(54) Title: METHOD FOR ESTABLISHING CONNECTIONS TO A DATA NETWORK

(57) Abstract: Method (500, 700) for establishing a connection to a data network, in which method a call is connected to the modem pool apparatus (211, 212, 503, 701) from a certain call number in the telephone network, the modem pool apparatus being connected to the data network of the connections operator. The further connections relating to the said call are given a certain data network address (213, 507, 705) as the output address, and the first connection is established to a certain data network address (214, 215, 507, 703). The method is characterised in that the said call number is connected to the modem pool apparatus, to which at least two call numbers may be connected; part of the line capacity of the modem pool apparatus is reserved for the said call number; and the data network address (204) is determined, to which the first connection is established.
Method for establishing connections to a data network

The invention generally relates to the establishment of connections to a data network. Especially the invention relates to the offering of data network connections, using the telephone network as access network.

The use of data networks, for example Internet and World Wide Web (www) increases all the time, and more and more people have a connection to a data network also from home. If the computer is not directly connected to the data network, the data network connection may be realised through the telephone network. A modem connected to the computer is used for calling to a modem pool, which is connected to the data network of a connections operator. In general, both the modem pool and the data network, to which it is connected, are owned and controlled by a specific connections operator. Usually, the data network of the connections operator is connected to a public data network, for example the Internet network, so that it is possible to establish a connection to servers connected to the public data network from a computer provided with a modem through the modem pool. During some times of the day, the number of telephone lines for the modem pool is not necessarily sufficient, and part of the users do not get a connection they want to the data network.

More and more companies want to serve their customers through data networks, and even wish that their customers use these network services instead of traditionally visiting the company’s office. The simplest way for offering network services is to connect the server offering the services to the public network. In this case, the company usually tries to inform its customers about the network services, for example, by ways of traditional advertising, but it depends on the activity of the customer, whether he/she will use these services.

Companies offering network services to their customers are probably interested in the possibility to offer their customers or other interest groups a direct access to the company’s network services. By offering data network connections through separate modem pools and other related installations, the company may design its equipment so that modem pools will not become jammed, and thus be able to offer its customers a data network connection service of better quality than the connections operator. This kind of service, in which the customer, for example, connects directly to the company’s network services from home using a computer and a modem, could also include access to a public data network.
A company, which is actually not engaged in the offering of data network connections, but which offers network services and related data network connections to one of its interest groups, is called a portal company, and the data network service it offers is called a portal. Besides network services offered by a portal company, the portal may, for example, include access to a public data network. For example, banks, insurance companies, or shops, are possible portal companies.

Figure 1 shows a typical state-of-the-art installation for establishing a connection to a data network so that a telephone network works as the access network. The user’s computer 101 comprises a modem 102. This modem is connected to the modem pool 120 through the telephone network 110. The connection travels through a circuit-switched connection 111, and data transmission protocols defined for modems are used in it. The modem pool is connected to the own data network 130 of the connections operator. This data network uses data transmission protocols, for example Internet protocol (IP), or other packet-based protocols. The data network 130 is provided with an authentication server 140, the task of which is to make sure that the user calling the modem pool is a customer of the connections operator, before the connection is allowed further into the data network. The authentication is usually conducted by supplying user ID and password. After the user has been authenticated, a connection is generally established, for example, to the www server of the connections operator, and the main page of the connections operator is loaded to the user’s browser.

In the data network 130 of the connections operator, there often is also a chat group server 141 and an e-mail server 142. Further, the connections operator may offer the user a possibility to form, for example, own www homepages. For this purpose, the user receives a certain amount of disc space from the www server. If the connections operator offers access to the public data network 131, the data network 130 is connected to the public data network at least through one edge router 150. This public data network generally is the Internet network.

In order for the connections operator to offer its services nationally, it has to have at least one modem pool in every telecommunications area. Otherwise the calls of the users to the modem pool are expensive long-distance calls. In Figure 1, there is shown a second local telephone network 112 and modem pool 121, and the connection 113 travelling through them to the data network of the connections operator. The connection of a user calling from another telecommunications area to the data network of the connections operator and therethrough to the public data network
travels through these installations. In addition, the connections operator has to have a national core network for data transmission connections.

Thus, operating as a connections operator demands a lot merely from the installations, with which the connection to the data network is offered. If it is desired to invoice something else besides the fixed monthly fee from the users, a system further has to be built, which follows, for example, the connection time of each user. In addition, a help desk service is required, which helps the users in problematic situations and preferably at any time of the day or night. Offering data network connections especially to home users thus requires a considerable number of devices and personnel. It hardly is profitable for a portal company to acquire and maintain all the required installations.

In a state-of-the art solution, operating as a portal company is possible in the most economical way by renting modem pools for the use of the portal company from a connections operator. If the portal company wishes to offer the users a connection to a public data network, the only practicable alternative should be the renting of a modem pool. The modem pool number of the portal may be connected to the rented modem pool, and the modem pool in question will be reserved for the users of the portal, only. The callers are authenticated, and if the authentication is successful, a connection is established to the network service of the portal company, for example to the www server. After this, the user may connect to any addresses in the public data network he/she wishes through the installations of the connections operator.

A problem with this kind of portal operation is that the portal company has to rent or otherwise acquire a modem pool from every telecommunications area. The renting price is higher than what the connections operator invests in the operation in question, as the connections operator has to gain profits from the renting activities. In addition, the price goes up also because the connections operator, from which the modem pool has been rented, cannot use the possibly free line capacity for other connections.

Problematic is also that modem pools are generally designed for large numbers of connections. A portal company may thus acquire for its use only large numbers of telephone lines at a time. For example in a telecommunications area, in which there are only few portal users, part of the capacity of a modem pool may always remain unused. Also in a situation in which the line capacity of a certain modem pool is no more sufficient, the portal company cannot acquire just the exact number of tele-
phone lines it needs, but it probably has to pay rent for a large number of unused telephone lines.

The object of the invention is to present a flexible method for offering data transmission connections in the portal company's own name by using the installations of the connections operator. The objective is that the line capacity of the portal may be changed according to need. Further it is preferable that the portal company may determine the data network services that will be offered to its users.

The object of the invention is achieved by reserving the portal a modem pool number of its own and a related number of lines from such a modem pool, which groups the callers on the basis of the call number used, and by determining the data network address, to which the connection is first opened.

A method according to the invention for establishing a connection to a data network that in this method

- the call is connected from a certain call number of the telephone network to a modem pool apparatus, which is connected to the data network of the connections operator;

- the further connections related with the said call are given a certain data network address as the output address; and

- a first connection is established to a certain data network address is characterised in that

- the said call number is connected to a modem pool apparatus, to which at least two call numbers may be connected;

- part of the line capacity of the modem pool apparatus is reserved for the said call number; and

- the data network address is determined, to which the first connection is established.

In the method of the invention, a modem pool is utilised, to which several call numbers may be connected and in which a certain number of lines may be reserved for each call number. Such a modem pool is suitable for the priorisation of users, i.e. certain users may be offered a better service by reserving a certain number of lines for their use only. In addition, the reserved number of lines may be increased or de-
creased continuously according to need. The users of the portal (for example customers or employees of the portal company) are thus given an own call number for the modem pool. When required, the portal company may arrange more line capacity for its use from the modem pools, to which most of its customers call. Thus, this arrangement is flexible from the point of view of the portal company. The connections operator may rent out line capacity for several portals from the same modem pool.

In the method of the invention, the modem pool or a similar installation of the network connections operator is used. Then it is also possible to easily offer connections elsewhere than to the network services provided by the portal company. From the point of view of the users, the portal is the more attractive, the better connections it is able to offer to the data network. The first connection to the data network is established to a predefined data network address, which may, for example, be the www server of the portal company. Thus it is guaranteed that the users of the portal company visit the www page of the portal company. Further, if the portal company wishes to call the data network connection service provided by it, for example, by the name "portal network", it is important that the user's impression is that by calling a certain number he/she will get a connection to this portal network, and from there possibly further to a public data network. The address of the first connection may be determined, for example, on the basis of the call number or by placing fixedly a certain data network address to a program delivered to the user, which he/she uses for establishing the data network connections.

Each person calling the modem pool is given a data network address, which usually is relating to the particular call. In the method of the invention, the users connecting to the portal company may be given data network addresses from a certain group of addresses reserved for the portal company. In this case, the users of the portal may be separated from the connections operator's own customers also on the side of the data network. For example, the access of the portal's users to chat group servers may be denied or it may be restricted, if the portal company does not wish to offer this service. Also access to a public data network may be restricted on the basis of the output address; for example, international connections may be denied from certain output addresses.

The users are generally authenticated before the establishment of the first connection. However, if the portal company, for example, offers mainly information and advertising services, the authentication may be left undone. In this case anyone, who has knowledge of the call number for the portal, may connect to the portal
network. If for example, the portal company wishes to offer its users certain services, all customers may be given the same authentication data. This method may also be used in the case in which every caller has to be authenticated for technical reasons.

The users may also be given personal authentication data. For example, when offering connections for remote work, the data security requirements are high, and besides authenticating the caller, the connections have to be encrypted. The method of the invention may also be used for offering remote work connections, if it is only provided with the necessary data security functions. Connections for remote work have traditionally been realised by using a data transmission capacity exclusively reserved for a certain company for the data network connections.

The users of the portal pay the portal company for the use of the data network connections according to an agreement. The portal company again rents the modem pools and other possible network services from the connections operator. The connections operator may also manage, for example, the help desk service on behalf of the portal company, to which the users of the portal may call and ask about matters related with the data network connections. The portal may be given an own help desk telephone number, and the help desk personnel of the connections operator may answer the calls coming to the number in question with the portal’s name.

The advantages of the method of the invention include at least the following matters. The portal company may continuously rent line capacity from the connection operator according to need. The users of the portal may be offered a connection to the data network so that the connection operator remains invisible: from the point of view of the user, the portal company offers both the data network connections and the certain network services. The users of the portal may be separated from the customers of the connections operator, for example, on the basis of the given network address, and the access of the users of the portal to different network services may easily be restricted, when desired. Certain extra services, which the connections operator usually offers its users, may be combined to the portal. For example, the help desk service is such an extra service. Also these extra services may be offered in the own name of the portal company.

The invention is next described in more detail, referring to the advantageous forms of embodiment of the invention and to the enclosed drawings, in which

Fig. 1 shows the state-of-the-art way for establishing data network connections;
Fig. 2 shows the method according to the first advantageous embodiment of the invention for establishing data network connections;

Fig. 3 is a diagrammatic view of the installation, with which the method according to the second advantageous embodiment of the invention may be realised for establishing data network connections;

Fig. 4 is a diagrammatic view of the installation, with which the method according to the third advantageous embodiment of the invention may be realised for establishing data network connections;

Fig. 5 is a flow diagram of the method according to the fourth advantageous embodiment of the invention for registering the users of the portal;

Fig. 6 is a diagrammatic view of the installation, with which the method according to the fifth advantageous embodiment of the invention may be realised for establishing remote work connections; and

Fig. 7 is a flow diagram of the method according to the fifth embodiment of the invention for establishing remote work connections.

Figure 1 was referred to already in connection with the explanation of the state of the art.

Figure 2 shows the method according to the first advantageous embodiment of the invention for offering data network connections. In the method, the user connects to a certain call number reserved for the portal company in a telephone network with a modem 102 connected to his/her computer 101 or a similar device transmitting digital data over the telephone network. This number is indicated with the letter A in Fig. 2, and the call between the user’s modem and the telephone network is indicated with the arrow 210. From the local telephone network 110, the call is connected to the part 202 of the modem pool 201, corresponding to the call number A (arrow 212). The portal company has reserved a certain number of lines from the modem pool of the data network connections operator, which are reserved for the users of the portal. The modem pool may, for example, be a Cisco 5X00 modem pool, the software of which makes it possible to reserve modem pool capacity for different call numbers and to group the callers on the basis of the call number.

It is possible for the connections operator to rent lines to several portal companies from the same modem pool. The connections operator may have left part of the ca-
pacity of the part 203 for the use of its own customers or left it unreserved for any modem pool. The unreserved capacity may be used in rush situations, if for example, the line capacity reserved for a certain portal is completely in use. In this kind of situation, it is also alternatively possible to act so that a call called to the call number of the portal in question is not connected, or it is connected by using a line capacity, which is reserved for some other portal or for own customers of the connection operator.

Next it is checked to which data network address the user is first to be connected (arrow 213). In Fig. 2, this is shown in the separate block 204, in which the calls to the call number A are directed to the address B. This block, in which the address for the connection to be established onwards from the first modem pool is determined, may, for example, be realised with the software of the modem pool or, if the caller is authenticated, with the help of the authentication server. Another alternative is that the program, which is driven in the computer of the user, comprises this information, and it relays the address to the data network of the connections operator through the modem pool. In Fig. 2, the first connection is established in an exemplary way to the www server 220 of the portal company through the data network 130 of the connections operator (arrows 214 and 215).

Each caller has to be given a data network address as output address. If the user does not have access to public data networks, this address may be the address of the internal network of the connections operator, for example, an IP address in the form of 10.xxx.xxx.xxx. If the user establishes connections to public networks, the output address has to be unequivocal world-wide outside the data network of the connections operator during the connection. For example, the address of the user in the network of the connections operator may always be the address of the internal network of the connections operator. If the user establishes connections outside the network of the connections operator, his/her network address is modified at the edge of the network of the connections operator to an address of the public network reserved to the connections operator, for example, with the Network Address Translation method. The connections operator may, for example, have a number of IP addresses, of which it selects one that is free.

In the second advantageous embodiment of the invention, a program to be installed to the computer is delivered to the user, to which both the call number of the portal and the address of the www server of the portal company are determined. For example, it is possible to determine the starting page into browser programs so that it
cannot be changed. As the user starts the browser program, it may automatically connect to a predefined call number and from there to the said starting page.

In the method according to the second advantageous embodiment of the invention, the user is authenticated before further connections are established. For example, the portal company may have distributed the same authentication data to all its customers.

Figure 3 presents an example of an installation needed for the establishment of connections to data networks according to the second advantageous method of the invention. The modem pool 201 is connected to the data network 130 of the connections operator. The server 220 of the portal company is either connected to the data network 130 of the connections operator or to the public data network 131, for example the Internet network. These networks are connected to each other with at least one router 150.

If the server of the portal company is connected to the data network 130 of the connections operator, the connections operator may also be in charge of the maintenance of the server. In this case, the portal company only needs to provide the contents, for example, to its www pages. The authentication server 140, which may, for example, be a Radius or Tacacs server, is in charge of the authentication. The users of the portal may also be allowed access to the e-mail server 142 and the chat group server 141.

In the method according to the third advantageous embodiment of the invention, the data network for establishing connections restricts the access of users related with the portal company to the public data network. The users may be totally denied access to the public data network, so that the portal comprises the network services provided by the portal company, and according to agreement, the services maintained by the connections operator in its data network. The access of the users to the public data network may also be restricted so that they have access to certain addresses, for example addresses, which are accessible through the domestic trunk network.

Figure 4 shows an example of an installation, with which the method according to the third advantageous embodiment of the invention for establishing data network connections may be realised. The modem pool 201 is connected to the data network 130 of the connections operator. Also the server 220 of the portal company has been connected to the same network in an exemplary way. Thus, the connections estab-
lished by the users of the portal may be restricted only to devices the data network 130 comprises, when desired.

If one wishes to restrict the connections established by the users of the portal, for example, to internal connections in the domestic trunk network, this may be done, for example, in the router 401, which connects the data network 130 of the connections operator through the connection 403 (domestic trunk network) to the domestic data network 131a and through the connection 402 (connection to the connecting point of a foreign data network) to the data network 131b. The router 401 has to know how to restrict through-going connections on the basis of the output address. If it has been defined into the router that a certain IP address group is prevented access out from the network 403 through the connection 402, the input address of the users of the portal may be selected from this IP address group.

Another example of the restriction of connections established by users is the use of the proxy server 410. It may be defined either into the browser program in the user’s computer or into the network elements of the data network of the connection operator, that the connections will be established through a certain proxy server. This proxy server 410 is located in the data network of the connections operator, and if the establishment of a certain requested connection is allowed, the connection is established. The proxy server may also keep a certain number of files retrieved last in its memory (for example, www pages), and to return the desired file from the memory to the user, if it is fresh enough. Thus, connections abroad may be reduced, even if they were allowed.

In the method according to the fourth embodiment of the invention, a certain program is distributed to the users, into which the data network address of the first further connection is defined. In addition, all the users are given a common registration identifier. As long as the user has not been registered as a user of the portal and given an identifier of his/her own in connection of the registration, his/her access to the network services is restricted.

Figure 5 shows a flow diagram of the method according to the fourth advantageous embodiment of the invention. At 501, the user is supplied with a data network connection program, for example a www browser program, and all users related with the portal company are given a common registration identifier and password. For example, a certain starting address is defined to the browser program as the starting page. At 502, the user calls the modem pool, in which a certain number of lines has been reserved for the portal company, and at 503, the user is authenticated. If the
authentication is not successful, the telephone connection to the modem pool is cut off. This is not shown in Figure 5. At 504, the user identifier given by the user is checked, and at 505 and 506, the user is supplied with a data network address of a certain type as the output address. If the user is authenticated by using the common registration identifier, his/her output address is, for example, an IP address of the form 10.xxx.xxx.xxx (505). A user using his/her own identifier in the registration, gets, for example, an IP address of the form 193.xxx.xxx.xxx (506).

At 507, the first further connection of the user is established to the predefined starting address. In this starting address the program, which is realised, for example, with the cgi (computer graphics interface) commands, checks the network address requesting the connection. If it is of the form, which is given to unregistered users, the user is connected to the address at 508, comprising the registration page. When the user has filled in the registration form or otherwise supplied the corresponding data, he/she is given a personal authentication identifier and password. Upon calling the call number of the portal company the next time and upon using his/her own authentication identifier, he/she is connected, for example, to the home pages of the portal company at the address www.portaali.fi (509).

The IP address the user has received may be used for restricting the network service range. For example, the access of IP addresses of a certain form, such as 10.xxx.xxx.xxx, to the public data network may be prevented.

Determining the data network address of the user on the basis of authentication data or determining the network address of the further connection on the basis of the user's network address that are used in the fourth advantageous embodiment of the invention are very suitable to be used also in separating the users of the portal and the own customers of the connections operator. Even if network addresses, with which it is possible to establish connections to the public network, were given both to the users of the portal and the users of the connections operator, they may still be selected from different address groups. The address group reserved for the portal may be prevented access, for example, to the chat group server.

A corresponding separation of registered and unregistered users, or different user groups in general, may be conducted also by reserving an own call number for both the user groups. In this case, the output address may be given on the basis of the call number.
The network address of the first further connection may also guide the connection forwards. Such a forwarding guidance may, for example, be utilised during certain advertising campaigns: usually, the user is first connected to the home page of the portal company, but during the campaign, the starting page may be a page advertising some product.

With the method of the fifth advantageous embodiment of the invention, it is possible to offer secured remote work connections through the public data network. An example is taken up next, in which a certain company has rented line capacity from the modern pools of a data network connections operator in order to make remote work possible for its employees. Thus, the company in question works as a portal company, offering data network connections for its employees.

Figure 6 shows an installation, with the help of which, for example, remote work connections according to the invention may be provided. The portal company wishes to offer its employees a secured connection to its data network 600, which is connected to the public data network 131 through the firewall server 601. Also the data security server 602 is located in the network of the portal company, this server being in charge of the authentication of persons entering the network and of the encryption of the connections. The company has distributed authentication data for its employees. In general, the user identifier and password are not considered a very strong authentication, so the company may, for example, have distributed an intelligent card 605 and an intelligent card reader 606 for its employees engaging in remote work. Besides the intelligent card and the intelligent card reader, the employee has to install a certain program controlling the reader into his/her computer.

Figure 7 shows a flow diagram of opening the remote work connection. As an employee tries to call the company’s call number (701), he/she may, for example, authenticate himself/herself as an employee of the portal company by using a group identifier (702). This authentication is carried out by the authentication server 140 of the connections operator. This authentication may also be skipped, and a further connection of the employee may be established directly to the profile data security server 603, which is located in the data network 130 of the connections operator (at 703). This profile data security server 603 contains the necessary data of the employees of the portal company. If, for example, data security functions using the public-key cryptography is used, the intelligent card 605 and the profile data security server 603 may authenticate each other with methods of public keys (704). Further, they may encrypt the encryption key by using the public keys of each other, this encryption key being then used for encrypting the connection. Thus, the encryp-
tion key does not travel in the data network or telephone network in plain text. For example, the encryption key may be agreed upon so that the first party of the connection generates the encryption key and sends it then to the second party, encrypted with the public key of the second party. It is also possible, that both parties participate in the generation of the secret key by using, for example, the Diffie-Hellman method. Generally, traditional encryption methods are used for encrypting the actual connection, in which an encryption key agreed upon beforehand is used.

As the employee has authenticated him-/herself, for example, with an intelligent card, and a secured connection has been established between his/her computer 101 and the data network 130 of the connection operator, the employee is given a data network address as output address, which is, for example, of the same form as the addresses used in the data network 500 of the portal company (705). This is necessary, if the firewall server of the portal company has been configured so that only certain data network addresses may establish a connection through it.

Next, a secured connection is established between the data network of the portal company and the data network of the connections operator. This may, for example, be done so that the profile data security server 603 contacts the data security server 602 of the portal company, and these agree upon the encryption key to be used for securing the further connections established by the employee (706). These servers may also be responsible for data encryption and decryption. Another alternative is that these servers relay the agreed encryption keys, for example, to routers, which actually are responsible for the data encryption and decryption.

Thus, the connection between the computer of the employee and the data network of the portal company is secured (707) in two parts: first, the distance from the employee’s computer to the data network of the connections operator, and then from the data network of the connection operator to the data network of the portal company. For example, IPSEC methods may be used for encrypting the connection between the data networks of the connection operator and the portal company, with which it is, for example, possible to encrypt the contents of the IP packets. Inside the data network of the portal company, the connection again is in plain text.

If for example, the intelligent card is in charge of the connection travelling over the telephone network, it may be necessary to encrypt this connection with a shorter encryption key than a connection travelling in the public data network, as the processing capacity of the intelligent cards is not necessarily sufficient otherwise. The shorter encryption key does not necessarily deteriorate the level of data security in a
substantial manner, as the telephone network is physically more secure than, for example, the Internet network.

Another alternative is to encrypt the connection so that the employee’s computer and the data security server 602 are responsible for data encryption and decryption. In this case, the data encryption is conducted, for example, with a program suitable for this purpose, and the IPSEC protocol is not necessarily needed for securing the connection between the data networks of the connections operator and the portal company.

With its certain profile data security server or server cluster, the connection operator may serve several portal companies. The name VPN (virtual private networks) is often used of the encrypted connections over the public network. The authentication data used may either be distributed by the company for its employees or, for example, it may comprise identifiers granted to citizens by authorities.

A corresponding method may, for example, be used by a bank, if it wishes to offer its customers secured network services. If a browser program has been supplied to a user, it may have been modified so that it does not save temporary files to the disk. In this way it is prevented that account data or some other data of the user remains in the computer disk to be read by other users.

Above, the www server, e-mail server and chat group server have been used as examples of network services and their realisation in the data network. However, the network services referred to in the invention are not limited to these services only, and the term server refers generally to a network element to be connected to the data network, to which a connection may be established in some defined way through the data network.

Above, a browser program has been used as an example of a program, which is installed into the computer of the user and which the user uses for establishing data network connections or using network services. Also other programs, with which connections may be established to the data network, may be used in methods according to the invention.

The methods according to advantageous embodiments of the inventions shown above are only examples of applying the invention. The invention may also be applied in may other ways within the scope of the enclosed claims.
Claims

1. Method (500, 700) for establishing a connection to a data network, in which method
   - a call is connected from a certain call number in a telephone network to a modem pool apparatus (211, 212, 503, 701), which is connected to the data network of a connections operator;
   - a first further connection is established to a certain data network address (214, 215, 507, 703), characterised in that
     - the said call number is connected to the modem pool apparatus, to which at least two call numbers may be connected;
     - part of the line capacity of the modem pool apparatus is reserved for the said call number; and
     - the data network address (204) is determined, to which the first further connection is established.

2. Method according to claim 1, characterised in that as the line capacity reserved for said call number is entirely in use, the call is not connected.

3. Method according to claim 1, characterised in that as the line capacity reserved for said call number is in use, the call is connected to a free line in the same modem pool.

4. Method according to claim 3, characterised in that part of the line capacity of the modem pool is left unreserved for the call numbers.

5. Method according to claim 1, characterised in that
   - the user is supplied with a browser program to be installed into the computer (501); and
   - said data network address, to which the connection is first established, is determined by locking a certain property of the said browser program.

6. Method according to claim 1, characterised in that the data network address is determined in said data network of the connections operator, into which data network address all first further connections related to calls made to a certain call number are established.

7. Method according to claim 1, characterised in that said output address is determined on the basis of the call number.
8. Method according to claim 1, characterised in that the target addresses for the further connections are restricted on the basis of the output address.

9. Method according to claim 1, characterised in that the user is authenticated upon calling said call number.

10. Method according to claim 9, characterised in that the user is authenticated with the help of the user identifier and password.

11. Method according to claim 9, characterised in that each user is given his/her own authentication data.

12. Method according to claim 9, characterised in that all users calling a certain call number are given the same authentication data.

13. Method according to claim 9, characterised in that
- all users are first given the same authentication data (501); and
- own authentication data is given for each user upon registration of the user (508).

14. Method according to claim 13, characterised in that with said same authentication data given for all users, the target address for the first further connection of the authenticated user is determined to be registration service (508).

15. Method according to claim 13, characterised in that
- the user is supplied with a browser program to be installed into the computer (501)
- the said data network address, to which the connection is first established, is determined by locking a certain property of the said browser program;
- the user is authenticated before the first further connection is established (503);
- further connections related to said call are given a certain output address (504, 505, 506) depending on the authentication data;
- at the target address for said first further connection, the output address (507) given to the further connections is checked; and
- the target address for the second further connection related to the output address related to the authentication data first given to all users is determined to be registration service (508).

16. Method according to claim 9, characterised in that said output address is determined on the basis of the authentication data.

17. Method according to claim 16, characterised in that
- the user is authenticated with own authentication data (704);
- the data related to said call is encrypted; and
- the further connections related to the call in the data network of the connection operator and the public data network are encrypted.

18. Method according to claim 17, characterised in that the user is authenticated with the help of an intelligent card.

19. Method according to claim 17, characterised in that the first further connection is established to the data security server, the user is authenticated with the help of the data security server, and the data relating to said call is encrypted with the help of the data security server.
browser and registration identifier for the user

call to the call number

user authentication

authentication identifier common registration identifier?

yes

user's network address 10.xxx.xxx.xxx

no

user's network address 193.xxx.xxx.xxx

further connection on the basis of the user's network address

registration and own authentication data

connection to the server of the portal company

FIG. 5
701 call to the call number

702 authentication with the group identifier

703 further connection to the data security server

704 authentication and agreeing upon the 1. encryption key

705 user's network address from the address space of the portal company

706 agreeing upon the second encryption key between the data security servers

707 connection to the server of the portal company

FIG. 7
INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00469

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/66, H04L 29/02
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q, H04M

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

SE, DK, FI, NO classes as above

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>P,A</td>
<td>WO 9854868 A1 (NORTHERN TELECOM LIMITED), 3 December 1998 (03.12.98), see the whole document</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>IEEE Communications Magazine, Volume 36, No 1, Sept. 1997, (Germany), Schoen, U. et al, &quot;Convergence between public switching and the Internet&quot;, see the whole document</td>
<td>1</td>
</tr>
</tbody>
</table>

[X] Further documents are listed in the continuation of Box C.  [X] See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "E" earlier document but published on or after the international filing date
  "L" document which may throw doubts on priority claimed or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search: 23 October 2000

Date of mailing of the international search report: 24-10-2000

Form PCT/ISA/210 (second sheet) (July 1992)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>P,A</td>
<td>WO 0010344 A1 (BELL SOUTH INTELLECTUAL PROPERTY CORPORATION), 24 February 2000 (24.02.00), abstract</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>US 5546379 A (LADAVAN THAWETHAI ET AL), 13 August 1996 (13.08.96), column 1, line 64 - column 3, line 40</td>
<td>1</td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (continuation of second sheet) (July 1992)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WO 9854868 A1</td>
<td>03/12/98</td>
<td>CA 2206616 A</td>
<td>30/11/98</td>
</tr>
<tr>
<td>EP 0985295 A</td>
<td></td>
<td></td>
<td>15/03/00</td>
</tr>
<tr>
<td>US 6070192 A</td>
<td></td>
<td></td>
<td>30/05/00</td>
</tr>
<tr>
<td>WO 9966690 A1</td>
<td>23/12/99</td>
<td>AU 4508899 A</td>
<td>05/01/00</td>
</tr>
<tr>
<td>FI 981364 A</td>
<td></td>
<td></td>
<td>13/12/99</td>
</tr>
<tr>
<td>WO 0010344 A1</td>
<td>24/02/00</td>
<td>AU 3093799 A</td>
<td>06/03/00</td>
</tr>
<tr>
<td>US 5546379 A</td>
<td>13/08/96</td>
<td>JP 7107114 A</td>
<td>21/04/95</td>
</tr>
<tr>
<td>US 5631897 A</td>
<td></td>
<td></td>
<td>20/05/97</td>
</tr>
<tr>
<td>US 5678004 A</td>
<td></td>
<td></td>
<td>14/10/97</td>
</tr>
</tbody>
</table>