



(86) Date de dépôt PCT/PCT Filing Date: 2000/03/17

(87) Date publication PCT/PCT Publication Date: 2000/10/05

(85) Entrée phase nationale/National Entry: 2001/10/01

(86) N° demande PCT/PCT Application No.: GB 2000/001010

(87) N° publication PCT/PCT Publication No.: 2000/058808

(30) Priorités/Priorities: 1999/03/31 (9907430.4) GB;
1999/07/02 (99305272.0) EP

(51) Cl.Int.⁷/Int.Cl.⁷ G06F 1/00

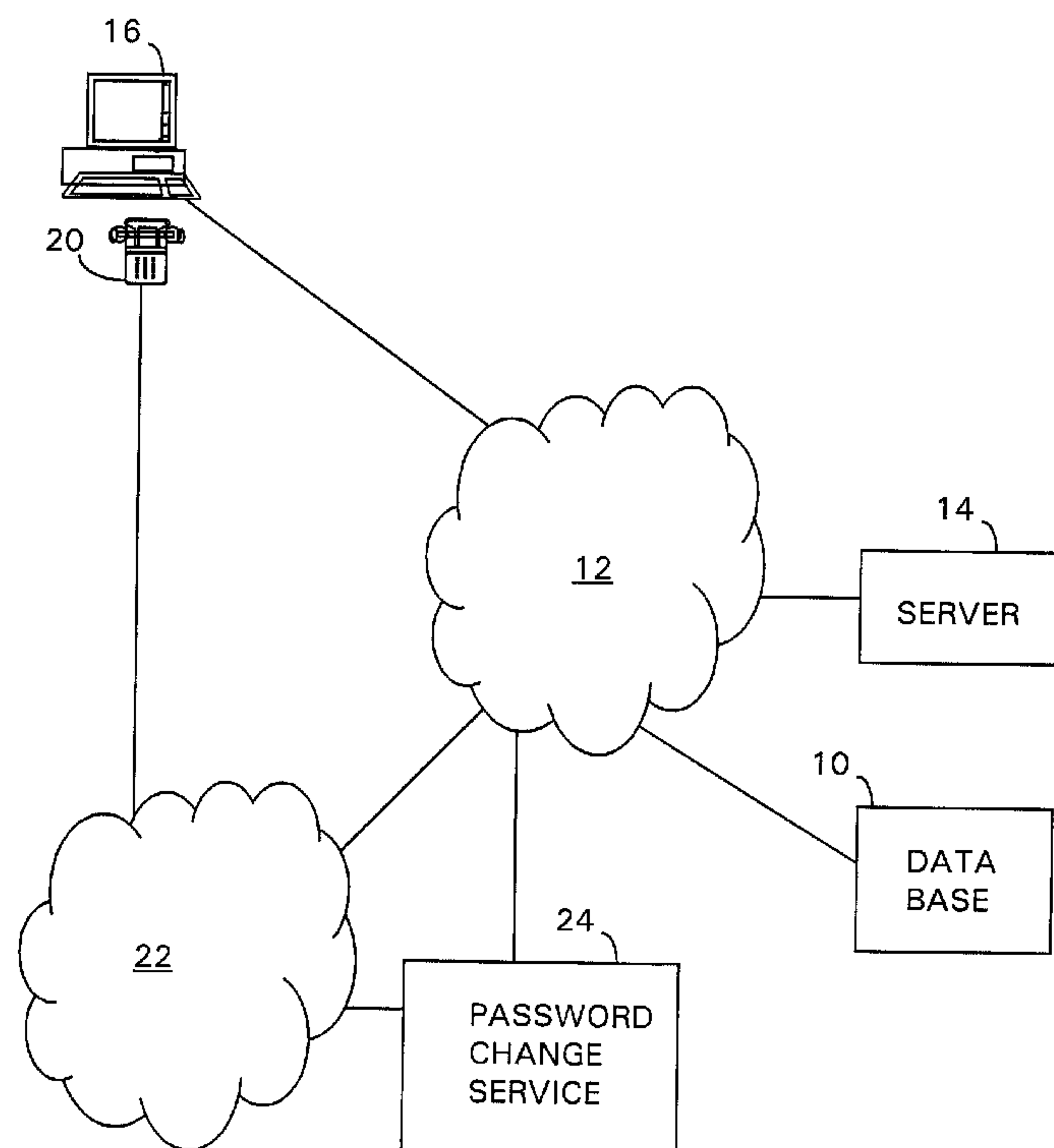
(71) Demandeur/Applicant:
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED
COMPANY, GB

(72) Inventeurs/Inventors:
EMERSON, DEREK JOHN, GB;
BROCKBANK, ROBERT GRENVILLE, GB

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : PROTECTION DE MOT DE PASSE

(54) Title: PASSWORD PROTECTION



(57) Abrégé/Abstract:

In password protection access, a nominated telephone number is used as the user identity associated with the protected information. If the user needs to change his password, he makes a call from the nominated telephone to a change password service, which automatically retrieves the calling line identity from the signalling information of the incoming call, prompts for a new password, receives the new password from the user, and records the new password in place of the previous password. There is no involvement of system administration personnel, and no consequent delay while a manual reset of the user's password is effected.

**PCT**WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ :**G06F 1/00****A1****(11) International Publication Number:****WO 00/58808****(43) International Publication Date:**

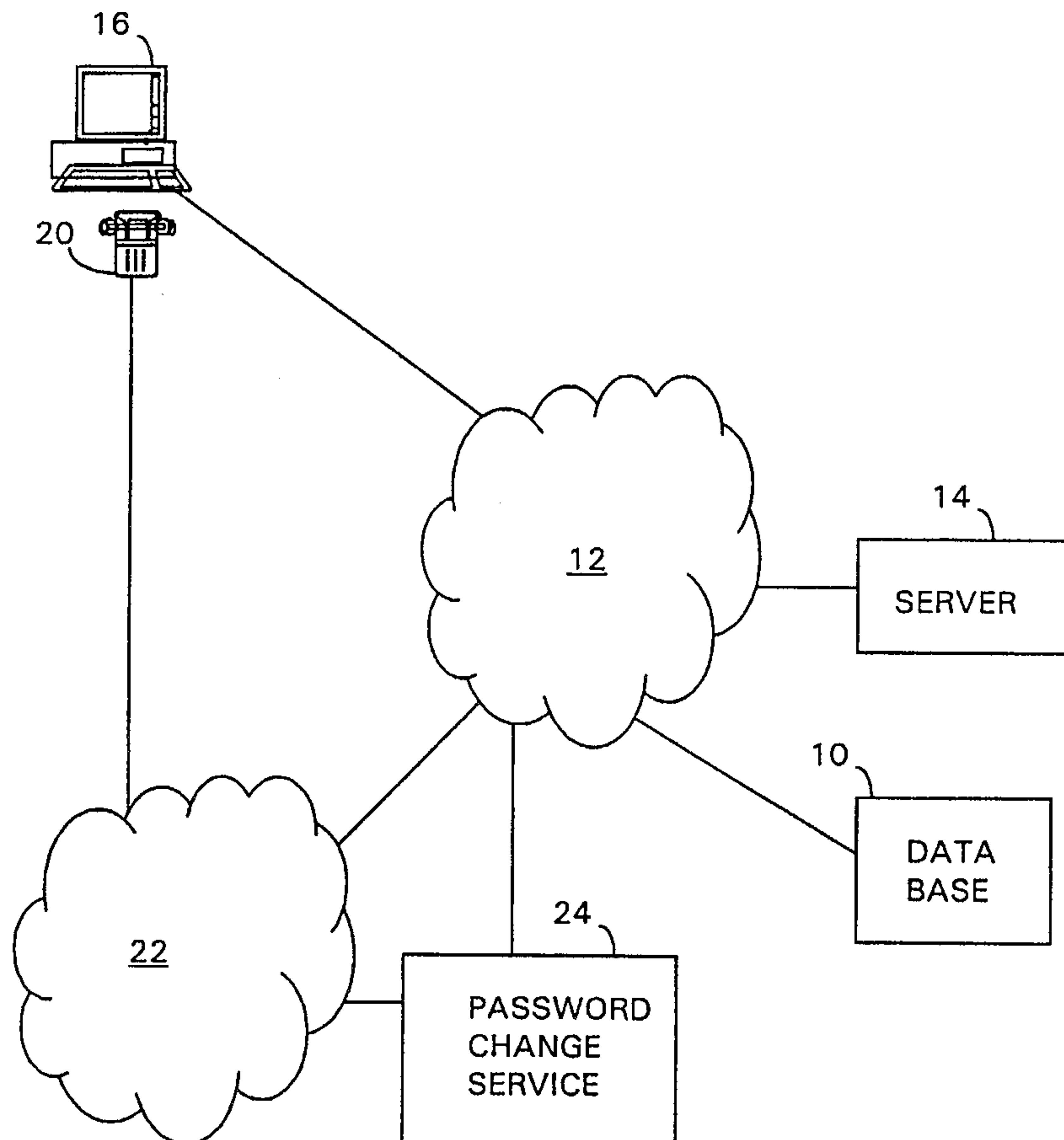
5 October 2000 (05.10.00)

(21) International Application Number: PCT/GB00/01010**(22) International Filing Date:** 17 March 2000 (17.03.00)**(30) Priority Data:**

9907430.4	31 March 1999 (31.03.99)	GB
99305272.0	2 July 1999 (02.07.99)	EP

(71) Applicant (for all designated States except US): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).**(72) Inventors; and****(75) Inventors/Applicants (for US only):** BROCKBANK, Robert, Grenville [GB/GB]; Stellar House, 78 Castle Street, Woodbridge, Suffolk IP12 1HL (GB). EMERSON, Derek, John [GB/GB]; 28 Cedar Avenue, Kesgrave, Ipswich, Suffolk IP5 1EZ (GB).**(74) Agent:** SEMOS, Robert, Ernest, Vickers; BT Group Legal Services, Intellectual Property Dept., Holborn Centre, 8th floor, 120 Holborn, London EC1N 2TE (GB).**(81) Designated States:** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, 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, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, 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.***(54) Title:** PASSWORD PROTECTION**(57) Abstract**

In password protection access, a nominated telephone number is used as the user identity associated with the protected information. If the user needs to change his password, he makes a call from the nominated telephone to a change password service, which automatically retrieves the calling line identity from the signalling information of the incoming call, prompts for a new password, receives the new password from the user, and records the new password in place of the previous password. There is no involvement of system administration personnel, and no consequent delay while a manual reset of the user's password is effected.



PASSWORD PROTECTION

This invention relates to password protection and particularly, but not exclusively, to a method of updating a password by direct user input from a telephone. In this application, the terms updating and changing are used synonymously.

European Patent Application EP 0 862 104 A (Casio Computer Co., Ltd.) discloses an authentication system in which a user's terminal device stores the user's username and his password, and for each access attempt authentication is based upon the username and password read out of the store in the terminal device and sent to the authentication server. This avoids the need for the user to remember his username and password. There is also disclosed the use of the telephone number of the terminal device as the user's username, and obtaining this telephone number from the incoming access attempt call. Thus, in this case only the user's password is required to be read from the store in the terminal device and sent to the authentication server.

European Patent Application EP 0 541 435 A (Fujitsu Limited) discloses an authentication system in which a caller provides a username and a password, which are checked. If they match an existing entry, the telephone number from which that current access attempt is being made is obtained from the incoming call, stored for use with the next access attempt for that username, and compared with the corresponding telephone number stored for the previous access attempt. If there is no match, a warning message is played and the caller is requested to enter a second password. This system helps to prevent fraudulent use of a person's username and password from a telephone different from the one that the person normally uses.

European Patent Application EP 0 745 924 A (AT&T) discloses a method of authenticating user terminal access to a service provider by means of a service bureau. The service bureau sets up a new user terminal for password authenticated access by encrypting the calling line identity (CLI) associated with that user's terminal, which the service bureau obtains from a network-based automatic number identification (ANI) unit, and sending the encrypted CLI to the user's terminal for storage as a password. When the user desires access to the service provider, he makes a call from his user terminal to the service bureau, which encrypts the CLI of

that call, automatically retrieves the password stored in the user's terminal and, upon finding a match between the retrieved password and the newly encrypted CLI, permits access to the service provider.

The service bureau is programmed for automatically changing the password
5 stored in the user's terminal. This change is effected following normal authentication of a user terminal by the service bureau re-encrypting the CLI using a different encryption key, and sending the newly-encrypted CLI to the user's terminal to be stored for use instead of the previously stored password.

Japanese Patent Application JP 07 129511 A (Nippon Telegraph and
10 Telephone Corporation) discloses a method of changing a user's password in which the user contacts the password change service (PCS) from a telephone previously designated to the PCS, gives his user ID, and then enters a new password. The PCS looks up the user's ID in its database and retrieves the designated telephone number associated with that user's ID. The PCS makes a call to that designated telephone
15 number and requests the user to enter the password again. The PCS compares this second entered password with the first entered password, and upon a match writes the password to its database in association with that user's ID.

In accordance with a first aspect of the present invention, there is provided a method of password update for a password protected access system having a
20 password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

receiving at a password update service a call from a network terminal;
retrieving by the password update service from signalling information of that
25 received call the identity of the network terminal from which that call was made;
accessing the password store in accordance with the retrieved network terminal identity; and
characterised by the steps of:

upon locating an entry whose stored network terminal identity matches that
30 retrieved network terminal identity, playing an announcement to the caller requesting the entry of a password at that network terminal; and

upon receipt at the password update service of a password entered in response to that request, writing that received password into the associated respective password store of the located entry.

An advantage of a method of the present invention is the avoidance of
5 manual password resetting procedures performed by system administration personnel. Another advantage is that it is a quick and simple one-step password entry procedure that does not involve any call-back to a designated number, and thus avoids any problems that would arise should that designated number have special call handling set, such as divert, which would result in that call not being
10 delivered to the designated number.

In accordance with a second aspect of the present invention, there is provided a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, and including a password update system
15 comprising:

means for receiving a call from a network terminal;

means for retrieving from signalling information of that received call the identity of the network terminal from which that call was made; and

means for accessing the password store in accordance with the retrieved
20 network terminal identity; and
characterised by:

means responsive to a successful location of an entry whose stored network terminal identity matches that retrieved network terminal identity, for playing an announcement to the caller requesting the entry of a password at that network
25 terminal; and

means responsive to receipt of a password entered in response to that request, for writing that received password into the associated respective password store of the located entry.

In accordance with a third aspect of the present invention, there is provided
30 a method of registering a new user of a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

4

receiving at a password management service a call from a network terminal;
retrieving by the password management service from signalling information
of that received call the identity of the network terminal from which that call was
made;

5 accessing the password store in accordance with the retrieved network
terminal identity;

 upon failure to locate an entry whose stored network terminal identity
matches that retrieved network terminal identity, making a new entry in respect of
that retrieved network terminal identity;

10 playing an announcement to the caller requesting the entry of a password at
that network terminal; and

 upon receipt at the password management service of a password entered in
response to that request, writing that received password into the associated
respective password store of the newly made entry.

15 In accordance with a fourth aspect of the present invention, there is
provided a password protected access system having a password store in which
each entry is constituted by a respective network terminal identity store and an
associated respective password store, and including a password management
system comprising:

20 means for receiving a call from a network terminal;

 means for retrieving from signalling information of that received call the
identity of the network terminal from which that call was made; and

 means for accessing the password store in accordance with the retrieved
network terminal identity; and

25 characterised by:

 means responsive to an unsuccessful location of an entry whose stored
network terminal identity matches that retrieved network terminal identity, for
making a new entry in respect of that retrieved network terminal identity and for
triggering the playing of an announcement to the caller requesting the entry of a

30 password at that network terminal; and

 means responsive to receipt of a password entered in response to that
request, for writing that received password into the associated respective password
store of the newly made entry.

In accordance with a fifth aspect of the present invention, there is provided a method of user authentication in a password protected access system having a password store in which each entry is constituted by a respective user-nominated network terminal identity and an associated respective password, the method comprising the steps of:

in response to receipt at the password protected access system of a call from a calling user at a network terminal, requesting the calling user to enter at that network terminal his nominated terminal identity and password;

receiving the entered terminal identity and password;

accessing the password store in accordance with the received entered terminal identity; and

upon locating an entry whose stored network terminal identity and associated password match the received entered terminal identity and password, authenticating that calling user.

Specific embodiments of the present invention will now be described by way of example with reference to the drawing in which Figure 1 shows component parts of a password change service of the present invention.

By way of background to the present invention, it is known for password protected access to, for example, a remote database holding a user's personal information, to be performed by user providing a user identity (user ID or userID), also called a username, to identify the particular stored information which the user is requesting access to, and a password. The user identity is commonly a set of letters, often the initials of the user's names, e.g. dje or rgb. The provided password is compared with a password previously provided by the user and stored in association with the user identity, and, if there is a match, the user is granted access.

In this known arrangement, if the user forgets his password, he has to contact the system administrator responsible for the database, provide sufficient proof of his identity, and request a reset of his password. The system administrator has to effect a change of the recorded password to a nominal password, for example "password", and notify the user of that nominal password. The user can thereafter access his information using that nominal password, but for security reasons usually performs a change password procedure to change that nominal password to one which is more secure. In this change password procedure, the user is asked to enter

the existing password, then his newly chosen password, and, for confirmation, to enter the new password again.

In the present invention, the user identity is not in the form of the user's initials, but is a nominated network terminal identity, which in this embodiment is a
5 telephone number, and this will usually be the number of the user's home or work telephone. Herein the terms nominated telephone number and nominated telephone are used synonymously and interchangeably.

For normal access, the user calls the password protection system from any telephone, and when prompted for a user identity he enters the nominated telephone
10 number via the keypad, or speaks it if there is an interactive voice response unit (IVR) at the password protection system. The user will then be prompted in the usual manner for entry of his password, which, likewise, he enters via the keypad or the IVR.

If the user has forgotten his password, he makes a call from the telephone
15 corresponding to the nominated number, i.e. the nominated telephone, to a password change service of the password protection system. On receipt at the password protection system of the incoming call from the user, the signalling information is examined and the content of the calling line identity field (CLI) is retrieved, and the user is prompted to enter a new password, via keypad or the IVR.
20 This new password is then stored in place of the previously stored password in association with the user identity in the form of the retrieved CLI, i.e. the nominated telephone number.

This password change procedure avoids the inefficient use of system administration personnel, the delay to the user when such system administration
25 personnel perform a manual change, and the risk that the user fails to change from the nominal password, which is inherently insecure, to a more secure password.

In a specific embodiment shown in Figure 1, the password protected information is a electronic personal telephone or email address book remotely stored on a database 10, accessed via a data network 12, such as the Internet or a
30 corporate intranet, and a server 14.

The user activates a computer 16 at any suitable site, and launches a browser in known manner to access the server 14. He receives from the server 14 an access page having text boxes for the entry of a user identity and a password.

Using the keyboard, the user enters the nominated telephone number for the user identity, and the current password. The server 14 performs a comparison of the entered password with the stored password associated with that user identity, and upon a match permits the user access to his address book.

5 If the user has forgotten his password, or if someone has managed to obtain access to the user's nominated telephone, say his work telephone 20, and change the password, then the user makes a call from his nominated telephone 20, via a telephone network, for example a private telephone network 22, to a predetermined destination terminal number at a CTI system 24 operating a change password
10 service.

As shown in the Figure, the change password service is operated by a CTI system 24 which is at a geographically separate location from the server 14. In variants, the CTI system 24 operating a change password service can be local to the server 14, or that function can even be made integral with the server 14.

15 In the present embodiment, the CTI system 24 will send the user's identity (CLI) and new password to the database 10. Thus in this specific embodiment, the CTI system 24 constitutes means for receiving a call from a network terminal and for retrieving from signalling information of the call the identity of the network terminal from which that call was made, means for receiving from that network terminal
20 information representative of a password, and means for updating a current password stored in association with that network terminal identity by replacing it with said information representative of a password. In a variant, the CTI system 24 sends the user's identity (CLI) and new password to the database 10 via the server 14.

25 The change password service, also referred to in this respect as a password management service, is also responsible for establishing a new user area in the database. A new user makes a call to the change password service, and upon prompting for a telephone number enters a telephone number, and upon prompting for a password the user either enters a password or, if the user chooses not to
30 provide a password at this initial area set up stage, terminates the user area set up procedure in some appropriate manner, e.g. by going on hook or entering "#" on the keypad. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user. The change password service now

8

communicates with the database 10 and requests the allocation of a new user area, i.e. a telephone number store and an associated password store, and provides that entered telephone number to the database 10, together with the entered password, if provided by the user at this stage.

5 If the user enters a password at the password prompt, the database 10 sets a Password Set flag associated with that newly established user area. If the user did not enter a password at the password prompt, the content of the password store in that user area remains filled with null characters, and the Password Set flag remains reset. The establishing of a new user area can alternatively be performed by system
10 administration personnel upon receipt of the required information from a new user via, for example, the postal service. Once a new user area has been established, the user then updates the latest recorded password in his area using the method of the present invention by making a call to the change password service from the nominated telephone. It will be understood that the latest recorded password can be
15 any of: null characters when the user has set up a new area but has not provided a password; or an initially provided password; or the password entered at the latest use of the change password service.

In a variant, the new user area can be set up via the user's computer 16 by downloading a set up page from the server 14, entering the nominated telephone
20 number and, if required at this stage, a password, in respective text entry boxes, and clicking on a submit button in known manner. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user.

In a further variant, since the change password service retrieves a CLI from
25 an incoming call, the user can indicate to the change password service, by entering # on the telephone keypad, that he wishes that CLI to be used as the nominated telephone number. This utilising by the change password service of the CLI in response to a command ("#") from the user constitutes indirect provision of a network terminal identity by the user. The change password service will respond by
30 requesting the user to enter a password. If the user is merely setting up a new user area and intending to defer providing a password, he need not supply a password at this time, and can indicate this by again entering #.

Whereas it is most convenient for the nominated telephone number to be the telephone where the user is most likely to be located when he needs to call the change password service, it need not be so. As an example of a different procedure, a user may nominate the telephone number of a trusted person, e.g. his father, living
5 in a completely different area to where he works, possibly even a different country. The present invention will still work, provided that the calling line identity is delivered. The user now calls his trusted person, gives him a new password and asks him to call the change password service and enter the new password when prompted.

10 It will now be appreciated that the present invention is concerned with a password change facility in a password protected access for human users, where those users have user identities in the form of network terminal identity (also referred to as a network address). When a user desires access to a required target, e.g. a remote database such as mentioned above, he dials the normal access number
15 for the protection system from any terminal in the network, and provides to the protection system his user identity and password by voice or key input. The protection system uses that provided identity to locate the user's entry and checks the provided password against the stored password. The user decides when he wants to change his password, and dials the special number for the password
20 change service of the protection system. It is this change service that obtains the CLI of the call and upon receipt of the new password entered by the user immediately stores that newly received password in association with that CLI. The procedure of the present invention is easy and quick, avoids any need to use known update procedures, and whenever the user wishes to update his password, whether
25 because he has forgotten it, or because he thinks that its security has been compromised and he wishes to update it for security reasons, or because he thinks that he might have entered his intended new password incorrectly, or whatever, the user only has to repeat the simple method of the present invention.

The present invention distinguishes from the abovementioned A1 & I
30 disclosure which is not concerned with human user authentication, but with authentication of an actual terminal equipment by ensuring that the terminal equipment is attached to the network termination corresponding with its original registration. The AT&T authentication system prevents a terminal equipment from

being taken to a different network termination, i.e. telephone line, but it does not provide any protection against a different human user activating the terminal equipment; it does not require the user to provide any personal identity, but merely encrypts the number provided by the network ANI equipment, i.e. the CLI; and it
5 requires the terminal equipment to store that encrypted CLI as a password retrievable from the terminal equipment upon command by the authentication system.
Furthermore, it is the authentication system, and not the user, that decides when to replace the stored encrypted CLI in the terminal equipment, that decides the new encryption key, that generates the replacement password rather than receiving the
10 replacement password from a user.

The present invention distinguishes from the abovementioned Casio Computer Co. disclosure which is concerned with capturing a user's originally submitted password, storing it with his username within his terminal device, and instead of using a step of requesting the user to enter his password and username, reads out
15 the stored password and username. In this way, there is no username or password entered by the user at each access attempt, and therefore no possibility of the user forgetting his details and having to contact authentication personnel for password reset (update).

The present invention distinguishes from the abovementioned Nippon
20 Telegraph and Telephone Corporation disclosure which is concerned with authenticating a password update attempt by a combination of dialback security, i.e. making contact with the user by calling him back on a telephone number known to be secure, and requesting a second entry of the new password.

Unless the context clearly requires otherwise, throughout the description and
25 the claims, the words "comprise", "comprising" and the like are to be construed in an inclusive as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to".

CLAIMS

1. A method of password update for a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:
- receiving at a password update service a call from a network terminal;
- retrieving by the password update service from signalling information of that received call the identity of the network terminal from which that call was made;
- 10 accessing the password store in accordance with the retrieved network terminal identity; and
- characterised by the steps of:
- upon locating an entry whose stored network terminal identity matches that retrieved network terminal identity, playing an announcement to the caller requesting
- 15 the entry of a password at that network terminal; and
- upon receipt at the password update service of a password entered in response to that request, writing that received password into the associated respective password store of the located entry.
- 20 2. A password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, and including a password update system comprising:
- means for receiving a call from a network terminal;
- 25 means for retrieving from signalling information of that received call the identity of the network terminal from which that call was made; and
- means for accessing the password store in accordance with the retrieved network terminal identity; and
- characterised by:
- 30 means responsive to a successful location of an entry whose stored network terminal identity matches that retrieved network terminal identity, for playing an announcement to the caller requesting the entry of a password at that network terminal; and

means responsive to receipt of a password entered in response to that request, for writing that received password into the associated respective password store of the located entry.

- 5 3. A method of registering a new user of a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

receiving at a password management service a call from a network terminal;
10 retrieving by the password management service from signalling information of that received call the identity of the network terminal from which that call was made;

accessing the password store in accordance with the retrieved network terminal identity;

15 upon failure to locate an entry whose stored network terminal identity matches that retrieved network terminal identity, making a new entry in respect of that retrieved network terminal identity;

playing an announcement to the caller requesting the entry of a password at that network terminal; and

20 upon receipt at the password management service of a password entered in response to that request, writing that received password into the associated respective password store of the newly made entry.

4. A password protected access system having a password store in which
25 each entry is constituted by a respective network terminal identity store and an associated respective password store, and including a password management system comprising:

means for receiving a call from a network terminal;
means for retrieving from signalling information of that received call the
30 identity of the network terminal from which that call was made; and

means for accessing the password store in accordance with the retrieved network terminal identity; and

characterised by:

means responsive to an unsuccessful location of an entry whose stored network terminal identity matches that retrieved network terminal identity, for making a new entry in respect of that retrieved network terminal identity and for triggering the playing of an announcement to the caller requesting the entry of a password at that network terminal; and

means responsive to receipt of a password entered in response to that request, for writing that received password into the associated respective password store of the newly made entry.

5. A method of user authentication in a password protected access system having a password store in which each entry is constituted by a respective user-nominated network terminal identity and an associated respective password, the method comprising the steps of;

in response to receipt at the password protected access system of a call from a calling user at a network terminal, requesting the calling user to enter at that network terminal his nominated terminal identity and password;

receiving the entered terminal identity and password;

accessing the password store in accordance with the received entered terminal identity; and

upon locating an entry whose stored network terminal identity and associated password match the received entered terminal identity and password, authenticating that calling user.

6. A method of password update for a password protected access system, the method being as claimed in claim 1 and substantially as hereinbefore described with reference to the drawing.

7. A password protected access system as claimed in claim 2, and substantially as hereinbefore described with reference to the drawing.

8. A method of registering a new user of a password protected access system, the method being as claimed in claim 3 and substantially as hereinbefore described with reference to the drawing.

9. A password protected access system as claimed in claim 4, and substantially as hereinbefore described with reference to the drawing.

5 10. A method of user authentication in a password protected access system, the method being as claim in claim 5 and substantially as hereinbefore described with reference to the drawing.

1/1

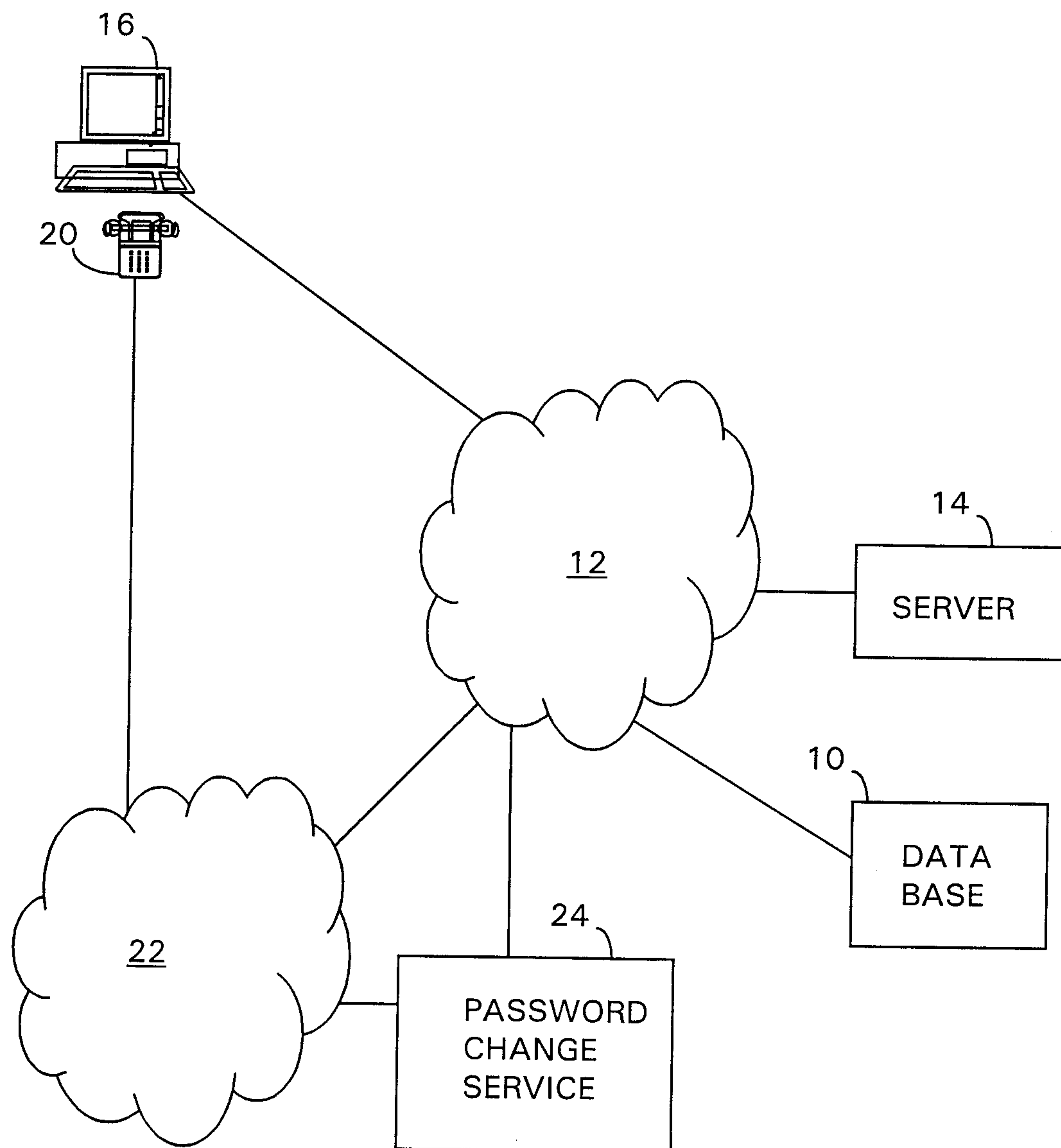


Fig. 1

