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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 April 2008 (03.04.2008)

PCT

(10) International Publication Number
WO 2008/039114 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *H04Q 7/38* (2006.01)

(21) International Application Number:
PCT/SE2006/001093

(22) International Filing Date:
26 September 2006 (26.09.2006)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: ZHAO, Wei [SE/SE]; Professorsslingan 31-204, S-104 05 Stockholm (SE).

(74) Agents: SJÖBERG, Mats et al.; Ericsson AB, Patent Unit IP Networks, Box 1505, S-125 25 Älvsjö (SE).

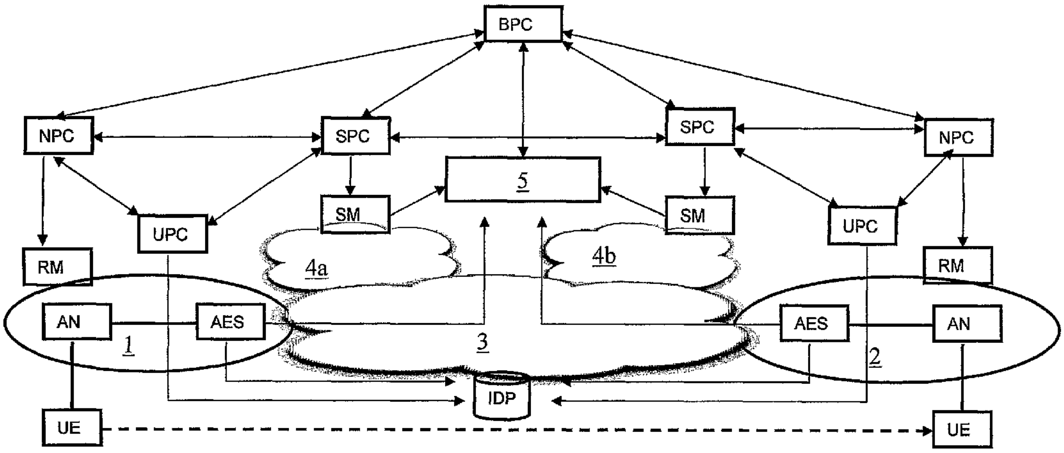
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ,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

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(54) Title: POLICY CONTROL ARCHITECTURE COMPRISING AN INDEPENT IDENTITY PROVIDER



(57) Abstract: A policy control architecture arranged to handle policies in communication networks, the architecture comprising an independent Identity Provider (IDP) arranged to generate IDP-user terminal-entries for policy control information. It further comprises policy controllers logically divided into separate policy control units, including a User policy controller (UPC) arranged to generate UPC-user terminal-entries for service subscriptions and a Business policy controller (BPC) arranged to apply business related policies on said services.

Policy control architecture comprising an independent identity provider

TECHNICAL FIELD

The present invention relates to a policy control architecture enabling policy controller discovery between different types of access networks, in particular to support roaming. The present invention also relates to an independent Identity Provider, a User policy controller and a Business policy controller for said policy control architecture, as well as to methods in a user terminal, in an Identity provider, in a User policy controller, in a Business policy controller, in a Service policy controller and in a Network policy controller within such a policy control architecture.

BACKGROUND

The integration of wireline and wireless technologies in order to create a common telecommunication network foundation may be referred to as Fixed-Mobile Convergence, FMC, enabling wireline service providers and wireless network operators to use the same physical infrastructure, involving several advantages for the end users, as well as to the service providers and operators. An end user may access wireline and wireless services by the same user terminal, such as a mobile phone or a personal computer, and fixed and mobile services may be offered to the end user in one package.

Within the technical field related to FMC, the policy control architecture plays a vital role, e.g. regarding roaming support and QoS (Quality of Service). Currently, one object of various standardization bodies, such as the 3GPP PCC work-item, the Tispan RACS, the WiMax Forum and the DSL Forum is to agree on a policy control architecture specification, providing a common policy control architecture that is applicable regardless of the access network type. However, several technical problems still need to be solved, the mapping and aligning is far from complete, and the different organizations propose different solutions. The TISPAN and the DSL Forum (DSLF) both have a focus on the fixed access-side, which typically is more influenced by the so called "equal-access" concept. Therefore, they propose a distributed policy control architecture, while the 3GPP (3rd Generation Partnership Project), which relates to radio access networks, prefers a more enclosed policy control architecture, since the mobile/cellular network operators conventionally prefer to give services mainly to their own subscribers. For instance, in DSLF, a PDP (policy decision point) is separated into three parts, an SPC (service policy controller), an NPC (network policy controller) and a UPC (user policy controller), while the policy controlling functions normally are closely coupled in the 3GPP, e.g. according to the PCRF (combined Policy and Charging Rules Functions), which allows rule management of service flow response, gating, QoS and flow based charging independently of the subscriber access technology.

However, in order to allow an end user to move freely from one network to another, of which one of the networks may be a fixed (wireline or wireless) network and the other a radio access network, while the end user at least partly retains his subscribed services, a policy controller in one network must be able to discover its peering policy controller in the other network, and any roaming agreement between the two parties must be detected and retrieved. These objects are not achieved by any existing solution today.

Roaming refers to the extension of a service to a different location than the home location where the service was registered, by means of a roaming agreement. Roaming occurs when a subscriber to one network operator uses the facilities of another operator, such as e.g. when a mobile phone has relocated to another region or another country, where its home operator does not have coverage.

A conventional roaming process when a mobile phone has relocated to a new network involves the following: When the mobile phone is turned on in a new network, or transferred via handover to the new network, the new, visited network detects the phone, notices that it is not registered, and attempts to identify the home network of the mobile phone. If there is no roaming agreement between the home network and the visited network, the mobile phone will be denied services by the visited network. Otherwise, the visited network contacts the home network and requests service information regarding the phone, said information including whether or not the mobile phone is allowed to roam. If the request is successful, the visited network will maintain a temporary subscriber record for the phone, and the home network will update its information to indicate that the phone has relocated to the visited network, allowing a correct routing of information.

The 3GPP provides policy controller discovery between different radio access networks, but in fixed access-networks, e.g. in the fixed broadband world, the principle of equal access leads to a different business model and approach than in the 3GPP. For example, the DSL Forum proposes a policy control architecture composed of a number of separate policy controllers, of which each may belong to a different service provider. However, in the 3GPP, those functions are performed by only one network operator.

Further, according to the 3GPP, the user identity is associated with a specific network operator, which is not the case in the fixed broadband. One way to break to coupling between the identity and the network operator is the introduction of an entity called Identity Provider IDP, which may be totally independent of any network operator, functioning as a trusted third party. Therefore, a so-called independent Identity Provider is not associated with any network operator, but instead with any other suitable and independent organization, such as e.g. a bank.

Thus, when a user terminal, e.g. a mobile phone or a personal computer, accesses different types of networks, the discovery of policy controllers and the roaming may present a problem.

SUMMARY

The object of the present invention is to address the problems outlined above, and to provide an improved policy architecture allowing policy controller discovery between different types of access networks, as well as roaming support, with equal access. This object and others are achieved by the policy control architecture, the individual nodes of the policy control architecture, and the methods in the individual nodes of the policy architecture, according to the appended independent claims.

According to one aspect, the invention provides a policy control architecture for handling policies in communication networks, as well as an independent Identity Provider, a User policy controller and a Business policy controller arranged to function as nodes in such a policy control architecture.

The policy control architecture comprises an independent Identity Provider arranged to generate IDP-user terminal-entries for policy control information, and policy controllers logically divided into policy control units. The policy control units include a User Policy Controller arranged to generate UPC-user terminal-entries for service subscriptions.

The policy control information in the IDP-user terminal entry of the Identity Provider may comprise the address of the User Policy Controller in the home network of the user terminal, and the logically divided policy control units may further include a Business Policy Controller arranged to apply business related policies on service subscriptions. The business related policies of the Business Policy Controller may comprise roaming agreements.

The logically divided policy control units may further include a Service Policy Controller arranged to apply service related policies subscribed services, and a Network Policy Controller arranged to map service policies on network dependent policies, which may be arranged to create network related policies based on network status.

According to another aspect, a method is provided in a user terminal of launching a service in a first home network handled by said policy control architecture. The user terminal performs at least the following steps:

- Receiving an identity from an independent Identity provider before connecting to a first home network;
- Connecting to a first home network and receiving an IP address;
- Subscribing to an available service in the home network;
- Launching the subscribed service in the home network at least once.

When the user terminal launches said service in a second network, the user terminal may perform at least the additional steps of:

- Relocating to a second visited network;
- Performing roaming in the visited network by providing its identity;
- Receiving a list of available services through the Business policy controller;
- Launching said subscribes service, if it is available in the visited network.

An independent Identity Provider within a policy control architecture performs at least the following steps:

- Issuing an identity to a user terminal and generating a corresponding IDP-user terminal entry;
- Performing AAA on the user terminal when it connects to a first home network;
- Storing the address of the User policy controller of the first home network in said IDP-user terminal entry;
- Providing the address of the home-UPC to the Network policy controller when the user terminal launches a subscribed service;
- Performing AAA on the user terminal when it relocates to a second network;
- Providing the address of the home-UPC to the User policy controller of the second network.

A User policy controller within a policy control architecture performs at least the following steps when a user terminal connects to a first home network:

- Generating a UPC-user terminal entry and storing the ID of a subscribed service;
- Accessing the independent Identity Provider and registering its UPC address in the corresponding IDP user terminal entry;
- Storing the address of the Service policy controller associated with the subscribed service in the UPC-user terminal entry;
- Storing the address of the Network policy controller of the home network in the UPC-user terminal entry;

A User policy controller may perform at least the following steps when said user terminal relocates to a second visited network:

- A User policy controller of the second, visited network acquiring the address of the User policy controller of the first, home network via the IDP-user terminal entry;

- The User policy controller of the home network sending the IDs of the user terminals subscribed services to the User policy controller in the visited network;
- The User policy controller of the home network sending the address of the Service policy controller associated with each subscribed service to the corresponding Service policy controller of the visited network;

A Business policy controller within said policy control architecture applies business related policies on the subscribed services of a roaming user terminal, and said business related policies may include roaming agreements.

A Service Policy Controller within said policy control applies service related policies on a subscribed service.

A Network Policy Controller within said policy control architecture maps service policies on network dependent policies, and may create network related policies based on network status.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail and with reference to the accompanying drawings, in which:

- Figure 1 is a block diagram schematically illustrating a first embodiment of a policy control architecture according to this invention;
- Figure 2 is a flow chart illustrating the performed steps when a user terminal relocates to a second, visited network;
- Figure 3 is a flow chart illustrating an exemplary embodiment of a method in a user terminal in a policy control architecture according the invention;
- Figure 4 is a flow chart illustrating an exemplary embodiment of a method in an independent Identity Provider within a policy control architecture according the invention, and

- Figure 5 is a flow chart illustrating an exemplary embodiment of a method in a User Policy Controller within a policy control architecture according to the invention.

DETAILED DESCRIPTION

In the following description, specific details are set forth, such as a particular architecture and sequences of steps in order to provide a thorough understanding of the present invention. However, it is apparent to a person skilled in the art that the present invention may be practised in other embodiments that may depart from these specific details.

Moreover, it is apparent that the described functions may be implemented using software functioning in conjunction with a programmed microprocessor or a general purpose computer, and/or using an application specific integrated circuit. Where the invention is described in the form of a method, the invention may also be embodied in a computer program product, as well as in a system comprising a computer processor and a memory, wherein the memory is encoded with one or more programs that may perform the described functions.

This invention provides a policy control architecture, comprising a policy controlling function divided into separate policy controlling functional units, e.g. four units, which may be denoted User Policy Controller, Network Policy Controller, Service Policy Controller and Business Policy Controller. Further, the architecture comprises an independent Identity Provider, which is not associated with any network operator, having an added functionality enabling it to function as the anchor and entry point for the policy controller discovery. When a user terminal has been given an identity in a home network, an entry will be created in the independent Identity Provider for this user terminal, and the user terminal is uniquely identified by this identity. When the user terminal first launches a service in its home network, it will first locate its policy controllers, comprising said e.g. four functional units, i.e. the User Policy Controller, Network Policy Controller, Service Policy Controller and Business Policy Controller. After all the policy controllers are found, information will also be pushed to the Identity Provider's entry associated to the specific user terminal. When the user terminal moves to a new location within another network, it will provide its identity to the visited network, which will use the identity to retrieve the Identity Provider. The Identity Provider will provide information regarding the policy controllers to the visited network, enabling the visited network to fetch service subscriptions and to determine whether any business agreement exists between the visited network and the home network, eventually allowing the roaming user terminal to launch said service.

According to the invention, the User Policy Controller UPC and the Business Policy Controller BPC are provided with new functionalities regarding roaming support. When a user terminal subscribes to a service, the subscription information will be added as a user terminal entry in a UPC User information table in the home UPC, together with the identity associated with this service. When the user terminal moves to another network, the Access Edge Site (AES) in the visited network will be able to retrieve the location of the independent Identity Provider IDP, and the Identity Provider will provide the address of the home UPC of the user terminal from the corresponding entry of its IDP User Information table. Thereafter, all related service subscriptions of the user terminal can be fetched from the home UPC, based on the user terminal identity. This information will be sent to the dedicated BPC serving the visited network, which will apply the roaming agreement policies. Thereby, the visited network will learn which services that is available to the user terminal.

A first embodiment of a policy controller architecture according to this invention is illustrated in the block diagram of figure

1, provided with separate functional entities related to policy decision making and enforcement, such as e.g. roaming, and all roaming agreement-related policies are controlled by a functional unit denoted Business policy controller BPC.

The figure illustrates a user terminal UE relocating from a first access network 1 to a second access network 2, as well as the policy control architecture enabling roaming of the user terminal in the second access network. The relocation of the user terminal is indicated by the hatched arrow between the two UE-blocks. The figure further illustrates the IP network 3, two service networks 4a, 4b and a Service publish manager 5.

IDP refers to an independent Identity Provider, which is associated with a trusted third party organization and not with any network operator, issuing identities to user terminals and thereby decoupling the user identity from the network operator, enabling an equal access. According to this invention, the independent Identity Provider IDP is provided with an added functionality to act as policy controller discovery anchor point and Identity verification authority.

As illustrated in figure 1, the policy controlling function according to this embodiment of the invention is logically divided into four functional units, a Business Policy Controller, a User policy controller, a Network policy controller and a Service policy controller. The Business policy controller and the User policy controller are provided with added functionalities to enable discovery and localization between different types of networks, and to allow roaming.

The BPC in the figure refers to a dedicated Business policy controller, which is responsible for generating business-related policies, such as roaming agreements between networks and SLA:s (Service Level Agreements), which is an agreement between a service provider and a service recipient, and to push them down to the correct policy enforcement point, PEP, e.g. an

Access Edge Site, AES.

UPC in the figure refers to the User policy controller, which controls all end-user related policies, among them the user identification, AAA (Authentication, Authorisation, Accounting), billing records, and all subscribed services of the user terminals, and is normally associated with the network operator.

SPC in the figure refers to a Service policy controller, which creates and pushes service related policies to correct policy enforcement point, PEP. Service policies describe the overall business logic that is applied to requests from application servers and peer service policy controllers. The Service policy controller may be a part of the home network, but it can also be a part of a network of an independent service provider.

NPC in the figure refers to a Network policy controller, which has two functions. Firstly, it receives service policies from service policy controllers and maps them onto network dependent policies. Secondly, it creates network related policies based on the existing network status.

RM in the figure refers to a Resource Manager, which manages the resources in the network.

SM in the figure refers to a Service Manager, which is responsible to manage and publish services at the service provider's network.

AES in the figure refers to an Access Edge Site, which acts as policy enforcement point, i.e. "enforces" the policies.

AN in the figure refers to the Access Node of a access network.

UE in the figure refers to a user terminal, which may be e.g. a mobile/cellular phone or a personal computer.

Hereinafter is described how policy controller discovery is performed and how roaming agreements are found and applied according to this invention, covering the steps from before a user terminal connects to a home network until it receives roaming services according to the pre-defined way in a visited network. Some of the individual steps corresponds to the ones in prior art, but the sequences of steps are new, since the Identity Provider IDP, the Business policy controller BPC and the User policy controllers UPCs that are involved in the steps have added functionalities according to this invention.

Before connecting to a network, the user terminal UE must receive an identity from an independent Identity Provider IDP, e.g. in the form of an IMSI (International Mobile Subscriber Identity)-card, or as a user/password pair, which is capable of uniquely identifying this user terminal UE. After subscribing to a service, the user terminal UE has to launch it at least once in the home network before roaming to a visited network.

*** Before a user terminal UE connects to a home network:**

a. The AES (Access Edge Site) gives network information, such as network operator name, to a service publish manager 5. This information can e.g. be added to the name of the AES, such as AES.telia.se.

b. Based on this information, the service publish manager 5 contacts a Business policy controller BPC, which is pre-defined for this service publish manager, and fetches policies regarding the service providers/services having agreement with the network operator.

c. The service publish manager searches its own service directory and sends all available services to the AES.

d. The AES generates a web portal listing all available services.

e. The user terminal UE receives an identity from an independent Identity Provider IDP.

**** The user terminal UE connects to a home network:**

a. The user terminal UE sends DHCP-requests which are received by the AES, and the AES sends back a default IP address to the user terminal UE.

b. The user terminal UE is re-directed to the web portal where all available services are listed.

***** The user terminal UE subscribes to a service:**

a. The user terminal UE provides its ID (identity) to the AES.

b. The ID is authorized and authenticated by the IDP by means of an AAA.

c. After the AAA, the AES will send the following information to the User policy controller UPC in the home network: UE ID, Subscribed service ID, Address or name of the IDP.

d. Based on the above information, the UPC will generate a UPC User information table with the UE entry for the identity of the user terminal. Under the UE entry, the identities of the subscribed services is registered, together with the addresses of the Service policy controller SPC associated with each subscribed service, as well as the address of the Network policy controller NPC of the home network. Before the user terminal UE launches a service for the first time, the UPC User information table (Table 1) may have the following content:

UE	NPC	Service	SPC
ID	Empty	ServiceID1	empty
		ServiceID2	empty
		...	...
		ServiceIDn	empty

d. The User policy controller UPC then accesses the UE entry in the IDP User information table on the independent Identity Provider IDP, and registers itself in the same entry, creating an UE-ID - UPC pair. In the independent Identity Provider IDP, said IDP User information table is kept for all users/devices that receive Ids from this independent Identity Provider IDP, together with their home UPC address, and an example of the content in this table is indicated below, denoted Table 2:

UE	UPC
ID1	Address
ID2	Address
...	...
IDn	Address

e. The user terminal UE receives a real IP address.

****** The user terminal UE launches a service:**

a. The user terminal UE and an application server (not shown in figure 1) find the same Service policy controller SPC by using a pre-defined algorithm, e.g. by a suitable signalling negotiation, which is well-known to the skilled person.

b. The Service policy controller SPC uses the UE's ID to access the IDP, and to fetch the corresponding UPC address from the IDP User information table.

c. The Service policy controller SPC registers its SPC address in the UPC User information table under the specific UE entry and Service ID.

d. The AES provides the UE ID to its Network policy controller NPC, which may be pre-defined for the AES or found via DNS-query.

d. The Network policy controller NPC fetches the UPC address from the IDP User information table.

e. The Network policy controller NPC registers its NPC address in the UPC User information table.

After these steps, the conventional service negotiation and signalling will continue, based on service type. After the user terminal UE has launched several services, the UE entry in the UPC User information table in the User policy controller UPC may correspond to the following Table 3:

UE	NPC	Service	SPC
ID	Address	ServiceID1	Address-1
		ServiceID2	Address-2
		...	...
		ServiceIDn	Address-n

When the signalling process is completed, the user terminal UE can start using the service.

******* The user terminal UE relocates to a second (visited) network:**

a. The user terminal UE connects to the visited network, and provides its ID.

b. The visited AES retrieves the address of the independent Identity Provider IDP based on the UE ID information, e.g. by means of a DNS-query.

c. The independent Identity Provider IDP performs AAA over the user terminals ID. Therafter, the user terminal home UPC address is fetched from the UE entry of the IDP User information table and sent back to the visited AES, enabling the User policy controller UPC of the visited network to acquire the address of the home User policy controller UPC.

d. The home UPC returns the service IDs of the subscribed services of the user terminal UE to the User policy controller UPC and the AES in the second, visited network, the service ID of a subscribed service comprising information regarding the service provider.

e. The visited AES communicates with the dedicated Business policy controller BPC via the service publish manager 5.

f. The Business policy controller BPC checks for each service provider if there is a business agreement between the service provider and the visited network. If a business agreement exists, the service can be used by the roaming user terminal UE, otherwise the user terminal UE will be denied the service.

g. The visited AES returns a list of available services to the roaming user terminal UE.

******** The user terminal UE launches a service from the visited network:**

The steps a, b, c are the same as in the previous sequence of steps, by which the visited network finds the home UPC. The only difference is that the visited AES returns not only the UE ID, but also the service ID relating to service that the roaming user terminal UE wants to launch.

d. The home UPC locates the user terminals entry from its UPC User information table, and finds the address of the Service policy controller SPC associated with the specific service that the roaming user terminal UE wants to launch.

e. Thereby, the visited SPC and AES discover the address of the SPC associated with the service of the roaming user terminal UE. The visited AES can fetch policies regarding this service, or the visited Service policy controller SPC can contact the Service policy controller SPC associated with the service for policies.

After these steps, the service proceeds in the conventional way.

In order to further explain and clarify the present invention, the steps performed when a user terminal relocates to a new network is illustrated in the flow chart in figure 2.

In step 21, the UE connects to the new, second network, and provides its ID. In step 22, the AES in the visited network retrieves the IDP based on the UE identity, via e.g. DNS-query.

In step 23, the IDP performs AAA over the UE's ID, and the address of the UPC in the home network is fetched from the IDP's UE entry in the IDP User information table in step 24, and sent back to the visited AES. Thereby, the UPC of the visited network acquires the address of the home UPC.

The home UPC sends, in step 25, the ID of the UE's subscribed service back to the UPC and AES in the visited network, the service ID comprising information regarding the service provider.

In step 26, the visited AES communicates with the BPC via the service publish manager 5, and the BPC determines, in step 27, for each service provider if there is a business agreement between the service provider and the visited network. If business agreement exists, the service may be used by the roaming UE, otherwise the UE will be denied the service, in step 28. The visited AES returns a list of available services to the roaming UE in step 29.

Figure 3 is a flow chart illustrating an exemplary embodiment of a method of a user terminal in a policy control architecture according to this invention, the flow chart comprising at least some of the steps performed by a user terminal from before connecting to a first network, until it launches a subscribed service in a second network.

In step 31, a user terminal registers with an independent Identity provider, IDP, and receives an identity, such as e.g. an IMSI-card or a password. Thereafter, in step 32, the user terminal connects to a first network 1, i.e. the home network, and provides its identity in order to subscribe to an available service, in step 33. The User terminal launches the subscribed service in step 34, and thereafter relocates to a second network 2, i.e. the visited network, providing its ID. In step 36 the user terminal receives a list of available services in the visited network from the AES of the visited network. The AES has obtained this information from a dedicated Business policy controller, via the service publish manager 5. If it is determined in step 37 that the subscribed service of the user terminal is available in the visited network, the user terminal launches the service, in step 39, otherwise the User terminal is denied to launch the service, in step 38.

Figure 4 is a flow chart illustrating an exemplary embodiment of the method of an independent Identity Provider within a policy control architecture according to this invention. The flow chart comprises at least some of the steps performed by an independent Identity provider IDP from before a UE connects to a first network, until the UE relocates a second (visited) network.

In step 41, the independent Identity provider issues an identity to a user terminal UE, and when this user terminal connects to a first network 1, i.e. the home network, the IDP performs AAA on the user terminal, in step 42. In step 43, the IDP stores the address of the UPC of the UE's home network in its IDP user information table. This step is performed by said home UPC accessing the UE entry in the IDP User information table and registering itself. When the user terminal launches a subscribed service in the home network, the IDP provides the address of the home UPC to the home Network policy controller NPC, in step 44, which is performed by the NPC fetching the home UPC address form the IDP.

When the user terminal relocates to a second network 2, i.e. a visited network, the IDP performs AAA on the user terminal, in step 45, and further provides the address of the home UPC to the visited UPC via the visited AES, in step 46.

Figure 5 is a flow chart illustrating an exemplary embodiment of a method of a User policy controller UPC within a policy control architecture according to this invention. The flow chart comprises at least some of the steps performed by a User policy controller UPC from when a UE is connected to a first network 1, until the UE may launch a subscribed service in a second (visited) network.

In step 51, the User policy controller generates a UPC User information table with an entry for the UE identity. Under the UE entry, the identities of the subscribed services can be registered, together with the addresses of the Service policy controller SPC associated with each subscribed service, as well as the address of the Network policy controller NPC of the home network. Since the UPC receives the UE identity, the subscribed service ID and the address or name of the IDP when the UE subscribes to a service, the ID of the subscribed service is added under the UE entry in the UPC User information table (Table 1).

In step 52, the UPC accesses the IDP User information table (Table 2) and registers its address under the UE entry, creating a UE-ID - UPC pair. In step 53, the UPC stores the address of the Service policy controller SPC associated with the subscribed service of the UE in its UPC User information table, and in step 54 the UPC stores the address of the Network policy controller NPC of the home network, thereby completing the UE entry in the UPC User information table.

When the user terminal relocates to a second (visited) network 2, the UPC in the visited network receives the address of the home UPC via the visited AES and the IDP user information table, in step 55. Thereby, the home UPC is able to retrieve user terminal-information from its UPC User information table and send the subscribed service-IDs for the roaming user terminal to the visited UPC, in step 56, the subscribed service ID comprising information relating to the service provider.

Further, the home UPC retrieves the address of the Service policy controller SPC associated with the subscribed services of the user terminal from its UPC User information table, and sends it to the corresponding Service policy controller SPC of the visited network, in step 57, eventually enabling the user terminal to launch a subscribed service in the visited network.

Thus, the present invention uses an independent Identity Provider, a Business policy controller and a User policy controller provided with added functionalities for enabling policy controllers in different types of networks to locate each other, and to support roaming of a user terminal moving between different types of networks, such as relocating e.g. from a fixed access networks to a radio access networks.

Thereby, the invention provides an improved policy control localization and roaming support when a user terminal relocates to an access network of a different type. By giving an independent Identity Provider the new functionalities according to this invention, the significance of the independent Identity Provider as an independent trust third party is strengthened. This is the one of the key steps towards a more loosely coupled network architecture that is capable of providing services to users based on the principal of equal access.

While the invention has been described with reference to specific exemplary embodiments, the description is in general only intended to illustrate the inventive concept and should not be taken as limiting the scope of the invention.

CLAIMS

1. A policy control architecture arranged to handle policies in communication networks (1, 2), **characterized in** that the policy control architecture comprises an independent Identity Provider (IDP) arranged to generate IDP-user terminal-entries for policy control information, the architecture further comprising policy controllers logically divided into policy control units, said policy control units including a User Policy Controller (UPC) arranged to generate UPC-user terminal-entries for service subscriptions.

2. A policy control architecture according to claim 1, wherein the policy control information in an IDP-user terminal entry of the Identity Provider (IDP) comprises the address of the User Policy Controller (UPC) in the home network (1) of the user terminal (UE).

3. A policy control architecture according to claim 1 or 2, wherein said logically divided policy control units further includes a Business Policy Controller (BPC) arranged to apply business related policies on service subscriptions.

4. A policy control architecture according to claim 3, wherein said business related policies of the Business Policy Controller comprises roaming agreements.

5. A policy control architecture according to any of the preceding clams, wherein said logically divided policy control units further include a Service Policy Controller (SPC) arranged to apply service related policies subscribed services.

6. A policy control architecture according to any of the preceding claims, wherein said logically divided policy control units further include a Network Policy Controller

(NPC) arranged to map service policies on network dependent policies.

7. A policy control architecture according to claim 6, wherein the Network Policy Controller is further arranged to create network related policies based on network status.

8. An independent Policy Controller (IDP) for a policy control architecture according to any of the preceding claim, **characterized in that** the independent Policy Controller is arranged to generate IDP-user terminal-entries for policy control information, said IDP-user terminal entries comprising the address of the User Policy Controller (UPC) in the home network (1) of a user terminal (UE).

9. A User policy controller (UPC) for a policy control architecture according to any of the claims 1-7, **characterised in that** the User policy controller is arranged to generate UPC-user terminal-entries comprising the ID of subscribed services of a user terminal (UE).

10. A User policy controller (UPC) according to claim 9, wherein the User policy controller is further arranged to store the address of the Service policy controller (SPC) associated with each subscribed service, and the address of the Network policy controller (NPC) of the home network, in said UPC-user terminal entry.

11. A Business policy controller (BPC) for a policy control architecture according to any of the claims 2-7, **characterised in that** the Business policy controller is arranged to apply business related policies on the subscribed services of a roaming user terminal.

12. A Business policy controller according to claim 11, wherein said business related policies include roaming agreements.

13. A method in a user terminal (UE) of launching a service in a first home network (1) handled by a policy control architecture according to any of the claims 1-7, **characterised by** the user terminal performing at least the following steps:

- Receiving (31) an identity from an independent Identity provider (IDP) before connecting to a first home network;
- Connecting (32) to a first home network and receiving an IP address;
- Subscribing (33) to an available service in the home network;
- Launching (34) the subscribed service in the home network at least once.

14. A method in a user terminal (UE), according to claim 13, of launching said service in a second network (2), **characterised by** the user terminal performing at least the additional steps of:

- Relocating (35) to a second visited network;
- Performing roaming (35) in the visited network by providing its identity;
- Receiving (36) a list of available services through a dedicated Business policy controller (BPC);
- Launching said subscribes service, if it is available in the visited network (37, 38, 39).

15. A method in an independent Identity Provider (IDP) within a policy control architecture according to any of the claims 1-7, **characterised by** the independent Identity Provider performing at least the following steps:

- Issuing (41) an identity to a user terminal (UE) and generating a corresponding IDP-user terminal entry;

- Performing AAA (42) on the user terminal (UE) when it connects to a first home network (1);
- Storing (43) the address of the User policy controller (UPC) of the first home network (1) in said IDP-user terminal entry;
- Providing (44) the address of the home-UPC to the Network policy controller (NPC) when the user terminal launches a subscribed service;
- Performing AAA (45) on the user terminal (UE) when it relocates to a second network;
- Providing (46) the address of the home-UPC to the User policy controller (UPC) of the second network (2).

16. A method in a User policy controller (UPC) within a policy control architecture according to any of the claims 1-7, **characterised by** the User policy controller performing at least the following steps when a user terminal (UE) connects to a first home network (1):

- Generating (51) a UPC-user terminal entry and storing the ID of a subscribed service;
- Accessing the independent Identity Provider (IDP) and registering (52) its UPC address in the corresponding IDP user terminal entry;
- Storing (53) the address of the Service policy controller (SPC) associated with the subscribed service in the UPC-user terminal entry;
- Storing (54) the address of the Network policy controller (NPC) of the home network in the UPC-user terminal entry;

17. A method in a User policy controller (UPC), according to claim 16, **characterised by** the User policy controller performing at least the following steps when said user terminal relocates to a second visited network (2):

- A User policy controller (UPC) of the second, visited network acquiring (55) the address of the User policy controller (UPC) of the first, home network via the IDP user terminal entry;

- The User policy controller (UPC) of the home network sending (56) the IDs of the user terminals subscribed services to the User policy controller in the visited network;
- The User policy controller (UPC) of the home network sending (57) the address of the Service policy controller (SPC) associated with each of said subscribed services to the corresponding Service policy controller of the visited network;

18. A method in a Business policy controller (BPC) within a policy control architecture according to any of the claims 2-7, **characterised by** the Business policy controller applying business related policies on the subscribed services of a roaming user terminal.

19. A method in a Business policy controller according to claim 18, wherein said business related policies include roaming agreements.

20. A method in a Service Policy Controller (SPC) within a policy control architecture according to any of the claims 5-7, **characterised by** the Service Policy Controller applying service related policies on a subscribed service.

21. A method in a Network Policy Controller (NPC) within a policy control architecture according to any of the claims 6-7, **characterised by** the Network Policy Controller mapping service policies on network dependent policies.

22. A method in a Network Policy Controller (NPC) according to claim 21, wherein the Network Policy Controller creates network related policies based on network status.

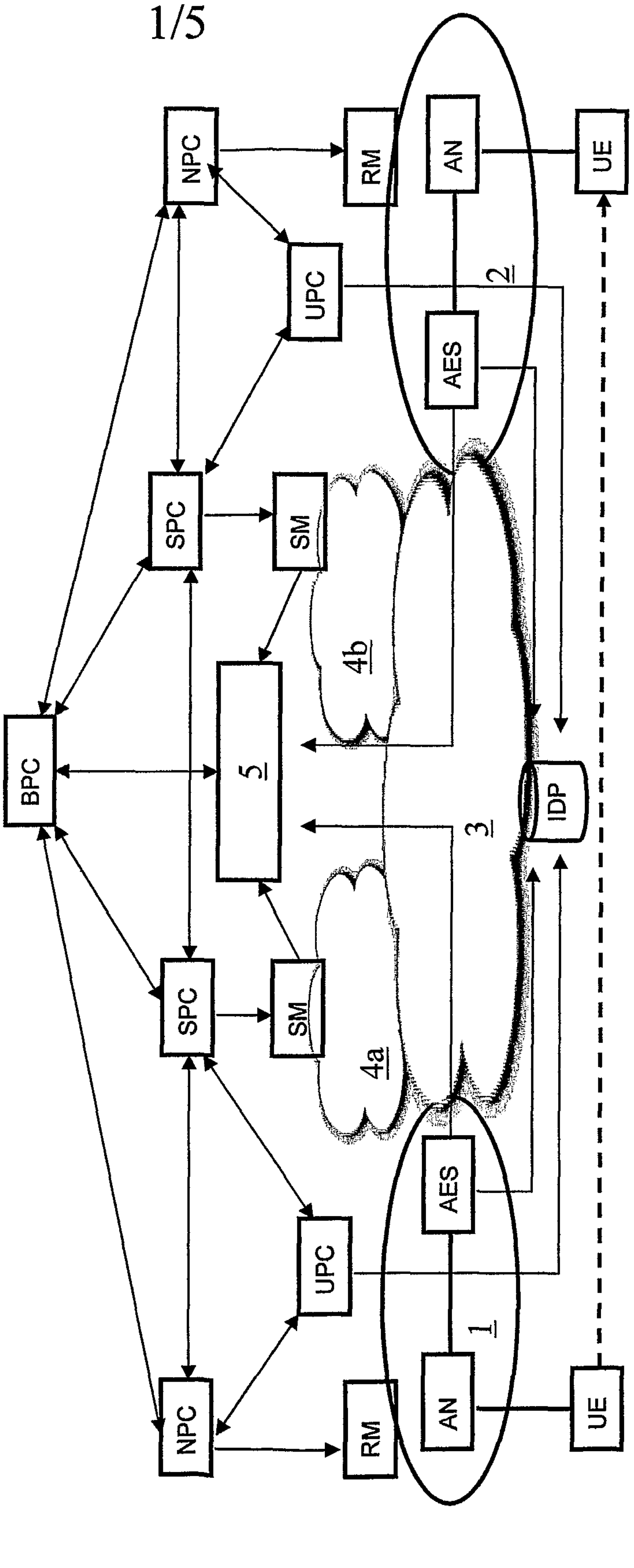

NPC
RM
AN
UE
UPC
AES
1
SPC
SM
4a
BPC
5
3
IDP
4b
SPC
SM
UPC
AES
2
NPC
RM
AN
UE

Figure 1

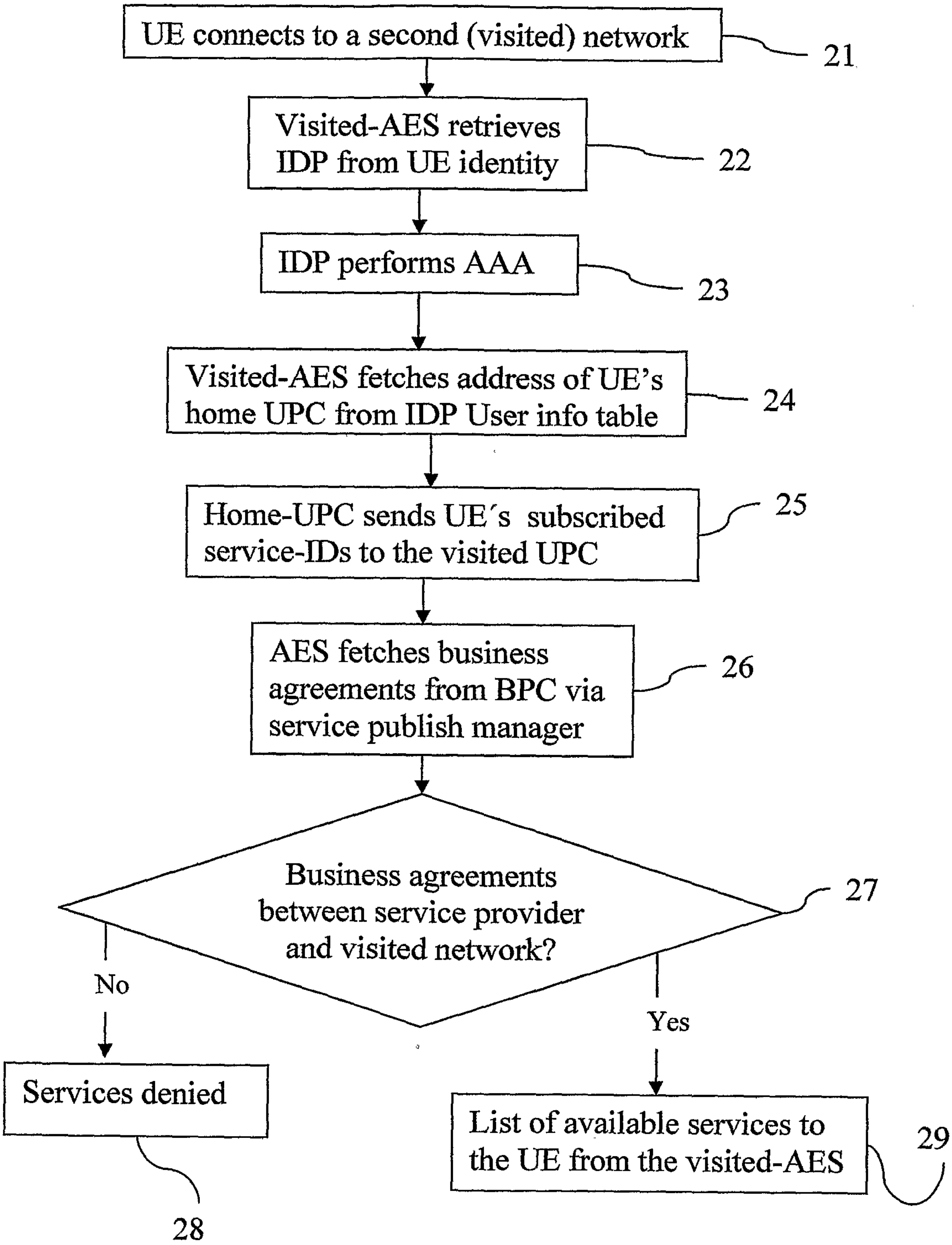

UE connects to a second (visited) network
21
Visited-AES retrieves IDP from UE identity
22
IDP performs AAA
23
Visited-AES fetches address of UE's home UPC from IDP User info table
24
Home-UPC sends UE´s subscribed service-IDs to the visited UPC
25
AES fetches business agreements from BPC via service publish manager
26
Business agreements between service provider and visited network?
27
No
Yes
Services denied
28
List of available services to the UE from the visited-AES
29

Fig. 2

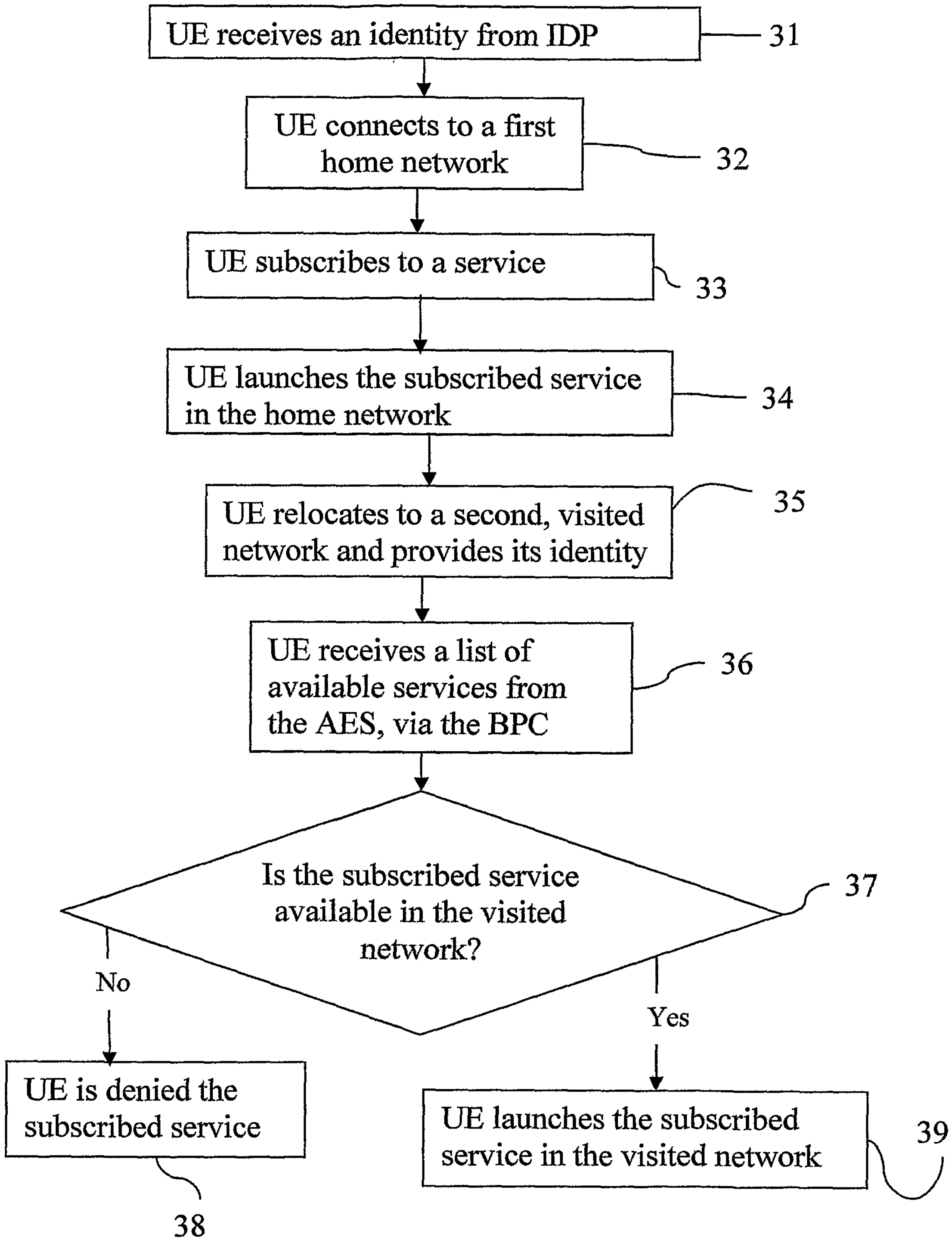

UE receives an identity from IDP
31
UE connects to a first home network
32
UE subscribes to a service
33
UE launches the subscribed service in the home network
34
UE relocates to a second, visited network and provides its identity
35
UE receives a list of available services from the AES, via the BPC
36
Is the subscribed service available in the visited network?
37
No
Yes
UE is denied the subscribed service
38
UE launches the subscribed service in the visited network
39

Fig. 3

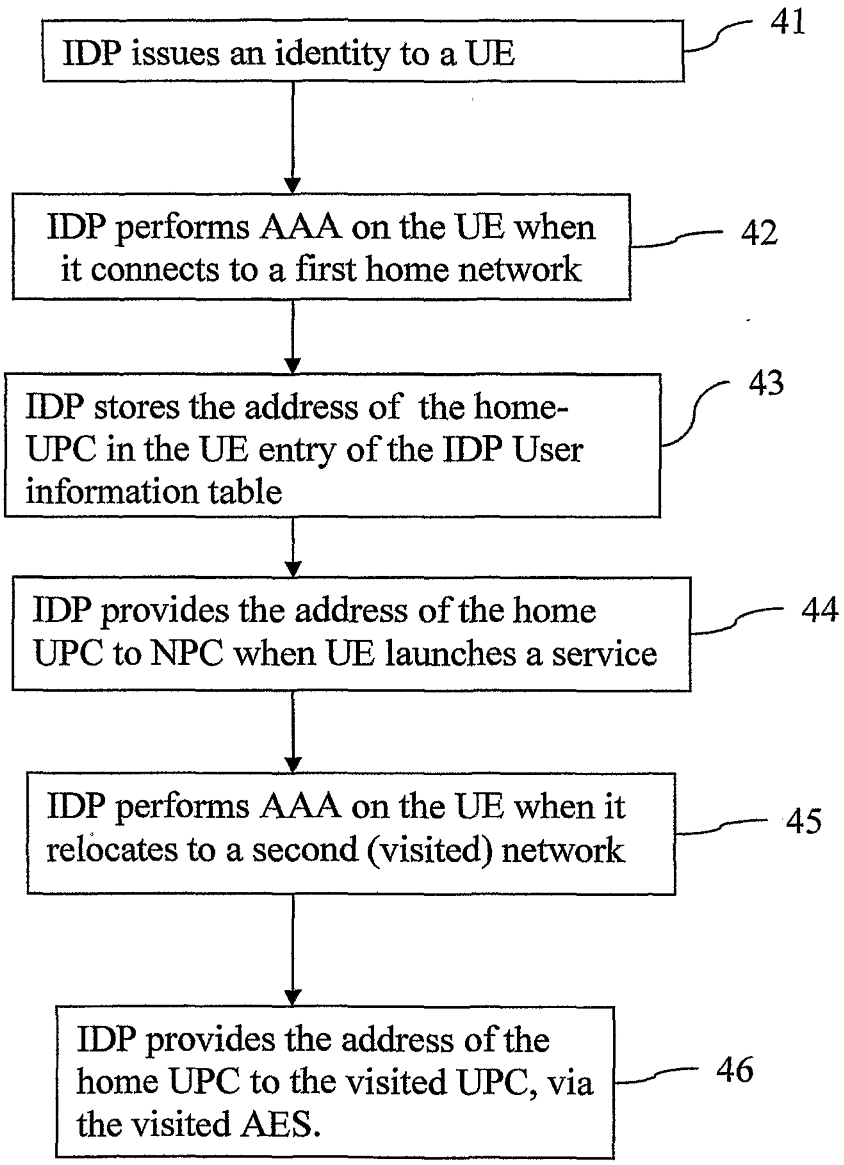

IDP issues an identity to a UE
41
IDP performs AAA on the UE when it connects to a first home network
42
IDP stores the address of the home-UPC in the UE entry of the IDP User information table
43
IDP provides the address of the home UPC to NPC when UE launches a service
44
IDP performs AAA on the UE when it relocates to a second (visited) network
45
IDP provides the address of the home UPC to the visited UPC, via the visited AES.
46

Fig. 4

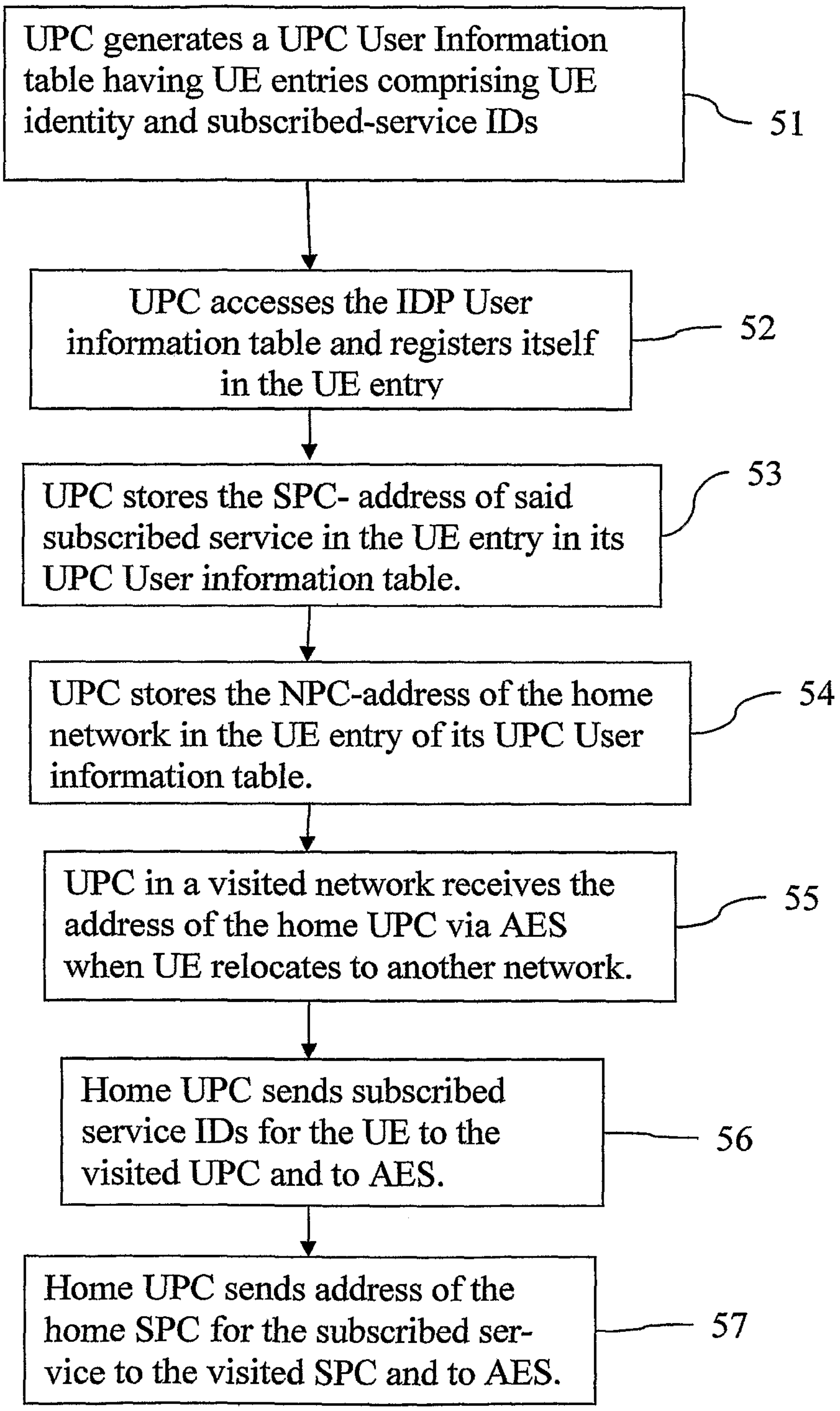

UPC generates a UPC User Information table having UE entries comprising UE identity and subscribed-service IDs
51
UPC accesses the IDP User information table and registers itself in the UE entry
52
UPC stores the SPC- address of said subscribed service in the UE entry in its UPC User information table.
53
UPC stores the NPC-address of the home network in the UE entry of its UPC User information table.
54
UPC in a visited network receives the address of the home UPC via AES when UE relocates to another network.
55
Home UPC sends subscribed service IDs for the UE to the visited UPC and to AES.
56
Home UPC sends address of the home SPC for the subscribed service to the visited SPC and to AES.
57

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2006/001093

A. CLASSIFICATION OF SUBJECT MATTER

IPC: 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)

IPC: H04L, H04Q

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ, INSPEC, INTERNET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1250023 A1 (ALCATEL), 16 October 2002 (16.10.2002), paragraphs 0002-0003; 0008-0011; figure 1, claim 1, abstract --	1-22
A	US 20060141995 A1 (PURNADI, R ET AL), 29 June 2006 (29.06.2006), paragraphs 0001-0028, figure 1, abstract --	1-22
A	IACONO, S ET AL: "Policy based management for next generation mobile networks", Wireless Communications and Networking, 2003, WCNC 2003, 2003 IEEE, 16-20 March 2003, ISBN 0-7803-7700-1, vol 2, pag 1350-1354, retrieved from http://ieeexplore.ieee.org /xpls/abs_all.jsp?arnumber=1200570, see sections III-IV --	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 3 July 2007	Date of mailing of the international search report 05-07-2007
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Sture Elnäs /LR Telephone No. +46 8 782 25 00

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MISTRY, NALIN: "The Importance of policy-based resource control in future networks", Nortel Technical Journal, Issue 4, August 2006, retrieved from: http://www.nortel.com/corporate/news/collateral/ntj4_policy.pdf, see figures 1-3 and abstract --	1-22
E	WO 2006107647 A1 (LUCENT TECHNOLOGIES INC), 12 October 2006 (12.10.2006), page 3 - page 4, figures 1-3, claims 1-10, abstract -- --------	1-22

International patent classification (IPC)
H04L 12/24 (2006.01)
H04Q 7/38 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument(service in Swedish).

Use the application number as username.
The password is **SMGXPROZGX**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/05/2007

International application No.

PCT/SE2006/001093

EP	1250023	A1	16/10/2002	US	7027818	B	11/04/2006
				US	20020151312	A	17/10/2002
US	20060141995	A1	29/06/2006	WO	2006067609	A	29/06/2006
WO	2006107647	A1	12/10/2006	AU	748754	B	13/06/2002
				AU	7692298	A	11/12/1998
				CA	2290502	A	26/11/1998
				EP	1014988	A	05/07/2000
				IL	132848	A	31/08/2004
				JP	2002515905	T	28/05/2002
				US	20060250956	A	09/11/2006