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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 August 2006 (24.08.2006)

PCT

(10) International Publication Number
WO 2006/087429 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04Q 7/22* (2006.01)

(21) International Application Number:
PCT/FI2006/050068

(22) International Filing Date:
16 February 2006 (16.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20055078 18 February 2005 (18.02.2005) FI

(71) Applicant *(for all designated States except US)*: **TELIASONERA AB** [SE/SE]; Sturegatan 1, S-10663 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ALA-LUUKKO, Sami** [FI/FI]; Gyldenintie 7 A 9, FI-00200 Helsinki (FI). **JALKANEN, Tero** [FI/FI]; Simo Klemetinpojan Tie 4 A 17, FI-00790 Helsinki (FI).

(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O. Box 148, FI-00121 Helsinki (FI).

(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, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(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, IS, IT, LT, LU, LV, 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).

Declaration under Rule 4.17:

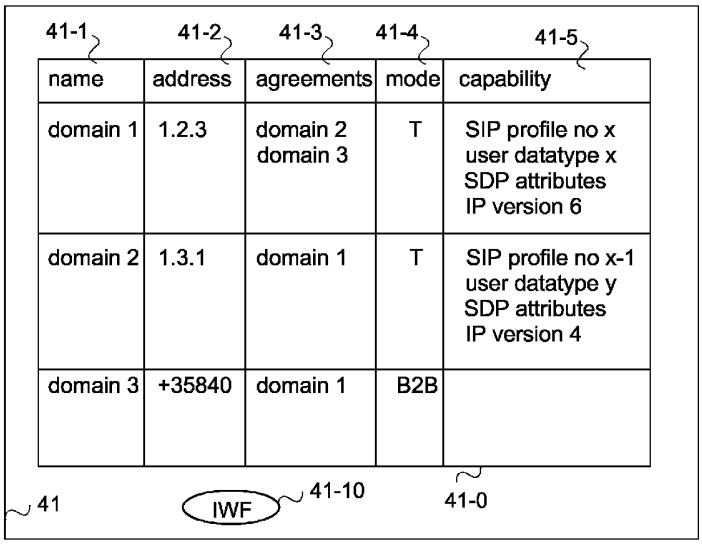
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report*

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.

(54) **Title:** INTERWORKING



(57) **Abstract:** In order to facilitate the maintaining of associations re- quired in inter-domain communications, preferably name (41-1) and address information (41-2) on domains and in- formation on interworking agreements (41-3) between dif- ferent domains is maintained in a reliable network external to said domains. A network node (41) via which inter- domain traffic is routed is arranged to use said maintained information when checking whether or not a sender of a message is the one the sender claims to be and preferably also whether or not an agreement exists between the sender's domain and a receiver's domain. Provided that the sender is the claimed one, the message is forwarded, preferably to an address maintained for the receiver's do- main.

WO 2006/087429 A1

Interworking

Field of the invention

The invention relates to interworking between domains, and particularly to interworking between various IP (Internet protocol) based domains.

Background of the invention

The evolvement of communication technology, particularly IP-based communication technology, and user terminals has enabled versatile communication possibilities. While communication technology and usage of communication possibilities have increased at a high pace, the number of domains and domain operators, such as service provides or conventional network operators, is also increasing at a high pace. A basic requirement for enabling use of various services between users in different domains and for enabling communication between subscribers of different domains is interworking among the domains of different operators.

A problem relating to interworking and IP based communication, especially to charging, is that there should be a mechanism for securing that the sender is the one who he claims to be.

Brief description of the invention

An object of the present invention is to provide a method and an apparatus for implementing the method so as to alleviate the above disadvantage and to facilitate interworking arrangements between domains. The object of the invention is achieved by a method, a system, a network node, a database and a computer program product which are characterized by what is stated in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

The invention is based on detecting the problem and solving it by utilizing a network node via which at least signalling and corresponding control plane traffic with other domains passes through. The network node comprises or has access to a logically centralized database containing information required for the interworking. Such information includes information on domains which have interworking agreements and address information relating to domains, for example. When the network node receives a message, the network node uses the information in the database to check the sender's correctness and the existence of an agreement. If the sender is not a fake and an agree-

ment exists, the network node forwards the message using address information in the database.

In an embodiment of the invention, the network node uses the information in the database to check the sender's correctness and the existence of an agreement. If the sender is not a fake one and an agreement exists, the network node forwards the message using address information in the database. An advantage of the embodiment is that each domain has to set up and maintain only one association, the association to the network node, regardless of the amount of domains with which the domain has interworking agreements. Thus, the embodiment facilitates providing secured communication, a prerequisite for enabling the charging. The interworking with secured communication according to prior art is typically implemented using what is known as IP security (IPsec) tunnelling. As known by a person skilled in the art, each domain has to set up and maintain IPsec security associations with each of the other domains for IPsec tunneling. Typically, the associations are maintained separately for inbound traffic and for outbound traffic. To set up, handle and maintain these associations with tens or hundreds of other domains is quite a heavy task which is avoided by the embodiment.

In another embodiment of the invention the network node is located in a reliable network. The fact that the network node is in a reliable network resolves security problems and enables charging.

Brief description of the drawings

In the following the invention will be described in greater detail by means of preferred embodiments with reference to the accompanying drawings, in which

Figure 1 is a block diagram illustrating an example of a system according to an embodiment of the invention;

Figure 2 is a block diagram of a proxy according to an embodiment of the invention;

Figure 3 is a flow chart illustrating functionality of a proxy according to an embodiment of the invention; and

Figure 4 is a signalling chart showing an example of signalling according to an embodiment of the invention.

Detailed description of some embodiments

The following embodiments are exemplary. Although the specifica-

tion may refer to "an", "one", or "some" embodiment(s) in several locations, this does not necessarily mean that each such reference is to the same embodiment(s), or that the feature only applies to a single embodiment.

The present invention is applicable virtually to any communications system providing interworking between different domains, and particularly applicable to domains supporting IP-based services. A domain is typically a network operated by a single administrative authority and the term domain covers here different networks covering both domains of service providers purchasing the required bearer services and domains of network operators. The communications system may be a fixed communications system and/or a wireless communications system or any combination thereof. An example of such a system is an IP-based system, such as the access independent IMS (IP multimedia subsystem) having a layered architecture in which user traffic is in the user plane and signalling traffic, including session management, utilizes the control plane. Communications systems, especially wireless communications systems, develop rapidly. Such development may require extra changes to the invention. Therefore, all words and expressions should be interpreted broadly, and they are intended to illustrate, not to restrict the invention. As far as the invention is concerned, the relevant point is the function rather than the network node in which the invention resides.

In the following, the present invention is described using a system utilizing the IMS and GRX (GPRS Roaming Exchange), as an example of a system to which the present invention may be applied, without restricting the invention thereto. It should be appreciated that the systems, networks, and the transmission methods used are irrelevant to the actual invention. Therefore, they need not to be discussed in more detail here. The present invention primarily relates to a network node via which network node connection establishments between IP-based domains, or in some embodiments even within an IP-based domain, pass through, the network node comprising a database containing domain-related information to be described in detail below, or having access thereto. The network node is preferably located in a reliable network external to domains. Below, the combination of the external node and the corresponding database is called a proxy regardless of whether or not they are actually located in the same unit.

Figure 1 shows a very simplified system architecture only comprising a communications system 1, three user devices 2, 2', 2'', different IP-based

domains 3, 3', 3", and two reliable networks 4, 4'. Each of the different domains is preferably only connected, directly or via domain(s) and/or reliable network(s) with or without a proxy, to one proxy 41, 41' located in a reliable network. However, according to an embodiment of the invention, the invention may be implemented even when a domain is connected to two or more proxies and/or the proxy is located within the domain. It is apparent to a person skilled in the art that the system also comprises other devices, network nodes, system entities, functions and structures that need not be described in detail herein.

The user devices illustrate different endpoints of a communication, and they can be mobile terminals or fixed terminals, such as personal computers or mobile phones. The type and the functionality of the user devices is irrelevant to the invention and therefore they are not discussed in detail here.

The domains may be of a similar type or a different type. They may be domains of operators who are both service providers and access operators, or domains of service providers who purchase the access service. The latter include different ADSL service providers and other private networks. The domains may use the same protocol or different protocols, or different versions of the same protocol. A domain may be an open domain or a closed domain. In the example of Figure 1, a domain 2 (IMS1) is an IMS-type domain using SIP, a domain 2" (IMS 2) is also an IMS-type domain using the same or another version of SIP and a domain 2" is a private domain using H.323, for example. The IMS-types domains typically comprise a GGSN (Gateway GPRS Support Node) via which control plane and user plane traffic goes to and from the user devices to the IMS part of the domain. The IMS part typically comprises one or more call session control functions CSCF and a border gateway BG preferably connected to the proxy. The user plane traffic to other domains typically goes from GGSN to BG and from there either to the proxy or directly to a BG in another domain, whereas the control plane traffic goes from the GGSN to corresponding CSCF(s), from there to a BG and then to the proxy.

A reliable network 4, 4' containing a proxy 41, 41' may be based on a centralized IP (Internet Protocol) routing network of a GRX, which enables connecting different domains, roaming and a closed system to be implemented. GRX provides a reliable network, i.e. access is controlled with an ability to guarantee a certain service level with predictable delays, thus enabling also IMS users to be provided with many kind of services requiring a specific service level and predictable delays, such as sharing of real-time videos. An-

other advantage of using the GRX as an inter-domain network is the fact that because of commercial charge docketing procedures the network has to be secured and reliable, as the existing GRX is, and therefore the proxy via which the inter-domain traffic is routed may be used for charging purposes, too. Yet another advantage is that an existing network infrastructure may be utilized, thereby avoiding the need to build a new network infrastructure.

The term "reliable network" covers here all kinds of reliable networks able to comprise a proxy according to an embodiment of the invention. It should be appreciated that the technology of a network containing the proxy bears no significance to the invention as long as the required reliability, i.e. at least controllable access, can be provided. Thus, the reliable network may be a private IP-based network or any public communications network. Even the Internet may be used as a reliable network, provided that security issues are taken care of.

Different embodiments of the proxy according to the invention are disclosed in more details below with Figures 2, 3 and 4.

Although not shown in Figure 1, the proxy may be connected to DNS (domain name server) and/or Number portability database and/or ENUM (electronic numbering) database and/or to any corresponding server/database containing address information. The same applies to different servers containing subscriber information. The proxy may also have legacy access to an SS7 (signalling system 7) network via a Signalling Gateway for requesting information from an operator not having an ENUM database. The implementation and functionality of these servers/databases and the way in which the proxy obtains the required information bear no significance to the invention and therefore they are not discussed in detail here.

Figure 2 is a block diagram of a proxy according to an embodiment of the invention. The proxy may be a SIP (session iniation protocol) network access gateway, for example. In the embodiment of Figure 2, the proxy 41 contains an interworking function 41-10 (IWF) according to an embodiment of the invention and a database 41-0. Alternatively, the proxy may have access to a corresponding database. The term database covers here different solutions used to store data, such as storing them in one or more files or using a decentralized database. Examples of different embodiments of the interworking function are disclosed in more detail below with reference to Figures 3 and 4. It is apparent to a person skilled in the art that the proxy also comprises other enti-

ties, functions and structures that need not be described in detail herein. Examples of these include processor(s), memory, input/output bus, different network interfaces, etc.

The database 41-0 contains for each domain the logical name 41-1 of the domain, the address 41-2 which is used when traffic is routed to the domain, the agreements 41-3, i.e. information on domains with which the domain has agreed to interwork, a mode 41-4 to be used with the domain and capability 41-5 information on the domain.

The logical name 41-1 of the domain may be a host part of a logical IP address, i.e. an IP address in the form a@x.y where the host-part comes after the @-sign. A logical name may also be the name of an operator, a dialled number or part of the dialled number, for example in domains not using IP addressing. The address 41-2 is the actual routing address which is used when traffic is routed to (or towards) the domain from this proxy. The address is typically an address of a gateway network node in the domain. It may also be the address of a proxy to which the domain is connected. If the domain uses IP addressing, the address is typically the numerical form of the numerical IP address.

The agreements section 41-3 contains preferably the logical names of the domains having interworking agreements with the domain in question. If the domain in question is connected to this proxy, they are preferably all partner domains. For domains connected to another proxy, it suffices that the agreement section contains those partner domains connected to this proxy. Thus, making an agreement with a new domain requires at its simplest only adding the logical name of the partner domain to the agreement section in the database, and the interworking may begin, provided that other domain-related information has already been stored. Although not shown in Figure 2, the database may also store agreement-specifically certain conditions or rules to be applied only to connections to and from the domain the agreement relates to, for example. One example of the agreement-specific information is information on whether or not the user plane traffic is routed via the proxy.

The mode 41-4 information indicates whether or not the operator wants the proxy to be a transparent proxy (T) or a back-to-back user agent (B2B) proxy amending headers in SIP messages. The back-to-back user agent participates to a connection by receiving and processing messages as a corresponding server, such as a user agent server, and by participating to all call

requests and by determining how the request should be answered and how to initiate outbound calls, i.e. as a corresponding user agent client.

The capability information 41-5 contains information on the properties of the domain and indicates the protocols and preferably the procedures by which network elements in the domain exchange information. Examples of such information in the IMS are the SIP profile number, user data type(s), values of SDP attributes, and the used IP version. On the basis of this information, the proxy knows what kind of messages and information can be sent to the domain and, in response to a message being in another format than the one used by the domain, to amend them to a proper format.

It is obvious that having this king of at least logically centralized database on domains with their interworking agreements, has the advantage that address information and capability information, for example, needs to be stored only once in a system. The updating of the information is also facilitated, since it has to be updated only once.

Figure 3 is a flow chart illustrating the functionality of a proxy according to an embodiment of the invention. In the embodiment of Figure 3 it is assumed, for the sake of clarity, that session invocation is accepted, the user plane traffic also goes through the proxy, and the proxy maintains session information session-specifically. Yet another assumption is that session-related traffic contains in this embodiment an indication on the basis of which the proxy recognizes the session to which the traffic relates, and therefore only a session set-up message is checked. However, it is apparent to a person skilled in the art, that the checking procedure or some of the following steps may be performed to each received message. Yet, for the sake of clarity, a further assumption is that one-to-many communication is transparent to the proxy, i.e. the proxy receives only messages having a single receiver. However, it is apparent to a person skilled in the art, how to implement the embodiment when one-to-many communication is not transparent to the proxy.

The checking procedure of Figure 3 begins when the proxy receives a message in step 300. In response to receiving the message the proxy checks in step 301 whether or not the message is a session termination related message, such as a SIP bye message. If it is not, the proxy checks in step 302 whether or not the message is a session set-up message, such as a SIP invoke message. If it is, the proxy checks in step 303, using the information in the database, the sender's name, such as the IP host-name, in the

message as well as the address wherefrom the message was received. In other words, using the example shown in Figure 2 and assuming that the sender's name in the message is domain 1, it is checked whether or not the message was received from 1.2.3. By performing this checking, the proxy ensures that the sender is the one who he claims to be, i.e. fake invitations are noticed at this stage.

If the message contains the same name-address pair as is in the database (step 304), the proxy then finds out, in step 305, the proper domain on the basis of a receiver's name in the message. The receiver's name is typically in a format of MSISDN (mobile subscriber ISDN number) or NAI (network access identifier), i.e. a logical IP address a@x.y. This step may include an ENUM/MAP inquiry to find out the proper domain, and possibly a proper routing address, if the receiver's name is in the MSISDN format and/or if the name is a ported name. (Ported name means that the subscriber has changed an operator without changing the logical name.) If the receiver's name is in the NAI format and the name is not ported to another domain, the proxy simply uses the host part of the NAI. Thus, the domain operator may leave issues relating to domain/number portability to be solved by the operator providing the proxy. This allows also non-public domains to be altered as public ones thus facilitating the handling of these domains.

The proxy then checks in step 306 by using information on the proxy's database whether or not there is a valid agreement between the sender's domain and the receiver's domain. If an agreement exists, the proxy initializes in step 307 session information for this session and compares in step 308, by using the information stored in the database, the capabilities of the sender's domain with the capabilities of the receiver's domain. If the control plane capabilities differ between the two (step 309), the proxy performs in step 310 the required amendments to the message and adds to the session information in step 310 information on the required control plane amendments or an indication that they are needed. One difference requiring control plane traffic amendment may be that the sender's domain uses IP version 4 whereas the receiver's domain uses IP version 6, and therefore the message has to be amended from IP version 4 message to IP version 6 message. After the amendments, or if no amendments are required (step 309), the proxy checks in step 311 whether or not the mode of the sender's domain in the database is transparent. If the mode is not transparent (step 311), the proxy performs in

step 312 the required amendments to the header and adds in step 312 to the session information an indication or information that B2B mode is to be used. After the amendments, or if no amendments are required (step 311), the proxy checks in step 313 whether or not the user plane capabilities differ between the two, and if they do, the proxy adds to the session information in step 314 information on the required user plane amendments or an indication that they are needed. One example of user plane amendments is change of codecs, such as a VoIP codec to a PoC (push-to-talk-over-cellular) codec. After having updated the session information, or if no amendments are required (step 313), the proxy forwards in step 315 the possible amended message to the address of the receiver's domain in the proxy's database.

The proxy then initializes in step 316 charging information for the session in question.

If there is no valid agreement between the sender's domain and the receiver's domains (step 306), or if the invitation was a fake invitation (step 304), the proxy sends an error in step 317.

If the message does not relate to the termination of a session (step 301) or to the establishment of the session (step 302), it is other session-related traffic and the proxy performs in step 318 required charging-related procedures, if any, and the required amendments, if any, and then forwards the traffic to the address of the receiver's domain in the proxy's database. Since the proxy knows how to amend the traffic, including the actual content of the traffic, the sender's domain or the receiver's domain does not have to perform this, neither maintain the required information.

If the message relates to the termination of the session (step 301), the proxy performs in step 319 required amendments, if any, and then forwards the traffic to the address of the receiver's domain in the proxy's database. The proxy also ends the charging and deletes the session information in step 319.

It is apparent from the above that the above described steps relating to charging enable both bit-based charging and charging based on something else, such as service-specific charging based on SIP/SDP messages. However, the implementation of the actual charging, such as forming charging data records etc. bears no significance to the invention and therefore it is not discussed in detail here.

As can be seen from the above, the proxy enables the connection legs to be different types of connections. For example, a connection leg may be a VoIP (Voice over IP) connection or a connection according to any H.323 or any SIP version regardless of the connection type of the other leg. The proxy performs the required amendments on the basis of the information in the proxy's database.

Figure 4 illustrates signalling according to an embodiment of the invention. In the example shown in Figure 4 it is assumed, for the sake of clarity, that domains MO1, MO2 and MO3 are using similar IMS networks, and reliable networks containing the proxies proxy 1 and proxy 2 are GRX networks. Yet another assumption made here is that in one-to-many communications the proxy performs the multiplication of the invite message.

In the example shown in Figure 4, user A, a client of domain MO1, starts a game session by sending a control plane message 4-1 to invite two friends, users B and C, to join the game session. The message may be a SIP message. The system, for example CSCF, in MO1 notices in point 4-2 that the session establishment is for users B and C who are not home users, i.e. they are clients of other domains. MO1 notices this on the basis of the identifiers, such as the MSISDN or NAI mentioned above in connection with Figure 3, of the receivers, i.e. users B and C,. MO1 may utilize a static list, MAP (mobile application part) inquiry, ENUM inquiry, etc. Since users B and C are not home users, message 4-1 is forwarded (via a border gateway, for example) to the proxy 1 in the reliable network to whose proxy MO1 is connected.

The proxy 1 performs in point 4-3 checking using its database. Depending on the implementation of the proxy 1, the checking may contain one or more of the steps described above in connection with Figure 3. In this example, the proxy 1 notices that MO1 has an agreement with MO2, the operator of the user B, and with MO3, the operator of the user C. Since in this example the domains are similar, no amendments of messages are needed; only the address field is amended in this example. Therefore, the proxy forwards the content of message 4-1 towards the addresses stored in the database of the proxy 1 for MO2 and MO3. Since MO2 is also connected to the proxy 1, message 4-1' containing the content of message 4-1 and user B as a receiver is sent to MO2, i.e. more precisely to the network node whose address is in the database, which then forwards message 4-1' to the user B. MO3 is connected to another proxy, proxy 2, whose address is in the database of the proxy 1 for

MO3, and therefore the proxy 1 sends message 4-1 to the proxy 2 in message 4-1", the message containing the content of message 4-1 and user C as a receiver. However, the proxy 1 is not aware that the address is for another proxy.

The proxy 2 performs in point 4-3a a checking using its database. Depending on the implementation of the proxy 2, the checking may contain one or more of the steps described above in connection with Figure 3. In this example, the proxy 2 notices that MO1 has an agreement with MO3 and that no amendments of messages are needed. The proxy 2 forwards the message 4-1" to MO3 on the basis of the address of MO3 in the database of proxy 2. MO3 then forwards message 4-1" to the user C.

Both the user B and the user C accept the invitation sent by the user A and send corresponding replies. The user B's reply, i.e. message 4-4, is sent via MO2 to the proxy 1 which then performs in point 4-3' the checking procedure using the database. Depending on the implementation, the checking may be the same as the one performed in point 4-3 in response to the reception of message 4-1, or it may contain only some steps of the checking performed in point 4-3. The proxy 1 then forwards the reply, i.e. message 4-4, to MO1 on the basis of the address of MO1 in the database of proxy 1. MO1 forwards the reply to the user A.

The user C's reply, i.e. message 4-5, is sent via MO3 to the proxy 2 which then performs in point 4-3a' the checking procedure using the database. Depending on the implementation, the checking may be the same as the one performed in point 4-3a in response to the reception of message 4-1' or it may contain only some steps of the checking performed in point 4-3a. The proxy 2 then forwards the reply to the proxy 1 on the basis of the address of MO1 given in the database of proxy 2. The proxy 1 then performs, in point 4-3", a similar checking using the database as was performed in point 4-3'. The proxy 1 then forwards message 4-5 to MO1 on the basis of the address of MO1 given in the database of proxy 1. The MO1 forwards the reply to the user A.

In response to the received replies the user A starts to establish a data connection for the game between users A, B and C, which is not, however, described in detail here. The data connection is a user plane connection and its routing within MOs may be different than the routing of a corresponding control plane signalling. It is also possible that, although control plane signalling passes all the time through a proxy or proxies, the user plane data trans-

mission does not pass through a proxy or proxies if the domains are connected to each other.

In another embodiment of the invention, all invitations are sent to the proxy, regardless of whether or not they are targeted to the same network. In other words, the checking in point 4-2 is skipped and even invitations targeted to other users of MO1 are routed to the proxy 1. The advantage of this solution is that the proxy takes care of security issues and domain/number portability issues so that an operator can outsource these tasks to the proxy service provider and the operator's need to build a separate infrastructure for the issues is avoided.

If tunnelling is used, one tunnel may exist between user A and the proxy 1, another from the proxy 1 to user B and still another from the proxy 1 to user C or, alternatively, a tunnel from the proxy 1 to the proxy 2, and yet another tunnel from proxy 2 to the user C. When the proxy is both an endpoint and a starting point of a tunnel, the proxy is able to monitor the traffic and perform the required functions.

The steps, points, messages and related functions described above in Figures 3 and 4 are in no absolute chronological order, and some of the steps, and/or points, and/or operations may be performed simultaneously or in an order differing from the one given here. Other functions can also be executed between the steps/points or within the steps/points. Some of the steps/points or part of the steps/points can also be omitted. Other messages can be transmitted and/or other steps/points can also be carried out between the illustrated ones. The messages are only examples and may also comprise other information. Furthermore, the messages may be different from the above-mentioned operations.

Although the invention is been described above assuming that the external proxy performs the checking, it is apparent to a person skilled in the art, that a domain may comprise a gateway, or a corresponding network node, which performs some or all of the above described checking. An example is an implementation in which the gateway in the domain checks whether or not the agreement exists and the proxy in the reliable network takes care of the other checking steps.

The system and network nodes implementing the functionality of the present invention not only comprise prior art means but also means for checking whether or not an agreement exists and preferably means for checking

whether or not the sender is the one he/she claims to be. More precisely, they comprise means for implementing an embodiment according to the present invention. Present systems and network nodes comprise processors and memory that can be utilized in the functions according to the invention. All modifications and configurations required for implementing the invention may be performed as routines which may be implemented as added or updated software routines, application circuits (ASIC) and/or programmable circuits. Generally, program products include routines, programs, modules, objects, components, segments, schemas, data structures, etc. which perform particular tasks or implement particular abstract data types and which can be stored in any computer-readable data storage medium and which may be downloaded into an apparatus, such as network nodes.

It will be obvious to a person skilled in the art that, as the technology advances, the inventive concept can be implemented in various ways. The invention and its embodiments are not limited to the examples described above but may vary within the scope of the claims.

Claims

1. A network node (41) in a communications system comprising at least a sender's domain and one or more receiver's domains, characterized in that the network node is arranged, in response to receiving a message targeted to a domain, to obtain at least name (41-1) and address (41-2) information on domains and information on interworking agreements (41-3) between domains from a database, to check, by using sender's name and address information in the message and information on the sender's domain obtained from the database, whether or not the sender of the message is the one the sender claims to be, and, by using said information obtained from the database, whether or not an agreement exists between the sender's domain and a receiver's domain, and, in response to the sender being the claimed one and the agreement existing, to forward the message.

2. A network node (41) according to claim 1, wherein the network node is further arranged to, in response to receiving the message, to obtain also information on interworking agreements (41-3) between domains, to check by using said information, whether or not an agreement exists between the sender's domain and a receiver's domain, and in response to the sender being the claimed one and the agreement existing, to forward the message.

3. A network node (41) according to claim 1 or 2, wherein the network node is further arranged to forward the message to an address obtained for the receiver's domain.

4. A network node (41) according to claim 1, 2 or 3, wherein the network node is further arranged to obtain information on the capabilities (41-5) of different domains and, in response to the capabilities of sender's and receiver's domains being different from one another, to perform necessary amendments to the message before forwarding it.

5. A network node (41) according to any one of the preceding claims, wherein the network node is further arranged to obtain mode information (41-4) indicating whether or not the network node should be a transparent network node and to act according said mode information.

6. A network node (41) according to any one of the preceding claims, wherein the network node is arranged to collect charging information on the message.

7. A network node (41) according to any one of the preceding claims, wherein the network contains a database (41-0) for storing said infor-

mation and the network node is arranged to obtain said information from the database.

8. A network node (41) according to any one of the preceding claims, wherein the network node (41) is further arranged to, in response to a ported receiver, to find out at least the receiver's proper domain.

9. A network node (41) according to any one of the preceding claims, wherein the network node (41) is further arranged to be both a tunnel endpoint and a tunnel starting point for inter-domain tunnelling.

10. A network node (41) in a communications system, the network node comprising a database (41-0), characterized in that the database includes at least domain-specifically name-address pairs each containing name (41-1) and address (41-2) information on a domain and information on interworking agreements (41-3) between domains.

11. A network node (41) according to claim 10, wherein the database further comprises information on the capabilities (41-5, 41-4) of different domains.

12. A communications system (1) comprising at least a sender's domain (3) and one or more receiver's domains (3', 3") and one or more reliable networks (4, 4') comprising one or more network nodes (44, 44'), characterized in that

the system (1) further comprises a database (41-0) for maintaining at least name and address information on domains and information on interworking agreements between different domains, the database being external to said domains,

the system (1) is arranged to route at least signalling to and from the sender's domain (3, 3') via a network node (41) in a reliable network (4) external to said domains, and

the network node (41) comprises said database or is arranged to have access to said database, the network node (41) being arranged to check, in response to receiving a message, by using sender's name and address information in the message and information on the sender's domain in the database, whether or not the sender is the one the sender claims to be and, by using said information in the database, whether or not an agreement exists between the sender's domain and a receiver's domain, and, in response to the sender being the claimed one and the agreement existing, to forward the message to an address maintained in the database for the receiver's domain.

13. A communications system according to claim 12, wherein

the database (41-0) further comprises information on the capabilities (41-5, 41-4) of different domains, and

the network node (41) is further arranged to check the capabilities (41-5, 41-4) of the sender's and receiver's domains and in response to the capabilities of the sender's and receiver's domains being different, to perform necessary amendments to the message before forwarding it.

14. A communications system according to claim 12 or 13, wherein a domain (3, 3', 3") is further arranged to route at least all connection-related signalling via the network node regardless of whether or not the sender's domain and the receiver's domain are the same.

15. A communications system according to claim 12, 13 or 14, wherein the system (1) is further arranged to route also user plane traffic via the network node.

16. A communications system according to claim 15, wherein the network node (41) is further arranged to perform said checking also to user plane traffic.

17. A communications system according to any one of claims 12, 13, 14, 15 or 16, wherein the domains (3, 3', 3") are based on IMS and the reliable network (4, 4') is based on GRX.

18. A method for providing inter-domain communications, the method comprising:

maintaining at least name and address information on domains and information on interworking agreements between different domains;

routing at least signalling to and from a sender's domain via a network node in a reliable network external to said domains, and

checking (306), in response to receiving a message, by using sender's name and address information in the message and maintained information on the sender's domain, whether or not a sender of the message is the one the sender claims to be;

checking (309) whether or not an agreement exists between a sender's domain and a receiver's domain; and

forwarding (318), in response to the sender being the claimed one and the agreement existing, the message to an address maintained for the receiver's domain.

19. A method according to claim 18, further comprising finding out (305), in response to a ported receiver, at least the receiver's proper domain.

20. A method according to claim 18 or 19, further comprising:

maintaining information on the capabilities of different domains; and

amending (313, 318, 319), in response to the capabilities of the sender's and receiver's domains being different from one another, the message to be in accordance with the capabilities of the receiver's domain before forwarding the message.

21. A method according to claim 18, 19 or 20, further comprising collecting charging information on the communication in a network node of the reliable network.

22. A computer program product embodied in a computer readable medium and comprising program instructions, wherein execution of said program instructions cause an apparatus containing the computer program product to obtain at least name (41-1) and address (41-2) information on domains and information on interworking agreements (41-3) between domains, to check by using sender's name and address information in the message and obtained information on a senders domain, whether or not a sender of a message is the one the sender claims to be and, by using the obtained information, whether or not an agreement exists between the sender's domain and a receiver's domain, and, in response to the sender being the claimed one and the agreement existing, to instruct the message to be forwarded.

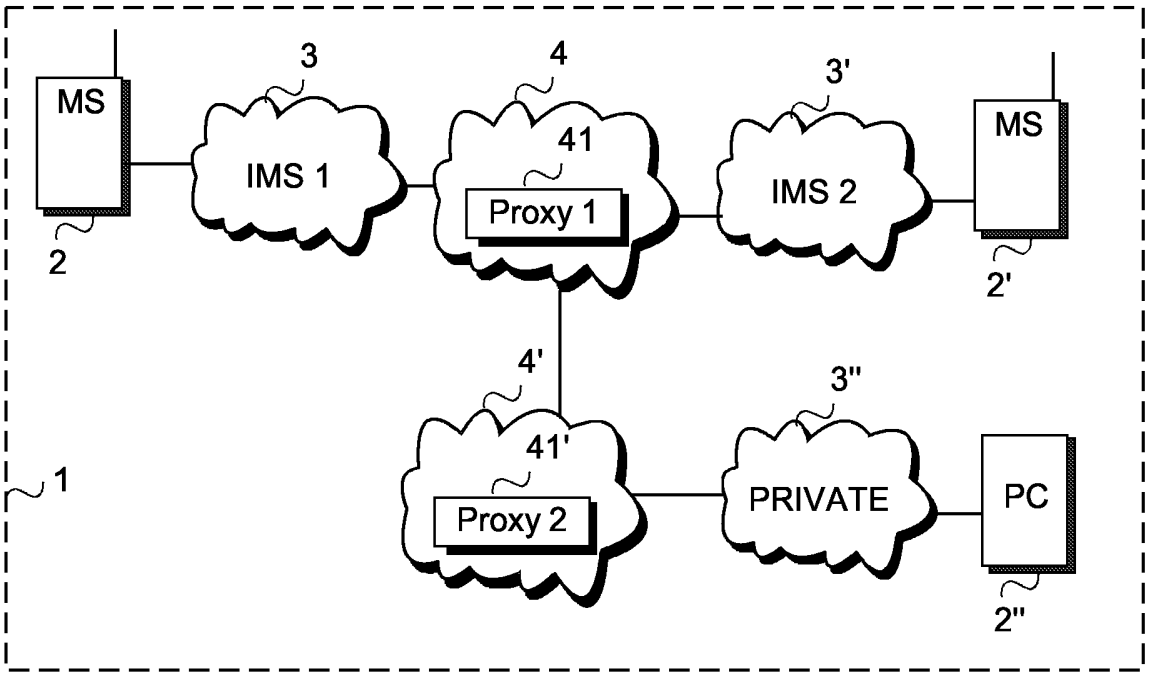


FIG.1

41-1 name	41-2 address	41-3 agreements	41-4 mode	41-5 capability
domain 1	1.2.3	domain 2 domain 3	T	SIP profile no x user datatype x SDP attributes IP version 6
domain 2	1.3.1	domain 1	T	SIP profile no x-1 user datatype y SDP attributes IP version 4
domain 3	+35840	domain 1	B2B	

41 IWF 41-10 41-0

FIG.2

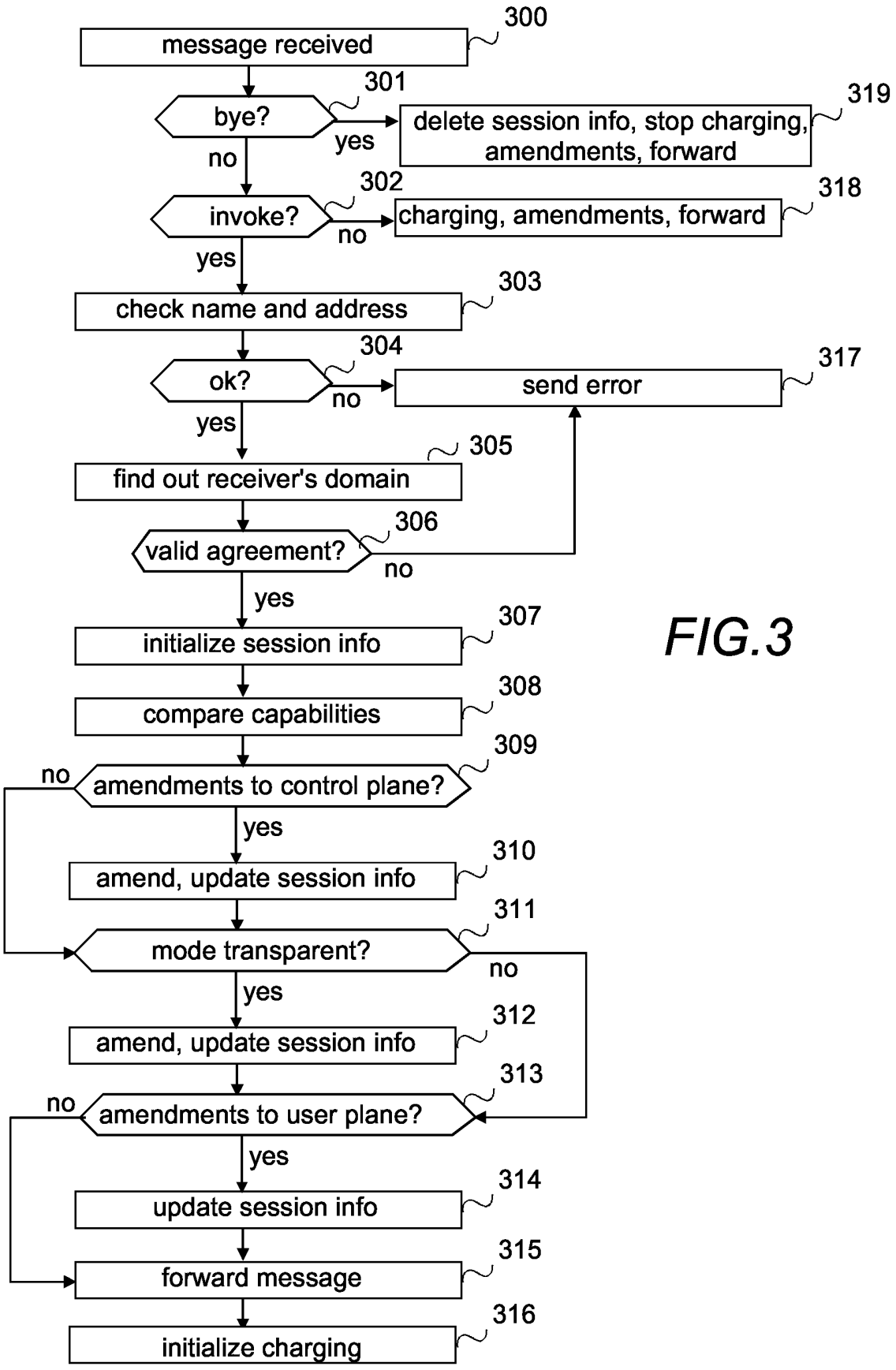

300
message received
301
bye?
yes
319
delete session info, stop charging, amendments, forward
no
302
invoke?
no
318
charging, amendments, forward
yes
303
check name and address
304
ok?
no
317
send error
yes
305
find out receiver's domain
306
valid agreement?
no
yes
307
initialize session info
308
compare capabilities
309
no
amendments to control plane?
yes
310
amend, update session info
311
mode transparent?
no
yes
312
amend, update session info
313
no
amendments to user plane?
yes
314
update session info
315
forward message
316
initialize charging

FIG.3

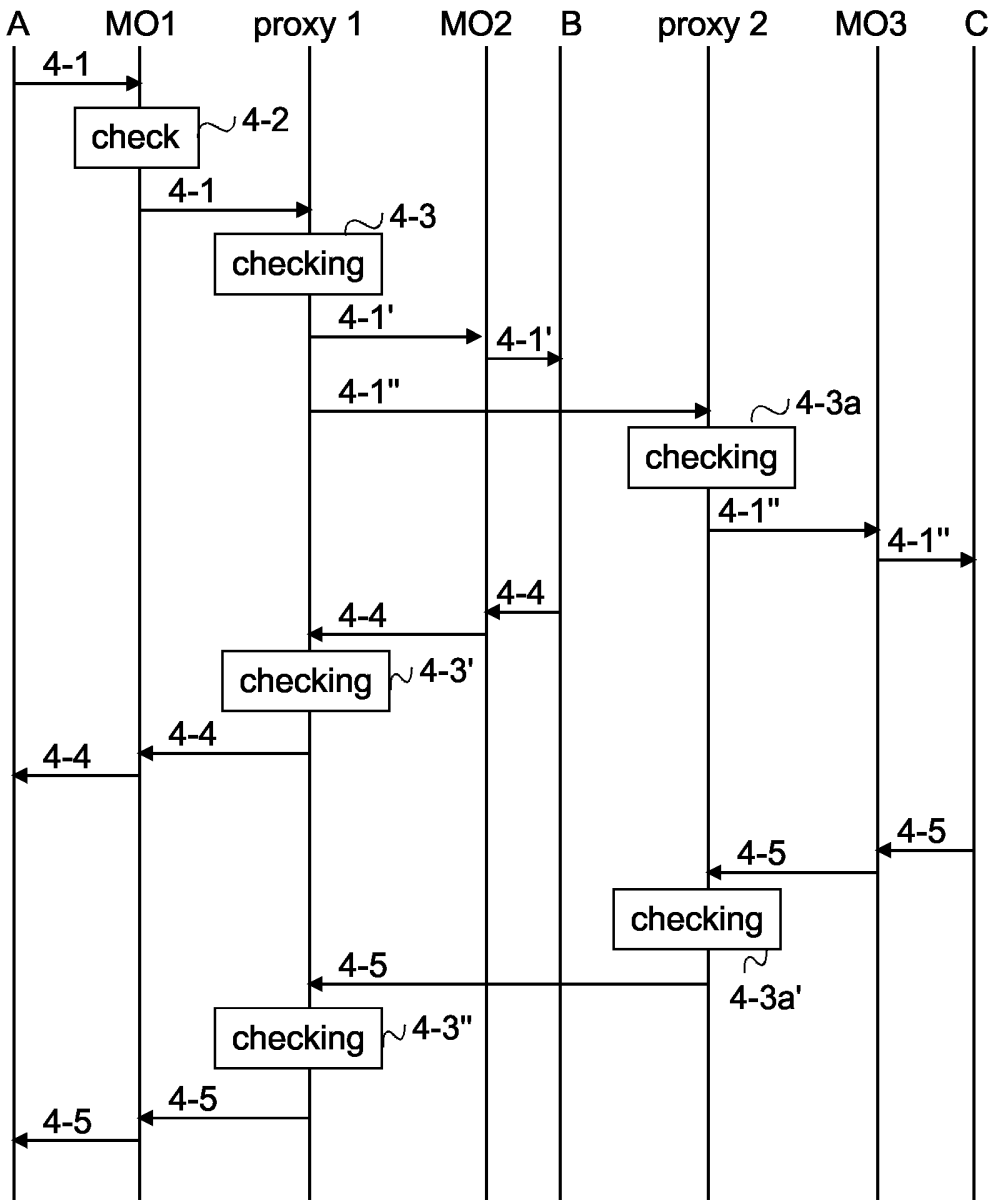

A
MO1
proxy 1
MO2
B
proxy 2
MO3
C
4-1
check
4-2
4-1
4-3
checking
4-1'
4-1'
4-1"
4-3a
checking
4-1"
4-1"
4-4
4-4
checking
4-3'
4-4
4-4
4-5
4-5
checking
4-3a'
4-5
checking
4-3"
4-5
4-5

FIG.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2006/050068

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC8: H04L, H04Q

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

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI, PAJ, XPI3E

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/0027595 A1 (EJZAK) 06 February 2003 (06.02.2003)	1-22
A	EP 1398978 A2 (TELIASONERA FINLAND OYJ) 17 March 2004 (17.03.2004)	1-22
A	WO 03/034772 A1 (SMARTTRUST SYSTEMS OY et al.) 24 April 2003 (24.04.2003)	1-22
A	WO 02/054665 A1 (VIQUITY CORP) 11 July 2002 (11.07.2002)	1-22
A	US 2003/0135740 A1 (TALMOR et al.) 17 July 2003 (17.07.2003)	1-22
A	US 2005/0039017 A1 (DELANY) 17 February 2005 (17.02.2005)	1-22

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

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

"E" earlier 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
05 May 2006 (05.05.2006)	15 May 2006 (15.05.2006)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Vesa-Matti Mäntylä
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050068

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2003/0027595 A1	06/02/2003	None	
EP 1398978 A2	17/03/2004	FI 20021616 A	11/03/2004
WO 03/034772 A1	24/04/2003	US 2005066057 A1 EP 1437024 A1 SE 0103485 A SE 523290 C2	24/03/2005 14/07/2004 20/04/2003 06/04/2004
WO 02/054665 A1	11/07/2002	US 2002087862 A1	04/07/2002
US 2003/0135740 A1	17/07/2003	WO 0223796 A1 AU 8867901 A	21/03/2002 26/03/2002
US 2005/0039017 A1	17/02/2005	US 2005039019 A1 WO 2005026921 A2	17/02/2005 24/03/2005

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2006/050068

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 12/56 (2006.01)
H04Q 7/22 (2006.01)