PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
G06F 1/00, H04L 29/06, G07F 7/08	A1	WO 99/44114
		(43) International Publication Date: 2 September 1999 (02.09.99)

(21) International Application Number: PCT/EP99/00763

(22) International Filing Date: 5 February 1999 (05.02.99)

(30) Priority Data:
980427 25 February 1998 (25.02.98) FI

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor: TURTIAINEN, Esa; Kartanonkuja 8 H, FIN-02360 Espoo (FI).

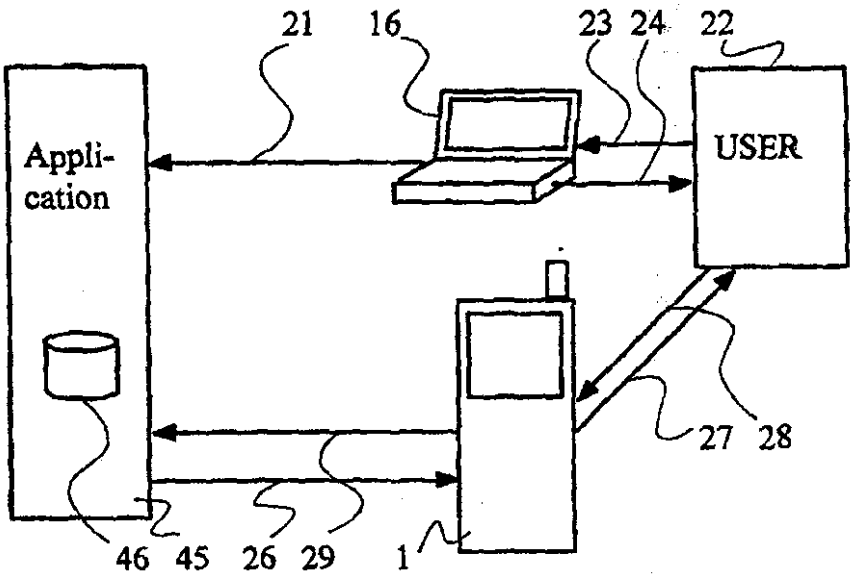
(74) Agent: BORENIUS & CO. OY AB; Kansakoulukuja 3, FIN-00100 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

修改页 图
7900+8200+100

(54) Title: METHOD, ARRANGEMENT AND APPARATUS FOR AUTHENTICATION THROUGH A COMMUNICATIONS NETWORK



(57) Abstract

A method, arrangement and apparatus for providing an authentication to an application provided through a communications network. A connection is established between the application and a user interface through said communications network so as to enable an access of a user to the application. An authentication is provided to said application by means of a mobile station communicating through a mobile communications network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD, ARRANGEMENT AND APPARATUS FOR AUTHENTICATION THROUGH A COMMUNICATIONS NETWORK

FIELD OF THE INVENTION

The present invention relates to a method for providing an authentication to an application. The invention relates further to an arrangement for providing an authentication to an application and further to an apparatus to be used in the authentication.

BACKGROUND OF THE INVENTION

Various electronic applications exist which involve a need for an authentication. Authentication may be required, for example, when a user is accessing a specific application and/or when a user already uses an application and there arises a need to verify the user or to receive such an acknowledgment from the user which allows the application to make some further proceedings.

Examples of applications which might require an authentication include various commercial services obtained through communications networks, such as Internet, Intranet or Local Area Networks (LAN), payments and banking services accessed through communications networks, resource access, remote programming, reprogramming or updating of software etc. Even certain free of charge services obtained through a communications networks may require an authentication. The amount of services or applications which require at least some degree of authentication of the user who is trying to access them (or of the user who is already using them but where there is a need to check authorisation during the use of the service or a need to acknowledge something during the use) has increased greatly during the past years. The need for the authentication is also expected

to increase further in the future.

At present there are already some well known solutions for communication authentication. These normally use various cryptographic techniques between two communicating computer devices. According to a basic scenario for the authentication, a random challenge is given to encryption functions of said two computer devices. Both of these computers have a secret, ie. an encryption key, which is also given to the encryption function in both of the computers. Thereafter, the results of the calculations of the two encryption functions are compared, and if the result of the comparison is positive, the authentication is considered as being in force. If the comparison gives a negative result, then the authentication test is considered as having failed.

There are also various already existing authentication arrangements. The following examples of the prior art arrangements are given with a brief description of some of the drawbacks thereof:

Passwords. At present, the use of a password or several passwords is the most often used approach for the authentication. The password is given to the remote application through an user interface, eg. through a computer terminal connected to a communications network. However, this solution does not take the vulnerability of the network into account, since the password is exposed to everyone who has access to the network (and who is skilled enough to read the passwords).

A secret. This may be described as an electronic password or a signature or an encryption key which is stored and used by for example the user interface. Even though the secret is not revealed to the network, it may

end up in the "wrong hands" and could be used by some party other than those who are originally intended to be the users of the secret.

Authentication software in the user interface. This is a more sophisticated approach to authentication. The password is given to a program in the user interface, which then automatically authenticates cryptographically access to the requested application. Even though this provides a more secure arrangement than the above solution, it still leaves a possibility for catching the passwords from the user interface. It is also possible to modify the software without notice to the actual user.

Smart cards with associated readers. A smart card is capable of communicating encrypted challenge-response messages, but it does not contain a user interface for receiving an authorization from the user itself. Such an interface may exist in the smart card readers, but such readers must be well protected against any possibilities for misuse, and thus the ordinary users (ie. the large majority of users, ie. the public) cannot usually have physical access to these reader interfaces, but they have to trust to the organization providing the smart cards. In addition, the smart card readers cannot be shared between organizations which do not have trust to each others.

Smart cards with a user interface. These do already exist, but they are expensive since each security processor must have a secure user interface of it's own. These are rare and the input/output capability thereof is still extremely limited, and thus they are not held to be an economically suitable solution for the authentication problem.

A separate personal authentication device. In this approach the user is used as "a communication means" between the user interface and a separate authentication device. The user interface gives a challenge which the user then types in to a hand held authentication device (pocket-calculator like device). The authentication device may, eg. give a number as a response, and the user then types this number in to the user interface. In this the problems relate to the need of purchasing, using and carrying a separate device. In some instances there is also a possibility of incorrect typing of the usually long and complex character strings.

The above already mentions some parties which may be involved when implementing the present authentication systems. They are briefly explained in more detail in the following:

The user is usually a human being who uses various applications or services. The user can be identified by means of a password (or secret) which is only known by him/her (a public key method), or by means of a secret which is shared between the user and the application (a secret key method).

The application is the party that wants to ensure the authenticity of the user. The application can also in some occasions be called as a service. From the application's point of view the authenticity question can be divided in four different categories (questions): 1) is the user at the moment in the other end? (so called peer-entity-authentication), 2) are the further messages received from the same user? (integrity of the message stream), 3) does a specific message originate from a certain user? (data origin authentication), and 4) is the message such that even a third party may believe it to

originate from a certain user? (non-repudiation).

The user interface is the device or arrangement which enables the user to access the application or service. In most instances it can also be referred to as a terminal, and may consist of devices such as computers (eg. Personal Computer, PC), workstations, telephone terminals, mobile stations such as mobile telephones or radios or pagers, automatic money teller and/or banking machines, etc. The user interface provides input/output facilities and it may possibly even provide a part of the application.

The Personal Authentication Device (PAD) is a piece of hardware that the user carries with him. The PAD may have some basic input/output functionality and even some processing facilities. The above referred smart cards and separate authentication devices may also be considered as PADs. In most cases the user can rely on his PAD, since the user has it (almost) always with him and thus under continuous control. All the possible passwords or secrets are hidden in the hardware thereof such that there is no easy manner to reveal them. The device itself is not easy to modify such that the communication path between the user and the security processor could be endangered. In addition, the PADs usually have a minimum amount of stored state and the programs thereof are not easily modifiable.

SUMMARY OF THE INVENTION

Even though the above described prior art solutions for authentication already exist, there are still some shortages, in addition to those already referred to above, in the area of authentication.

In case the access to the application is made absolutely

secure, or as secure as possible, the application easily becomes extremely complex from the architecture thereof, and becomes also complicated and more time consuming to access and use. The increased security level increases the amount of the required hardware and software, which leads to an increased need for maintenance and updating thereof, and thus the total costs of the authentication may become high. The complexity and costs could be decreased by lowering the level of security, but this is expected to lead to an insufficient security level in the communications. In addition, it is believed that an "absolutely secure" condition does not even exist in the communications networks, as the technical development makes it possible for hackers to solve even the most complicated security arrangements.

A human problem lies on the fact that the passwords or secrets may become quite complicated and/or too long, or that there may be too many of them. Thus the users may find it hard to remember them. Typically a secret which is considered as secure in the secret key method is 128 bits and in the public key method it is 1024 bits. For most people it is impossible to remember this kind of key.

In addition, users are not able to perform the calculations required in the authentication without external devices. As was explained above, the basic authentication is often made by challenge and response method. This would require the user (ie. a human) to encrypt something with his secret. This is not held to be possible in practice.

In addition to the possibility of catching the password or secret during it's transmission over an open communications network as was discussed above, today's solutions do not pay sufficient attention to the

vulnerability of the user interfaces either. The terminal devices have developed to be full of complex technology and software such that most of the users are no longer capable of fully controlling the terminals, or understanding the operation thereof. In addition, it often occurs that many users share the same terminal device (eg. is a commonly used PC) and/or that external maintenance personnel has access to the computers of a *per se* closed organization.

The computer terminals contain stored state and programs in the memory means thereof, which can be modified. In modern computers it is possible to modify the software thereof even such that the user does not notice this, and even through the communication paths without any physical access to the device itself. To give an example of the risks, it is possible to modify a program in a computer terminal such that it modifies the data the user sends for example to a bank such that the computer modifies all bank transfers on a certain day to another account than what was designated by the user. This modifying or reprogramming without notice may cause serious and huge damages when used against ordinary individual users, and especially when used against organizations such as companies or public administration. This all means that the ordinary terminal devices and communication paths cannot be trusted.

Therefore it is an object of the present invention to overcome the disadvantages of the prior art solutions and to provide a new type of solution for authentication.

An object is also to provide a method and an arrangement by means of which a user who wishes to access an application can be authenticated in a more secure manner

than has been possible in the prior art. An object is also to provide an authentication when a need for the authentication arises during the use of an already accessed application.

An object of the present invention is also to provide a method and arrangement by means of which a mobile station can be utilized in the authentication.

An additional object of the present invention is to provide a solution in which an identification module of a mobile station can be utilized in the authentication.

Other objects and advantages of the present invention will be brought out in the following part of the specification taken in conjunction with the accompanying drawings.

The objects are obtained by a new method for providing an authentication to an application provided through a communications network. According to the present invention a connection between the application and a user interface through said communications network is established so as to enable an access of a user to the application provided through the communications network, while an authentication to said application is provided by means of a mobile station communicating through a mobile communications network.

According to one further embodiment the authentication method comprises a step of establishing a connection between an application and a user interface through a communications network so as to enable an access of a user to the application provided through the communications network. The authentication to said application is provided by means of a mobile station such that a secret of a Subscription Identification Module (SIM) of the

mobile station is utilized in encryption operations of the authentication.

The invention provides further an arrangement for providing an authentication to an application provided by an application provider through a communications network. The arrangement comprises a user interface and a connection between the application and the user interface through said communications network so as to enable use of the application. The arrangement further comprises means for authenticating the use of the application, wherein said means for authenticating comprise a mobile station communicating through a mobile communications network and a link between the application implemented by the communications network and the mobile communications network.

According to an alternative embodiment the invention provides a mobile station for providing an authentication to an application provided through a communications network. In this embodiment the application is accessed by means of a user interface connected to the communications network, while said mobile station is using a different communications network for the communications than the user interface. Said mobile station is used for authenticating the use of said application accessed by the user interface.

Several advantages are obtained by means of the present invention, since the solution introduces a new reliable manner for authentication. The inventive authentication method and arrangement is easy to implement in already existing communications networks without any excessive alternations or additional devices. The arrangement can be used in connection with various different applications, in practice in connection with any such application

provided through a communications system which needs some kind of authentication.

The user is freed from carrying a separate authentication device (PAD) or many different authentication devices. The user can also trust to the personal authentication device (PAD) according to the present invention, as the mobile station is usually always with him, and the users tend to take good care of their mobile stations. In addition, for instance in case of theft of a mobile station, the mobile subscription and/or the SIM thereof can be easily canceled by the operator. All secrets of a mobile station are well hidden in the hardware thereof such that it is not easy to reveal them. In addition, the mobile station device itself is not easily modifiable in such a way that the communication path between the user and the security processors could be endangered.

The system includes a minimum amount of stored state and the programs are not easily modifiable. The existing SIM of a mobile station, and more precisely the secret thereof, can be utilized for the required encryption procedures. Thus the SIM can be utilized as a security card for new purposes, and there is already an existing party who will control the use of the SIM, ie. the mobile network operator who can immediately cancel a SIM if fraud is suspected.

In the following the present invention and the other objects and advantages thereof will be described by examples with reference to the annexed drawings, in which similar reference numerals throughout the various Figures refer to similar features. It should be understood that the following description of the invention is not meant to restrict the invention to the specific forms presented in this connection but rather the present invention is meant

to cover all modifications, similarities and alternatives which are included in the spirit and scope of the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a general view of one possible arrangement of communications networks in which it is possible to implement the present invention;

Figure 2 is a schematic presentation of an embodiment for authenticating a user according to the present invention;

Figure 3 discloses schematically one possible mobile station and an embodiment of the present invention;

Figures 4 and 5 disclose flow charts according to two embodiments of the present invention;

Figure 6 discloses an alternative embodiment for the authentication in accordance with the present invention; and

Figure 7 is a schematic presentation which relates to a further embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic representation of one network arrangement which can be used when implementing the present invention. The arrangement of Figure 1 comprises a Public Switched Telephone Network (PSTN) which is schematically shown as a box designated by 20. The exemplifying PSTN is a fixed line telephone network (or Plain Old Telephone Service, POTS), which forms a communications network through which a user interface 16

is enabled to access an application. According to this embodiment a user (not shown) may use the user terminal 16 connected to the PSTN as a user interface to access to the desired service in one of the WWW servers 45 obtainable through an Internet connection. The disclosed terminal 16 is a personal computer (PC), but other types of user interfaces, such as workstations, automatic public teller machines etc. may also be used.

A Public Land Mobile Network (PLMN) is also disclosed. This may be, for example, a cellular telephone network or similar mobile communications system. Two mobile stations MS 1 and MS+PC 2 are also disclosed. The MS+PC 2 may be defined as an integrated mobile phone and a portable computer. Both of these are capable of communicating through an air interface 3 with the PLMN through one of several base stations (BS) 4 of the PLMN.

One type of PLMN is a digital GSM network (GSM; Global System for Mobile Communications), which is well specified in the GSM recommendations by ETSI (European Telecommunications Standard Institute), the network architecture thereof being described in detail in recommendations GSM 01.02 or GSM 03.02 or the revised versions thereof. It is to be noted that while the invention is mainly described in the context of an exemplifying cellular telephone network using GSM terminology, those skilled in the art will appreciate that the present invention can be implemented in any mobile system. Furthermore, it is to be noted that for clarity reasons only those parts of a mobile network structure are shown which are considered as necessary for the purposes of illustrating the operation of the exemplifying system. The skilled person is well aware of the fact that the telephone networks may normally comprise also other necessary apparatus than those illustrated, that some the

disclosed elements of the PLMN or PSTN may be omitted or replaced by some other type of elements, and that a great number of mobile networks and ordinary fixed land line networks may cooperate and interchange with each other. The skilled man understands also that the connection to the Internet may also be a direct connection without any PSTN or similar network arrangement between the user terminal 16 and the Internet 43. These alternatives are, however, not shown and explained in more detail as they are known to skilled man in the art.

The GSM based public land mobile network (PLMN) usually includes several mobile service switching centers (MSC) 10. Each of these is, in turn, connected to a plurality of base station subsystems (BSS) 6 (only one MSC and BSS is shown for clarity). The base station subsystem 6 usually comprises a base station controller BSC and necessary interface apparatus, and is connected to a plurality of base stations (BS) 8, each of which supervises a certain geographical area, referred to as a cell (for the cells, see Figure 7).

The mobile services switching center 10 of Figure 1 is further connected or linked to the public switched telephone network (PSTN) 20 through an exchange 12 and lines 12. The MSC 10 is also connected to a global communications network, which in the example is the Internet (designated by numeral 43). The MSC may be connected to an integrated services digital network (ISDN) or any other type of appropriate communications network. The necessary links between different components of different telecommunication network systems are *per se* well known in the art.

The PLMN network includes further a database, the so called home location register (HLR) 9, which is connected

to the MSC. Those mobile terminals 1 and 2 which are subscribers of the mobile telecommunications network are registered in the HLR 10. Each local mobile telephone switching center 10 includes further a local database called a visitor location register (VLR) 8, into which is registered all such mobile stations 1 and 2 which are located within the area of one of the cells handled by that local mobile telephone services switching center MSC at any given moment.

The mobile stations are identified by a SIM (Subscriber Identification Module) which is usually mounted within each of the mobile stations, or otherwise physically connected thereto. A SIM is a module which includes various user (subscription) related information and secrets. It may also include further information which relates to the encryption of the radio communications. The SIM may be assembled fixedly or removably to the mobile station. The utilization of the SIM as well as the HLR and/or VLR registers in this invention will be discussed in more detail later in this specification.

As discussed, the user may be connected to the Internet 43 via a fixed or a mobile network or via a direct connection. However, there may be some differences between the connections when for example GPRS (General Packet Radio System) is concerned, but the service from the Internet network is available for the users of both PSTN and PLMN systems. In the example, the Mobile Switching Center (MSC) 10 as well as the PSTN 20 are provided with an access to the multiprotocol Internet 43 by access nodes (AN) 14 and 40. Even though only one AN per communications network is disclosed, it is to be understood that in practice the number of ANs may be essentially greater, and that the number of ANs is also increasing continuously. According to one solution a

special Internet Access Server IAS capable of converting the signal into data packets is used as an AN towards the Internet.

The users of the Internet 43 have made a contract with a Internet Service Provider (ISP) 42, who provides the communications connection to the Internet from the user terminals 1, 2 or 16. When the user desires to have an Internet connection, he calls to the Internet Service Provider (ISP) 42 so as to connect his terminal 16 to the desired address (so called Internet Protocol address). The call connection is established by the PSTN 20 and passes through at least the local exchanges 18, and perhaps one or several transit exchanges which are connected or interconnected through trunk lines (not shown). It is to be understood that even though Figure 1 discloses only one ISP through which both networks communicate towards the Internet, communication could be arranged through different ISPs.

Figure 1 discloses further a WWW server 45 (World Wide Web server) which includes server databases x, y and z providing different services. It discloses also a connection from the ISP through the router 44 to said server 45 via the Internet 43. It is to be understood that the service can be any service obtainable through any communications network, such as a banking service, an electronic shopping service etc., in which authentication is required.

The mobile station 1 (or 2) is used as a personal authentication device (PAD) when the user accesses, or has already accessed, via the user interface 16 through the PSTN 20, a service x provided by the WWW server 45. The mobile station 1 communicates with the service x through a separate communications path or channel than is used by

the actual user interface 16. The mobile station can be trusted because the user usually keeps it always with him. The ergonomic and functional requirements for the mobile stations and for the conventional PADs are essentially the same, and the MS has a user interface that is suitable for the PAD. A modern MS has even a security processor interface that is suitable for authentication purposes.

There are several alternatives to accomplish the authentication by means of the mobile station, and the examples thereof will be now discussed in the following in more detail.

Reference is now made to Figures 2 and 4, of which Figure 2 discloses schematically one arrangement for the authentication and Figure 4 a flow chart for the operation in accordance with one basic embodiment. The user 22 sends a request by means of the user terminal 16 to access a desired application 45, such as a banking service, through a connection established by means of a communications network (arrow 21 in Fig. 2; steps 102 and 104 in Fig. 4). The application 45 may comprise a database 46, or is connected to a separate database, such as the HLR 9 of the MSC 10 of Fig. 1, from which the application is enabled to retrieve the necessary user information. On the basis of this information the application establishes a connection to the mobile station 1 of the user 22 (arrow 26; step 106) for authentication purposes. At this stage the user may accept the connection 21 made by the user interface 16 by sending back a confirmation signal 29 (ie. an acknowledgment) using the mobile station 1 indicating that access is allowed and that the actual use of the service may begin (steps 108 and 112). In case the authentication fails, eg. on the basis that the application cannot reach the MS 1, all connections are closed (step 110). Alternatively

the user may be allowed to retry the access, either immediately or after a certain time period, or the user may be instructed by the user interface 16 to take some additional measures due to the failed authentication.

One way to implement the authentication, or the acknowledgment feature, is to use short messages of a short message system (SMS) of the PLMN. In the GSM system, a SMS MSC (SMS Message Service Center) designated by 7 in Fig. 1 is provided for the delivery of short messages to and from the mobile stations. The service center 7 sends the messages to the mobile subscribers using the same network elements as were discussed above and defined by the referred specifications. The SMS message signaling usually contains, eg. the receiver identification, sender information, time stamp etc.

Figure 3 discloses a solution in which the mobile station MS 1 has received a SMS message. The method steps for this are shown by the flow chart of Figure 5. According to this embodiment the user has requested, after having accessed the banking service through the user interface 16, that a sum of 200 FIM should be transferred from account No. 1234-4567 to an account No. 4321-7654 (step 204). The application retrieves the user related authentication data from an appropriate database (step 206), and sends accordingly a text message to the mobile station 1 (step 208). The MS 1 displays the text as shown, and asks the user to confirm or to deny the transaction by pressing "Yes" or "No" keys, respectively (step 210). The response is then transmitted back to the application, and in case of "Yes" the transaction proceeds (step 214) and in case of "No" some other measures are taken.

The arrows 27 and 28 of Figure 2 can also be seen as

illustrating the stage in which the MS 1 and the user 2 communicate: information received by looking at the display 31 of the MS 1 is indicated by arrow 27, and the response given by the user to the MS 1 is indicated by arrow 28. As explained, the user may choose a proper selection by pressing either Y or N key 32 of the MS. In case the user accepts, ie. "signs" the transaction, the banking service will then proceed accordingly. In case the user will not confirm the transaction, ie. presses the "No" key, the application may send a request to the user interface to feed in a correction, a cancellation, a new destination account etc. (steps 216, 218).

In case the application does not receive any response within a certain time period, or the response is somehow incorrect, the application may either send a second request for the confirmation, or close down all the connections.

The user may process several subsequent transactions and even some other banking services after having once accessed the application. When the user finally replies at step 216 to the user interface 16 that he does not want to continue, the connections are closed (step 220).

According to one embodiment of the present invention the information contained in the HLR and even in the VLR of the PLMN of Figure 1 can be utilized when implementing the inventive authentication arrangement. This is enabled by the fact that each of the mobile subscriptions includes, in the HLR 9 of Figure 1, information relating to the SIM (Subscriber Identification Module) already referred to, an IMSI (International Mobile Subscriber Identity) and MSISDN (Mobile Subscriber ISDN number) as well as to the location information (VLR number), basic telecommunications services subscriber information, service restrictions and

supplementary services etc.

Therefore Figure 3 can be seen to disclose also a SIM (Subscriber Identification Module) card 34 inserted within the MS 1. The telephone company usually uses the SIM for controlling payments and location of the user. Thus the SIM card 34 has to be connected to the MS 1 before taking it into use, and making telephone calls. The MS 1 of Figure 3 includes further a MS PAD controller 35 (Mobile Station Personal Authentication Device controller). From these the SIM 34 may be used in the invention as the means for identifying the user and/or including a secret or several secrets, and the MS PAD controller 35 is used for controlling the authentication operations. In addition to the general control of the authentication procedure, the controller 35 may, eg., be arranged to make all the calculations relating the various encryption operations. The arrangement in which the SIM 34, which is controlled by the MS PAD controller 35, can be utilized in the authentication procedure varies. Examples thereof are shortly explained in the following.

Instead of the above referred arrangement utilizing SMS services, the transactions can also be acknowledged such that the application, such as the banking service or another commercial service paid by an electronic transaction, sends the details of the transaction to the MS PAD 35 as a data signal through the mobile network. The correctness of the signal can be ensured by means of a checksum calculated by the MS PAD 35 in accordance with a predefined algorithm and utilizing the secret of the SIM 34: the checksum has to match with the sum displayed by the user terminal 16. If the user accepts the transaction, he acknowledges it and gives a permission for the MS PAD 35 to "sign" the message signal 26 from the application by using user's secret (eg. when using public

key encryption and a non-repudiation is required) or using a secret shared with the application. Thereafter the application will proceed as requested by means of the user interface. According to one embodiment, the secret or secrets of the SIM 34 can also be used for the encryption of the messages and/or signaling between the application and the MS.

Figure 6 discloses an alternative embodiment for Figure 2. In this embodiment the user interface 16 is in a form of an ordinary telephone terminal connected to the PSTN 20 in a *per se* known manner. The PSTN is further connected to intelligent network services (IN) 60 which forms the application in this embodiment. The mobile station 1 includes a PAD controller 35 and a SIM 34 as described above in connection with Figure 3. According to one embodiment MS PAD pairs, which contain a predefined pair of a service identifier for the given service and a personal secret, are stored within the PAD controller. These pairs may be used, eg., in the following manner.

The user accesses a service in said IN by establishing a telephone call to the service (arrow 21). The application challenges the user with a number given as a voice message, or by means of a possible display on said telephone terminal (arrow 61). The user keys in this challenge together with a specific number for the service to the MS by the keypad (arrow 28), whereafter the PAD controller accomplishes the necessary calculations according to predefined algorithm to receive a further number strings. In this calculation the secret stored to the SIM for that particular user may form a part of the algorithm. This secret may be either an application specific secret or a secret of the PLMN. The result of the calculation is then fed in to the user interface 16 (arrow 62), and transmitted to the IN service in question

through the PSTN 20. In case this matches to the expected value, the IN service 60 allows the user to initiate the use thereof by the fixed line terminal 16.

The above mentioned embodiment can be used, eg. when paying telephone calls or services obtained through any ordinary POTS line telephone. For instance, this enables an arrangement in which calls by any telephone terminal are charged from the mobile telephone subscription (ie. from the holder of a particular SIM card). The mobile subscribers may find this service useful, eg., in instances where the calls made by the mobile telephone are more expensive than calls by an ordinary POTS telephone, or when the MS 1 is not within an area of any such mobile network into which the user could have a proper radio connection.

According to one additional embodiment (not shown) the mobile station 1 and the user interface 16 are capable of directly communicating with each other through suitable operational connection, such as a radio connection, an infrared connection or a fixed conduit connection with necessary couplings. This reduces the risk for mistyping errors which the user might do when acting as a "link" between the MS 1 and the user interface 16.

According to one alternative a mobile station is arranged to receive more than one SIM card 34. By means of this, one single mobile station could be used for different authentication purposes. For example, a user could have three different SIMs: one for the authentications required by his work, one for the personal needs, and one for a still further need, eg. for a "chairman of an association". Each of the SIMs may have a telephone number, alarm tone etc. of their own.

According to a further alternative the MS 1 communicates through a PLMN with the application, and the messages and/or signaling required in this communication is encrypted using the secret or secrets of the SIM. This enables a secure communications using only one communications network, ie. the PLMN, as the secret of the SIM is unique, and it is not possible for third parties to obtain information contained in the signaling or to break into the signaling.

A further embodiment of the present invention is now explained with reference to Figures 1 and 7. Figure 7 discloses a schematic cell map of an arbitrary geographic area, which is divided into a plurality of contiguous radio coverage areas or cells. While the system of Figure 7 is illustrated so as to include only ten cells (C1 to C10), the number of cells may in practice be larger. A base station is associated with and located within each of the cells, these base stations being designated as BS1 to BS10, respectively. The base stations are connected to the base station subsystems (BSS 6 of Figure 1). A cell may also cover one or several base stations. The cells are grouped into four groups A to D, wherein each group may include one or more cells, as is marked by corresponding markings.

Each group is seen by the system as one unit, ie. one area, such that four different cell categories A to B are provided. The purpose of this is to illustrate that the cells may be divided into different authentication categories, or classes. The idea behind this is that the authentication data within the authentication database may include restrictions which do not allow the user to access the application in case he is not situated within a certain predefined cell area. For example, if a company uses a MS of an employee for authentication, it is

possible to limit the area such that the authentication possibility can be restricted to be allowed only in those cells (eg. within the area A) which are near to the office of the company.

The above can be easily implemented by means of the visitor location register VLR, designated by 8 in Fig. 1. The mobile station (MS) 1 or 2 roaming in the area of the MSC is controlled by the VLR 8 which is responsible for this area. When the MS 1 or 2 appears in the location area, the VLR initiates an updating procedure. The VLR 8 has also a database which includes, eg., the IMSI, MSISDN and location area in which the MS is registered according to, eg., GSM 09.02 specification. So-called cell global identification includes further a cell identity, and is included in the messages between the MS 1 and the MSC 10. This information may be used as an identification indicator to find the mobile station MS 1 location, which is then utilized in this embodiment.

It is noted herein that the mobile station can be any kind of apparatus providing a possibility for mobile communications for a user other than the mobile telephone 1 or the integrated unit of mobile telephone and a computer 2. The latter arrangement is sometimes also referred to as a "communicator". One example of other suitable mobile station is a pager, ie. the "beeper" capable of displaying a character string. What is important is that the mobile station is capable of receiving and/or transmitting desired information, which in some instances may even be in the form of text or voice messages only instead of a specific authentication signal or code.

In addition, in the above examples the application 45 is arranged to provide linking between the two communications

networks such that they both can be used for the connection of the user to the application. However, this may well be accomplished by some other party. For instance, the ISP or similar service provider or the telecommunications network operator may operate as an authenticating organization and/or provide the linking between the two communications networks, and provide a secure connection to the actual application.

Thus, the invention provides an apparatus and a method by which a significant improvement can be achieved in the area of authentication. The arrangement according to the present invention is easy and economical to realize by *per se* known components and is reliable in use. It should be noted that the foregoing examples of the embodiments of the invention are not intended to restrict the scope of the invention defined in the appended claims. All additional embodiments, modifications and applications obvious to those skilled in the art are thus included within the spirit and scope of the invention as set forth by the claims appended hereto.

Claims

1. A method for authenticating a user to an application, the application being available to the user through a first communications network, the method comprising:

establishing a connection between the application and a user interface through said first communications network so as to enable a user to access the application; and

authenticating the user to said application by means of a mobile station communicating with the application through a second communications network.

2. A method according to claim 1, wherein the step of authenticating comprises using the mobile station to verify the identity of the user as the user accesses the application by the user interface.

3. A method according to claim 1, wherein the step of authenticating comprises using the mobile station for acknowledging a transaction or proceeding which the user has previously requested from the application through the user interface.

4. A method according to any one of the preceding claims, wherein the mobile station is a cellular telephone and said second communications network comprises a digital cellular network.

5. A method according to any one of the preceding claims and comprising utilizing a secret of a Subscription Identification Module (SIM) of the mobile station for encryption of signalling associated with the authentication step.

6. A method according to any one of the preceding claims,

wherein a Subscription Identification Module (SIM) of the mobile station is used for providing the identity of the user.

7. A method according to claim 6 and comprising the step of charging the costs of the connection from the user interface to the application to the holder of the subscription identified by the SIM.

8. A method according to any one of the preceding claims, wherein at least part of the signaling between the application and the mobile station is in the form of short message system text messages.

9. A method according to any one of the preceding claims and comprising the step of using area location information of the mobile station as one parameter of the authentication procedure.

10. A method of providing an authentication to an application available to a user through a communications network, the method comprising:

establishing a connection between the application and a user interface through said communications network so as to enable access of a user to the application; and

providing an authentication to said application by means of a mobile station such that a secret of a Subscription Identification Module (SIM) of the mobile station is utilized in encryption operations of the authentication.

11. An arrangement for providing an authentication to an application provided by an application provider through a communications network, comprising:

a user interface;

a connection between the application and the user

interface through said communications network so as to enable use of the application; and

means for authenticating the use of the application, wherein said means for authenticating comprises a mobile station communicating through a mobile communications network, and a link between the application implemented by means of the communications network and the mobile communications network.

12. An arrangement according to claim 11, wherein the mobile station is a cellular telephone and the mobile communications network is a digital cellular network.

13. An arrangement according to claim 11 or 12, wherein authentication signaling to and from the mobile station are in the form of text messages provided by a short message system (SMS) of the mobile communications network.

14. An arrangement according to any one of claims 11 to 13, wherein the mobile station comprises a mobile station personal authentication device (MS PAD) arranged to control the authentication procedure, and a subscription identification module (SIM) including a secret and being operationally connected to the MS PAD, wherein the secret of the SIM is arranged to be utilized in the authentication procedure.

15. An arrangement according to any one of claims 11 to 14, characterised in that the application is a banking service, an electronic shopping service, or some other commercial service requiring an acknowledgment for an electronic transaction.

16. A mobile station for providing an authentication to an application provided through a communications network, wherein:

the application is accessed by means of a user interface connected to the communications network; and

said mobile station uses a different communications network for the communications than the user interface, and the mobile station is used for authenticating the use of said application accessed by the user interface.

17. A mobile station according to claim 16 and comprising an integrated mobile station personal authentication device (MS PAD) arranged to control the authentication procedure.

18. A mobile station according to claim 16 or 17, wherein the station is a digital mobile telephone and comprises a subscription identification module (SIM) including a secret, wherein the secret of the SIM is arranged to be utilized in the authentication procedure.

19. A mobile station according to claim 18 and comprising at least one additional SIM.

20. A mobile station according to claim 16 or 19 and comprising means for directly interfacing with the user interface, such as by an infrared or radio transceiver capable of communicating with the user interface.

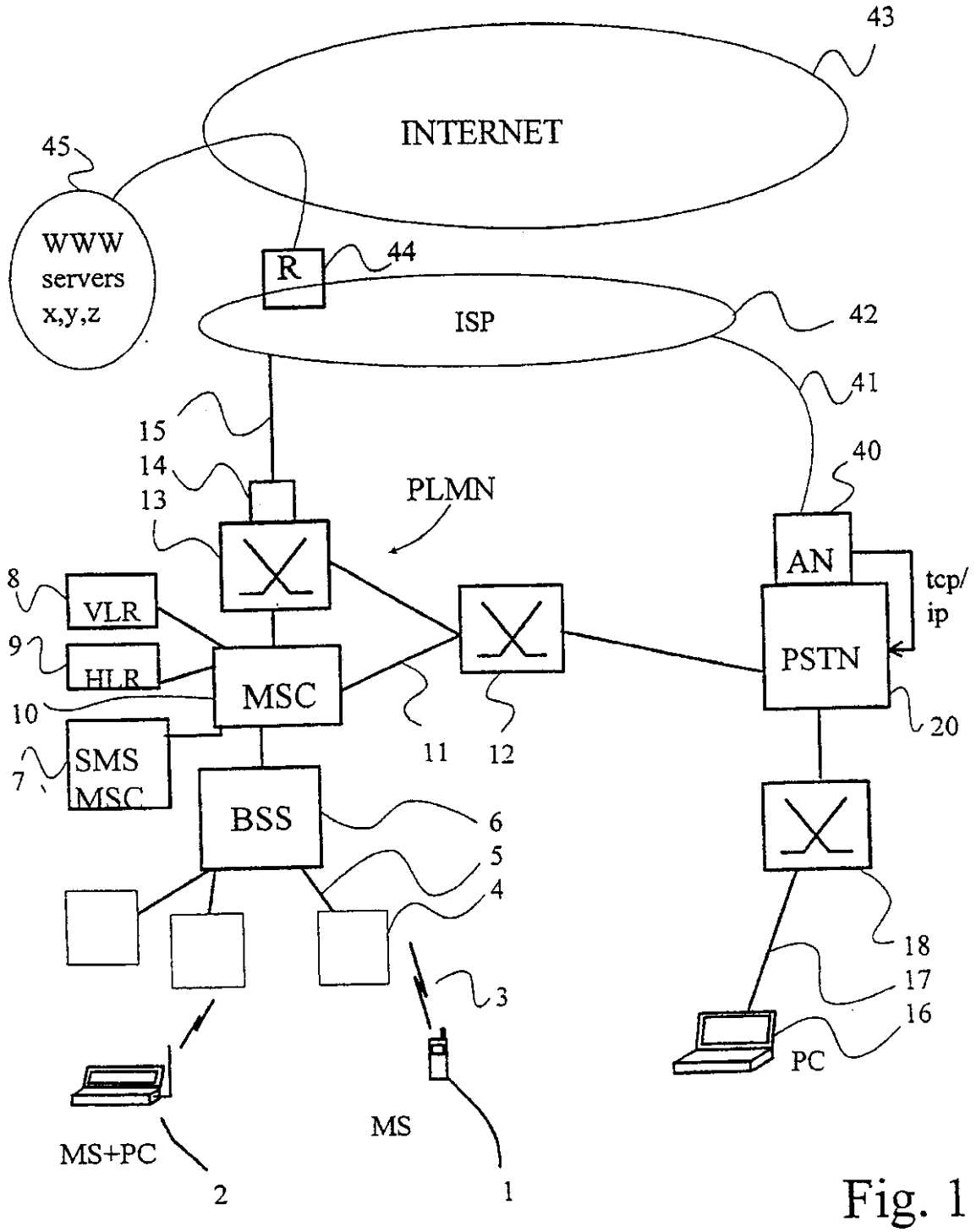

43
INTERNET
45
WWW
servers
x,y,z
R
44
ISP
42
41
15
14
13
PLMN
40
AN
tcp/
ip
8
VLR
9
HLR
MSC
PSTN
10
20
SMS
MSC
7
11
12
BSS
6
5
4
18
17
16
3
PC
MS
MS+PC
2
1

Fig. 1

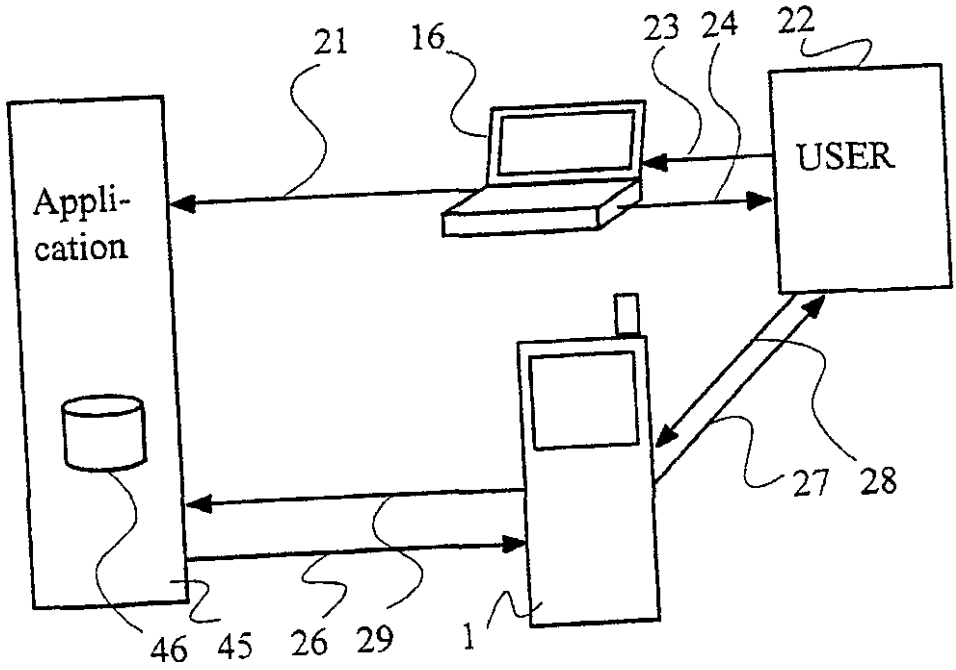

21
16
23
24
22
USER
Appli-
cation
27
28
46
45
26
29
1

Fig. 2

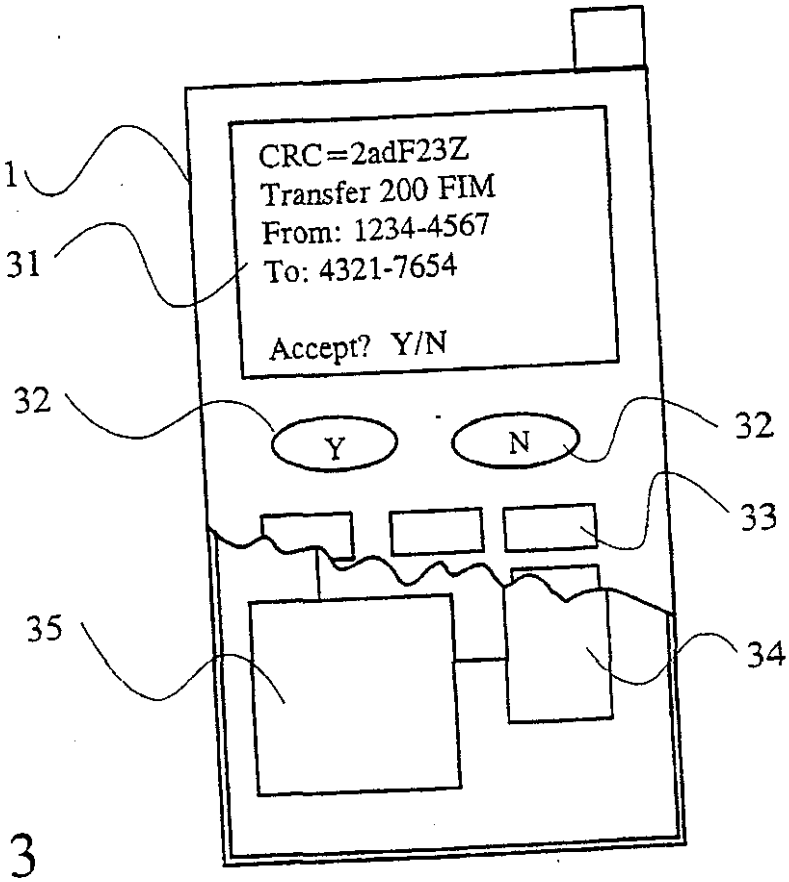

CRC=2adF23Z
Transfer 200 FIM
From: 1234-4567
To: 4321-7654
Accept? Y/N
1
31
32
Y
N
32
33
35
34

Fig. 3

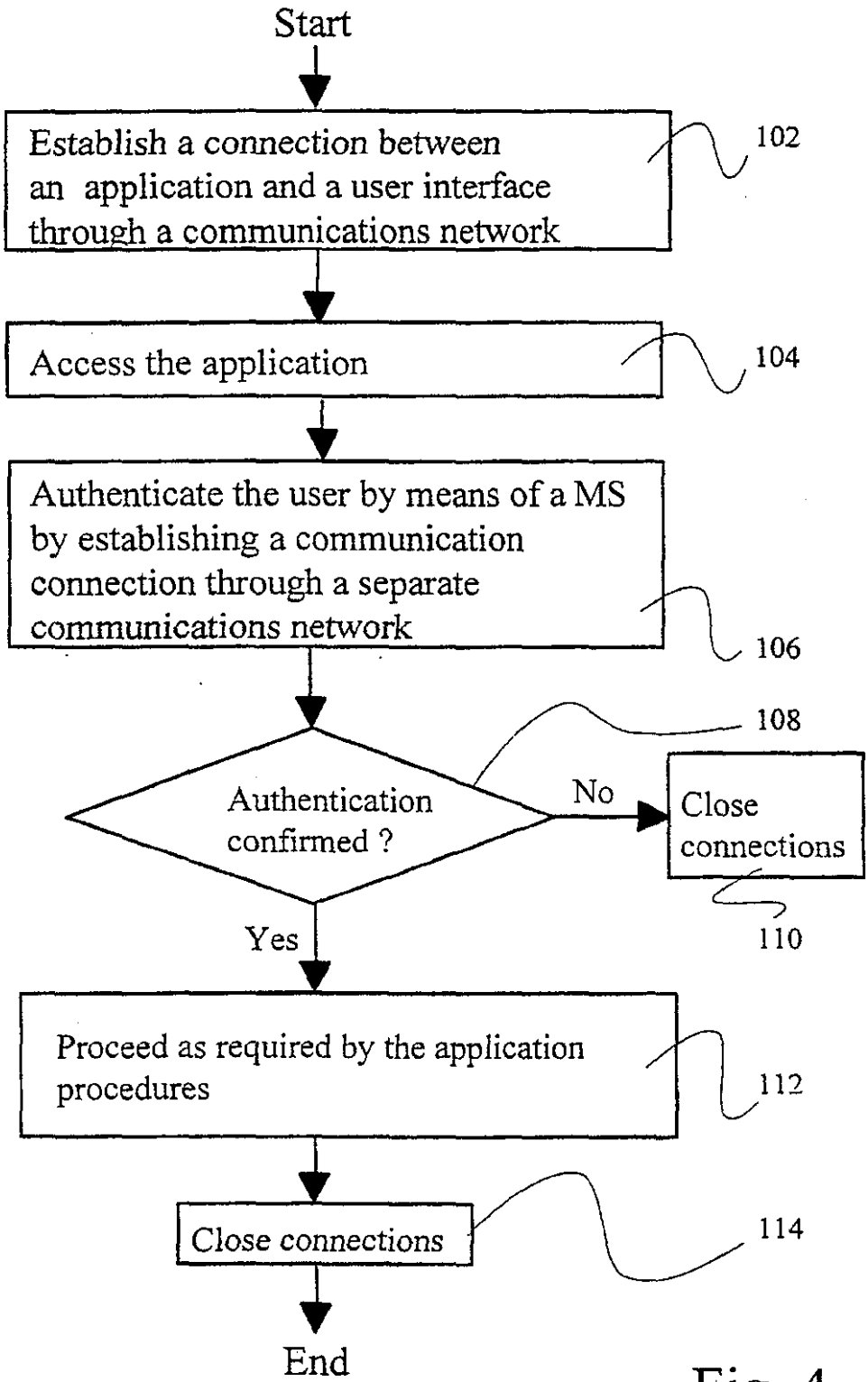

Start
Establish a connection between an application and a user interface through a communications network
102
Access the application
104
Authenticate the user by means of a MS by establishing a communication connection through a separate communications network
106
108
Authentication confirmed ?
No
Close connections
110
Yes
Proceed as required by the application procedures
112
Close connections
114
End

Fig. 4

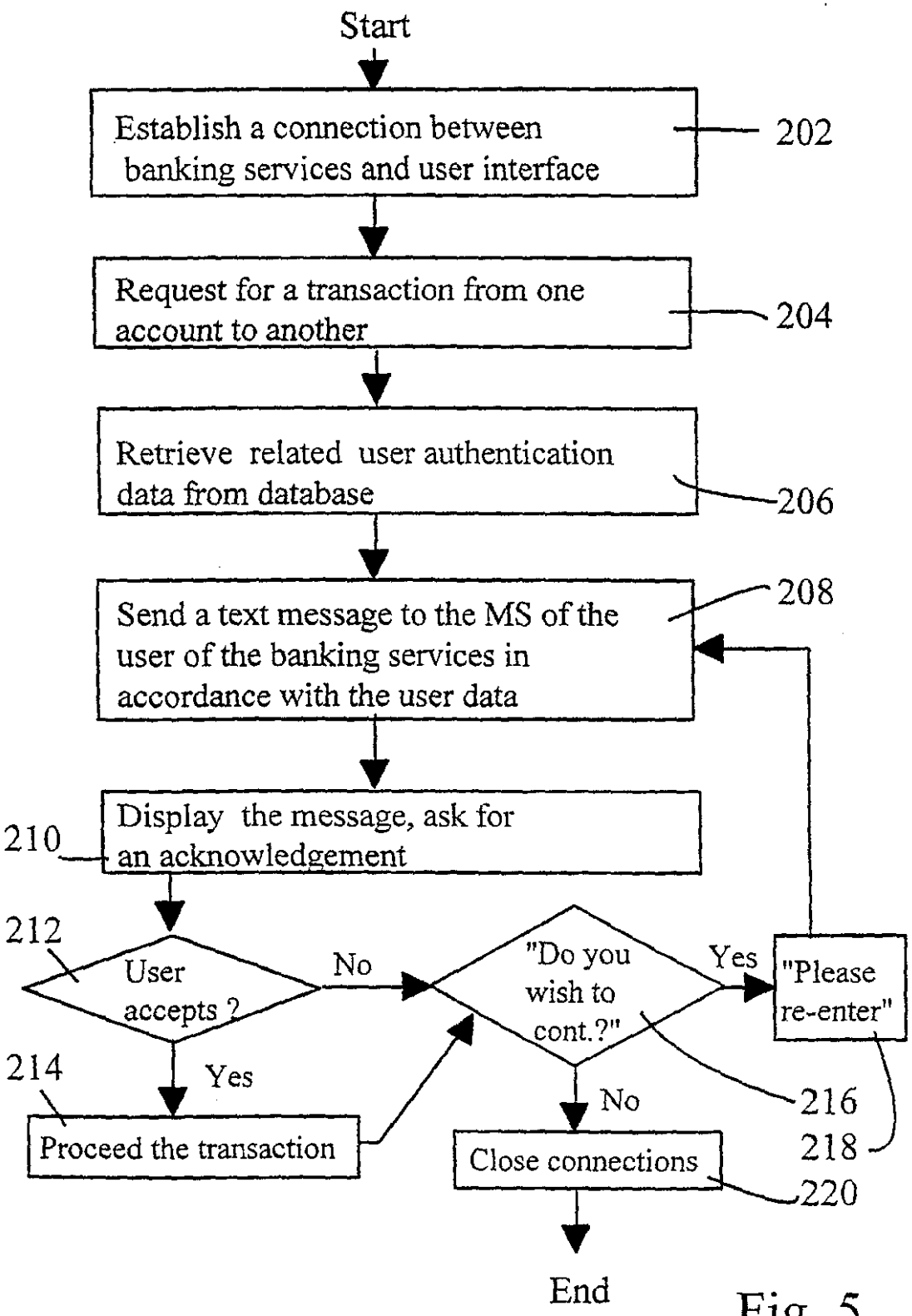

Start
Establish a connection between banking services and user interface
202
Request for a transaction from one account to another
204
Retrieve related user authentication data from database
206
Send a text message to the MS of the user of the banking services in accordance with the user data
208
Display the message, ask for an acknowledgement
210
212
User accepts ?
No
"Do you wish to cont.?"
Yes
"Please re-enter"
214
Yes
No
216
218
Proceed the transaction
Close connections
220
End

Fig. 5

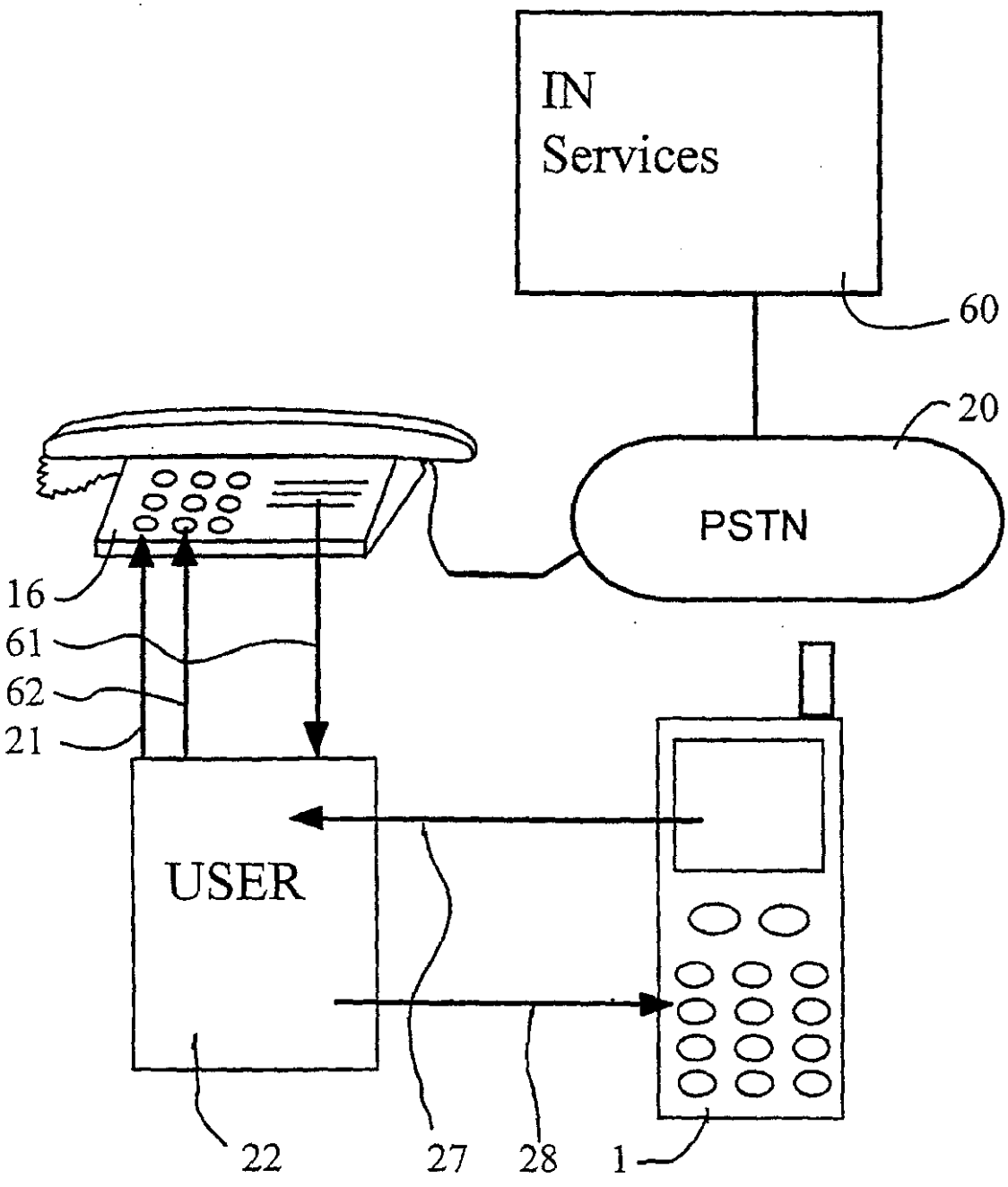


Fig. 6

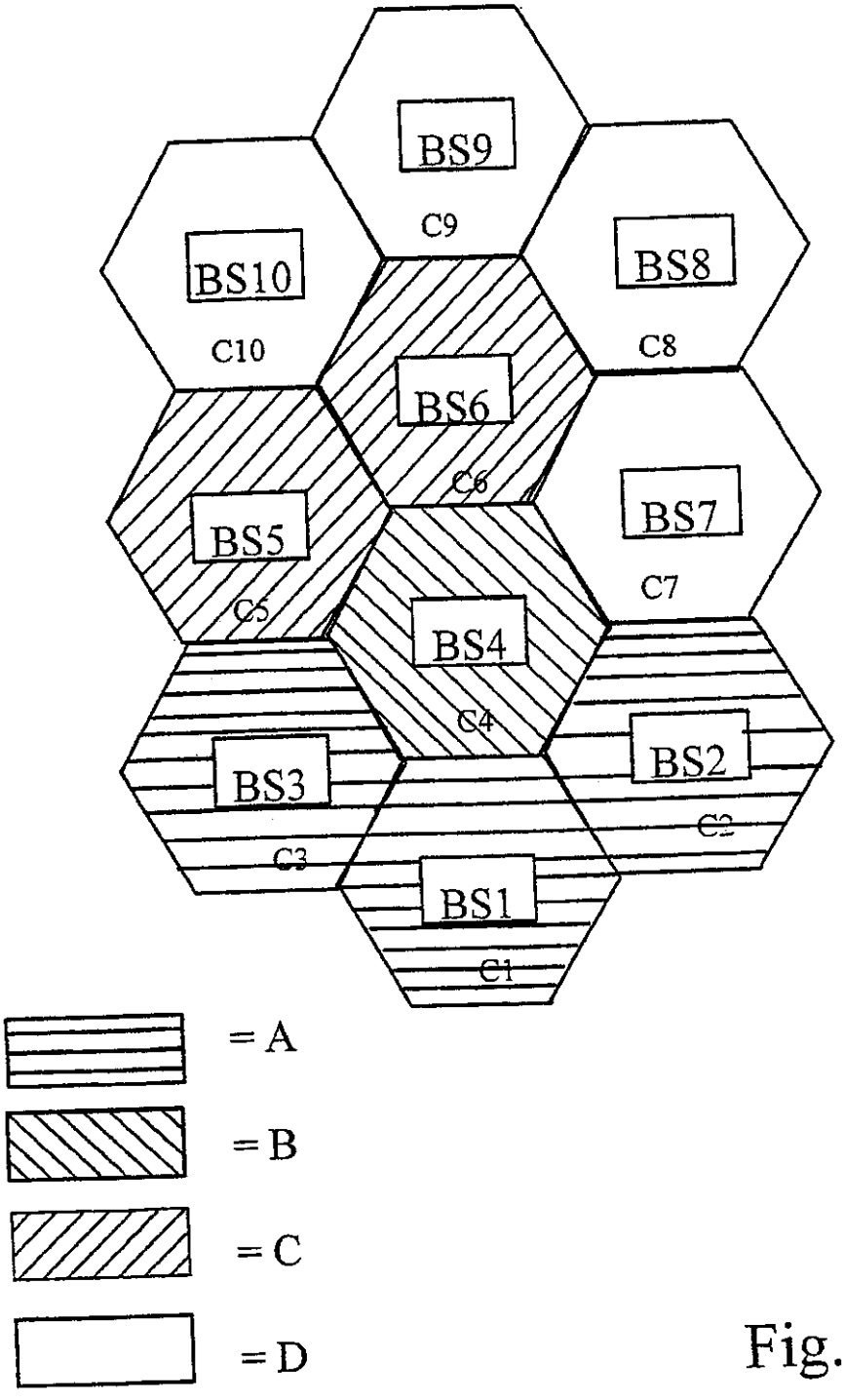

BS9
C9
BS10
C10
BS8
C8
BS6
C6
BS5
C5
BS7
C7
BS4
C4
BS3
C3
BS2
C2
BS1
C1
= A
= B
= C
= D

Fig. 7

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 1/00
H04L 29/06 G07F 7/08

[12]发明专利申请公开说明书

[21]申请号 99803282.4

[43]公开日 2001年4月18日

[11]公开号 CN 1292108A

[22]申请日 1999.2.5 [21]申请号 99803282.4
[30]优先权
[32]1998.2.25 [33]FI [31]980427
[86]国际申请 PCT/EP99/00763 1999.2.5
[87]国际公布 WO99/44114 英 1999.9.2
[85]进入国家阶段日期 2000.8.24
[71]申请人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72]发明人 E·图尔蒂埃宁

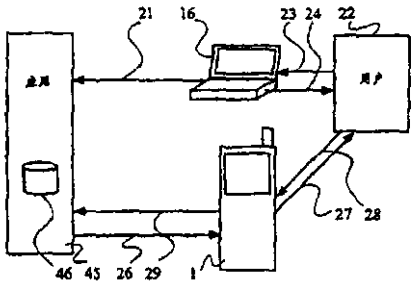
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 张志醒

权利要求书2页 说明书13页 附图页数6页

[54]发明名称 通过通信网络进行认证的方法,设备和装置

[57]摘要

对通过通信网络提供的应用提供认证的方法,设备和装置。通过所述通信网络 在应用和用户接口之间建立连接,以便使得用户访问应用。用移动工作站通过 移动通信网络通信的方法对所述应用提供认证。



ISSN1008-4274

知识产权出版社出版

权 利 要 求 书

1. 一种为应用认证用户的方法，该应用通过第一通信网络对用户是可用的，该方法包括：

在应用和用户接口之间通过第一通信网络建立连接以便使用户能够访问应用；和

通过第二通信网络用移动工作站与应用进行通信的方式对所述应用认证用户。

2. 根据权利要求 1 的方法，其中认证步骤包括当用户通过用户接口访问应用时使用移动工作站来确认用户身份。

3. 根据权利要求 1 的方法，其中认证步骤包括使用移动工作站来确认一个交易或处理用户先前通过用户接口从应用请求的事情。

4. 根据上述权利要求任一个的方法，其中使用移动工作站是移动电话，以及所述第二通信网络包括数字蜂窝网络。

5. 根据上述权利要求任一个的方法，包括利用移动工作站的预定确认模块（SIM）的密码来加密与认证步骤有关的信令。

6. 根据上述权利要求任一个的方法，其中移动工作站的预定确认模块（SIM）用来提供用户身份。

7. 根据权利要求 6 的方法，包括向由 SIM 确认的订户持有人收取从用户接口至应用的连接费用的步骤。

8. 根据上述权利要求任一个的方法，其中应用和移动工作站之间的至少部分信令是以短消息文本信息的形式。

9. 根据上述权利要求任一个的方法，包括使用移动工作站的区域位置信息作为认证程序的一个参数的步骤。

10. 一种通过通信网络向对用户可用的应用提供认证的方法，该方法包括：

在应用和用户接口之间通过所述通信网络建立连接以便使用户能够访问应用；和

用移动工作站的方式对所述应用提供认证以便在认证的加密操作中利用移动工作站的预定确认模块（SIM）中的密码。

11. 一种向由应用提供者通过通信网络提供的应用提供认证的

装置，包括：

用户接口；

应用和用户接口之间通过通信网络的连接，以便能够使用该应用；以及

认证应用使用的装置，其中所述认证装置包括通过移动通信网络进行通信的移动工作站，和在以通信网络和移动通信网络的方式实现的应用之间的链接。

12. 根据权利要求 11 的装置，其中移动工作站是一个蜂窝电话，移动通信网络为一个数字移动网络。

13. 根据权利要求 11 或 12 的装置，其中至移动工作站的认证信令和来自移动工作站的认证信令具有由移动通信网络的短消息系统（SMS）提供的文本消息的形式。

14. 根据权利要求 11 至 13 任一个的装置，其中移动工作站包括用来控制认证程序的移动工作站认证装置（MS PAD），以及包括密码并与 MS PAD 操作连接的预定确认模块（SIM），其中 SIM 的密码用在认证程序中。

15. 根据权利要求 11 至 14 任一个的设备，其特征为：应用是银行服务，电子购物服务，或一些其它的需要确认电子交易的商业服务。

16. 向通过通信网络提供的应用提供认证的移动工作站，其中：

通过连接至通信网络的用户接口的方式访问应用；和

所述移动工作站使用不是用户接口的不同的通信网络来通信，移动工作站通过用户接口用于认证所述应用。

17. 根据权利要求 16 的移动工作站，包括用来控制认证程序的集成的移动工作站个人认证装置（MS PAD）。

18. 根据权利要求 16 或 17 的移动工作站，其中工作站是一个数字移动电话并包括一个有密码的预定确认模块（SIM），其中利用 SIM 的密码于认证程序中。

19. 根据权利要求 18 的移动工作站，包括至少一个额外的 SIM。

20. 根据权利要求 16 或 19 的移动工作站，包括与用户接口直接接口的装置，如用能够与用户接口通信的红外线或无线收发机。

说　明　书

通过通信网络进行认证的方法，设备和装置

本发明涉及给一个应用程序提供认证的方法。本发明还涉及给一个应用程序提供认证设备以及用于认证的装置。

存在各种各样需要认证的电子应用。例如，当用户正在访问一个特别的应用和/或当用户已经使用一个应用，有需要证实该用户或从用户收到这样一个认可，即它容许该应用作进一步处理。

可能需要认证的应用的例子包括通过通信网络，如因特网，企业内部互联网（Intranet）或局域网（LAN）获得的各种各样的商业服务，通过通信网络访问的支付和银行服务，资源访问，远程编程，重编程或软件更新等等。甚至通过通信网络获得的某些免费服务可能需要认证。用户正在要访问（或者用户已经在使用的服务或应用，但那里在使用该访问过程中需要检查认证或在使用时需要承认什么）的，至少要求一定程度的用户认证的服务或应用的数量在过去几年大大增长。将来这种认证需要还要进一步增长。

现在对于通信认证已经有一些已知的方案。通常它们在两个通信计算机装置之间使用各种各样的加密技术。根据认证的基本情况，给予所述两个计算机装置的加密函数一个随机询问（challenge）。这两台计算机都有一个秘密，如加密密钥，它也给予两个计算机的加密函数。然后，两个加密函数的计算结果加以比较，如果比较结果是正面的，认证认为是有效的。如果比较结果为负面，那么认证测试认为已经失败。

已经有许多现有的认证设备。下面提出了现有技术设备的实例以及它们的缺点的简短描述。

口令。现在，使用一个口令或几个口令是认证的最常用的方法。口令通过用户界面，如通过连接至通信网络的计算机终端，给远程应用程序。然而，这种方案并没有考虑网络的弱点，因为口令公开给访问网络的每个人（以及那些有足够技术读取口令的人）。

密码。这可以描述为存储着的和被例如用户界面使用的电子口令或签名或加密密钥。即使密码对网络不公开，它可能由于“误操

作”而结束并被某些方使用，而不是那些原来就想成为密码使用者的人。

用户界面中的认证软件。这是认证的一个更复杂的方法。在用户界面中向程序赋予口令，然后自动地加密认证以访问所请求的应用。即使这比以上方案提供了一个更安全的设备，但仍然有可能从用户界面获取口令。也有可能不通知真正用户而修改软件。

带有关读卡器的智能卡。智能卡能通信已加密的问题－回答消息，但并不包括接收用户本身授权的用户接口。这样的接口可以在智能卡的读卡器中，但这样的读卡器必须很好地防止任何可能的误用，因此一般用户（即，绝大多数用户，如公众）不能经常物理访问这些读卡器接口，但他们要信任提供智能卡的机构。而且，智能卡读卡器不能在不互信的机构之间共享。

有用户接口的智能卡。这些已经存在，但很昂贵，因为安全处理器必须有它自己的安全用户接口。这些是不多见的并且它们的输入/输出能力仍然受带极大限制，因此他们并不为认证问题的有关经济可行的解决方案。

独立的个人认证装置。在该方法中，用户作为在用户接口和独立认证装置之间的“通信手段”使用。用户接口提出问题，然后用户键入手持认证装置（类似袖珍计算机的装置）。认证装置可以，例如给一个数字作为回答，用户键入该数字至用户接口。这里问题涉及需要购买，使用和携带一个独立装置。在某些情况下，也有可能不正确的键入那些通常长而且复杂的字符串。

上面已提及的一些方，当实现本认证系统时，可能涉及到它们。下面将他们作更详细简要解释。

用户通常为使用各种应用或服务的人。用户能通过只有他或她知道的口令（或密码）的方式来确认（公共键方法），或通过在用户和应用之间共享的密码的方式来确认（秘密密钥方法）。

应用是要确保用户认证的一方。在一些场合应用也能称为服务。从应用的观点，认证问题能分成 4 个不同的种类（问题）：1〕此时用户在另一端？（因此称为端实体认证），2〕进一步的消息是从同一用户收到？（消息流的完整性），3〕特别的消息来自某个用户？（数据源认证），和 4〕消息是这样，即使第三方可能相信它源自某

个用户？（认可）。

用户接口是使得用户能访问应用或服务的装置或设备。在大多数场合，它也指终端，并可能包含诸如计算机（即个人计算机，PC），工作站，电话终端，诸如移动电话或无线电或呼机的移动工作站，自动提款机和/或柜员机等等之类的装置。用户接口提供输入/输出功能，它可能甚至提供部分应用。

个人认证装置（PAD）是用户随身携带的一块硬件。PAD 可以有一些基本的输入/输出功能甚至一些处理功能。上面所指的智能卡和独立认证装置也可以认为是 PAD。在大多数情况下，用户能依靠他的 PAD，因为用户经常随身携带因而几乎处于不间断的控制之中。所有可能的口令或密码隐藏在硬件之中，因此没有容易的方式来发现它。装置本身不易修改以致威胁用户和安全处理器之间的通信路径。而且，PAD 通常有最少量的保存状态，其中的程序不易修改。

即使以上描述的用于认证的现有技术方案已经存在，除了上面已指出的缺点，在认证领域仍然有一些缺点。

如果使得访问应用程序绝对安全或尽可能安全，从结构上应用程序容易变得极其复杂，而且访问和使用应用程序本身也变得复杂和更加耗时。增加的安全级增加了所需的软硬件的数量，这导致增长的维护和更新它们的需要，因此认证的整个成本可能变得高昂。通过降低安全级能降低复杂性和成本，但这可能引起通信的安全级不够。而且，相信在通信网络中不存在“绝对安全”的条件，因为技术发展使得黑客有可能甚至攻破最复杂的保安设备。

人们的困难存在于这样的现实，即口令或密码可能变得很复杂和/或太长或者太多。因此用户可能发现很难记住他们。一般地在秘密密钥方法中认为是安全的密码为 128 位，在公共密钥方法中为 1024 位。大多数人是不可能记住这种密钥的。

而且，用户没有外接装置不能进行在认证中所需的计算。同上面所解释的，经常通过问题和回答方式进行基本认证。这可能需要用户（即人）用密码来加密某些东西。现实中是不可能成立的。

除了上面讨论的通过开放的通信网络在传送过程中获取口令和密码的可能性外，今天的方案并不太注意用户接口的弱点。终端设备已发展为充满了复杂技术和软件，以致大多数用户不再全面控制

终端，或理解内部的操作。而且，时常出现许多用户共享同一终端设备（如公用 PC）和/或外勤人员能访问完全封闭组织的计算机。

计算机终端包含保存的状态和能修改的存储器方式的程序。现代计算机中可能修改其中的软件甚至用户还没有注意到它，甚至通过通信途径而不是物理地访问设备本身。举一个这种风险的例子，有可能修改计算机终端中的某个程序，以致它修改用户发送至如某银行的数据，以致该计算机修改某一天的对另一帐户的而不是由用户指定的所有银行转帐。这种不加提示的修改或重编程当用于攻击普通个人用户，特别用于攻击诸如公司或公共机构时可能引起严重的和巨大的损失。这都意味着普通终端装置和通信途径不可信。

因此，本发明的目的之一是克服现有技术方案的缺点，并提供一个新型的认证方案。

另一个目的是提供一个方法和设备，使用这种方法，希望访问某个应用程序的用户能以一种比现有技术更安全的方式得到认证。本发明的另一个目的是在使用一个已经访问的应用过程中当有认证的需要时提供一种认证。

本发明的目的之一是提供一种方法和设备，通过这种方法和设备能在认证中利用移动工作站。

本发明的另一个目的是提供一个解决方案，使用该方案，移动工作站的认证模块能用于认证中。

本发明的其它目的和优点将结合附图在以下的说明书部分提出。

通过对通过通信网络提供的应用提供一种认证的新方法达到这些目的。根据本发明，通过所述通信网络建立在应用和用户接口之间的连接，以便用户能访问通过通信网络提供的应用，同时，用通过移动通信网络进行通信的移动工作站的方法，提供对所述应用的一种认证。

根据另一个实施例，认证方法包括在应用和用户接口之间通过通信网络建立连接，以便使得用户能够访问通过通信网络提供的应用。对所述应用的认证是通过移动工作站的方式提供的，这样能利用移动工作站的预定确认模块（SIM）的密码于认证的加密操作中。

本发明还提供了一种设备，用于提供对应用提供者通过通信网

络提供的应用的一种认证。该设备包括一个用户接口和一个通过所述通信网络在应用和用户接口之间的一种连接，以便能使用该应用。该设备还包括认证使用应用的装置，其中所述认证装置包括通过移动通信网络进行通信的移动工作站，以及在由通信网络实现的应用和移动通信网络之间链结。

根据另一个实施例，本发明提供一个移动工作站，它用来对通过通信网络提供的应用提供认证。在这个实施例中，其中应用是通过连接至通信网络的用户接口的方式来访问的，并且所述移动工作站使用一个不同于用户接口的通信网络来通信。所述移动工作站对通过用户接口访问的所述应用的使用进行认证。

使用本发明的方法能获得几个优点，因为该方案引进了一个新的可信赖的认证方式。这个富于创造性的认证方法和设备在已存在的通信网络中是容易实现的，不需任何过多的变化和附加装置。本设备能用于有各种不同应用的连接中，实际上用于有任何这样的应用的连接中，即该应用通过一个通信系统提供，它需要某种认证。

用户不需携带一个独立认证装置（PAD）或许多不同的认证装置。根据本发明，用户也能信任个人认证装置（PAD），因为移动工作站时常傍身而且用户会十分留意他们的移动工作站。而且，例如在万一移动工作站被窃取的情况下，移动预定和/或随之的 SIM 能容易被营运商取消。一个移动工作站的所有密码在它的硬件中隐藏得很好以致不易发现它们。而且，移动工作站装置本身以不易修改成使在用户和安全处理器之间的通信途径可能受到威胁的方式。

该系统包括最小量的保存状态，而且该程序是不易修改的。移动工作站的现有的 SIM，更准确地说是其中的密码能被利用作所需的加密程序。因此，SIM 能用作一种新用途的安全卡，已经有现成的一方控制 SIM 的使用，即如果检测到假冒使用，移动网络营运商能迅速取消 SIM。

下面本发明和本发明的其它目的和优点将参照附图通过实例描述，这里，在不同图中的同样的参照编号指同样功能。应该理解，本发明的下列描述不意味着限制本发明在该连接中展示的特定形式，而是本发明意味着覆盖所有修改，类似和替换，它们包括在附加的权利要求书的原理和范围之中。

图 1 示出了通信网络的一个可能设备的一般视图，用该设备可以实现本发明；

图 2 是根据本发明认证用户的一个实施例的示意性图；

图 3 示意性公开了一个可能的移动工作站和本发明的一个实施例；

图 4 和图 5 公开了根据本发明的两个实施例的流程图；

图 6 公开了依照本发明用于认证的另一个实施例；

图 7 是有关本发明的另一个实施例的示意性图；

图 1 是能用于实现本发明的一个网络设备的示意性表示。图 1 的设备包括公共交换电话网（PSTN），它用一个指定为 20 的方框示意性示出。这个示例性的 PSTN 是一个固定线路的电话网（或普通旧式电话服务 POTS），它形成一个通信网络，通过它，用户接口 16 能够访问应用。根据本实施例，一个用户（未示出）可以使用连接至 PSTN 的用户终端 16，作为用户接口通过互联网连接在一个可获得的 WWW 服务器 45 中来访问所需的服务。公开的终端 16 为一个人计算机（PC），但也可以使用其它类型的用户接口，如工作站，自动公众柜员机等等。

也公开了一个公共陆地移动网（PLMN）。这可以是，例如，一个蜂窝移动电话网络或相似的移动通信系统。也公开了两个移动工作站 MS 1 和 MS + PC 2。MS + PC 2 可以定义为一个集成移动电话和一个便携式计算机。两者都能够通过 PLMN 的数个基站（BS）之一通过与 PLMN 的空中接口 3 通信。

一种类型的 PLMN 是数字 GSM 网（GSM；移动通信全球系统），它在 ETSI（欧洲电讯标准组织）的 GSM 推荐标准中已明确规定，其中的网络结构也在推荐标准 GSM 01.02 或 GSM03.02 或其后的新版中详细描述。注意到在一个示例性的移动电话网络的上下文中主要使用 GSM 术语描述本发明，本领域的技术人员应该理解，本发明能在任何移动系统中实现。而且，注意到由于清楚起见，只示出了那些移动网络结构部分，它们用于解释示例性系统的运行时被认为是必须的。技术人员很清楚这样的事实，即电话网络一般也可以包括不同于那些示出的装置的其它必要装置，PLMN 或 PSTN 的一些公开部件可以省略或被其它类型部件替换，大量的移动网络或普通的固定场

合线路网络可以互相合作并彼此互换。技术人员也能理解，不需任何 PSTN 或在用户终端 16 和互联网 43 之间的类似网络设备，连接至互联网也可以是直接连接。然而，这些选择方案没有示出和更详细解释，因为对于本领域的技术人员来说它们是已知的。

以 GSM 为基础的公共陆地移动网络（PLMN）通常包括几个移动服务交换中心（MSC）10。每个这样的中心连接至多个基站子系统（BSS）6（为清楚起见，只示出了一个 MSC 和 BSS）。该基站子系统 6 通常包括一个基站控制器 BSC 和必要的接口装置，并连接至多个基站 4，每个基站监视称作为一个单元（对于单元，见图 7）的一定的地理区域。

图 1 的移动服务交换中心 10 还通过一个交换机 12 和线路 12 连接或链接至公共交换电话网（PSTN）。MSC 也连接至全球通信网，在本例中为互联网（由数字 43 标明）。MSC 可以连接至集成服务数字网络（ISDN）或任何其它类型的合适的通信网络。在不同电讯网络系统的不同部件之间的必要链接本身在技术上是已知的。

PLMN 网络还包括连接至 MSC 的称为本地位置注册表（HLR）的一个数据库。这些为移动电讯网络的订户的移动终端 1 和 2 在 HLR 9 中注册。每个本地移动电话交换中心 10 还包括一个称为访问者位置寄存器（VLR）8 的本地数据库，其中注册了所有这样的移动工作站 1 和 2，它们定位于由本地移动电话服务交换中心在给定时间处理的一个单元的区域之内。

移动工作站由通常在每个移动工作站安装好的，或者物理地连接的 SIM（预定确认模块）标识。SIM 为包括不同用户（预定）相关信息和密码的一个模块。它还可以包括有关无线通信加密的信息。SIM 可以固定地或可移动地安装在移动工作站上。利用 SIM 和本发明中的 HLR 和/或 VLR 寄存器将在该说明书的后面作更详细阐述。

如同已讨论的一样，用户可以通过固网或移动网或直接连接与互联网 43 连接。然而，当考虑到例如 GPRS（通用包无线系统）时在连接上有一些不同，但是互联网网络的服务对 PSTN 和 PLMN 系统的用户来说都是可用的。在本例中，移动交换中心（MSC）和 PSTN 20 通过访问节点（AN）14 和 40 提供对多重协议互联网 43 的访问。即使公开的是每个通信网络只有一个 AN，可以理解，实际上 AN 的数量

一般可以较大，而且 AN 的数量也在不断增长。根据某一个方案，一个特殊的能够转换信号为数据包的互联网访问服务器（IAS）作为互联网的一个 AN（访问节点）使用。

互联网 43 的用户已经同互联网访问提供商（ISP）42 订立合约，ISP 提供从用户端 1，2 或 16 至互联网的通信连接。当用户希望建立互联网连接时，他向互联网访问提供商（ISP）42 拨号以便将他的终端 16 连接至所希望的地址（称为互联网协议地址）。拨号连接由 PSTN 20 建立并至少通过本地交换机 18，并且可能通过一个或几个通过干线（未示出）连接或互联的转换交换机。应该理解，即使图 1 只公开一个 ISP，通过该 ISP 网络都向互联网通信，通信可以通过不同的 ISP 设备。

图 1 还公开了一个 WWW 服务器 45（万维网服务器），它包括提供不同服务的服务器数据库 x，y，z。它也公开了通过路由器 44 从 ISP 经过互联网 43 至所述服务器 45 的一个连接。可以理解，服务可以是通过任何通信网络的可获得需要认证的任何服务，如银行服务，电子商店服务等等。

当用户通过 PSTN 20，经过用户接口 16 访问，或已经访问由 WWW 服务器 45 提供的服务 x 时，移动工作站 1（或 2）作为个人认证装置（PAD）使用。移动工作站 1 通过单独的通信路径或信道与服务 x 通信，而不是被真正的用户接口 16 使用。移动工作站能被信任，因为用户通常随身携带它。移动站点和传统 PAD 在人体工程学上和功能上的要求基本上是一样的，而且 MS 有一个适用于 PAD 的用户接口。现代 MS 甚至有一个适用认证用途的安全处理器接口。

有几个选择来通过移动工作站的方式完成认证，它们的实例将在以下作更详细讨论。

现在参照图 2 和 4，其中图 2 示意性地公开了一个用于认证的设备，图 4 为依照一个基本实施例的操作的流程图。用户 22 使用用户终端 16 的方式，通过用通信网络的方式（图 2 的箭头 21；图 4 中的步骤 102 和 104）建立的连接，发送一个请求来访问所需应用 45，例如银行服务。应用 45 可以包括数据库 46，或连接至一个单独数据库，如图 1 的 MSC 10 的 HLR 9，从该数据库使该应用能取得必要的用户信息。在该信息的基础上，该应用出于认证目的，建立与用户 22

的移动工作站 1 的连接（箭头 26; 步骤 106）。在该阶段，用户可以通过送回一个确认信号 29（如，承认），接收由用户接口建立的连接，使用该移动工作站表示访问获得许可并表示服务的真正使用可以开始（步骤 108 和 112）。在认证失败的情况下，如，在该基础上应用不能到达 MS 1，关闭所有连接（步骤 110）。或者，用户可以容许立即或在一段时间段以后重试访问，或者由于认证失败用户可以由用户接口 16 指示用户采取一些额外措施。

实现本认证的一种途径或这种确认特性是使用 PLMN 的短消息系统（SMS）的短消息。在 GSM 系统中，SMS MSC（SMC 的消息服务中心）在图 1 中用 7 表示，它向移动工作站和从移动工作站分发短消息。该服务中心 7 给使用同一网络部件的移动订户发送消息，象上面讨论的一样并由参考标准。SMS 消息信令通常包括例如接收者的认证，发送者信息，时间戳等等。

图 3 公开了一个解决方案，使用该方案，移动工作站 MS 1 已接收一条 SMS 消息。它的方法步骤由图 5 的流程图示出。根据本实施例，在通过用户接口 16 访问完银行服务之后，用户已请求总数 200FIM 应从帐号 1234－4567 转移给帐号 4321－7654（步骤 204）。应用从适当的数据库取得用户有关认证数据（步骤 206），并相应地发送文本消息给移动工作站 1（步骤 208）。MS 1 如同示出的一样显示文本，并请求用户通过按“是”或“否”键来分别地确认或取消交易（步骤 210）。然后响应传送回应用，如果为“是”，交易进行（步骤 214），如果为“否”，采取一些其它步骤。

图 2 的箭头 27 和 28 也能视为说明该阶段，在该阶段 MS 1 和用户 2 通信，通过观看 MS 1 的显示 31，收到的信息用箭头 27 表示，用户给 MS 1 的响应用箭头 28 表示。如同已解释一样，用户可以通过按 MS 的 Y 或 N 键 32 来选择适当的选择。如果用户接收，即“签署”交易，银行服务将相应地进行。如果用户不确认该交易，即按“否”键，应用可以发送一个请求给用户接口来反馈一个更正，一个取消或一个新目的帐户等等（步骤 216，218）。

如果应用在某个时间段没有收到任何响应，或响应在一定程度上不正确，应用可以要么发送第两个确认请求，要么关闭所有连接。

用户可以在访问应用一次后处理几个后续交易甚至一些其它银

行服务。当用户在步骤 216 最终回答用户接口 16 他不想继续时，关闭连接（步骤 220）。

根据本发明的一个实施例，当实现创造性的认证设备时，能利用包含在 HLR 甚至包含在图 1 的 PLMN 的 VLR 中的信息。由于下列事实使之成为可能，在图 1 中的 HLR 9，每个移动预定包括已提及的有关 SIM（订户确认模块）信息，如 IMSI（国际移动订户标识）和 MSISDN（移动订户 ISDN 号码）以及位置信息（VLR 号码），基本电讯服务预定信息，服务限制和附加服务等等。

因此图 3 也公开了插在 MS 1 中的 SIM（订户确认模块）卡。电话公司通常使用 SIM 来控制支付和用户位置。因此 SIM 卡在使用和打出电话之前得连接至 MS 1。图 3 的 MS 1 还包括一个 MS PAD 控制器 35（移动工作站个人认证装置控制器）。从这里 SIM 34 可以用在本发明中作为识别用户和/或包含一个密码和几个密码的装置，MS PAD 控制器 35 用作控制认证操作。除了认证程序的一般控制之外，控制器 35 可以，例如，设备来作出所有有关各种加密操作的计算。由 MS PAD 控制器 35 控制的 SIM 34 中的装置使用的能用于认证程序的设备各有不同。这样的例子在下面作简短解释。

除了上面所指的利用 SMS 服务的设备，应用，例如银行服务或由电子交易支付的另一个商业服务，将交易详情通过移动网络作为数据信号发送至 MS PAD35 也能确认交易。信号的正确性能依照预先定义的算法并利用 SIM 34 的密码，通过 MS PAD 35 计算出的校验求和的方式得到保证：校验求和必须与用户终端 16 显示的和匹配。如果用户接收交易，他通过使用用户密码（如，当使用公共密钥加密和需要认可时），或通过使用与应用共享的一个密码，来确认它并允许 MS PAD 35 “标记”来自应用的消息信号。接着，应用将用用户接口的方法按需进行。根据某个实施例，该密码或 SIM 34 的密码能用于应用与 MS 之间的消息和/或信令的加密。

图 6 公开了图 2 的另一个实施例。在该实施例中，用户接口 16 是一个以本质上已知的方式连接至 PSTN 20 的一个普通电话终端的形式。在本实施例中该 PSTN 还连接至形成应用的智能网络服务（IN）60。移动工作站 1 包括一个 PAD 控制器 35 和一个 SIM 34，它们结合图 3 在上面已作描述。根据某个实施例，MS PAD 对，它们包括一个

给定服务的服务标识符和一个个人密码的预定义对，保存在 PAD 控制器中。这些对可以以下面方式使用。

用户通过建立对服务的电话呼叫访问所述 IN 中的服务（箭头 21）。应用用以声音消息给出的一个数字，或用可能显示在所述电话终端上的方法来询问用户（箭头 61）。用户用键盘键入回答该问题以及 MS 服务的特别数字（箭头 28），然后 PAD 控制器根据预先定义的算法完成必要的计算，来接收下一个数字字符串。在该计算中，为特别用户保存至 SIM 的密码可以形成该算法的一部分。该密码可以为一个特定于应用的密码或 PLMN 的一个密码。然后该计算结果反馈给用户接口 16（箭头 62），并通过 PSTN 20 以问题形式传送至 IN 服务。如果这与期望值匹配，IN 服务 60 容许用户通过固定线路终端 16 开始使用。

当支付通过任何普通的 POTS 线电话获得的电话呼叫或服务时，能使用上面提及的实施例。例如，这使得设备有效，它使得任何电话终端的拨叫从移动电话订户（如，从特定 SIM 卡的持有人）收费。移动订户可能发现这种服务的用处，如，在当由移动电话打出的电话比由普通 POTS 电话打出的电话贵得多时，或当 MS 1 不在任何一个用户能有一个合适的无线连接到的这样的移动网络的区域内时。

根据另一个实施例（未示出），移动工作站 1 和用户接口 16 能够直接通过适当的操作连接，如无线连接，红外线连接或与必要耦合的固定导管连接，彼此通信。这减少了误键入错误的风险，当用户作为 MS 1 和用户接口 16 之间的“链结”时可能发生这种错误。

根据另一个实施例，移动工作站 1 用来接收不只一个 SIM 卡 34。用此方式，单个移动工作站能用作不同的认证目的。例如，用户可能有 3 种不同的 SIM: 一个用于他工作所需的认证，一个用于个人需要，一个用于其它需要，如用于“协会主席”。每个 SIM 可以有一个它们自己的电话号码，振铃声等等。

根据另一个实施例，MS 1 通过 PLMN 与应用通信，这种通信所需的消息和/或信令使用密码或 SIM 的密码加密。这使得安全通信只使用一种通信网络，如 PLMN，因为 SIM 的密码是唯一的，对第三方来说是不可能获得包含在信令中的信息或破解信令。

现在参考图 1 和图 7 解释本发明的另一个实施例。图 7 公开了

一个任意地理区域的示意性单元地图，它分成几个邻近的无线覆盖区域或单元。图 7 的系统解释为只包括 10 个单元（C1 至 C10），实际上单元数量可以更大。一个基站关联于并定位于每个单元之中，这些基站分别指定为 BS1 至 BS10。这些基站连接至基站子系统（图 1 的 BSS6）。一个单元也覆盖一个或几个基站。这些单元分成四个组 A 至 D，其中某个组可以包括一个或多个单元，由相应的标记标识。

系统将每组视为一个单元，即一个区域，这样提供了四个不同的单元种类 A 至 B。这样的目的是为了说明单元可以分成不同的认证种类或类别。其背后的含义是，在认证数据库内的认证数据可以包括限制，即如果用户不在某个预先定义的单元区域之内，该限制不容许用户访问应用。例如，如果某公司使用某雇员的移动工作站用作认证，可能要限制该区域使得认证的可能性限制在只容许在公司办公室附近的那些单元内（如在区域 A 内）。

以上容易用图 1 中指定为 8 的访问者位置寄存器 VLR 的方法实现。移动工作站（MS）1 或 2 在 MSC 区域内的漫游由负责该区域的 VLR 8 控制。当 MS 1 或 2 出现在位置区域时，VLR 开始更新程序。VLR 8 也有一个数据库，它包括例如 IMSI，MSISDN 以及位置区域，在该位置区域，MS 按照例如 GSM09.02 规格注册。称之为单元全球确认，它还包括一个单元身份，并包括在 MS 1 和 MSC 10 之间的消息中。该信息可以作为确认指示器使用，来找到移动工作站 MS 1 的位置，然后用于该实施例中。

这里注意到，移动工作站能是给用户提供移动通信可能性的任何种类的装置，而不是移动电话或移动电话和计算机 2 的集成单位。后面的设备有时也指“通信工具”。其它的适合的移动工作站的一个例子是呼机，即能显示字符串的“寻呼机”。重要的是移动工作站能够接收和/或传送所需信息，在有些情况下甚至是只以文本或声音的形式而不是特定的认证信号或代码的形式。

而且，在上述实例中，应用 45 是用来提供在二个通信网络之间的链接，这样它们都能用于将用户与应用连接起来。然而，这可由一些其它方很好地完成。例如，ISP 或类似服务提供商或电讯网络营运商可以作为一个认证机构运行和/或提供二个通信网络之间链接，并向真正应用提供一个安全连接。

因此，本发明提供了一个装置和一种方法，用该方法能在认证领域实现重要改进。依照本发明的设备对于用已知的部件来实现是容易和经济可行的，并在使用上是可靠的。应该注意，本发明的实施例的前面一些例子并不是要限制定义在附加的权利要求书中的发明范畴。对于本领域的技术人员是显然的所有附加实施例，修改和应用因此也包括在本发明的主旨和范畴之中，这由附加的权利要求书提出。

00·06·24

说 明 书 附 图

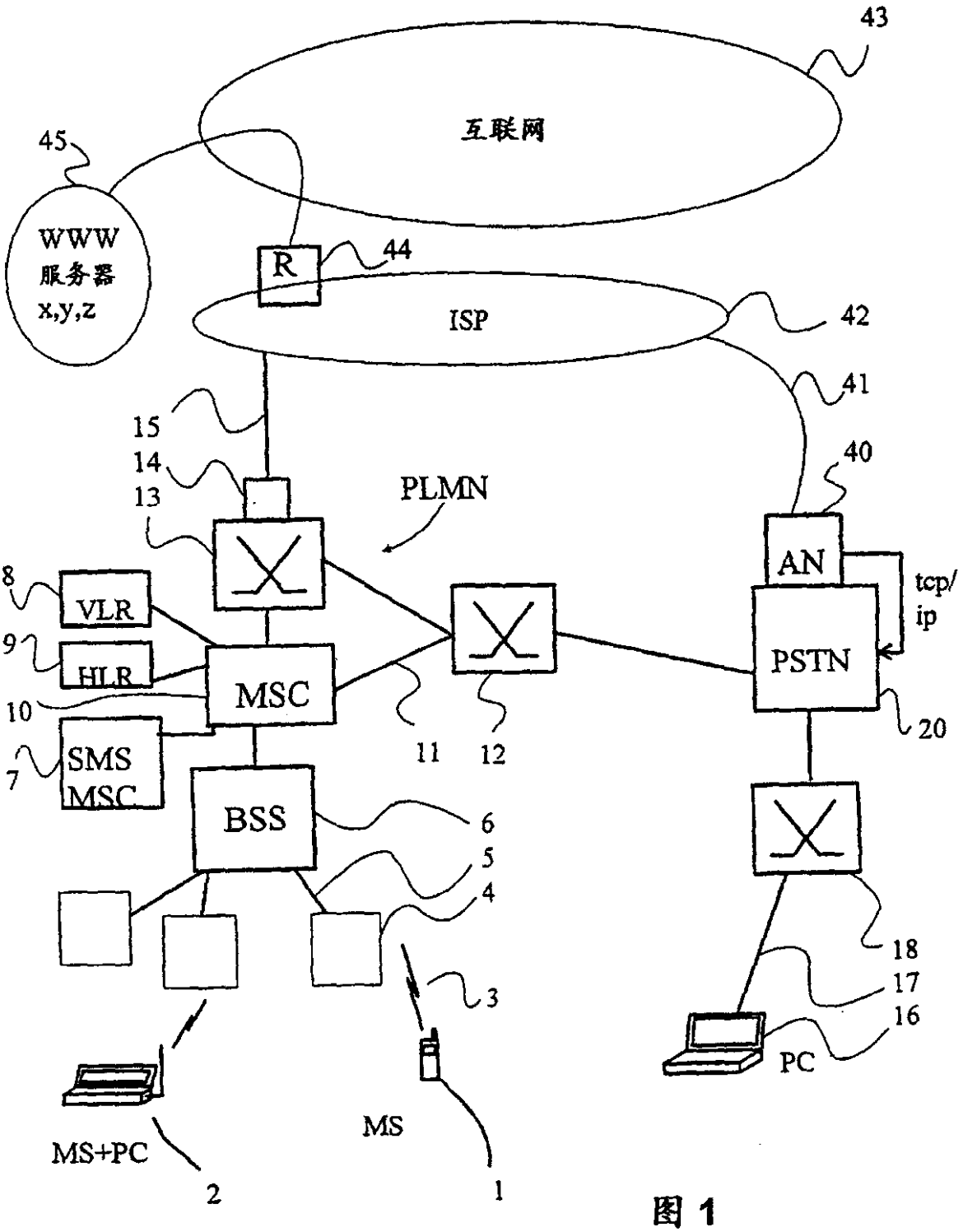


图 1

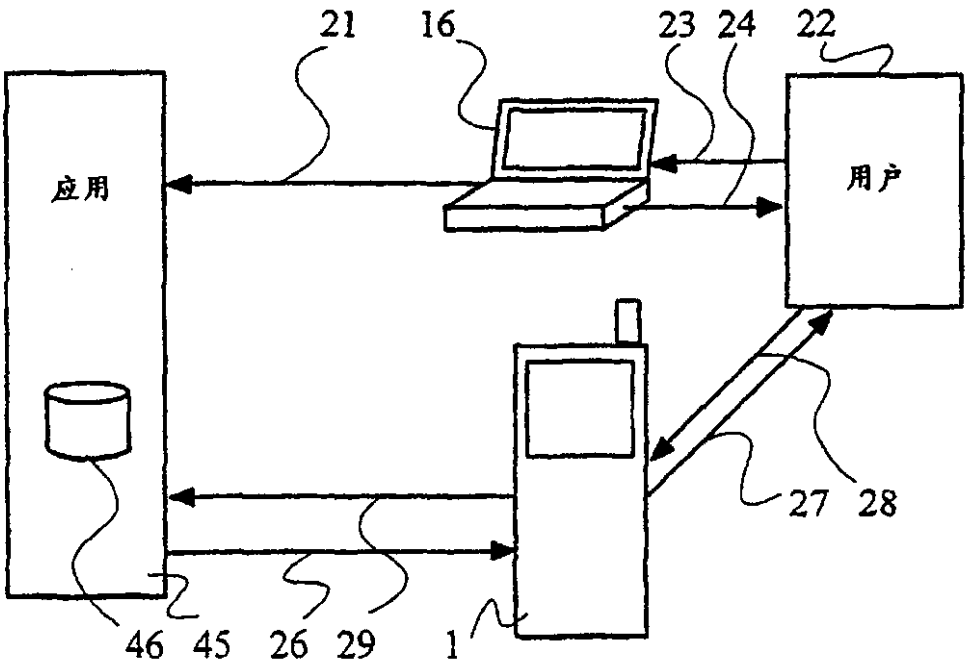

21
16
23
24
22
应用
用户
27
28
46
45
26
29
1

图 2

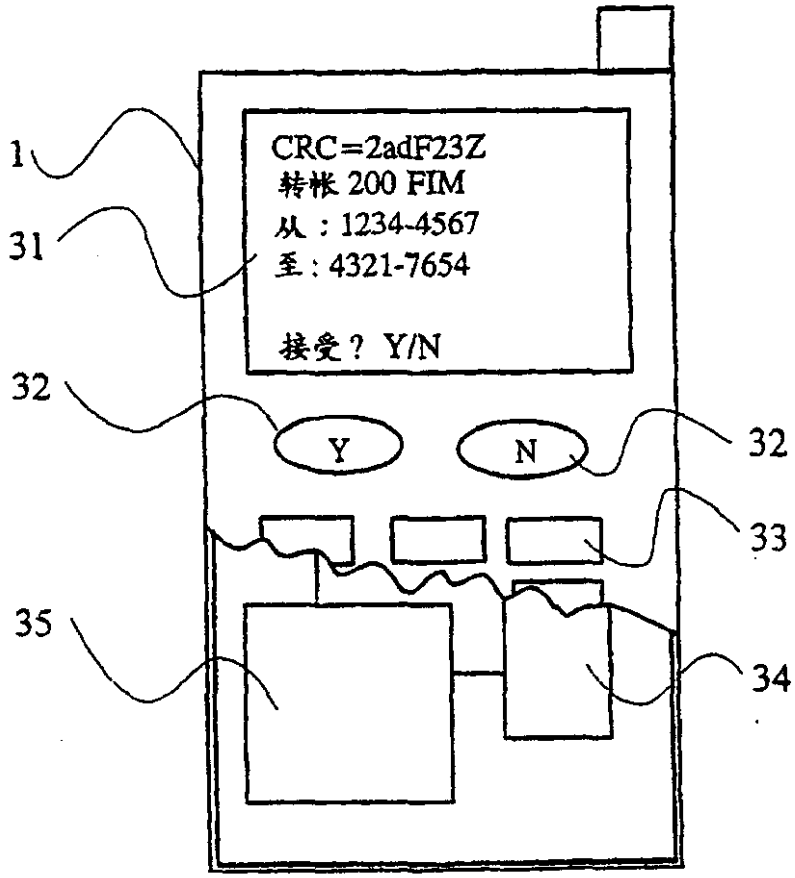

1
CRC=2adF23Z
转帐 200 FIM
从：1234-4567
至：4321-7654
接受？ Y/N
31
32
Y
N
32
33
35
34

图 3

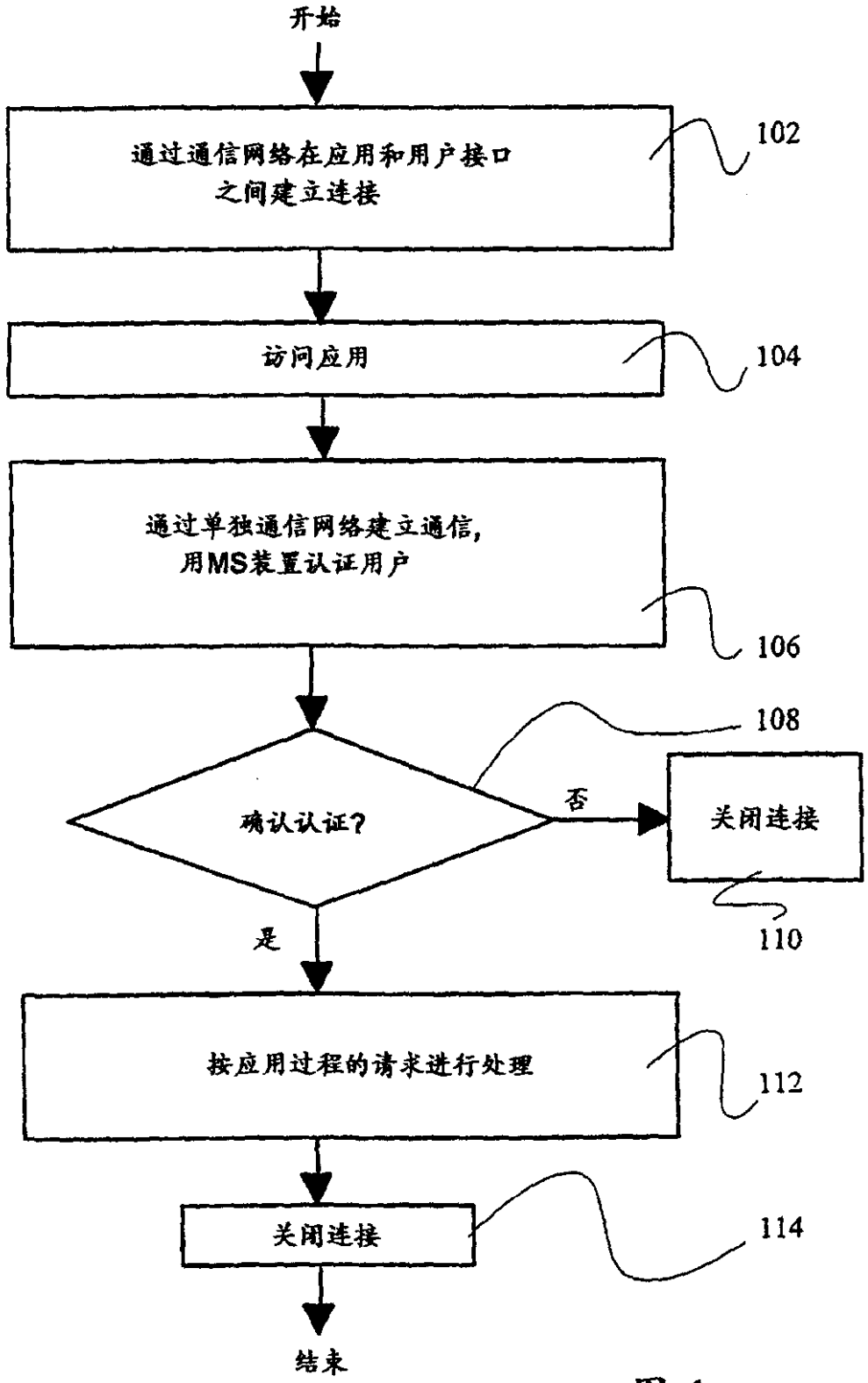

开始
通过通信网络在应用和用户接口之间建立连接
102
访问应用
104
通过单独通信网络建立通信，用MS装置认证用户
106
确认认证?
108
否
关闭连接
110
是
按应用过程的请求进行处理
112
关闭连接
114
结束

图 4

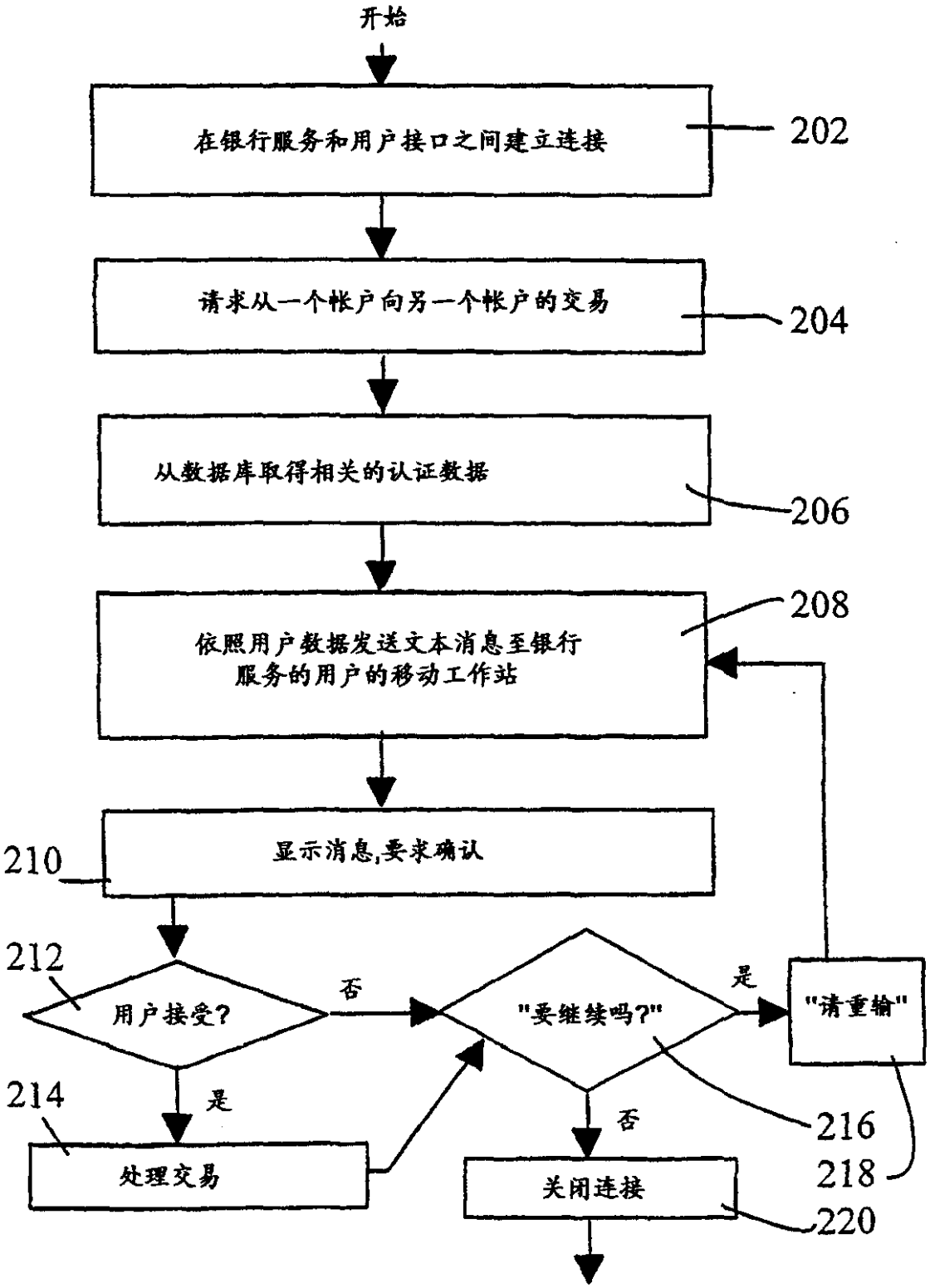

开始
在银行服务和用户接口之间建立连接
202
请求从一个帐户向另一个帐户的交易
204
从数据库取得相关的认证数据
206
依照用户数据发送文本消息至银行服务的用户的移动工作站
208
显示消息,要求确认
210
212
用户接受?
否
"要继续吗?"
是
"请重输"
214
是
处理交易
否
关闭连接
216
218
220

图 5

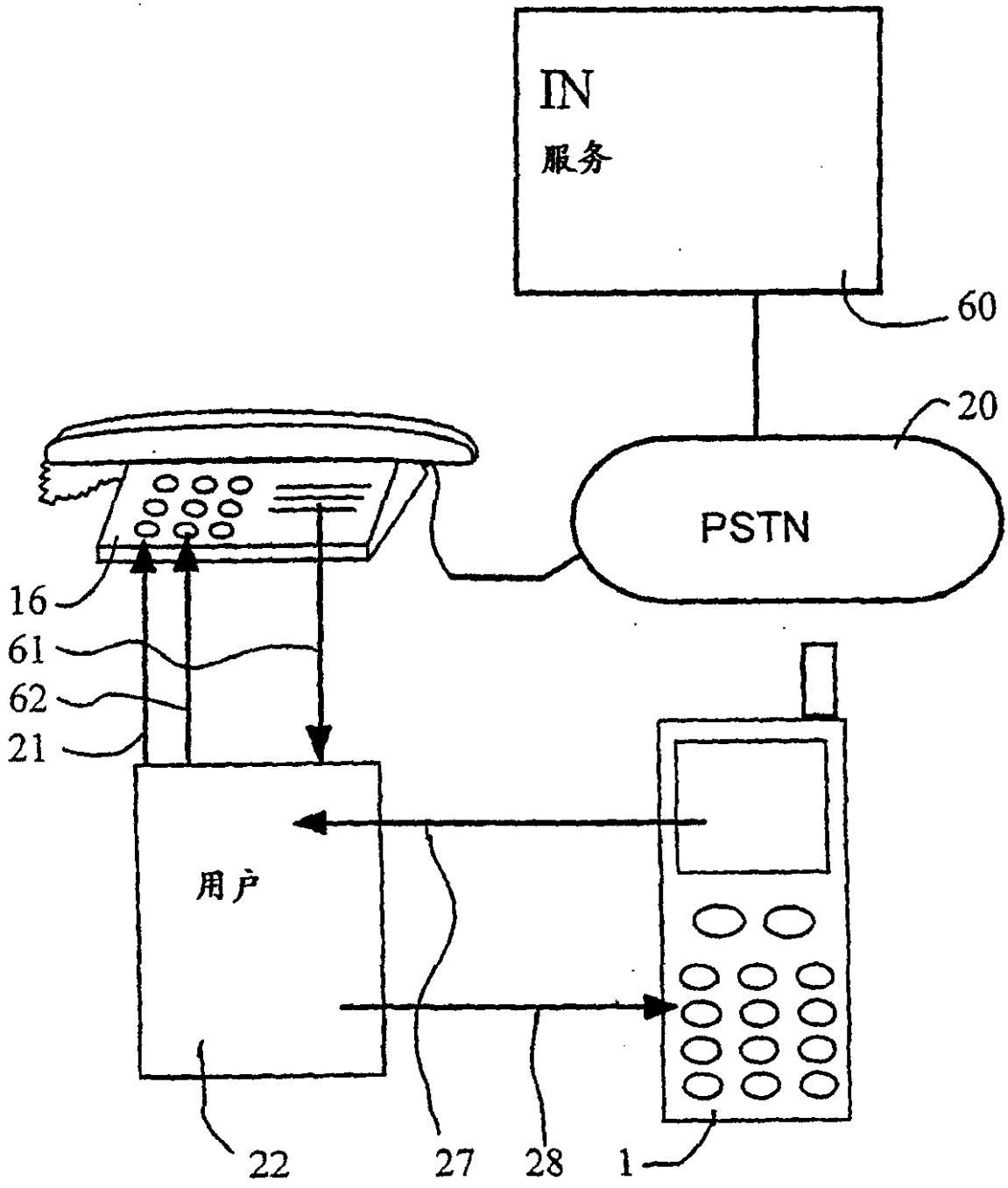


图 6

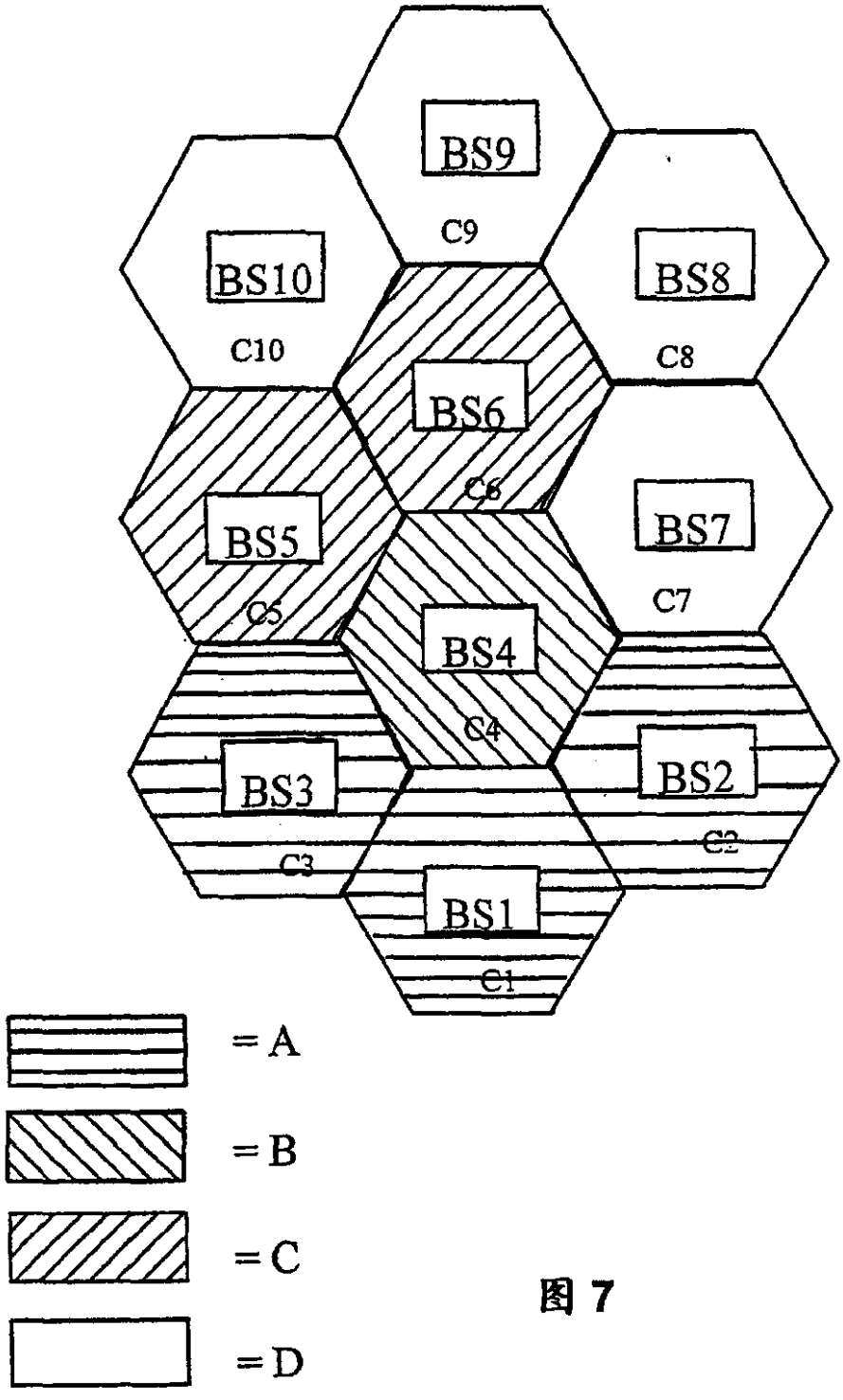

BS9
C9
BS10
C10
BS8
C8
BS6
C6
BS5
C5
BS7
C7
BS4
C4
BS3
C3
BS2
C2
BS1
C1
=A
=B
=C
=D

图 7