in which each gateway support node has a dedicated IP address pool.

10. A method as claimed in claim 9 in which steps (b) and (c) include the use of an IP address lookup to identify the gateway support node via which traffic has been routed to the home network server(s).

11. A method as claimed in claim 3 or claim 8 in which step (a) comprises selecting the networks of one or more states and step (c) comprises barring the

supply of services to users on the basis of the laws in the states of the selected network(s).

12. A method as claimed in claim 4 or 5 in which step (a) comprises selecting one or more networks having lower level of QoS than the home network and step (c) comprises barring the supply of certain services to mobile devices using the selected network(s).

1/8

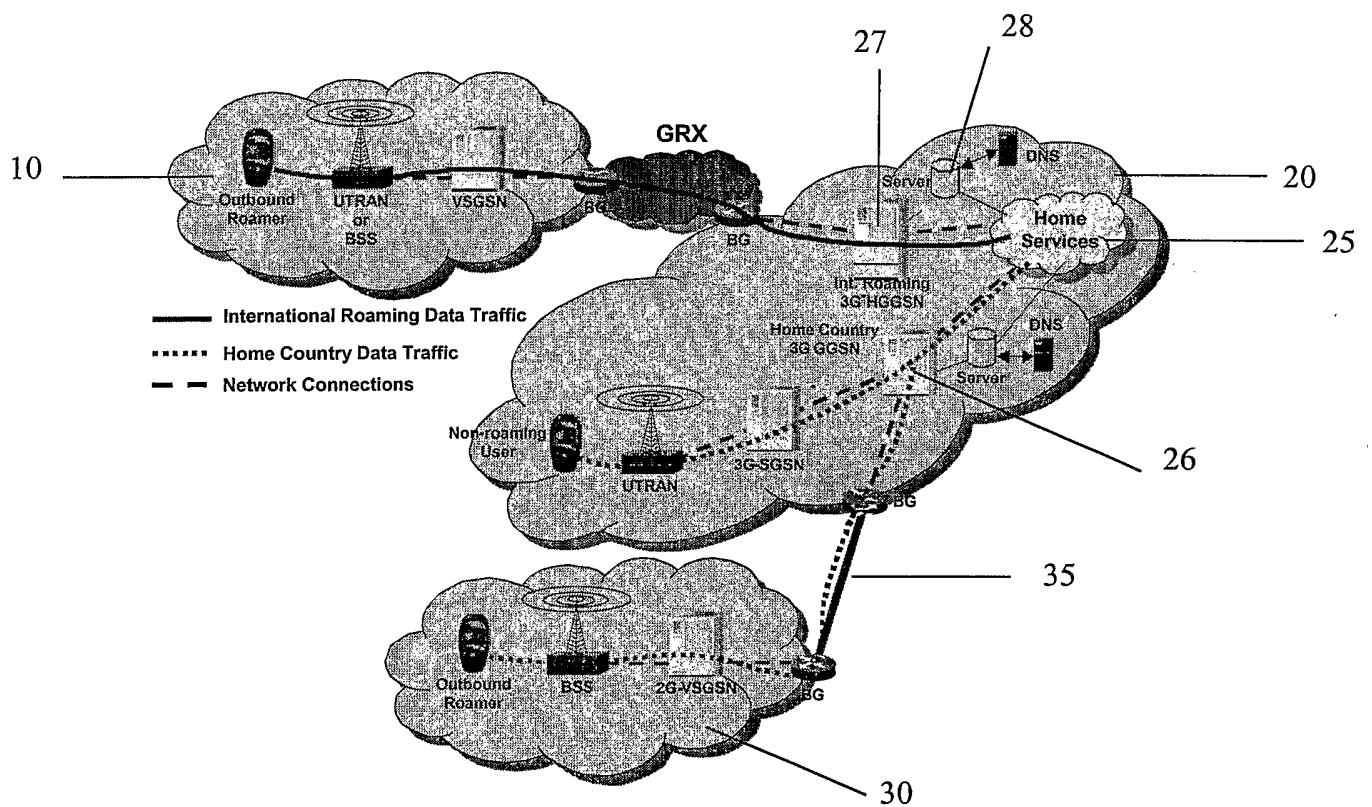


Figure 1. Separating International & Home Country PS Traffic

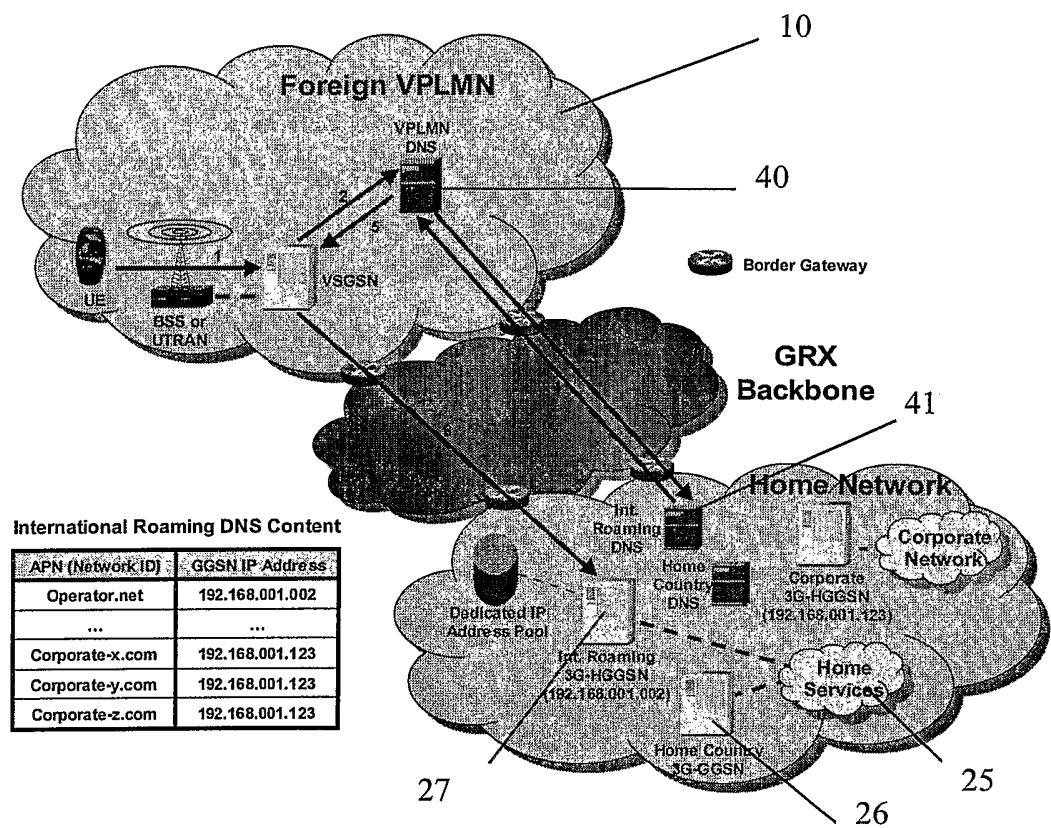


Figure 2. Session Setup towards International Roaming GGSN

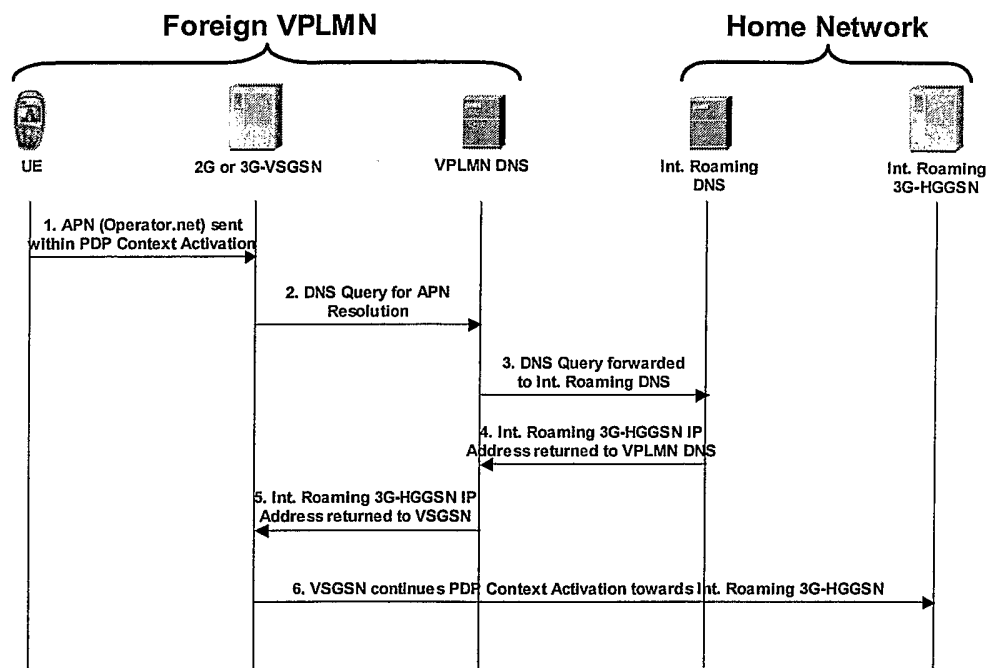


Figure 3. Call Flow for Session Setup towards International Roaming GGSN

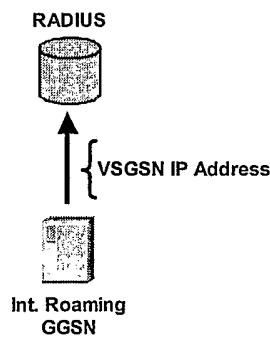


Figure 4. Information Transferred to Server for Solution 1

4/8

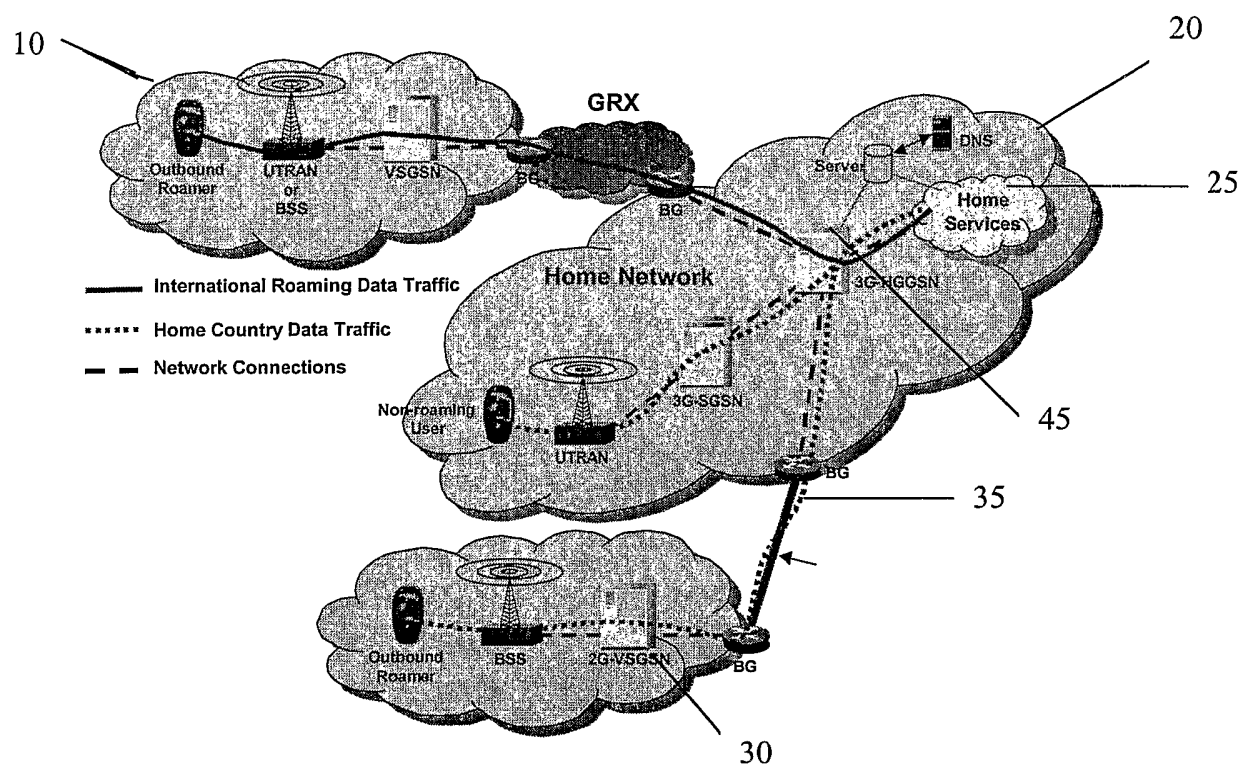


Figure 5. Use of a single GGSN for International & Home Country PS Traffic

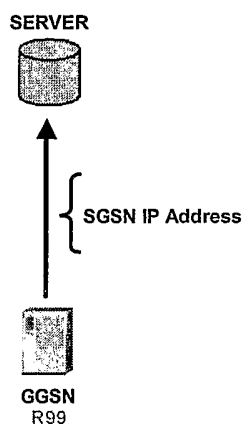


Figure 6. Information Transferred to Server for Solution 2

5/8

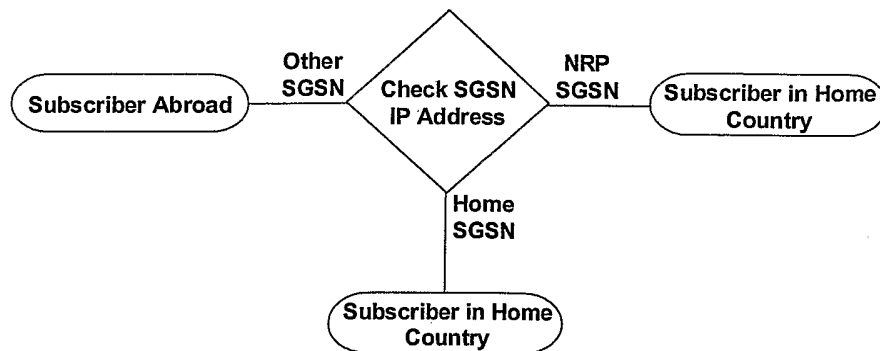


Figure 7. Decision Tree for Solution 2

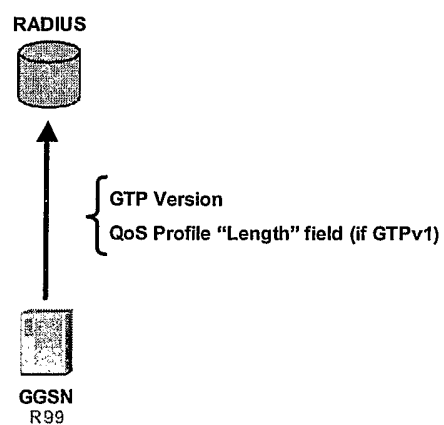


Figure 8. Information Transferred to RADIUS for 3.1 Solution 1

6/8

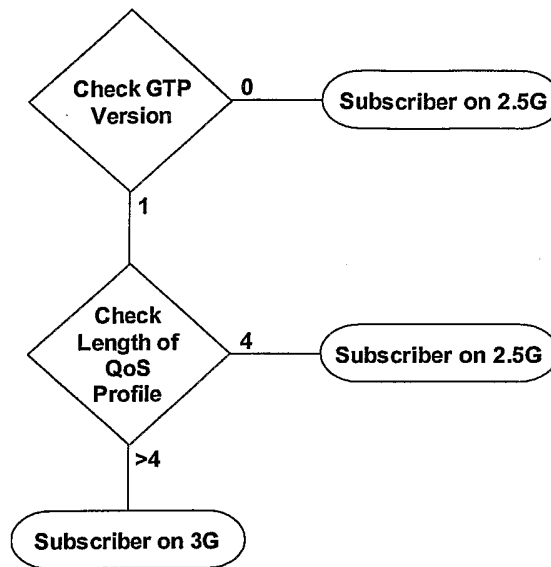


Figure 9. Decision Tree for 3.1 Solution 1

7/8

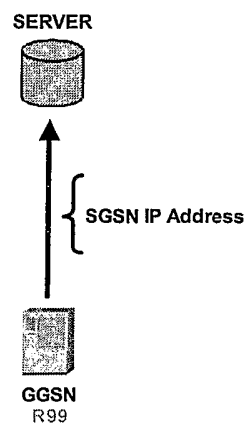


Figure 10. Information Transferred to Server for 3.1 Solution 2
(Home Country Traffic only)

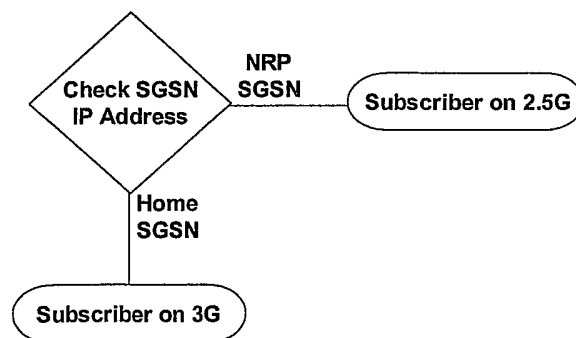


Figure 11. Decision Tree for 3.1 Solution 2
(Home Country Based Traffic only)

8/8

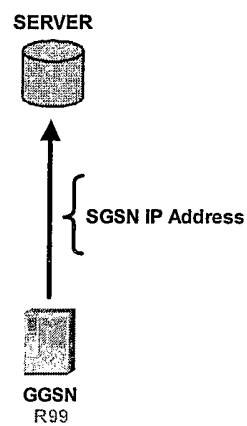


Figure 12 Information Transferred to Radius for 3.1 Solution 3

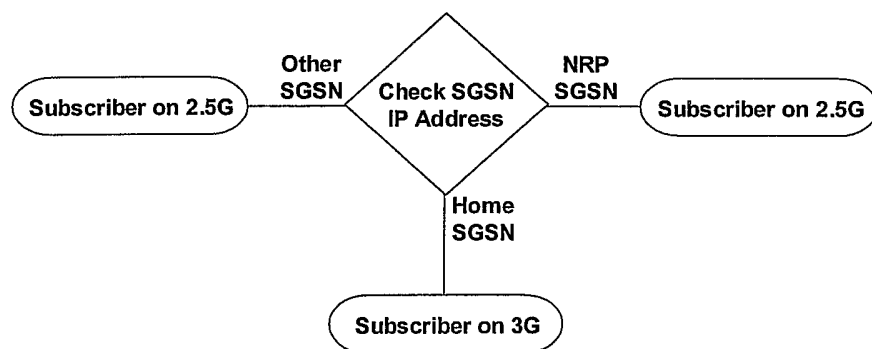


Figure 13. Decision Tree for 3.1 Solution 3

INTERNATIONAL SEARCH REPORT

PCT/GB2004/002020

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

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)
IPC 7 H04Q

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	WO 03/015353 A (HAUMONT SERGE ; HURTTA TUIJA (FI); NOKIA CORP (FI)) 20 February 2003 (2003-02-20) abstract page 4, line 10 - page 8, line 24	1-12
A	WO 02/089442 A (NOKIA CORP) 7 November 2002 (2002-11-07) abstract page 1, line 6 - line 15 page 4, line 11 - line 27 page 8, line 25 - page 9, line 2	1-12

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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.
- *G* document member of the same patent family

Date of the actual completion of the international search

30 August 2004

Date of mailing of the international search report

07/09/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Harrysson, A

INTERNATIONAL SEARCH REPORT

PCT/GB2004/002020

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/164983 A1 (BIRAN ORY ET AL) 7 November 2002 (2002-11-07) abstract paragraph '0012! - paragraph '0014! paragraph '0024! - paragraph '0025! paragraph '0034! - paragraph '0037! paragraph '0072! paragraph '0114! paragraph '0245! paragraph '0254! - paragraph '0257! -----	1-12
A	US 2002/023010 A1 (PICCIONELLI GREG A ET AL) 21 February 2002 (2002-02-21) abstract paragraph '0009! - paragraph '0015! paragraph '0039! -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

PCT/GB2004/002020

Patent document cited in search report			Publication date		Patent family member(s)		Publication date	
WO 03015353	A	20-02-2003	WO	03015353	A1		20-02-2003	
			EP	1421745	A1		26-05-2004	
WO 02089442	A	07-11-2002	WO	02089442	A1		07-11-2002	
			EP	1384363	A1		28-01-2004	
			US	2003023578	A1		30-01-2003	
US 2002164983	A1	07-11-2002	EP	1241902	A2		18-09-2002	
			EP	1347661	A1		24-09-2003	
US 2002023010	A1	21-02-2002	AU	5089101	A		03-10-2001	
			CA	2403737	A1		27-09-2001	
			EP	1266336	A1		18-12-2002	
			JP	2003528398	T		24-09-2003	
			WO	0171622	A1		27-09-2001	