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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2006 (21.12.2006)

PCT

(10) International Publication Number
WO 2006/135285 A2

(51) International Patent Classification:
H04Q 7/38 (2006.01)

(21) International Application Number:
PCT/SE2005/000916

(22) International Filing Date: 15 June 2005 (15.06.2005)

(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) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GONZALEZ PLAZA, Alfredo** [ES/ES]; C/ Omega 87 5° A, E-28032 Madrid (ES). **RAMOS ROBLES, Luis** [ES/ES]; C/Juan de la Hoz, 28, 2° B, E-28028 Madrid (ES).

(74) Agents: **BOESTAD, Karin** et al.; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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.

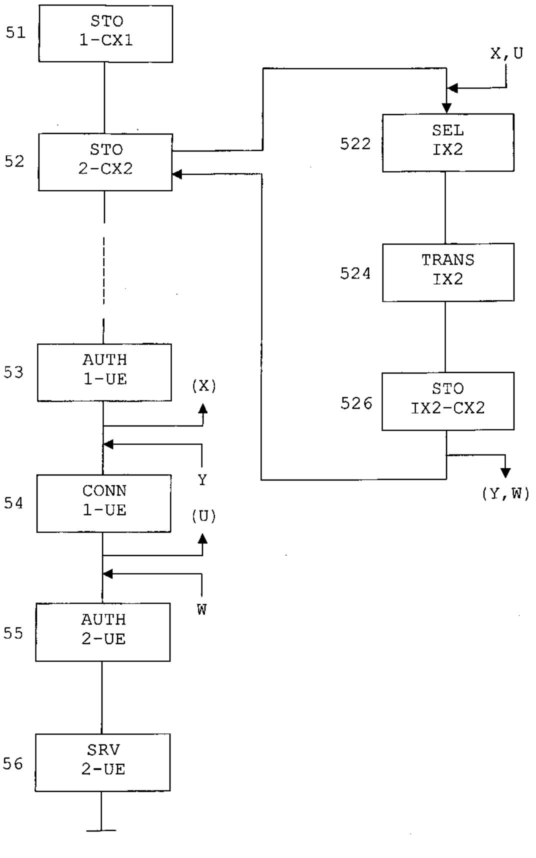
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, 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:
— *of inventorship (Rule 4.17(iv))*

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) **Title:** METHOD AND APPARATUS FOR PROVIDING A TELECOMMUNICATIONS SERVICE



(57) Abstract: Method and apparatuses for providing a user terminal 11, 12 connectable to a first telecommunications network 1A, 1B with access to telecommunications services provided from a second telecommunications network 2 through said first network. An identifier IX2 usable as user credentials before the second network is selected 522. From the first telecommunications network an account association message 524 is sent to the second telecommunications network requesting the assignation of a service account SA-2N and comprising the selected identifier IX2. The identifier IX2 is stored 526 in the second telecommunications network as user credentials CX2 for a service account SA-2N in said second network. Since service accounts in the second network are dynamically provided from cooperating first networks, occasional users of services provided by the second network can be alleviated of having to intervene personally so as to subscribe in advance permanent pre-paid or post-paid service accounts in said second network.

WO 2006/135285 A2

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.

METHOD AND APPARATUS FOR PROVIDING A TELECOMMUNICATIONS SERVICE

FIELD OF THE INVENTION

The present invention relates to telecommunications services provided from telecommunications networks to user terminals, and particularly to the provision of access to telecommunications services in interworking scenarios comprising a first telecommunications network, to which a user terminal is connected, and a second telecommunications network providing the telecommunications service to the user terminal through the first telecommunications network.

BACKGROUND

Traditionally, the services provided from a particular telecommunications network have been closely related to the particular access technologies and/or communication protocols used to communicate with user terminals that were able to connect directly to said network, as well as to the capabilities and limitations of these terminals.

As a result, the access to telecommunications services provided by a particular telecommunications network has been traditionally limited to user terminals connectable directly to said network. This factor also brought about that a telecommunications operator wanting to offer telecommunications services usually had to deploy a telecommunications network infrastructure comprising, not only the specific servers so as to provide the final telecommunications services to the user terminals (e.g. signaling handling servers, specific application servers, etc), but also specific access servers arranged to provide access connection for said terminals to the rest of the telecommunications network (e.g. local exchanges, radio access servers, etc) as well as the rest of the access infrastructure (cables, antennae, etc).

However, a main challenge for operators of telecommunications networks is to provide seamless telecommunications services to end users; namely, provide services without concern or limitation being imposed by the particular aspects of the particular telecommunications networks to which the eventual users might connect their terminals; thereby, allowing advantageously to develop telecommunications services which can be substantially independent of the particular access technologies.

The wide adoption of interworking tools for achieving more homogeneous, and thus, interoperable communication frameworks, such as the extended usage of the Internet Protocol IP as a (inter)network protocol, as well as the wide use of protocol and media gateways for allowing interconnection of heterogeneous telecommunications networks, have helped to overcome some of the compatibility problems arising in earlier telecommunications networks, and have consequently allowed to devise and offer telecommunications services that, for example, can be served from the same service platform (e.g. one or more specific application servers) within the telecommunications network of a network operator to user terminals that are not necessarily connected to said telecommunications network, but that can be connected to another cooperating telecommunications network(s) instead, which may even belong to a different network operator.

Accordingly, new interworking scenarios involving at least two telecommunications networks are presently envisaged which goes beyond the mere provision of interconnection services for end user's terminals, like interconnection services providing voice communications between a terminal connected to cellular network (such as a Global System for Mobile communications network, GSM) and another terminal connected to a fixed network (such as a Public Switched Telephone Network, PSTN). These new interworking scenarios comprise a telecommunications network having the means to provide a telecommunications service to a user terminal (e.g. one or more specific service application servers devoted to provide one or more service), and another telecommunications network to which a user terminal can be connected and through which the access to the telecommunications service may be provided. In short, in these new interworking scenarios, a user terminal connected to a first telecommunications network may access a service provided from (i.e. by, or with the intervention of) a second telecommunications network.

The concept underlying these new interworking scenarios allows a new kind of network operator which do not necessarily need to deploy its own access means (e.g. specific access servers, cables, antennae, etc) for providing access connection for user terminals to its telecommunications network, since it would merely need to have a telecommunications network comprising the specific service servers, so as to provide the final telecommunications services to the user terminals, and the necessary communication links and gateways with another telecommunications networks, to which the users terminals could be connectable and through which a communication with said terminals would be provided. These new kind of network operators are sometimes referred as "service providers", while the network operators able to offer direct connectivity to user terminals are sometimes referred as "access providers". Similarly, the telecommunications network of a service provider is sometimes referred as "service network", while the telecommunications network of an access provider is sometimes referred as "access network".

An example of these kind of interworking scenarios for the provision of telecommunications services may be given considering the IP-Multimedia-System IMS (described in 3rd Generation Partnership Project 3GPP specification TS 23.228 V6.9.0, March-2005) as the telecommunications network providing telecommunications services (in this particular case the so called "IP Multimedia Services" - referred hereinafter as "IMS services"-, as described for example in the related 3GPP specification TS 22.228 V7.1.0, March-2005), which can be accessible to user terminals connected to a variety of further telecommunications networks in so far as they get IP connectivity through said further networks (i.e. the so called "access independence" principle recited in chapter 3.1 of the aforementioned TS 22.228). Examples of telecommunications networks to which user terminals can attach so as get IP connectivity and then obtain access to the IMS services provided by a IMS are: a Local Area Network LAN, a Wireless LAN WLAN, a PSTN, or the General Packet Radio System GPRS of a cellular telecommunications network. However, interworking scenarios of this or similar nature can also be envisaged in so far as they involve a first telecommunications network to which user terminals are connectable so as to access through it a service provided from a second telecommunications network.

Regardless details related to interworking scenarios involving two or more telecommunications networks, there are some aspects common to most of the telecommunications networks which are usually independent of the nature of the telecommunications services they can offer, which can range from mere bearer services for providing physical connection to a user terminal, so as to allow it to communicate with another user terminal or server, to more complex services such as: personalized information services (e.g. location-based services, stock market information), messaging services (e.g. short message services, multimedia services, voice messaging services, messaging format conversion), services involving intelligent call processing, digital identity support for electronic commerce, etc.

In particular, a common aspect is that the access to the services provided from a telecommunications network is usually subject to a previous subscription of a "service account" in said network. This aspect uses to be common except in cases in which the nature of the service is such that it may given to anyone without restriction nor personalization criteria (e.g. the service is a general information service given without any kind of discrimination criteria based on the served user).

In general, a user wanting to access from a suitable user terminal to the telecommunications services provided from a telecommunications network of a network operator, signs a business agreement with said operator, which is an administrative transaction that establishes a direct business relationship between them in virtue of which the user (also called "subscriber" from that moment) subscribes to a pre-paid or post-paid service account with said operator and, in some cases, can receive, among other, user credentials for authenticating him from a given terminal. For the particular case of pre-paid accounts (and also for the so called "voucher accounts", later referred), the signing of the business agreement can, in some cases, comprise merely the acquisition by the user of the necessary item(s) containing the corresponding user credentials (e.g. for a GSM pre-paid subscription it is sufficient for the user to buy the corresponding Subscriber Identity Module SIM). For the particular case of post-paid account, the business agreement usually further comprises the provision from the subscriber of a payment account to which the costs of the serviced services are to be ascribed.

For a subscriber of a particular telecommunications network, the data of his corresponding service account (usually referred as "subscription data" or "subscriber data") are usually managed by administration and maintenance procedures of the operator of said network, which normally comprise initial data provision in the relevant server(s) of said network upon subscription of the service account. It is well known by those skilled that details related to the quantity, specific nature and storage details (e.g. if distributed or centralized) of the data related to a service account may vary according to the kind of telecommunications network and also according to the operator of said network. However, in general terms and regardless these specific details, it can be stated that a service account comprise the necessary static and dynamic data that are stored in relationship with a subscription and that may be required for service provision to the corresponding subscriber, such as: identification information (e.g. a telephone number, a Session Initiation Protocol Uniform Resource Identifier SIP-URI, etc), user credentials for authentication (secret keys, password, private user identifier, etc), configuration preferences for some services, specific barring for services, registration status of a user terminal for said subscription, IP-address assigned to the user terminal, etc.

It shall be noticed here that, with regard to the new interworking scenarios mentioned above, this first common aspect uses to imply that the user may be required to subscribe service accounts in advance in all the telecommunications networks he might eventually use for accessing a telecommunications service provided by a certain telecommunications network.

A further common aspect is that, when service provision in a telecommunications network depends on the existence of the corresponding service account, authentication of user terminal according to the corresponding user credentials uses to be required in some cases; for example, whenever the user terminal may access a telecommunications network from different access points of said network (or even via another telecommunications network), or whenever the user terminal may be used by different users and/or a personalized service (e.g. based on user subscription) is intended to be provided. The purpose of authentication is to assert the ownership of a service account in the telecommunications network before granting a terminal the access to a service provided from said network. Accordingly, authentication is commonly used, not only in wireless networks (such as cellular networks or WLANs), but also in other telecommunications networks for which the aforementioned access flexibility exists. Furthermore, it does not necessarily depend on the different kinds of service accounts in what regards to the type of settlement established for paying for the services provided; thus, authentication uses to be common for post-paid and pre-paid service accounts, and also for the so called "voucher accounts".

Voucher accounts are accounts predefined in certain telecommunications networks and, usually, have a limited validity of use from its first activation, which makes them suitable for occasional users of certain telecommunications services. Accordingly, a user may acquire the right to use a voucher account at a sales point and use it for accessing to telecommunications services provided from a telecommunications network for a limited period of time, or other accountable event, such as volume of data or the number of served services. As part of the voucher acquisition the user is usually provided with the user credentials needed to access the telecommunications network, typically a user identifier, or a user identifier and password (e.g. a card comprising the corresponding user credentials). The service account data for voucher service accounts are commonly provisioned in the telecommunications network as any other account; i.e. they can comprise essentially the same kind of data as referred above for other kind of service accounts.

With regard to the new interworking scenarios mentioned above, and considering that services account are needed in both telecommunications networks (first and second telecommunications networks), authentication of a user terminal in both networks might be required; namely, it may be common that, first, the user terminal is authenticated from the first network, so as to allow it to obtain a connection (e.g. a data connection) through said first network which may allow it to communicate with a further telecommunications network, and then, the user terminal is authenticated from the second telecommunications network so as to allow it to access to a service provided from said second network.

For example, patent application US 2002/0191597 A1 discloses an interworking scenario wherein the first network to which the user terminal ("1" in Fig.1 of US

2002/0191597) is connected is a GPRS network ("2" in Fig.1 of US 2002/0191597), and wherein the second network providing the final service to the terminal is a IMS network ("7" in Fig.1 of US 2002/0191597). As cited by US application (e.g. paragraphs 32 to 38), the user terminal first attaches and is authenticated from the GPRS network, which gives it a data connection through it allowing to further communicate with the IMS network, and then, it is authenticated from the IMS network so as to assert the ownership of the corresponding service account, which gives said terminal the right to access IMS services provided from the IMS network.

The interworking scenarios mentioned above bring about new issues concerning revenue generation models between the network operators owning each of said telecommunications networks, which, eventually, may require business agreements between them so as to allow to exchange and process the accounting information of the consumed services for charging purposes. For example, addressing to this issue, the aforementioned patent application US 2002/0191597 A1 discloses a solution for associating charging information in an interworking scenario wherein the first network to which the user terminal is connected is a GPRS network, and wherein the second network providing the final service to the terminal is a IMS network. Furthermore, the solution provided by said patent application is also suitable to improve the processing of the charging events even with both telecommunications networks (access -first- network and service -second- network) belongs to the same operator.

However, although US 2002/0191597 provides a charging solution for the provision of telecommunications services in this new kind of interworking scenarios, the need for a user to subscribe service accounts in both telecommunications networks (i.e. the one providing the service and the one providing the access to the user terminal) still remains.

Although this might not represent a problem for frequent users of the telecommunications services provided by any of these two networks, it might represent some inconvenience for users who could be occasional users of, for example, the services provided from the operator owning the second telecommunications network, and for whom it might not be worthwhile to subscribe and maintain a permanent pre-paid or post-paid subscriptions in said second telecommunications network and also in all the eventual first networks from which the services provided by said second network could be accessible. Nevertheless, occasional users, or, more generally, users who do not want, or who do not consider advantageous, to have a permanent subscription in a plurality of telecommunications networks, might represent an interesting business segment for network operators if no complex requirements are put on the user side.

SUMMARY OF THE INVENTION

The present invention allows a user terminal connectable to a first telecommunications network to access a telecommunications service provided by a second telecommunications network via said first network by providing a service account in said second network without a user of the terminal needing to take an active role to subscribe said service account.

According to aspects of the invention, this is achieved by a method as claimed in claim 1, or by an apparatus as claimed in claim 15 in cooperation with an apparatus as claimed in claim 19. Embodiments of the invention are set out in the dependent claims.

The method and apparatuses of the invention are characterized in that from the first telecommunications network an account association message is sent to the second telecommunications network, the message requesting the assignation of a service account in said second network and comprising an identifier which is usable as user credentials before said second network, and in that said identifier is stored in the second telecommunications network as user credentials in relationship with a service account which is assigned in said second network upon request from the first network; thereby, allowing from that moment to provide from the second network access to a telecommunications service through the first network to a user terminal connected to the first network for which the ownership of the corresponding user credentials in relationship with the assigned service account can be asserted.

Since service accounts in the second network are dynamically provided upon requests from cooperating first networks, occasional users of the services provided by the second network can be alleviated of having to intervene personally so as to subscribe in advance permanent pre-paid or post-paid service accounts in said second network. Furthermore, the operator of the second telecommunications network can be alleviated of having to keep a direct business relationship with all of its eventual users for subscribing and/or maintaining directly the corresponding subscriptions.

According to one embodiment, a service account in the second network can be created at reception of an account association message from a first network, and the identifier comprised in said message becomes user credentials in relationship with said service account being then usable to authenticate a user terminal connected to said first network, so as to allow it to obtain access to a service provided by said second network.

According to another embodiment, the second telecommunications network can store a plurality of identifiers usable as user credentials before said network, wherein a specific set of them, or all of them, can be made accessible for being selected from one or more cooperating first telecommunications networks, through which access to telecommunications services provided from the second network can be requested from user terminals connected to them. In yet another embodiment, these identifiers can be stored in advance in relationship with idle service accounts in the second network, which can be specially devoted for dynamic assignation and activation upon requests from a cooperating first networks.

Accordingly, an idle service account in the second network can be set to active at reception of an account association message from a first network comprising the associated identifier, which then becomes user credentials usable to authenticate a user terminal connected to said first network so as to allow it to obtain access to a service provided by said second network.

For making accessible all or part of the identifiers to a cooperating first network, the second network can forward a set of the available identifiers to said first network, or all of them, so as to make possible these identifiers to be stored in the first network and be selected from there. Alternatively, the available identifiers can be keep stored in the second network, wherein a cooperating first network may send a request to obtain one or more of said identifiers which can be available for it.

By controlling the distribution of, or the access to, the available identifiers, the second telecommunications network can then manage what cooperating first telecommunications network can request dynamic account assignations and, if desired, for what identifiers.

According to another embodiment, the first telecommunications network can store a mark for account association in relationship with some of its service accounts; wherein account association requests can selectively be sent for service accounts which are so marked. According to yet another embodiment, an identifier that has been selected for being sent in an account association request from the first telecommunications network to the second telecommunications network is stored in relationship with a service account in the first network; which can also be used as a mark for account association in relationship with said service account, so as to determine the sending of an account association request for said service account.

By selectively marking service accounts in the first telecommunications network, a new marketable concept of combined voucher accounts can be easily deployed, which can allow a user to acquire a single voucher for connecting to a first telecommunications network and to gain access through it to telecommunications services provided from a second telecommunications network. In this case, the acquired voucher would give the user access to first user credentials in relationship with a service account in the first network, which would allow to authenticate a user terminal of the user so as to allow it to access to the first network. Accordingly, the service account in the first network could have been previously marked for account association, so as to provide a further service account in the second telecommunications network and the necessary second user credentials in relationship with said further service account, which would allow to authenticate the user terminal and allow it to access to a telecommunications service provided by the second network.

According to another embodiments, an account association message can also comprise further data that can be stored by the second network as user credentials in relationship with the service account assigned in said second network, so as to grant from the second network the access to a service requested from a user terminal connected to the first network upon authentication of said terminal according to any of the stored credentials.

If the account association message is sent for a specifically marked service account in the first network, it can comprise user credentials related to said service account. If the account association message is sent from the first to the second network for a user terminal connected to the first network, it can, additionally or alternatively, comprise a trust token identifying univocally said user terminal. The trust token can comprise a network address assigned to the user terminal for communicating with the second network through the first network. Alternatively or additionally, the trust token can comprise a key shared between the first terminal and the first network, which may have been established as a result of authenticating from the first network user credentials presented by the user terminals related to a service account in said first network according to a challenge request and challenge response authentication mechanism.

According to a further embodiment, the service account assigned in the second network upon request from the first network can be revoked, either: from the first network, or from the second network; thereby allowing to deny further access to the services provided by the second network via the first network when, among other criteria, the service usage, the time elapsed from the association or the volume of data exchanged by the concerned user terminal, exceed a certain limit.

If the initiative is taken from the first network, an account dissociation message can be sent from the first network to the second network requesting to dissociate a previously associated service account from the corresponding related user credentials. If the initiative is taken from the second network, an account dissociation notification message can be sent from the second network to the first network notifying the dissociation of a service account in the second network that was associated to the corresponding related user credentials upon request from said first network. The account dissociation message and the account dissociation notification message can comprise an information element previously sent in an account association message, which, in the first case, may be used in the second network to identify the concerned service account, and, in the second case, may be used in the first network to identify, if proceeds, the concerned service account in said first network as well as the concerned user terminal.

By allowing either of the telecommunications networks to revoke the usage of the service account associated in the second network for the corresponding user credentials, flexible accounting policies can be deployed in either or both telecommunications networks, as this embodiment makes possible to deny further access to the services provided by the second network via the first network when the accounting of, among other: service usage, time elapsed from the association or volume of data exchanged by the concerned user terminal, exceed a certain limit.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 shows a schematic view of a telecommunications system comprising a plurality of telecommunications networks.

Figure 2 shows a schematic representation of some functional modules of apparatuses for controlling the access of a user terminal to a service provided from a telecommunications network, as well as some of the data they handle for controlling said access.

Figure 3 shows a flowchart illustrating steps of a method for providing access to a telecommunications service according to the invention in interworking scenarios comprising a plurality of telecommunications networks.

Figure 4 shows a simplified signaling flow illustrating some embodiments of the method according to the invention.

DETAILED DESCRIPTION

Some exemplary embodiments of the invention shall now be described more in detail with references to figures 1 to 4.

For illustrating in a generic way interworking scenarios comprising: one or more telecommunications networks to which user terminals can be directly connected, and one or more telecommunications networks from which telecommunications services can be provided to said user terminals, the system shown in Fig.1 represents a simplified view of a telecommunications system comprising three telecommunications networks: 1A, 1B and 2, which can belong to one or more network operators. Within the domain of each network (1A, 1B, 2) a set of state-of-the-art functional server entities 'are depicted, the functionality of which shall be briefly described below.

As depicted in Fig.1, networks 1A and 1B comprise access means (AP 2A, 2B) for providing access connection for user terminals (UE 11, 12) to said networks. For illustration purposes, it can be assumed that network 1A represents schematically the GPRS network infrastructure of a cellular operator and that network 1B represents the WLAN network infrastructure of a WLAN operator. In that case, access means schematically represented by access server 2A would comprise radio base stations and base station controllers as well as other access servers entitled to primarily serve the access to the user terminal (e.g. route signaling and media to/from the user terminal), such as Serving GPRS Support Node(s) SGSNs. On the other hand, and considering also the aforementioned example case, access means schematically represented by access server 2B would comprise "hot-spots" of the WLAN network.

In what concerns to the telecommunications network 2, the basic functional characteristics of the relevant serving server entities comprised on it (22, 23, 24, 25) may be quite similar regardless of the nature of the telecommunications service(s) provided from said network. Accordingly, the server entities illustrated in Fig.1 within network 2 represent some of the most common functional elements within the network infrastructure of a (generic) service provider operator which offers services that, for example, might be accessed from a plurality of terminal types connected to different kind of access networks (1A, 1B), such as: messaging services, information services according to the current user location, etc. Also, network 2 might represent schematically the IMS network infrastructure of a service provider operator providing IMS services accessible to multimedia-enabled terminals.

For example, terminal 11 may be a GPRS enabled mobile phone which, through a connection provided trough a GPRS network 1A, access to service network 2 which provides his user with a network-based calendar service, a electronic mail service, a multimedia service, etc; while terminal 12 may be a personal computer equipped with a WLAN card which gives it access trough a WLAN network 1B to the same (or similar) services provided from telecommunications network 2.

As will be apparent from the description, the specific nature of the telecommunications networks used herein as example (1A, 1B, 2), or the specific type of telecommunications services that can be provided from a telecommunications network (e.g. 2) to a user terminal (e.g. 11) connected to another telecommunications network (e.g. 1A), are details which do not constrict the scope of the invention.

Reference 3 in Fig.1 represents schematically an interconnection network that allows the establishment of communications between server entities belonging to telecommunications networks 1A, 1B and 2, which also allow to establish communications between terminals, or between terminals and servers, connected to different telecommunications networks, so as to convey the necessary signaling and media for the provision of the required telecommunications services. The interconnection network 3 may comprise, for example, intranets, the Internet, dedicated signaling lines, and combinations thereof. Internal communications means within each network are schematically represented in Fig.1 by communication lines 6A, 6B and 26.

Server entities IGW 5A, 5B, 22 represent interworking server gateways that are commonly used in interworking scenarios involving more than one telecommunications network, which can be used for carrying out a variety of functions, such as protocol translation, proxy functions, routing and/or control functions for signaling or media, etc, that, generally, can be needed when establishing communications between a server (or terminal) belonging (or connected) to the network of an operator and another server (or terminal) belonging (or connected) to the network of another operator. For example, if, following with the aforementioned example, network 1A is a GPRS network and network 1B is a WLAN network, then, the interworking gateway 5A can represent a Gateway GPRS Support Node GGSN and the interworking gateway 5B can represent a connection server assigned to provide data connectivity to a user terminal 12 connected to the WLAN network 1B for communicating beyond the WLAN network domain. If network 2 is, e.g., a IMS network, the interworking gateway 22 may represent a IMS specific server entity known as "Call State Control Function CSCF" (e.g. in any or all its functional roles; i.e. as "Proxy-CSCF" P-CSCF, "Interrogating-CSCF" I-CSCF, or "Serving-CSCF" S-CSCF). If network 2 is the telecommunications network of another kind of service provider, such as a specialized content provider, the interworking gateway 22 may represent router and proxy servers arranged to route and mediate in communications with server entities or terminals in other telecommunications networks.

It shall be noticed that the schematic illustration given in Fig.1 for the represented interworking gateways IGW (5A, 5B, 22) does not preclude interworking scenarios in which some of the other server entities represented in Fig.1 for a given telecommunications network (e.g. 3A or 4A in network 1A) are arranged to communicate directly (i.e. without the mediation of a IGW) with other entities in another telecommunications network (e.g. 23 or 24 in network 2). For example, two server entities belonging to different telecommunications network may communicate directly if they comprise direct communication links with an interconnection network 3, use a common communication protocol and, preferably, use an authentication mechanism which allow establish a trusted communication between them.

Application servers AS 24 and 25 represent the server entities assigned to accomplish with the execution of high-layer aspects of some telecommunications service(s) that can be provided from the telecommunications network 2. For simplicity, in the scenario illustrated in Fig.1, it can be assumed that network 1A provides basic (e.g. bearer) data communication services to terminal 11, while network 2 provides some extra telecommunication services. However, it shall be noticed that, depending on the specific nature of a telecommunication service, and beyond the servers that intervene for its provision and that allow, for example, basic low-layer functions for routing signaling or media (such as routers, access servers, gateways, etc), there can be one or more than one application server involved in the high-layer aspects of the service provision for the same kind of service. Also, a given physical machine can be arranged to provide (or to cooperate in the provision of) more than one service type.

For example, AS 24 and/or 25 can be arranged with the communication means (e.g. protocol stacks, communication links, etc) and service logic (e.g. provided by computer programs comprising the appropriate computer readable instructions to be executed by a processor in the AS) so as to perform intelligent signaling handling for multimedia session (e.g. to divert, accept or reject incoming multimedia sessions for a IMS subscriber based on the time of the day, date of the week, or the identifier of the originator). Similarly, AS 24 and/or 25 can be provided with the appropriate communication means and service logic so as to provide a terminal with a location-based information service; in which case, e.g., AS 24 can obtain from another server in network 1A or 1B geographical location information of user terminal 11 or 12 (if available), or even receive it from the terminal, and provide the user terminal with, e.g., information about the nearest hospital, local transport information, local weather forecast, etc.

Also, for accomplishing with the high-layer aspects of a service, ASs 24 or 25 might cooperate with further servers in other telecommunications networks, which are not necessarily the one wherein the served user terminal is connected to. That could be the case wherein the service provided is, for example, an electronic commerce transaction service (e.g. AS 24 might act as a payment broker server) or when the service provided is, for example, a flight reservation comprising, as an extra feature, the updating of a network-based calendar of the user (e.g. AS 25 might be the flight broker and would have to cooperate with another AS serving a calendar service for the served user, or vice versa).

It shall be noticed here that, in the particular case of network 2 providing IMS services, the correspondence between server entities cited above (IGW 22 and ASs 24 or 25) may be logically considered in a different way. For example, the basic treatment of a multimedia session within the IMS might not need to imply the intervention of "Application Servers, AS" for intelligent signaling handling as recited above (i.e. Application Servers ASs as referred in the aforementioned specification 23.228, chapter 4.2.4). In that case, and considering the functional task in regard to the highest aspects of the provided service, the illustrated AS 24 could be a S-CSCF (e.g. the one assigned to serve to the originating user) while the IGW 22 could be a P-CSCF.

Fig.1 shows networks 1A and 1B as also comprising application servers (4A, 4B) from which services can be provided to user terminals (11, 12) connected to the same or different telecommunications network. This intends to illustrate a common situation in which the telecommunications network of a given operator comprises, not only the necessary infrastructure for providing access and further connectivity to user terminals, but also the necessary infrastructure to provide further telecommunications services going beyond basic telecommunications services, such as voice or data calls between user terminals. Said services may comprise some of the already related (e.g.: integrated messaging, multimedia calls, personalized information services, presence services, location based services, etc), wherein the access to some of them could also be allowed, upon previous subscription, for user terminals connected to the telecommunications networks of another operators. It shall be noticed here that, although network 2 is shown in Fig.1 as lacking of access infrastructure where user terminals may directly connect to it (e.g. access servers similar to AP 2A or 2B), it may also comprise them within its domain. Accordingly, the interworking scenarios detailed herein as examples, in which the first (access) network is assumed to be 1A or 1B, and the second (service) network is assumed to be network 2, may also involve scenarios in which the first (access) network or the second (service) network are any of the telecommunications networks shown in Fig.1.

Authentication servers (AA): 3A, 3B and 23 perform authentication functions on, respectively, each of the illustrated telecommunications networks 1A, 1B and 2. The specific characteristics of the authentication mechanism(s) that can be utilized in a particular telecommunications network for authenticating a user terminal may vary. Examples of commonly used authentication mechanisms are SIM authentication (as described in chapters 3 or D.3 of 3GPP TS 43.020 V6.1.0, December 2004), Authentication and Key Agreement AKA (as described in chapter 6.3 of 3GPP TS 33.102 V6.3.0, December 2004), and Basic and Digest Access Authentication (as described in IETF RFC2617, June 1999). Accordingly, the specific features that characterize any of said AA servers may also vary according to the authentication mechanism(s) they have to use. However, the basic functional characteristics of authentication servers AA are substantially similar, in so far as they provide the means to assert the ownership of the corresponding service account; for example, by checking directly with the user terminal, or indirectly via a cooperating network, the ownership of the corresponding associated user credentials before granting a terminal the access to a service provided from said network.

Authentication mechanisms commonly rely in user credentials comprising at least a secret key shared between the telecommunications network and the user, his terminal or a usually tamper-resistant device connectable to the user terminal (or embedded on it) that is arranged to contain a secret key (such as a SIM card or another kind of similar smart card). Regardless specific details related to specific authentication mechanisms, the authentication procedure usually involves an interaction between the user terminal and the authenticating network in which the user terminal is asked to provide the user credentials (which may require an interaction with the user) that are then verified by the network.

In said interaction the authentication server may be directly or indirectly involved in the authentication process; i.e., the authentication server may check directly the credentials submitted by the user terminal, or may send the necessary authentication material to a server entity primarily contacted from said terminal. For example, authentication server 3A (e.g. a Home Location Register with Authentication Centre capability HLR/AuC of a cellular network 1A) may send authentication material (e.g. GSM triplets) to access server 2A (e.g. SGSN or MSC/VLR) so as to authenticate user terminal 11 from there (2A), while authentication server 23 (e.g. a RADIUS authentication server) may run directly the authentication of a user terminal when accessing to network 2, e.g., by verifying that the user terminal owns the corresponding user credentials, by asking the user of the terminal to enter a user identifier and/or a password, etc. Also, authentication server 3B on network 1B may check user credentials received from the user terminal 12, such as user identifier and/or a password, while authentication server 23 (e.g. a Home Subscriber Server HSS of a IMS network 2) may send authentication material (e.g.

Authentication Vectors) to the S-CSCF (22, 24) so as to authenticate a user terminal from there.

A further interworking scenario that could be embodied by the schematic illustration represented in Fig.1 is that any of the access networks 1A or 1B may in turn be comprised of two sub-networks. That can be the case wherein network 1A would comprise, for example: a WLAN radio access infrastructure comprising WLAN hot-spots and WLAN access server(s), to which the hot-spots are connected, and an interworking cellular network providing IP connectivity trough its GPRS access infrastructure. Such particular scenario is described in 3GPP specification TS 23.234 V6.4.0, March 2005. In that case IGW 5A represented in Fig.1 would comprise the Packet Data Gateway PDG disclosed in said specification, and the AA 3A could be the named 3GPP AAA Server. Accordingly, the user terminal 11 would be given access if the existence of a service account in the GPRS (sub)network is asserted.

For simplicity reasons, in some of the following examples it shall be considered that an authentication server (3A, 3B, 23) executes directly the authentication of a user terminal (11, 12) that accesses, either: directly or through another telecommunications network, to the telecommunications network where it resides (1A, 1B, 2). However, as mentioned above, it shall be apparent that in some cases the functionality disclosed for an authentication server may be shared with another servers performing another functions (such as access control or signaling handling).

As those skilled will appreciate, a particular telecommunications network may (e.g. due to scalability and/or reliability reasons) have a plurality of authentication servers. Also, it is well known that a particular authentication server (3A, 3B, 23) may also be arranged to perform further functions such as service authorization and accounting functions. In particular, authorization and authentication functions are closely related, since, when the access to a service is subject to a previous subscription, the access to said service uses to be subject to authorization, which leads to a previous authentication. Accordingly, authentication and authorization functions for a given terminal connected to a telecommunications network (directly, or through another telecommunications network) uses to be performed by the same kind of authentication server entity, which functional role is, in summary, to control in a given telecommunications network the access of a user terminal, which is directly or indirectly connected to said network, to a telecommunications service provided by said network or provided from another telecommunications network. Also, accounting of the services requested and consumed by a user use to be performed by the same server that authorizes said services. Therefore, authentication, authorization and accounting functions are commonly performed by the same kind of server (usually known as AAA server).

In the following examples, and for the sake of illustrating the novel procedures of the invention in the interworking scenarios where they can take place, authentication servers 3A or 3B are assumed to be the servers entitled for controlling from a first network (1A, 1B) the access of a user terminal (11, 12) to a telecommunications service provided from a second network (such as network 2) through said first network (1A, 1B), while authentication server 23 is assumed to be a server entitled for controlling from telecommunications network 2 the access of a user terminal to a service provided by said network.

The internal simplified structure of an authentication server AA (3A, 3B, 23) shown in Fig.1 shall now be described with reference to Fig.2, which considers a possible implementation as a computer-based apparatus, which, as in most of the modern telecommunications networks, is a preferred implementation basis for telecommunication servers.

A telecommunications server which serves or mediates in the services provided by or through a telecommunications network (such as application servers AS, gateways IGW, authentication servers AA, etc.), regardless its specific construction details, may be considered as comprising of one or more functional modules, each of them arranged to perform a specific sub-function of the total functionality implemented by said server and, eventually, arranged to cooperate with some of the others. Furthermore, the functionality of a given telecommunications server (which in fact may be considered as a "functional entity") may be distributed across various physical machines, each performing a part of the total functionality said server is assigned to perform. An example of this is a HSS comprising a first machine implementing HLR functionality and a second machine implementing AuC functionality. Also, in some implementations, the same physical machine may implement the functionality of two or more different servers (e.g. a computer-based machine may implement the functionality of two functional entities such as a SGSN and a GGSN, or the functionality of two ASs providing two different services).

Once the functionality of a functional server entity in a telecommunications network has been defined (e.g. by a Standard document), the construction of the functional modules to build up a realization of the corresponding physical machine(s) is a matter of routine work for those skilled in the art. Accordingly, the explanation given with reference to Fig.2 shall describe some basic functional components of authentication servers 1A, 1B and 23 without falling into specific construction details concerning the possible physical realizations, which are well known by those skilled and, consequently, which are not needed to understand the invention. In particular, a server implemented as a computer-based apparatus comprises: software and hardware, which can be distributed along various cooperating physical machines; wherein a specific functional module of the server implemented by a computer-based apparatus may comprise: software, hardware, or a combination of both, and wherein said functional modules are designed to perform a specific (sub)function and, if proceeds, to cooperate with software and/or hardware parts which implements other functional module(s). The software comprises one or more computer programs (computer readable program code) that, when executed by a computer-based apparatus makes it to behave according to a predefined manner, as determined by the specific program instructions in said programs, which is in accordance to its specific functionality. Thus, those skilled in creating and/or modifying computer programs, would, without departing of the teachings of the present invention, readily apply them to create and/or modify computer programs which, when executed in a computer-based authentication server (3A, 3B, 23), would make it to behave according to any of the described embodiments.

The simplified internal structure shown in Fig.2 for authentication server 3A or 3B comprises: a processing module 301, a communications module 302, a data storage module 303 and one or more internal communication buses 304 which allow data communication and cooperation between them. For authentication server 23 a similar functional structure is given, comprising: a processing module 231, a communications module 232, a data storage module 233 and internal communication buses 234.

On each authentication server, each of the processing modules (301, 231) can comprise, respectively, one or more processors (illustrated, respectively on each server, as 3010 and 2310), which can be arranged to work in load-sharing or active-backup mode. Processor 3010 in AA 3A executes service logic for checking if user credentials received from a user terminal 11 connected to network 1A relate to a service account in said network, so as to allow said terminal to obtain a service from said network 1A. In what concerns the invention, the service may comprise the provision to terminal 11 of a connection through the network 1A, which may be used by terminal 11 to access to a further network (e.g. 1B or 2). A similar service logic is executed (*mutatis mutandis*) by processor 3010 in AA 3B for user terminal 12 connected to network 1B. Processor 2310 in AA 23 executes service logic for checking (directly with the user terminal, or indirectly via the cooperating access network 1A or 1B) if user credentials received for a user terminal (11, 12) relate to a service account in the network 2 before allowing the user terminal to obtain access to a telecommunications service provided by said network. The service logic executed by processors (3010, 2310) in authentication servers 3A, 3B and 23 is further enhanced with the novel functionality of the invention that shall be later detailed.

External communications in server 3A or 3B are performed through a communications module 302 that is illustrated as comprising two communication devices 3021 and 3022. For authentication server 23 a similar structure is given, wherein the communications module 232 also comprises two communication devices 2321 and 2322. The communications module allows an authentication server to exchange signaling with other server entities, including another authentication server(s), so as to accomplish with its function.

Depending on implementation alternatives, some of the communication devices (2321, 2322) of an authentication server (23) may be devoted to a specific kind of communication (e.g. only with some other server entity with which a standardized or proprietary signaling interface is used, only for a given type of communication protocol, etc). Also, some of said communication devices may be suited to allow any kind of communication that may be handled between the authentication server (23) and another server entity (24, 25, 22), including another authentication server (3A, 3B). RADIUS protocol (IETF RFC2865, June 2000) or DIAMETER protocol (IETF RFC3588, September 2003) are example of communication protocols that are commonly used by authentication servers (3A, 3B, 23) to communicate with other server entities in a telecommunications network (such as access servers or even another authentication servers) and that can be easily extended, which allow them to convey new messages and/or new or modified contents for new kind of applications. In any case, the number of communication devices (e.g. 3021, 3022) in the communications module (302) of an authentication server (3A) may vary according to their respective capacity for handling signaling to/from another server entities compared with the overall signaling estimated for the authentication server (3A). Depending also on implementation details, the communications module (e.g. 302) of an authentication server (3A) may comprise some functional or physical elements (hardware, software or combination) that may be common to one or more communication devices (3021, 3022), such as a part of a given communications protocol stack, being the other (protocol specific) parts residing on the corresponding communication device.

Data storage modules 303 and 233 store data needed for the operation of, respectively, authentication server 3B (or 3A) and 23. Each data storage module may comprise one or more data storage devices (illustrated as 3031 and 3032 for servers 3A or 3B, and 2331 and 2332 for server 23), which may comprise memory chips, magnetic or optical discs, etc, and combinations thereof; wherein the data storage module (233) of an authentication server (23) may incorporate one or more storage devices (2331, 2332) of the same or different kind according to different implementation criteria, such as data access speed required or the reliability desired for certain stored data. According to alternative realizations, the data storage module of an authentication server can reside within the same physical machine, or can be distributed. For example, computer readable program code that may be needed to control the operation of the authentication server 23 as well as temporary data storage of dynamic information (e.g. information related to currently registered user terminals) may reside within the same physical machine hosting the processor(s) of the processing module, while some other data, such as part or all of subscriber data, may be stored in another machine, such as an external database (not shown in Fig.1), and obtained/updated remotely.

Regardless physical data distribution details Fig.2 illustrates schematically some of the data that can be handled by authentication servers 3A or 3B, and authentication server 23, which shall now be described. In Fig.2 all the illustrated data (303-1, 303-2, 233-1, 233-2, 233-3) appear as belonging to the corresponding storage module (303, 233); however, as commented above, for a particular authentication server this not implies that all these data belong to its own storage means.

The operation of, e.g., authentication server 3B is controlled by computer-readable program code 303-1 comprising instructions (CI-11..., CI-1N) that, when executed by processor 3010, make authentication server 3B to perform as described heretofore, and also performing new functions according to embodiments of the invention. Similarly, the operation of authentication server 23 is controlled by computer-readable program code 233-1 that comprises instructions (CI-21..., CI-2N) adapted to be executed by processor 2310 so as to perform the aforementioned functions and also new functions according to embodiments of the invention, which shall be later described.

In Fig.2, reference 303-2 represents the set of data that constitute the service accounts of, e.g., subscribers of network 1B, and reference 233-2 the service accounts of subscribers of network 2. As mentioned earlier, data related to a service account may be dynamically provided within the telecommunications network upon subscription of the service account. Alternatively, some of said data may be already preset with some values (e.g. from default subscription data templates), wherein a particular service account could be marked as "idle" while not yet subscribed by any user, and then marked as "active" upon account subscription from a user. This is illustrated in Fig.2 with respect to network 2, wherein service accounts 233-2 would represent active service accounts, and service accounts 233-3 would represent idle service accounts which, according to an embodiment of the invention, may be assigned in telecommunications network 2 upon requests from another telecommunications network (e.g. 3B, 3A), e.g. by setting the necessary further data on them, so as to set them as active (subscribed) service accounts; namely, as if they were service accounts subscribed directly by the users.

Fig.2 also illustrates the content of a generic service account SA-1N in, e.g., network 1B, and a generic service account SA-2N (or SA-2M) in network 2. It shall be noticed that the illustration does not intend to refer to any particular storage data structure for keeping in relationship the relevant data of a particular service account, an implementation detail which is not relevant for the invention.

The data in the service account of a subscriber in a given telecommunications network may vary according to a plurality of factors such as: the nature of the services provided by said network (e.g. if they may be served to any subscriber without restriction and/or personalization, or not), the nature of the access that can be utilized from user terminals (e.g. if said terminals are always connected to the same access point, or if the access point may vary), and also depending on the operator of the network (e.g. two cellular operators owning different cellular networks may store some different data). Accordingly, the following description concerning the data content of the service accounts in networks 1A or 1B, and 2 shall be given considering the data content that can be relevant for illustrating embodiments of the invention, as well as some new data which, according to it, may also be advantageously stored in relationship with a service account.

If, as mentioned earlier, pre-defined service accounts are assigned upon user subscription, or upon request from another network, one data that can be stored in relationship with a service account may be the account status AST, which may store a value indicating whether the service account is in fact active or idle, and which can advantageously be used to determine in a given moment whether the data in the service account are usable to provide or grant access to a service which is subject to the subscription of a service account. If a user terminal (11, 12) is not supposed to be always connected (directly or indirectly) to a telecommunications network (1A, 1B, 2), but it is expected that the terminal may dynamically attach/detach to it or, more generally, when said terminal may dynamically register/deregister in one, or more, telecommunications networks, then, information about the registration status RST of a user terminal for a particular subscription may also be stored in relationship with other data in the corresponding service account. The registration status RST can be used to determine, for example, whether an incoming service (e.g. an incoming call or multimedia session, data pushed from an application server, etc) may be delivered to the corresponding user terminal, or shall be treated in other way, and can also be usable to start the execution of some actions from the authentication server (3A, 3B, 23) depending on its value (e.g. depending on whether the terminal is registered, registering or unregistered).

For allowing e.g. user terminal 12 to access to telecommunications network 1B, user credentials CX1 are stored in relationship with the corresponding service account so as to authenticate it before granting access to a service provided from (by or through) network 1B. Similarly, if a user from a user terminal (11, 12) intends to access a service subject to user subscription from network 2, user credentials CX2 to assert the existence of a service account are stored in relationship with his corresponding service account in network 2. Depending on the nature of the network, as well as on policies deployed by the operator, authentication can take place, not only when the user terminal request access to the telecommunications network (e.g. at registration), but also after a certain period of time and/or upon request of some service. In summary, a user terminal (11, 12) may be requested to authenticate when it request a service from a telecommunications network (1A, 1B, 2), since an access request message (e.g. a SIP message "register", or an equivalent access request message which request registration of a user from a terminal in a network) gives, when accepted by the receiving network, granted access to said network, which may also be considered as a service provided from said network.

A service account may comprise some dynamic data which can be relevant when a user terminal is connected to network 1A or 1B. For example (as illustrated for the generic service account SA-1N), the service account related to a registered (attached) terminal 12 in network 1B can comprise a token CTK comprising information which univocally identifies said terminal in its current active connection. The token CTK can comprise, for example, a network address (e.g. an IP-address) assigned to terminal 12 and usable to communicate with servers (e.g. 4B) in network 1A, as well as with servers in other networks (e.g. 4A, 24, 25, etc). Additionally, or alternatively, the token CTK can comprise a key that may have been derived as a result of authenticating from a telecommunications network a user terminal according to a challenge-request/challenge-response authentication mechanism. For example, additional keys are derived (both: in the network and in the user terminal) from user credentials in challenge request/challenge response authentication mechanisms, such as the aforementioned SIM authentication or AKA (e.g. a "Ciphering Key" Kc is derived in SIM authentication, and "Ciphering Key" and "Integrity Key" are derived in AKA authentication). The token information CTK can be used for various purposes, such as for delivering it to a further server so as to encrypt/decrypt from there information sent/received to/from the user terminal (e.g. in case it comprises a derived key), or for delivering it to a server needing to route some data to a user terminal (e.g. in case it comprises a network address).

A service account SA-1N of a subscriber of network 1A or 1B can, according to the invention, comprise further data (MRK, IX2) that shall be referred in the following description given with reference to the flowchart of Fig.3 and to the signaling flow of Fig.4.

Fig.3 illustrates the steps of a method for providing a user terminal (11, 12) connectable to a first telecommunications network (1A, 1B) with access to a telecommunications service provided from a second telecommunications network (2) through said first network (1A, 1B).

In step 51, a service account is provided in the first telecommunications network (e.g. 1B) comprising the necessary user credentials (CX1). This allow to authenticate a user terminal (11, 12) so as to allow it to access to a telecommunications service provided by the first network (11, 12), such as the obtainment of a connection through the first network, which can allow the user terminal to communicate with servers in further telecommunications networks. Similarly, step 52 represents that a service account is provided in the second telecommunications network 2, and that the corresponding user credentials (CX2) are stored in relationship with it so as to authenticate a user terminal (11, 12) before granting it access to a service provided from the second telecommunications network. Namely, steps 51 and 52 represent the provision for a user of, respectively, a first service account SA-1N in a first network 1A or 1B, and a second service account SA-2N in a second network 2, wherein the provided service accounts comprise, at least, user credentials CX1, CX2, that allow a user terminal 11 or 12 to access to the services provided respectively by said fist and second networks.

Once the corresponding service accounts SA-1N and SA-2N have been provided, respectively, in telecommunications networks 1A or 1B and 2, a user terminal 11 or 12 connectable to a first network 1A or 1B may access to a service provided from a second network 2 through a connection provided by the first network when said terminal connects to it. Subsequent steps 53 to 56 take place when a user terminal connects to a first network and access through it to a service provided by a second network.

For example, when user terminal 12 request access to a service provided by network 1B it is authenticated from there in step 53. If the terminal 12 proves the ownership of the corresponding credentials (CX1), authentication is successful and a connection through network 1B is provided to the user terminal 12 in step 54 (e.g. if the requested service is, or involves, the provision to terminal 11 of a connection through the network 1B). The connection through network 1B can comprise, for example, the assignment of a IP-address to the terminal 12, and/or the provision of an internal communication channel between the terminal 12 and the IGW 5B and the assignment of e.g. a globally routable IP-address in relationship with said channel in the IGW 5B, which would allow (e.g. using address translation) to route information to/from the terminal, via the internal channel, to/from another external server in another telecommunications network (e.g. network 2).

Using the provided connection, the user terminal 12 may then request access to a service provided by network 2. For example, the user terminal sends a service request message to a server in network 2 which request explicitly a given service, or which request a generic access to a set of services that can be provided from network 2 (e.g. an access request message such as a SIP "register" message). Then, in step 55, authentication for user terminal 12 is carried out from network 2, which, for example, can comprise a direct interaction between an authentication server in network 2 (23) and user terminal 12, and/or an interaction between an authentication server in network 2 (23) and an authentication server in network 1B (3B), so as to assert the ownership of the corresponding credentials (CX2) before granting user terminal 12 the access to the requested service. Finally, if the user terminal 12 has been successfully authenticated, the access to the requested service is provided in step 56.

As illustrated by Fig.3, the step (52) of providing a usable service account SA-2N in the second network 2, by storing in said network 2 at least the corresponding user credentials CX2 in relationship with said service account, may by accomplished by a set of steps (522, 524, 526) that, according to the invention, can alleviate a user of having to take an active role (e.g. being personally involved in some administrative transaction) for subscribing a further service account in a further network (e.g. network 2), when he already has got a subscription in another network (e.g. network 1A or 1B).

In step 522 an identifier IX2 is selected from the first network (1B). The identifier is such that it is usable as user credentials before the second network (2). That is, the selected identifier IX2 is a data element having a format that can be accepted by e.g. authentication server 23 as user credentials for granting access to a terminal (12) to a service provided by network 2; thus, it may comprise: a single component (e.g. an arbitrary alphanumeric string, or a structured string, such as a SIP-URI as defined by IETF RFC3261, or a NAI as defined by IETF RFC2486), or a complex component (e.g. containing a first component to be used as user-identifier, and a second component to be used as password).

There are several alternative embodiments to implement the selection of step 522. For example, network 1B may store a set plurality of said identifiers (e.g. in a database belonging or accessible to AA server 3B), wherein the selection of step 522 would comprise to select an available identifier IX2 stored by the first network 1B. The plurality of identifiers that can be selected from a first network (1A, 1B) can be primarily stored by the second network 2, wherein a specific set of them, or all of them, can be made accessible for being selected from one or more cooperating first telecommunications networks (1A, 1B). In that case, a first option for making them accessible for selection to a particular cooperating first network is to send sub-sets of said identifiers from network 2 to, respectively network 1A and network 1B. A second option is that, for selecting available identifier(s), a server in a first network (e.g. AA server 3B) sends a request for one or more identifier to a server (or accessible database) in network 2 (e.g. AA server 23). In both options, by controlling the distribution or the access to the available identifiers, the second telecommunications network 2 can manage what cooperating first network can request an account association according to the invention. Furthermore, if in network 2 idle service accounts 233-3 are pre-defined (e.g. devoted for account assignation upon request from another telecommunications network), the corresponding identifiers that shall be used as credentials for said idle accounts (i.e. when they become assigned) can be stored in relationship with them; thereby, allowing to pre-define also certain (default) data in said accounts in network 2, which may vary according to the first network (1A, 1B) to which the corresponding identifier(s) is(are) made accessible. Accordingly, the access to certain services in network 2 may be advantageously controlled (e.g. barred, limited, etc) depending on the first network 1A, 1B to which the requesting user terminal 11, 12 is attached.

When an available identifier IX2 has been selected, in step 524 an account association message is transmitted from the first network (e.g. 1B) to the second network 2 comprising the selected identifier. The message requests to assign a service account in the second network 2 in relationship with said identifier IX2. At reception of the account association message, in step 526 the received identifier IX2 is stored as the corresponding user credentials CX2 in relationship with a service account assigned in network 2.

The assigned service account can be new service account SA-2N which is provided in that moment. Also, step 526 may comprise the setting in network 2 of an idle service account SA-2M as an active service account SA-2N.

In that case, the corresponding idle service account SA-2M that is to be activated (SA-2N) can be identified according to the received identifier IX2, for example, if it had been pre-stored in advance as user credentials CX2 for said idle service account SA-2M. The idle service account SA-2M could have been (pre)assigned in network 2, for example, when an available identifier IX2 was sent to, or selected by, networks 1A or 1B, as recited above.

Regardless the aforementioned embodiments for the selection made in step 522, the selected identifier(s) IX2 is (are) preferably marked as not selectable in the corresponding network (1A, 1B, 2); thereby, avoiding to associate two service accounts SA-2N in the second network with the same user credentials.

It shall be noticed that a terminal (11, 12) which can benefit from the service account provision process described heretofore (steps 522, 524, 526) does not need to be connected to the first network (1A or 1B) when said process takes place, and that it is sufficient it is arranged to connect (i.e. connectable) to it. For example, a mark for account association MRK (Fig.2) can be stored in relationship with one or more service accounts SA-1N in a first network (1A, 1B); thereby, allowing to determine whether an account association message can be sent to the second network 2 in relationship with a service account SA-1N in the first network 1B, independently on whether a user terminal (11, 12) is currently registered for said service account (e.g. status of RST within the corresponding service account). Accordingly account association messages can be sent from a first network (1A or 1B) to the second network 2, for example: as a part of a batch process performed by the first network, upon account provision/activation in the first network, or when a user terminal (11, 12) registers for a particular service account in a first network. Furthermore, a single account association message can be sent comprising a plurality of selected identifiers IX2, and requesting to assign a service account SA-2N in network 2 for each of them, wherein each identifier IX2 would become user credentials CX2 in relationship with the corresponding service account SA-2N.

An identifier IX2 that has been selected (step 522) for being sent in an account association message can be stored in relationship with a service account SA-1N in the first network 1B as the mark MRK for account association. Namely, the mark MRK for account association can comprise a single (e.g. binary) value which determines a yes/no condition for sending an account association message, or can comprise another kind of value, wherein the condition for sending or not the account association message can be the existence of a value different from a pre-defined default value. Additionally, as illustrated in Fig.2, the selected identifier IX2 (or the plurality of them, as will be later referred) may be stored in relationship with a service account SA-1N in the first network. In either case, this can allow to reuse the same identifier IX2 in situations wherein the assigned service account in the second network 2 can be revoked (as will be later detailed) and it is desirable to use the same identifier IX2 in relationship with the same service account SA-1N in a further assignation requested from the first network 1B.

Transition flow lines, marked as X-Y and U-W in Fig.3, illustrate an embodiment in which the process comprising the steps 522, 524 and 526, is performed when a terminal (11, 12) is connected to the first network (1A, 1B) and, for example, the service account identified by the credentials CX1 used for granting its access to the first network is marked MRK for account association. Accordingly, steps 522, 524 and 526, can take place after successful authentication 53 of the user terminal (as indicated by transition X-Y), or, after authentication, when a connection through the first network is provided 54 to the user terminal (as indicated by transition U-V), which, for example, can be the case if the successful authentication in network 1B involves the provision of connection through network 1B, or if the user terminal has requested explicitly said service (or a service that requires it).

Although not illustrated by the sequence of steps shown in Fig.3, step 522 can be performed for a service account SA-1N in the first network 1B before any terminal has registered for it (i.e. an identifier IX2 is selected for said service account), while steps 524 and 526 can take place when a user terminal 12 registers for it after being successfully authenticated according to the corresponding credentials CX1. Furthermore, steps 522 to 526 can take place independently of any service account in the first network 1B, wherein the identifiers IX2 that were sent in account association messages (step 524) are kept as pre-assigned in network 1B, and wherein one of them can be later assigned to a service account SA-1N in said network, for example, after successful authentication of a terminal 12 according to the credentials CX1 of said service account.

For illustrating some embodiments of the method according to the invention, Fig.4 shows a simplified signaling flow representing a user terminal 12 connecting to a first network 1B and accessing to a telecommunications service provided by an application server 25 in a second network 2 which is subject to subscription in said second network. In the depicted signaling, authentication servers 3B and 23 in, respectively, networks 1B and 2, appear as interacting directly with the user terminal 12 or between them. Similarly, some of the steps aforementioned are illustrated as performed by servers 3B and 23. However, as referred earlier, there can be more intervening cooperating servers entities which, for the sake of clarity, are not shown in Fig.4.

In addition to user terminal 12, and servers 3B, 23 and 25, storages 70 and 70B are also shown in Fig.4. Storage 70 represents a database in network 2 that stores the available identifiers IX2 that can be used as user credentials CX2 in relationship with service accounts that can be assigned in network 2 upon request of other networks (1A, 1B). Some of these identifiers, or all of them, can be made accessible to network 1B, wherein flow 601 can represent: the request for one or more of these identifiers from network 1B and the subsequent delivery from network 2, or a direct delivery of one or more of these identifiers without a previous request. Flow 601 may also represent an updating sent from network 2 to network 1B about the currently available identifiers (e.g. if some of the previously sent is no longer valid). On the other hand, storage 70B represents a database in network 1B that stores the identifiers IX2 received (or obtained) from network 2. Storages 70 and 70B can be stand-alone databases, or can respectively belong to other servers (e.g. they can respectively belong to authentication servers 3B and 23). Dots in flow 601 illustrate a possible embodiment in which any of the authentication servers (3B, 23) is involved in the obtainment/sending of identifiers IX2 between network 2 and network 1B.

In flow 602 the user terminal 12 sends an access request message to network 2. Subsequently the authentication server 3B runs in step 53 the authentication of the user terminal. Depending on factors such as the access protocols and authentication mechanism(s) supported by network 1B, the message in 602 can comprise a user identifier assigned to the user of the terminal (or an identifier assigned to the terminal) in relationship with a service account in network 1B, which can be the user credentials CX1 for said account (e.g. received in clear, or encoded according to a pre-defined key or encoding mechanism). In that case, the authentication step 53 may comprise the verification by server 3B that the received user identifier corresponds with the credentials stored in relationship with a service account in network 2. Alternatively, the received user identifier can be used by the authentication server 3B to find out the related service account and, subsequently, the corresponding user credentials CX1. In that case, the authentication step 53 can comprise the sending of a challenge to the user terminal to assert the ownership of the user credentials CX1, the reception of the subsequent challenge response, and its verification (flows not shown in Fig.4).

As described earlier, some service accounts SA-1N may have been marked MRK for account association. This is illustrated in Fig.4 by step 521 (not shown in Fig.3). Accordingly, if the user terminal 12 is successfully authenticated, the value of the mark for account association MRK is checked in the service account used by the terminal 12 on its registration. For example, the user of terminal 12 has acquired a voucher account in a sales point and, as a result of the transaction, he has been provided with e.g. a card or another kind of item bearing the corresponding user credentials CX1 to access to network

1B, e.g. during a given period of time, wherein the agreement of the acquisition comprises the right of accessing to a further telecommunications network (e.g. network 2, and/or other networks) through network 1B. On network 1B, the corresponding service account SA-1N had been marked MRK for account association, and the mark can be checked when the user attach its terminal to network 1B, as illustrated in step 523.

Although the acquisition of a single voucher for a service account can be an attractive option for occasional users, it shall be noticed that the account combination advantages that can be achieved according to the invention are not limited to the aforementioned voucher accounts (i.e. service accounts generally intended for a short-term use, and thus, being usually intended for very occasional users of the services of a telecommunications network). In fact, the service account of a pre-paid or post-paid subscriber in a telecommunications network can benefit from the combination with service accounts in further telecommunications networks by the automatic assignation process of the invention; wherein, the operator of a given network may, for example, reward some of its subscribers with a temporary subscription to a services provided by other networks that can be accessed through its network, or wherein the operator of a given network (e.g. a service provider), willing to promote some new service(s) signs service agreements with other operators which has a widely deployed access networks (e.g. network providers), so as to make some subscribers of said other operators to experience said service(s).

If the mark for account association indicates that an account association message is to be sent, then, an identifier IX2 usable as user credentials before network 2 can be selected at that point, if not selected previously for said service account SA-1N. Flow 522-a represents an embodiment referred earlier in which authentication server 3B selects an identifier from storage 70 in network 2, and flow 522-b represents another embodiment in which the identifier is selected from storage 70B in network 1B. The selected identifier IX2 is then sent in an account association message 524 to network 2, e.g. to authentication server 23), which then stores the received identifier as user credentials CX2 in relationship with a service account SA-2N that is assigned in network 2, as illustrated by step 526. It is to be noticed here that more than one identifiers IX2 can be selected to be used in relationship with a service account SA-1N in the first network 1B, each one usable as user credentials CX2 before further second networks, wherein more than one account association messages 524 could be sent; thereby allowing the user of terminal 12 to access from network 1B to the services provided from further telecommunications networks (2, 1A, etc) which are subject to subscription in said networks.

Flow 603 represents an acknowledgement message that can be sent to the user terminal 12 so as to notify the successful result of the access request (602). As referred earlier, as a result of the successful authentication, or upon a further service request, in step 54 the user terminal gets a connection through network 1B. For allowing the user terminal to use later the credentials that can be requested from network 2 when it request access to a service from there, the selected identifier IX2 can be sent within the acknowledgement 603, or can be made accessible to the user terminal 12 by other means (e.g. sent to the terminal in another message upon reception of a specific request). However, as will be later referred, the sending of the selected identifier IX2 to the user terminal 12 can be facultative, as it depends on the kind of authentication that can be requested, or accepted, by authentication server 23, which can vary depending e.g. on special mark (not shown in Fig.2) associated to service accounts assigned SA-2N upon request from a cooperating first network (1A, 1B). Nevertheless, if the selected identifier IX2 is sent (603) to the user terminal 12, network 1B can obviate the storage of the selected identifier in relationship with the corresponding service account SA-1N in said network.

The account association message 524 can comprise further data that can also be stored (step 526) in network 2 as user credentials CX2 in relationship with the assigned service account SA-2N, so as to later grant from authentication server 23 the access to a service of network 2 requested by user terminal 12 by authenticating the request made from the terminal according to any of the stored credentials. For example, the account association message can comprise credentials CX1 of the service account SA-1N in network 1B that were used to authenticate user terminal 12. Alternatively or additionally, the account association message can comprise the aforementioned connection token CTK, which can also be used as a trust token so as to allow univocal identification of the user terminal 12 connected to network 1B. The connection token CTK may thus be used as some kind of authentication artifact that can be asserted from network 1B.

For accessing to a service provided from network 2, the user terminal 12 sends in flow 604 a service request message. Depending on the nature of the telecommunications network 2, before sending a service request for one specific message, the network 2 may require that the user terminal first register on it. Therefore, as commented earlier, the message represented by flow 604 can be a service request message requesting registration. In any case, if authentication server 23 determines that there is no ongoing session authenticated for user terminal 12 (e.g. no active registration RST, a pre-determined time has lapsed from the last authorized service request, etc), authentication takes place in step 55. In a simple case, authentication 55 can be carried out in a simple manner; for example, the authentication server 23 may examine the content of the received message and check if any of its information elements comprise credentials CX2 stored in relationship with a service account SA-2N. Accordingly, the authentication server 23 may examine e.g. the IP-address corresponding to the origin of the message. Also, the user terminal can include in the request 604 a data element that were stored as credentials CX2 in step 526, such as the credentials CX1 in the network 1B, or the credentials CX2 that were received from network 1B upon successful authentication from there (step 53), or a key derived as a result of said authentication, which can be used by authentication server 23 to perform the authentication of the terminal 12. Step 55 may also comprise an interaction (not shown in Fig.4) between the authentication server 23 and the terminal 12 and/or between the authentication server 23 and the authentication server 3B. For example, step 55 can comprise the sending of a challenge to the user terminal 12 (e.g. requesting a user-identifier and/or a password, or requesting to cipher a given random string with a certain key known by the authentication server and, supposedly, known also by the user terminal) to assert the ownership of the user credentials CX2, the reception of the subsequent challenge response, and its verification. Also, step 55 can comprise a check requested from authentication server 23 to authentication server 3B about the current validity of certain data element presented by the user terminal 12 as user credentials CX2 before network 2 in the message 604.

If the authentication 55 is successful, the user terminal 12 gets granted access 56 to the service provided from application server 25.

In interworking scenarios as described herein, accounting functions can be performed in either or both telecommunications networks 1B and 2. For example, server 3B in network 1B can keep track about: the connection time spent by terminal 12, the volume of data exchanged with other servers or terminals, the services requested from network 1B, etc, and server 23 can perform similar accounting functions about the consumed services, time, data volume, etc, in respect of network 2. Also, the accounting information in both networks may be associated (e.g. as disclosed by US 2002/0191597 A1). In any case, the usage of the service account SA-2N assigned in the second network 2 may be revoked due to different reasons, such as when the service usage (either or both: in network 1B or network 2), the time elapsed from the association request (step 524), the volume of data exchanged by user terminal 12, etc, exceed a certain limit, or, for example, when the credit of the service account SA-1N used by the user terminal 12 in the network 1B (e.g. a pre-paid account or a voucher account) gets exhausted. Therefore, the initiative for the revocation is preferably taken by any of the telecommunications networks involved in the account association. Next flows in Fig.4 shows authentication servers 3B and 23 directly involved in the signaling and its processing, however, other servers in networks 1B and 2 can, additionally or alternatively, be involved in the process.

If the initiative is taken from network 1B, an account dissociation message 605-a can be sent from server 3B in network 1B to server 23 in network 2 requesting to dissociate a previously associated service account SA-2N in network 2 from the corresponding related user credentials CX2. Flow 605-b shows the case in which the initiative is taken from network 2, wherein network 1B is notified that the dissociation has been executed in network 2 with the reception of an account dissociation notification message. Instead of a different alternative, flow 605-b can also represent a confirmation from network 2 that the request made in flow 605-a has been executed by network 2. Flows 606 and 607 represent possible embodiments wherein the concerned identifier IX2 is set again as selectable for further account association in the corresponding storage(s) 70 and/or 70B.

The account dissociation message 605-a, or the account dissociation notification message 605-b, can comprise the identifier IX2 that was sent in an account association message 524. Additionally, or alternatively, it can comprise one or more of the information elements previously sent in an account association message 524, such as the selected identifier IX2, the trust token CTK, or the credentials CX1 in the first network 1B. In the first case, the content of message received by network 2 in flow 605-a can be used to identify in step 528 the concerned service account SA-2N and to unbind in network 2 the relationship established between the selected identifier IX2, or any other information element received (524) as credentials CX2 for the assigned service account SA-2N, and said service account SA-2N. Also, step 528 may comprise the setting of the concerned service account SA-2N back as an idle service account SA-2M. In the second case, the content of message received by network 1B in flow 605-B may be used in step

529 to identify, if proceeds, the concerned service account SA-1N in network 1B; for example: if a terminal is registered for it and is to be notified, if it is desirable to remove the stored mark MRK or identifier IX2 stored in relationship with the concerned service account SA-1N, etc, and, in general, whenever it is needed to obtain a data stored in relationship with said service account. However, the mark for account association MRK can be kept in relationship with the concerned service account SA-1N in the first network 1B, which can allow a further service account association in the network 2 using the same or a different identifier IX2 as user credentials CX2.

The invention has been described in respect to some exemplary embodiments in an illustrative and non-restrictive manner. Variations can be readily apparent to those of ordinary skill in the art. For this reason, the invention is to be interpreted and limited in view of the claims.

CLAIMS

1. A method for providing a user terminal (11, 12) connectable to a first telecommunications network (1A, 1B) with access to a telecommunications service provided from a second telecommunications network (2) through said first network, comprising the steps of:

a) storing (51) in the first network first user credentials (CX1) in relationship with a first service account (SA-1N) in said first network, and

b) storing (52) in the second network second user credentials (CX2) in relationship with a second service account (SA-2N) in said second network,

the first user credentials usable to authenticate (53) a user terminal for allowing said terminal to obtain a connection through the first network, and the second user credentials usable to authenticate (55) a user terminal for allowing said terminal to obtain access to the telecommunications service;

CHARACTERIZED in that the step "b" comprises the steps of:

b1) selecting (522) from the first network an identifier (IX2) usable as user credentials before the second network,

b2) transmitting (524) from the first network to the second network an account association message comprising the selected identifier (IX2) and requesting to assign a service account in said second network for said identifier, and

b3) storing (526) in the second network the selected identifier (IX2) as user credentials (CX2) in relationship with a service account assigned in said second network for allowing a user terminal connected to the first network to obtain access to a telecommunications service provided from the second network.

2. The method of claim 1, further comprising the steps of:

c) storing (70) in the second network a plurality of identifiers (IX2), each usable as user credentials (CX2) before said second network, and

d) storing (601, 70B) accessible to the first network at least a set of said plurality of identifiers,

and wherein the step "b1" comprises the step of selecting (522-a, 522-b) said identifier from said set of identifiers.

3. The method of claim 1, wherein said identifier (IX2) identifies an idle service account (SA-2M) in said second network, further comprising the step of:

e) setting (526) in the second network said idle service account (SA-2M) as an active service account (SA-2N) at reception of the account association message.

4. The method of claim 1, further comprising the steps of:

f) storing (521) in the first network a mark for account association (MRK) in relationship with a service account (SA-1N) in said first network, and

g) checking (523) that said mark exist before executing the step "b2" for said service account.

5. The method of claim 4, wherein the step "f" comprises the step of storing in the first network the selected identifier (IX2) in relationship with said service account (SA-1N).

6. The method of claim 4, wherein the account association message further comprises first user credentials (CX1) related to said service account (SA-1N).

7. The method of claim 1, wherein the step "b2" takes place after the step of:

h) receiving (602) in the first network an access request message from a user terminal (12) connected to said first network.

8. The method of claim 7, wherein the account association message further comprises a trust token (CTK) identifying univocally said user terminal (12) connected to said first network.

9. The method of claim 8, wherein the trust token comprises a network address assigned to the user terminal for communicating with the second network through the first network.

10. The method of claim 8, wherein the trust token comprises a key shared between the first network and the user terminal.

11. The method of claim 10, wherein the shared key has been established between the user terminal and the first network as a result of authenticating (53) first user credentials (CX1) related to a first service account (SA-1N) in said first network according to a challenge request and challenge response authentication mechanism.

12. The method of claims 6 or 8 further comprising the step of:

i) storing (526) in the second network at least said first user credentials or at least said token as user credentials in relationship with the assigned service account (SA-2N) in said second network.

13. The method of claims 1 or 12 further comprising the step of:

j) checking (55) in the second network a service request message (604) received from a user terminal

(12) according to at least one data element selected from: said selected identifier (IX2), said first user credentials (CX1) , and said trust token (CTK), before granting a telecommunications service requested in said request message.

14. The method of claims 1, 6 or 8, further comprising at least one step selected from:

k1) transmitting (605-a) from the first network to the second network an account dissociation message requesting to dissociate a service account (SA-2N) assigned in said second network upon request from said first network, and

k2) transmitting (605-b) from the second network to the first network an account dissociation notification message notifying the dissociation of a service account (SA-2M) assigned in said second network upon request from said first network,

the account dissociation message or the account dissociation notification message comprising at least one data element selected from: said selected identifier (IX-2) , said first user credentials (CX1), and said trust token (CTK),

and further comprising the step of,

l) unbinding (528) in the second network the relationship established between said selected identifier, said first user credentials, or said trust token, and the assigned service account (SA-2M).

15. Apparatus (3A, 3B) for controlling from a first telecommunications network (1A, 1B) the access of a user terminal (11, 12) to a telecommunications service provided from a second telecommunications network (2) through said first network, the apparatus comprising a processor (3010) and a storage device (3031) in

communication with said processor and storing instructions (303-1) adapted to be executed by said processor to:

- check (53) if user credentials received from a user terminal (12) connected to the first network relate to a service account (SA-1N) in said first network for allowing said terminal to obtain a connection (54) through the first network;

CHARACTERIZED in that the storage device further stores instructions adapted to be executed by said processor to:

- select (522) from the first network an identifier (IX2) usable as user credentials (CX2) before the second network, and
- transmit (524) from the first network to the first network to the second network an account association message comprising the selected identifier (IX2) and requesting to assign a service account (SA-2N) in said second network for said identifier.

16. The apparatus of claim 15, wherein the storage device further stores instructions adapted to be executed by said processor to:

- store (521) in the first network a mark for account association (MRK) in relationship with a service account (SA-1N) in said first network, and
- check (523) that said mark exist before transmitting the account association message for said service account.

17. The apparatus of claim 15, wherein the storage device further stores instructions adapted to be executed by said processor to further include in an account association message at least one data element selected from:

- user credentials (CX1) related to a service account (SA-1N) in the first network, and
- a trust token (CTK) identifying univocally a user terminal (12) connected to said first network.

18. The apparatus of claims 15 or 17 wherein the storage device further stores instructions adapted to be executed by said processor to:
 - transmit (605-a) from the first network to the second network an account dissociation message requesting to dissociate a service account (SA-2N) assigned in said second network upon request from said first network,
 the account dissociation message comprising at least one data element selected from: said selected identifier (IX2), said user credentials (CX1) related to a service account in the first network, and said trust token (CTK).

19. Apparatus (23) for controlling from a second telecommunications network (2) the access of a user terminal (11, 12) to a telecommunications service provided from said second network, the apparatus comprising a processor (2310) and a storage device (2331) in communication with said processor and storing instructions (233-1) adapted to be executed by said processor to:
 - check (55) if user credentials (CX2) received in the second network for a user terminal (12) connected to a first telecommunications network (1B) relate to a service account (SA-2N) in the second network for allowing said terminal to obtain access (56) to the telecommunications service;

CHARACTERIZED in that the storage device further stores instructions adapted to be executed by said processor to:

- process the reception from the first network of an account association message (524) comprising a selected identifier (IX2) and requesting to assign a service account (SA-2N) in said second network for said identifier, so as to store (526) in the second network the selected identifier as user credentials (CX2) in relationship with a service account assigned in said second network for allowing a user terminal connected to the first network to obtain access to a telecommunications service provided from the second network.

20. The apparatus of claim 19, wherein the account association message further comprises at least one data element selected from:

- user credentials (CX1) related to a service account (SA-1N) in the first network, and
- a trust token (CTK) identifying univocally a user terminal (12) connected to said first network,

and wherein the storage device further stores instructions adapted to be executed by said processor to:

- store (526) in the second network at least said received user credentials or at least said received token as user credentials (CX2) in relationship with the assigned service account (SA-2N) in said second network.

21. The apparatus of claims 19 or 20, wherein the storage device further stores instructions adapted to be executed by said processor to:

- check (55) a service request message (604) received from a user terminal (12) according to at least one data element selected from: said selected identifier (IX2), said received user credentials (CX1), and said received trust token (CTK), before granting a telecommunications service requested in said request message.

22. The apparatus of claims 19 or 20, wherein the storage device further stores instructions adapted to be executed by said processor to:

- process the reception from the first network of an account dissociation message (605-a) requesting to dissociate a service account (SA-2N) assigned in said second network upon request from said first network and comprising at least one data element selected from: said selected identifier (IX2), said user credentials (CX1) related to a service account in the first network, and said trust token (CTK), so as to unbind (528) in the second network the relationship established between said selected identifier, said received user credentials, or said trust token, and the assigned service account (SA-2N).

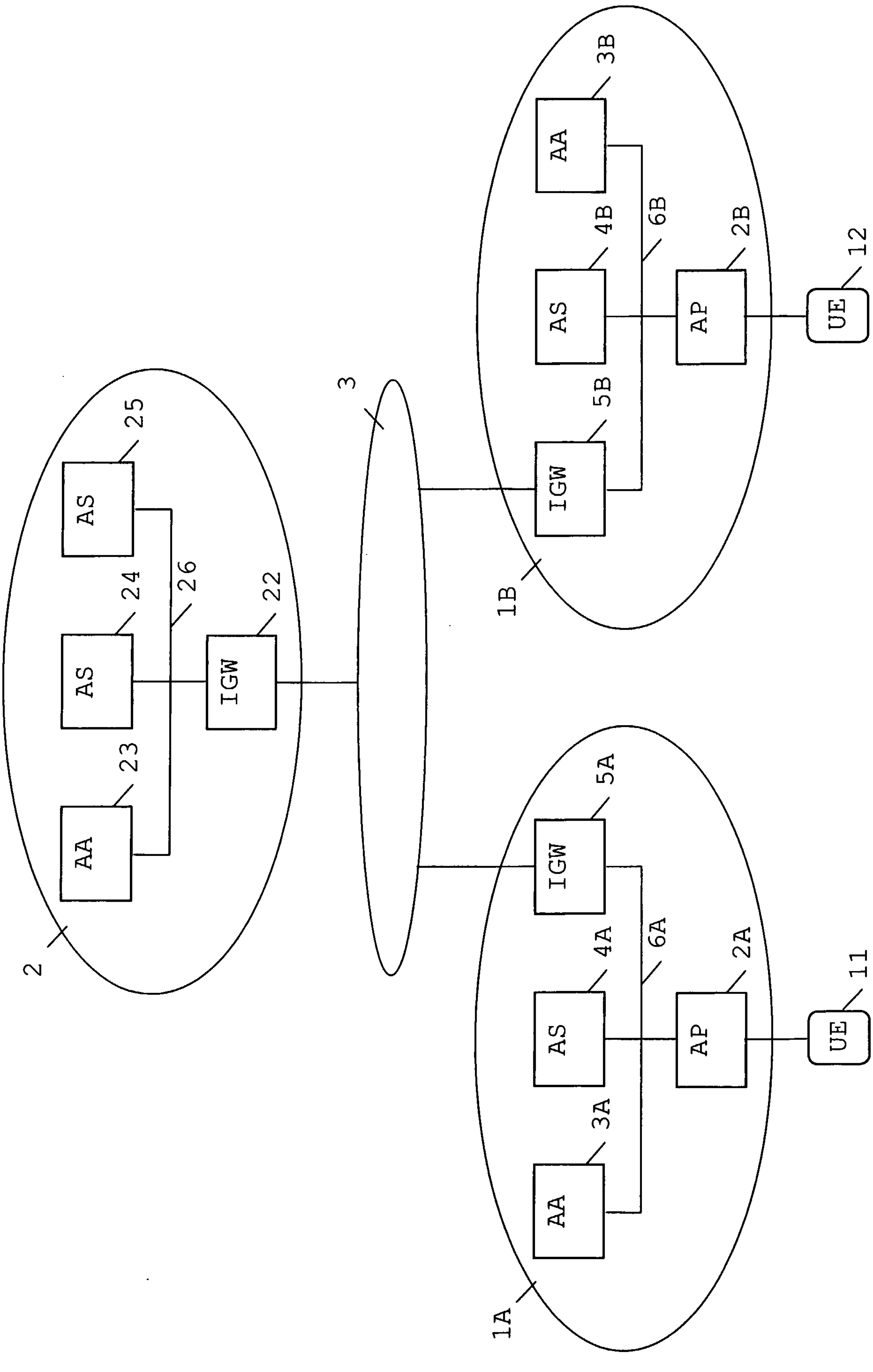

2
AA
23
AS
24
AS
25
26
IGW
22
3
1A
AA
3A
AS
4A
6A
IGW
5A
AP
2A
UE
11
1B
IGW
5B
AS
4B
6B
AA
3B
AP
2B
UE
12

Fig.1

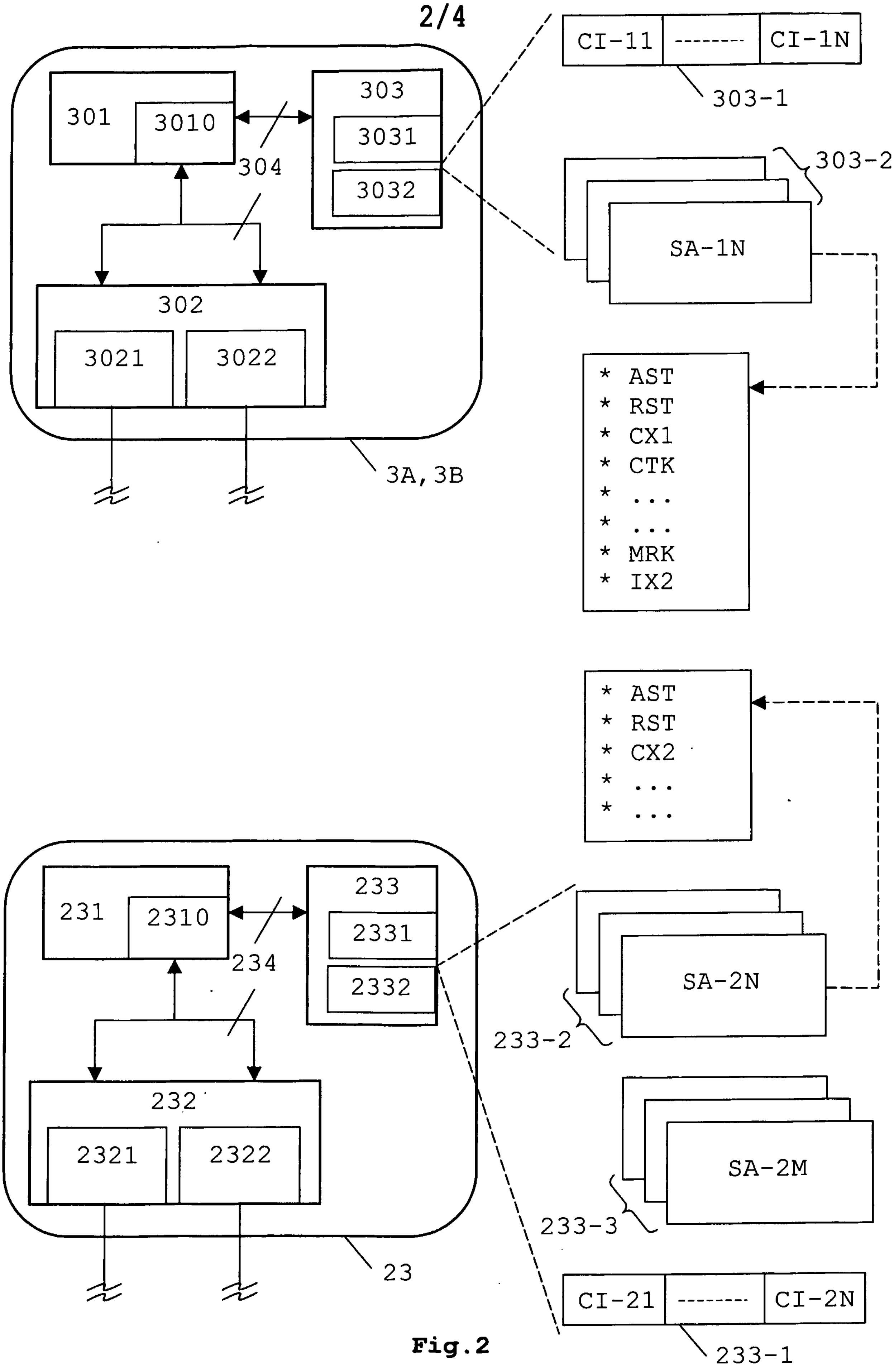

301
3010
303
3031
3032
304
302
3021
3022
3A, 3B
CI-11
CI-1N
303-1
303-2
SA-1N
* AST
* RST
* CX1
* CTK
* ...
* ...
* MRK
* IX2
* AST
* RST
* CX2
* ...
* ...
231
2310
233
2331
2332
234
232
2321
2322
23
SA-2N
233-2
SA-2M
233-3
CI-21
CI-2N
233-1

Fig.2

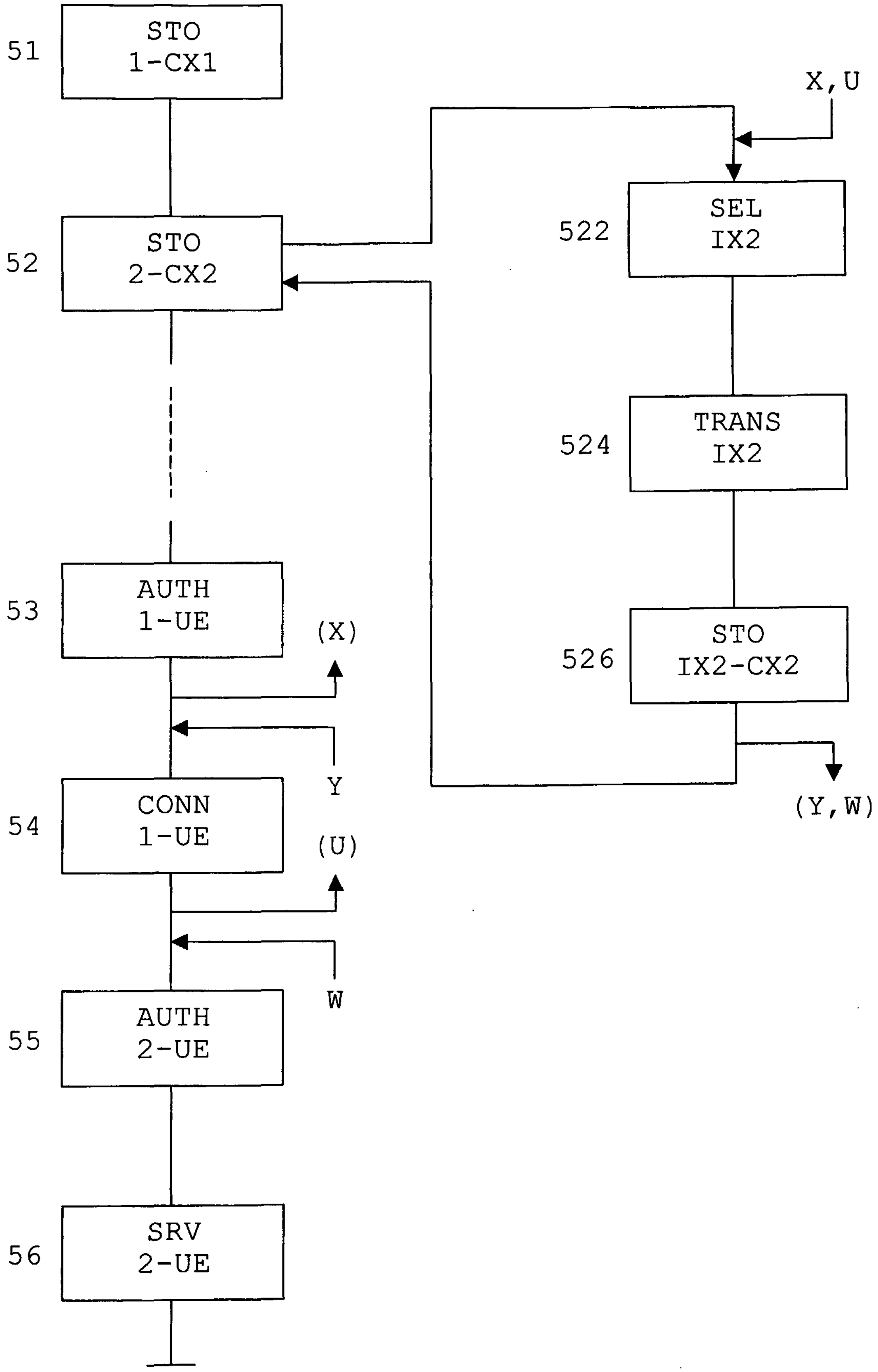

51
STO
1-CX1
X,U
52
STO
2-CX2
522
SEL
IX2
524
TRANS
IX2
53
AUTH
1-UE
(X)
526
STO
IX2-CX2
Y
(Y,W)
54
CONN
1-UE
(U)
W
55
AUTH
2-UE
56
SRV
2-UE

Fig.3

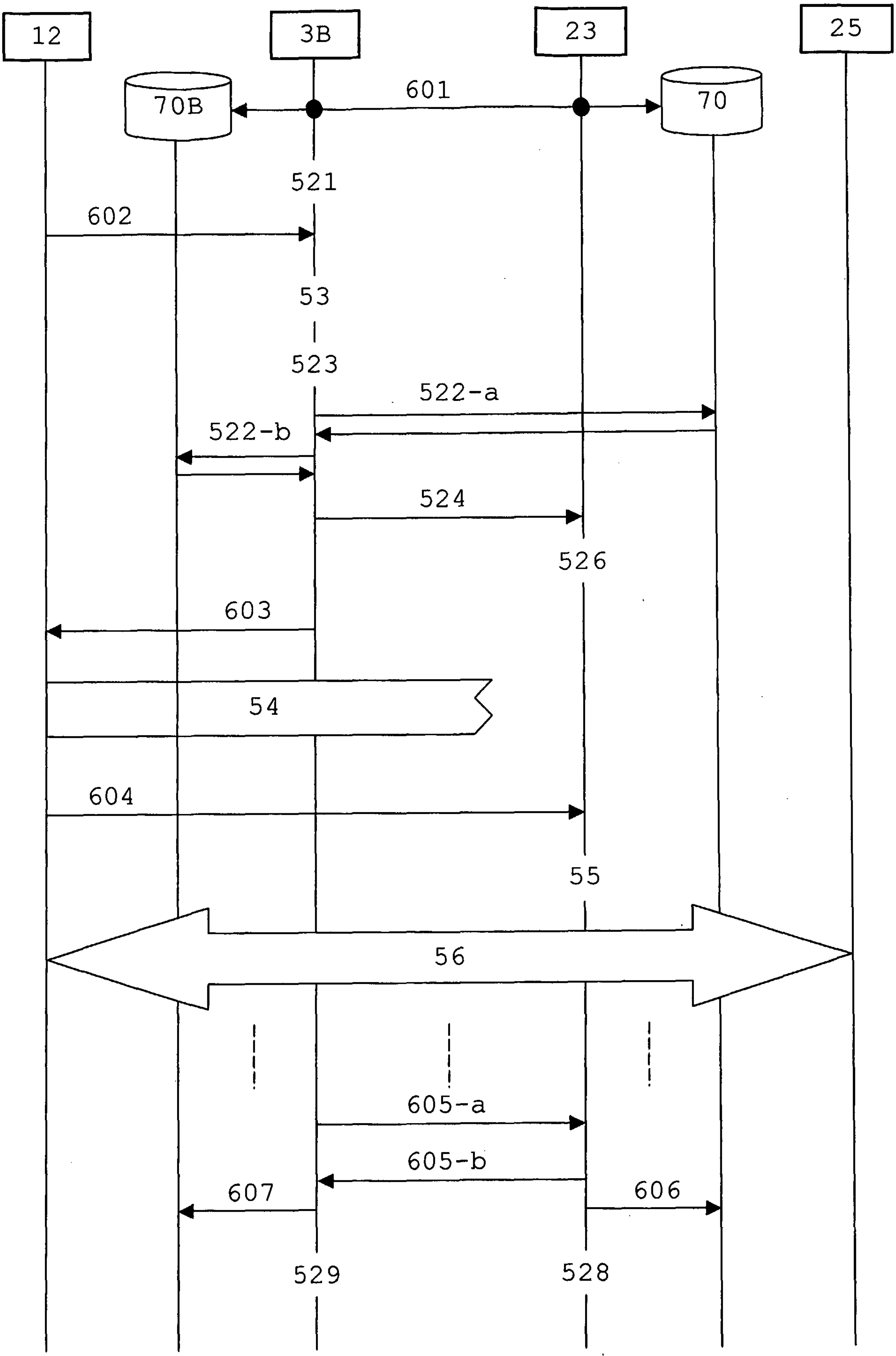

12
3B
23
25
70B
601
70
521
602
53
523
522-a
522-b
524
526
603
54
604
55
56
605-a
605-b
607
606
529
528

Fig.4