

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/029938 A1

(51) International Patent Classification⁷: **G06F 1/00**

(74) Agents: **GROSSMAN, Kurt, L.** et al.; Wood, Herron & Evans, L.L.P., 2700 Carew Tower, Cincinnati, OH 45202 (US).

(21) International Application Number: PCT/US01/30458

(22) International Filing Date:
28 September 2001 (28.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US):
SAFLINK CORPORATION [US/US]; 11911 NE 1ST Street, Bellevue, WA 98005 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, 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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MERCREDI, Dwayne** [CA/CA]; 27 Starling Drive, Sherwood Park, Alberta T8A 0A6 (CA). **FREY, Rod** [CA/CA]; 9906 88 Avenue, Edmonton, Alberta T6E 2R3 (CA). **JENSEN, Gregory**, [US/US]; 26325 Northeast 24th Street, Redmond, WA 98053 (US).

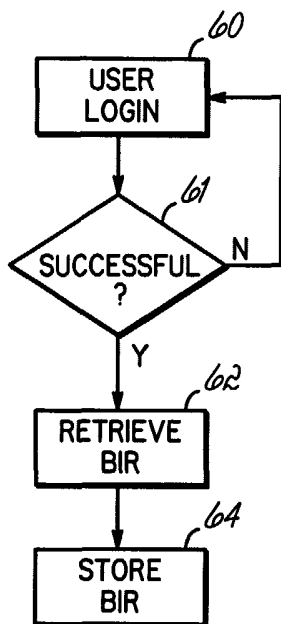
Published:

— with international search report

[Continued on next page]

(54) Title: BIOMETRIC AUTHENTICATION

(57) Abstract: An apparatus, method and program product locally stores biometric data in response to a user accessing a network (38). Local storage of the biometric data allows the user to biometrically access a local computer (20) in the absence of a network connection (18) and/or submitted ID.



WO 03/029938 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BIOMETRIC AUTHENTICATION

Field of the Invention

5 The present invention relates generally to biometric technologies,
and more particularly, to biometrically-controlled access of computer resources.

Background of the Invention

 Considerations regarding the safeguarding of computer resources
have become ubiquitous throughout industry, government and private channels.
Security concerns are exacerbated in networked environments, where the desire
10 to exchange data is often at odds with attempts to ensure system integrity.
Networks typically include one or more servers and numerous client computer
terminals, referred to herein as local computers, communicating over network
communication links. The communication links may be comprised of cables,

wireless links, optical fibers, and/or other communication media. Similarly, the local computers may be desktop personal computers, laptop computers, PDA's, or other computing devices to which or through which a user desires to obtain access. Secure networks commonly incorporate password software and procedures configured to restrict and control access to the network. However, despite such provision, password-controlled access remains fraught with security concerns, such as ease of duplication. Users may additionally have difficulty remembering passwords.

Consequently, many networks rely on biometric authentication processes to safeguard computer resources. With biometric authentication, a measurable physical characteristic of a potential user is obtained as a signature rather than a password. Such physical characteristics are usually very unique to the user and thus difficult to duplicate, defeat, or forget. Examples include fingerprints, retinal scans and voice signatures. Other examples might include hand, facial and/or cranial measurements and dimensions. For biometric access, a user who desires to access a network must first be enrolled on the network with that person's unique biometric data. That unique biometric data is typically obtained by the user logging in to the network with an administrator who oversees the process, such as at an administrator's or specially designated enrollment computer.

At that designated computer, the user will provide his or her user ID and also provide the requisite biometric data to one or more biometric access devices associated with the computer, such as by placing the appropriate finger in a fingerprint scanner or reader, exposing the eye to a retinal scan, or speaking into a microphone or the like, by way of examples, connected to that designated computer. The administrator typically oversees this process, which results in the generation of a set of data referred to herein as a biometric identification record ("BIR"), or perhaps multiple BIR's depending upon the number and type of biometric access devices to be used. The BIR is then stored on a network server as enrollment BIR data in a file associated with the particularly identified user ("privileged user"), such as by associating the enrollment BIR data with that user's ID.

When a user desires thereafter to access the network through a local computer coupled to the network, the user again provides the ID and the requested biometric information through a biometric access device associated with the local computer. The biometric data captured at the local computer produces a temporary BIR referred to hereinafter as "capture BIR data." The local computer and the server on the network communicate in an effort to authenticate the capture BIR data with the enrollment BIR data to determine whether the accessing user should be given access as if he or she were the privileged user who had enrolled at the network.

The enrollment BIR data is highly unique, as is the capture BIR data, thus presenting a formidable challenge to falsify, or otherwise defeat for purposes of accessing the network. The same enrollment and capture BIR data techniques can be applied to stand-alone computers as well, provided that the privileged user has gone through the enrollment process at that computer to provide an enrollment BIR thereto. The practical difficulties in having enrollments both at the network and at the local computers become more apparent when the significant time, effort and resources required to provide the enrollment process are understood.

The difficulties become especially compounded in large enterprises with a great many users and/or local computers. That problem becomes even more exacerbated in enterprises where the various users may move from computer to computer, thus necessitating multiple enrollments. Thus, in a network-based system, users will not typically be enrolled at their local computers. Instead, enrollment will typically be only at the network level, so as to avoid the time and expense of such enrollment procedures for the administrative staff. As a result, then, enrollment is accomplished only once per privileged user at the designated enrollment computer, and the enrollment BIR data held at the network server. That way, the user may seek to login through any local computer on the network using biometric access and

the enrollment BIR data is available for the authentication without multiple enrollments.

Limiting enrollment to the network level, however, can present additional drawbacks. For example, there may be times when the user wishes
5 to access the local computer, but the local computer is not able to communicate with the network server. That situation can arise when the network or server is down, or if the local computer is simply disconnected from the network, a not uncommon problem in the case of laptops, PDA's or other mobile computing devices. But, because an enrollment process has not
10 been undertaken with that now-disconnected local computer, the only security available thereon is the traditional and unreliable password method. It would be desirable to still have biometrically controlled access to the local computer, but without requiring that the privileged user have specifically undergone the time consuming enrollment procedure with that particular local computer.

15 In addition, and as indicated above, the accessing user must provide his or her ID, in addition to the capture BIR data. Where many users enjoy access to the same local computer, the requirement to provide the ID is seen as a practical necessity, but is also the source of frustration and delay. That frustration is particularly evident where the local computer, on an
20 attempted login, brings up the ID of the last user, and the current accessing user does not notice that the ID is for another user. That accessing user will

proceed to provide his biometric data, but will not be authenticated because the ID for another user. The result is at least a delay, if not lock-out from the system for that accessing user or perhaps the true privileged user. Such frustrations, among others, may ultimately translate into a reluctance on behalf of users to login with biometric access devices, opting instead for the conventional password approach, with its many security problems.

Summary of the Invention

The present invention provides an improved method, apparatus and program product for controlling biometric access to a computer of a user in a manner that addresses above-identified shortcomings of known biometric systems. To this end, and in accordance with the principles of the present invention, after the accessing user seeking access through a local computer is authenticated (i.e., the capture BIR and enrollment BIR data is found to match appropriately), a copy of the enrollment BIR data normally stored on the network server is further stored, or cached, in local computer for later use, such as after the current user has logged out of the network. In that way, the privileged user has automatically become enrolled on the local computer, without going through a formal, additional enrollment process at the local computer.

Instead, the enrollment at the local computer is, essentially, transparent to the user. However, because the copy of the enrollment BIR data, either directly or in encrypted form, is now also available at the local computer, access to the local computer, even when disconnected from the network, can be biometrically controlled without a further enrollment process by the user. The copy store technique may be applied to some or all of the local computers in an enterprise such that the administrative time, and the inconvenience of multiple enrollments that would otherwise militate against using biometrics to control access to the local computers in a stand-alone mode, becomes practical and easily accomplished.

In accordance with a further feature of the present invention, and based on the uniqueness of enrollment BIR data from user to user, it is now possible to also reduce or eliminate the need for user ID's. For example, the local computer may retain the copies of the enrollment BIR data, and associated ID's if necessary, for the last number of authenticated users. Due to the highly correlative nature of BIR data, an accessing user may now be permitted to log in using only capture BIR data, which is then compared against the stored copies of enrollment BIR data for an appropriate match. The absence of the ID is no longer a factor as the enrollment BIR data may be solely relied upon to control access and/or the ID may be retained with the stored copy to provide the same to the network or local computer operating

system if otherwise required. In that way, a fast login is accomplished because the delays involved with inputting or correcting the ID are eliminated.

The same fast login technique may be spread up to the network where privileged users, or certain sets of privileged users, may be permitted to login to the network through a local computer without the ID, and based only on a comparison of the capture BIR data and the enrollment BIR data.

By virtue of the foregoing there is thus provided an improved method, apparatus and program product for controlling biometric access to a computer of a user in a manner that addresses above-identified shortcomings of known biometric systems. These and other objects and advantages of the present invention shall be made apparent from the accompanying drawings and the description thereof.

Brief Description of the Drawing

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and, together with the general description of the invention given above and the detailed description of the embodiments given below, serve to explain the principles of the present invention.

Fig. 1 is a block diagram of a networked computer system consistent with the invention;

Fig. 2 is a block diagram of an exemplary hardware and software environment for a computer from the networked computer system of Fig. 1;

Fig. 3 is a flowchart outlining method steps suited for execution within the environments of Figs. 1 and 2;

Fig. 4 is a flowchart illustrate process steps associated with the BIR caching method of Fig. 3;

Fig. 5 is a dialog box having application within the process steps of Fig. 4;

Fig. 6 is a flowchart illustrating method steps in accordance with the principles of the present invention;

Fig. 7 is a dialog box consistent with the principles of the invention and having particular application within the process steps of Fig. 6.

Detailed Description of Drawings

With reference generally to Drawings, there is shown a system 10 configured to retrieve an enrollment BIR of a privileged user from a server 16 in response to that user gaining access to a network 18. The system 10 locally stores the retrieved BIR data on a computer 20. As such, the enrollment BIR is subsequently available locally for authentication purposes when the computer 20 becomes disconnected from the network 18. Having

thus obviated the need to retrieve enrollment data from the network 18, the user is permitted to gain access to the computer 20 irrespective of a network 18 connection.

Further, because the storage of the enrollment BIR data is accomplished locally, BIR data for multiple, prior users may be stored on the local computer 20. This feature allows a user to biometrically access the computer 20 without first providing his or her ID. Namely, a user may solely provide capture BIR data directly to the computer 20, which is evaluated against the locally stored enrollment BIR data of prior users. The highly correlative nature of the BIR's facilitate matching of the capture and enrollment data in the absence of a submitted ID. A subsequent correlation of the capture and enrollment BIR data may verify the status of the accessing user as being privileged as above. These and other exemplary embodiments in accordance with the principles of the present invention are described below in detail.

Hardware and Software Environment

Turning to the Drawings, wherein like numbers denote like parts throughout the several views, Fig. 1 illustrates an exemplary computer system 10 suitable for biometrically controlling access to a user computer 20 adapted to communicate with a network 18. As such, computer system 10 is illustrated as a networked system that includes one or more client computers

12, 14 and 20 (e.g., lap top, desktop or PC-based computers, workstations, etc.) coupled to server 16 (e.g., a PC-based server, a minicomputer, a midrange computer, a mainframe computer, etc.) through a network 18. Network 18 represents a networked interconnection, including, but not limited to local-
5 area, wide-area, wireless, and public networks (e.g., the Internet). Moreover, any number of computers and other devices may be networked through network 18, e.g., multiple servers. Significantly, the present invention may have particular application when a computer 12, 14, 20 becomes disconnected from the network 18.

10 User computer 20, which may be similar to computers 12, 14, may include: a central processing unit (CPU) 21, a number of peripheral components such as a computer display 22, a storage device 23, a printer 24, and various input devices (e.g., a mouse 26, keyboard 27) to include biometric login devices. Those skilled in the art will recognize that biometric devices
15 compatible with the present invention are not limited to the exemplary devices shown in Fig. 1 which include a fingerprint scanner 17 and microphone (voice recognition) 19. Consequently, suitable input devices may comprise any mechanism configured to receive BIR data. Server computer 16 may be
20 similarly configured, albeit typically with greater processing performance and storage capacity, as is well known in the art.

Fig. 2 illustrates a hardware and software environment for an apparatus 30 suited to control biometric access with regard to a user in a manner consistent with the principles of the invention. For the purposes of the invention, apparatus 30 may represent a computer, computer system or other programmable electronic device, including: a client computer (e.g., similar to computers 12, 14 and 20 of Fig. 1), a server computer (e.g., similar to server 16 of Fig. 1), a portable computer, an embedded controller, etc. Apparatus 30 will hereinafter also be referred to as a "computer," although it should be appreciated the term "apparatus" may also include other suitable programmable electronic devices consistent with the invention.

Computer 30 typically includes at least one processor 31 coupled to a memory 32. Processor 31 may represent one or more processors (e.g., microprocessors), and memory 32 may represent the random access memory (RAM) devices comprising the main storage of computer 30, as well as any supplemental levels of memory, e.g., cache memories, non-volatile or backup memories (e.g., programmable or flash memories), read-only memories, etc. In addition, memory 32 may be considered to include memory storage physically located elsewhere in computer 30, e.g., any cache memory in a processor 31, as well as any storage capacity used as a virtual memory, e.g., as stored within a biometric database 36 or on another computer coupled to computer 30 via network 38.

Computer 30 also may receive a number of inputs and outputs for communicating information externally. For interface with a user, computer 30 typically includes one or more input devices 33 (e.g., a keyboard, a mouse, a trackball, a joystick, a touchpad, retinal/fingerprint scanner, and/or a microphone, among others) and a display 34 (e.g., a CRT monitor, an LCD display panel, and/or a speaker, among others). It should be appreciated, however, that with some implementations of computer 30, e.g., some server implementations, direct user input and output may not be supported by the computer, and interface with the computer may be implemented through a client computer or workstation networked with computer 30.

For additional storage, computer 30 may also include one or more mass storage devices 36 configured to store a biometric database 37. Exemplary devices 36 can include: a floppy or other removable disk drive, a hard disk drive, a direct access storage device (DASD), an optical drive (e.g., a CD drive, a DVD drive, etc.), and/or a tape drive, among others. Furthermore, computer 30 may include an interface with one or more networks 38 (e.g., a LAN, a WAN, a wireless network, and/or the Internet, among others) to permit the communication of information with other computers coupled to the network. It should be appreciated that computer 30 typically includes suitable analog and/or digital interfaces between processor 31 and each of components 32, 33, 34, 36 and 38.

Computer 30 operates under the control of an operating system 40, and executes various computer software applications, components, programs, objects, modules, etc. (e.g., BIR caching program 50, disconnected login program 42, and fast login program 44, HA-API 43, among others). Of
5 note, Human Authentication Application Programming Interface (HA-API) regards an exemplary programming interface supplied by biometric service providers that provides enrollment and verification services for installed biometric devices. Moreover, various applications, components, programs, objects, modules, etc. may also execute on one or more processors in another
10 computer coupled to computer 30 via a network 38, e.g., in a distributed or client-server computing environment, whereby the processing required to implement the functions of a computer program may be allocated to multiple computers over a network.

In general, the routines executed to implement the
15 embodiments of the invention, whether implemented as part of an operating system or a specific application, component, program, object, module or sequence of instructions will be referred to herein as "computer programs," or simply "programs." The computer programs typically comprise one or more instructions that are resident at various times in various computer memory and
20 storage devices. When a program is read and executed by a processor, the

program causes the computer to execute steps or elements embodying the various aspects of the invention.

Moreover, while the invention has and hereinafter will be described in the context of fully functioning computers and computer systems, those skilled in the art will appreciate that the various embodiments of the invention are capable of being distributed as a program product in a variety of forms, and that the invention applies equally regardless of the particular type of signal bearing media used to actually carry out the distribution. Examples of signal bearing media include but are not limited to recordable type media such as volatile and non-volatile memory devices, floppy and other removable disks, hard disk drives, optical disks (e.g., CD-ROM's, DVD's, etc.), among others, and transmission type media such as digital and analog communication links.

In addition, various programs described hereinafter may be identified based upon the application for which they are implemented in a specific embodiment of the invention. However, it should be appreciated that any particular program nomenclature that follows is used merely for convenience, and thus the invention should not be limited to use solely in any specific application identified and/or implied by such nomenclature.

Those skilled in the art will recognize that the exemplary environments illustrated in Figs. 1 and 2 are not intended to limit the present

invention. Indeed, those skilled in the art will recognize that other alternative hardware and/or software environments may be used without departing from the scope of the invention.

BIR Caching

5 The flowchart of Fig. 3 illustrates an exemplary embodiment for biometrically controlling access of a user with regard to the hardware and software environments of Figs. 1 and 2. Generally, BIR caching calls for the local storage of enrollment BIR data correlated with a privileged user. The BIR caching program of Fig. 2 causes an accessing user to provide capture
10 BIR data to a local computer when accessing a network server. One embodiment retrieves and stores the enrollment BIR data from the server following a successful network login. As discussed below, such enrollment data may have application for facilitating remote and accelerated user access.

 More particularly, Fig. 3 illustrates sequenced steps suited to
15 locally store enrollment BIR data correlated with a user, subsequent to the user gaining access to a network. At block 60, the BIR caching program may recognize that a user is attempting to log into a computer system biometrically. As discussed above, this may involve fingerprint/voice recognition, retinal scans, or other known biometric techniques and procedures. Of note, should
20 the BIR caching program detect a unsuccessful biometric login at block 61 (as defined by the particular biometric testing application), then the BIR caching

processes described below in steps 62-64 go unexecuted. In this manner, local storage of the BIR data may only be accomplished after a successful biometric login to the network registers at block 61.

Assuming the user successfully gains access to the network at
5 block 61, BIR caching software incident on the local machine of the user retrieves the enrollment BIR of the user at block 62. The retrieval may involve recording the BIR from the network server at block 62. As such, the program will access network data base files to download the BIR onto the hard drive of the user's computer. Alternatively, the program may simultaneously record
10 the enrollment BIR as it is used to authenticate the user at block 60. As such, the program may initiate local storage of the BIR data incident with a successful login attempt at block 61.

A third embodiment may prompt a logged-in user to resubmit capture BIR data used explicitly for storage on the local hard drive of the
15 user's computer. For instance, the user may re-accomplish the biometric authentication sequence used to gain access at block 60. As such, the program may cache the capture BIR data for later use on the same computer.

In any case, the program stores and associates the retrieved BIR with the ID and/or operating system password information of the user. The
20 BIR data and associative relationships are stored within memory of the computer at block 64. Of note, the memory may comprise a cache or database

configured for quick retrieval of the BIR data. The program may further structure the memory to sequentially store BIR and ID information for a preset number of recent users. This feature may prove convenient in situations where multiple users exclusively share a computer. For instance, the program
5 can initiate a display of the ten most recent users to access the computer. In this manner, an accessing user may select their displayed ID from a scroll down bar menu as discussed below in detail.

The selection prompts the program to retrieve the enrollment BIR data and other information associated with the user from the hard drive of
10 the local computer. This provision facilitates login processes by enabling a direct comparison between the stored and capture BIR data. Of note, the BIR caching method of Fig. 3 may be repeated every time a user successfully logs into a computer. As such, the most recently stored BIR data accounts for subtle, physical changes in the biometric characteristics of the user that can
15 occur over time.

Disconnected Login

The methodology of the steps of Fig. 3 have application within the disconnected login sequence illustrated in Fig. 4. Generally, the BIR caching sequence of Fig. 3, integrated into the flowchart of Fig. 4, allows a
20 user who has been successfully granted access to a network via biometric authentication to subsequently use the same BIR to access the client computer

when disconnected from the network. Once a user has logged into the network through a specific computer, enrollment BIR data from the network is downloaded into the memory of the disconnected computer for subsequent access to the computer on a local basis. Of note, enrollment BIR data may not
5 be retrieved until after the accessing user has authenticated their data for the first time.

In this manner, the disconnected login program of Figs. 2 and 4 enables a user accessing a computer separated from network communications to nonetheless gain access to it biometrically. Significantly, the user accesses
10 the detached computer using the same BIR that is stored on the network. Absent such provision, a remote user would be unable to biometrically access their account. Of note, the flowchart of Fig. 4 presupposes that an account has been established for the user, as discussed in the text accompanying Fig. 3.

Turning more particularly to block 69 of Fig. 4, the user may
15 initiate normal startup processes at a computer terminal. For instance, the user may boot the computer or initiate proprietary software resident on the machine. For example, protocol may require all users to depress a sequence of keyboard symbols to initiate program execution. In response, the computer may activate the disconnected login program 42 of Fig. 2 at block 70 of Fig. 4.
20 In one embodiment, the program may initially query a server, operating

system, or user input to determine if disconnected login processes are required or requested.

If such a determination is made at block 70 of Fig. 4, then the program may retrieve at block 71 a list of prior users who have most recently
5 logged into the machine. Of note, the storage of the data associated with the users is accomplished locally at the client computer. This feature obviates any requirement to communicate with the network to retrieve prior user data. As above, the computer may display the list of users in the form of a drop-down screen box. An administrator may set the number of user ID's displayed
10 according to application and performance considerations. As such, a user may scroll down the drop-down box to select their name at block 72. If the name of an accessing user is not displayed by the computer at block 71, the embodiment may present the user with the option of typing their name onto a text field. Fig. 5 shows a suitable dialog box having such a text field 77 and
15 drop-down box 75. As shown in Fig. 5, the user may submit their designated user name 85 by depressing the "OK" button 83. The user may alternatively end a login session by selecting the "Cancel" button 84. In one embodiment, the dialog box may further include a password login option 79. As such, a client may access the computer using the conventional password option of
20 block 78 of Fig. 4 so long as allowed by the system administrator. Another

embodiment may require users to access their accounts using their conventional password in combination with biometric processes.

The program may subsequently evaluate which biometric devices are installed and available on the local machine at block 74 of Fig. 4.

5 For example, the local computer of the user may be equipped with both fingerprint and retinal biometric testing devices. Proprietary programs associated with conventional biometric testing devices place a marker within a registry of the computer upon installation and de-installation. This registry provides a mechanism for the embodiment to assess available devices at block 74. If no device is configured or available on the computer, then the user must
10 login using a password if the option is available at block 78.

At block 76, the computer may determine whether biometric enrollment on an available device has ever taken place on the computer with regard to the user desiring access. If not, then the user may again be relegated
15 to the password entry of block 78. Should the computer alternatively determine that the user has previously logged in using a biometric device detected at block 74, then the disconnected login program may next determine whether more than one biometric login device is available on the machine. Of note, should only one biometric device be available and previously accessed,
20 the program may initiate authentication processes directly at block 60.

Should the program determine that more than one device is available and previously utilized at block 80, then the embodiment may check to see if a policy setting has been established for the user at block 82. Such a setting acts as a default, or preference for a particular user, directing the computer to select a single or ordered group of biometric devices from among the available devices. As discussed herein, such a preference may be set by an administrator or designated by a prior designation of the user. For instance, the user may set a preference subsequent to login at block 90, as discussed below.

Should the program detect a preferred setting at block 82 that corresponds to an allowable testing device, then it may initiate testing sequences associated with the preferred biometric device at block 60. Should no single, biometric testing preference be recorded for the user at block 82, then one embodiment may prompt the user to select a biometric testing sequence at block 88 from a listing displayed at the terminal. As such, the user may select one or more biometric verification processes by typing in or clicking on a device displayed at block 88. The program may derive the list from those installed devices detected at block 74.

In response to any such designation, the program retrieves software associated with the designated biometric in preparation of the biometric challenge at block 60. The program then launches the

designated/preferred biometric test according to the preset parameters of the biometric verification sequence. Should the verification process be unsuccessful at block 61, the program relegates the user back to block 80 to select from the same or other available biometric login devices. Of note, the
5 respective login protocol may allow for multiple authentication attempts at block 61 before ending a session. Otherwise the user accesses the computer at block 86. The BIR enrollment data associated with the login may then be stored at block 64 along with other user data, as discussed above in the BIR caching sequences of Fig. 3. The privileged user may additionally click on a
10 dialog box at block 90 to set a biometric preference for subsequent logon sessions.

Fig. 7 shows an exemplary dialog box suited for application within the processes of Fig. 4. As shown, the user may select a desired domain 67 that the program will locate upon a subsequent login session or
15 after initialization processes of block 69 of Fig. 4. As such, the domain may relate to program and interface addresses required by the user to gain access to a biometric challenge. In another embodiment, domain selection may be transparent to the user as set by an administrator or software precept. Similarly, the user may enter a preferred biometric login device with a
20 preference field 66 of Fig. 7. As discussed above, this preference may direct policy determinations regarding login devices at block 82 of Fig. 4 on

subsequent login sessions. Thus, in use, the disconnected login feature frees up network resources, as an authentication process may be conducted without taxing CPU cycles of the central server.

Fast Login

5 Another embodiment consistent with the principles of the present invention and shown in Fig. 6 allows an accessing user to biometrically access a computer without first providing another source of identification. Of note, the embodiment may operate within the confines of the disconnected login processes of Fig. 4. To this end, the dialog box of Fig.
10 7 includes a "Fast Login" option 65 as discussed below. A system administrator may additionally configure multiple, networked computers to enable an accelerated biometric login. Such a designation obviates the conventional user requirement of providing the ID for the enabled client computers.

15 Unlike prior art systems, an accessing user merely provides capture BIR data at the local computer. For instance, the accessing user's first interaction with a machine may comprise the placement of an index finger onto a scanner in communication with the computer. Similarly, a microphone coupled to the computer may recognize the voice pattern of the accessing user
20 without first requiring identification information. Program software running on the computer compares capture BIR data to stored enrollment BIR data and

determines if a match is present. In the event of such a match, the program may retrieve and configure an ID and password associated with the enrollment BIR data to verify privileged access status of the user.

Figure 6 shows sequence steps suited to realize the fast login process described above. At block 69, the accessing user initiates any necessary, preliminary processes associated with the computer, operating system and/or network. For instance, the user may have to strike a particular combination on a keyboard, or merely power-up the computer. As discussed below in detail, the initialization sequence may prompt a fast login program to retrieve cached BIR data. At block 102, the program may first confirm that the computer/server is configured to allow fast login. For instance, a most recent user accessing the computer may check the "Fast Login" box 65 of Fig. 7 during normal login or log-out processes. Such a designation causes the fast login program to automatically initiate during subsequent login sessions.

Alternatively or in addition, a system administrator may set the domain of the computer and/or network such that the computer software locates the fast login address upon initialization at block 69. In either case, the computer accessed by the user recognizes at block 102 that fast login has been enabled. Regarding block 69, some computers and networks may not require such initialization processes, and rather allow the user to proceed directly to block 107. Of note, should fast login be disabled for the computer at block

102, the conventional login sequence for the computer may be invoked at block 104. Namely, the user may be prompted to enter in their ID prior to submitting capture BIR data.

In response to detecting an enabled fast login, the computer
5 may execute further fast login software processes at block 107. More particularly, the program may determine if a policy has been established for the accessed computer. A policy may include a programmed preference or mandate for a biometric testing device established by an administrator or a prior user. Should a connection to the network be established, the computer
10 may similarly query the server for a biometric testing device preference(s). Of note, should no preference be available via the server, the program may substitute a default preference, not shown in the embodiment of Fig. 6. The default preference, as discussed herein, may track a compilation of available biometric devices on the machine and ascertained at block 108. The policy
15 may further be specific to fast login applications. Alternatively at block 107, the absence of a preference may cause the program to force the user to provide an ID at block 104.

The fast login program may at block 108 determine which, if any, of the preferred biometric testing devices are actually installed on the
20 computer. To this end, the software program may query a registry value of the operating system at block 108. As is known, such registries contain

information entered incident upon the installation of a biometric testing device. In this manner, the register provides an accounting of devices installed on the computer. In an instance where the computer is in communication with the network, the computer may alternatively check the server to obtain status information pertinent to available biometric devices. Should no acceptable or preferred biometric testing device be located on the computer at block 108, the software will, as above, relegate the user to conventional ID login at block 104.

Should the preferred biometric testing device be thus available and approved, the user may be prompted to provide the appropriate capture BIR data at block 60. More particularly, the program may initiate and display a splash screen configured to cause the user to provide the preferred and appropriate biometric testing data. For instance, a fingerprint authentication application may prompt the user, "please place finger on pad." At block 60, the user may provide the appropriate capture BIR data. The computer, in turn, retrieves the capture BIR data according to the known biometric login sequence appropriate to the preferred testing device.

In response to receiving the capture BIR data at block 60, the software may recall at block 112 a stored list of ID's and associated enrollment BIR data corresponding to a number of most recent users accessing the computer. The program may limit the number of prior users stored to 5-10 for

processing and time considerations. Of note, however, an administrator may increase or decrease the number of users stored per application and CPU resource availability. For instance, an administrator could configure hundreds of workstations for fast login given adequate processing resources.

5 At block 61, the program may attempt to verify the capture BIR data using the retrieved history of recent logins. That is, the program sequentially evaluates stored enrollment BIR data until a numerical match is detected. Of note, the program may begin evaluating the stored data in chronological order beginning with the most recent user to access the
10 computer. Once a match is detected, the program may transparently recall and present any ID or password information associated with the matched BIR that is required by an operating system. As discussed below, this feature fulfills vendor and system requirements while liberating an accessing user from password/ID redundancies. As shown in Fig. 7, a privileged user may enter
15 within a text field 68 the number of prior users against which the program verifies the capture BIR data.

 Should the biometric match be detected at block 61, then the user gains access to the desired resources of the computer and/or network at block 86. Of note, one embodiment may repeat unsuccessful authentication
20 processes at block 61 three to five times prior to directing the client to use conventional user ID login sequences at block 104. The fast login program

may cache a successful biometric login memory at block 64, as well as alert the network server as to the successful login at block 88. This step may provide an additional layer of security to a network by insuring that the same user is not accessing the network concurrently from two separate locations.

5 Thus, in use, the fast login feature enables a user to bypass presentation of user identification information and merely provide an enrollment data to access the computer.

While the present invention has been illustrated by the description of embodiments thereof, and while the embodiments have been
10 described in considerable detail, it is not intended to restrict or in any way limit the scope of the appended claims to such detail. Additional advantages and modifications will readily appear to those skilled in the art. For example, a program of the invention may encrypt biometric data, conventional passwords and other information at any step delineated in the flowcharts of
15 Figs. 3, 4 and 6.

Further, one skilled in the art should appreciate that any of the embodiments and associated programs discussed above are compatible with all known biometric testing processes and may further be optimized to realize even greater efficiencies. For instance, an operating system executing a
20 program of the invention may dictate a login path or routine. The operating system or administrator may define the login path that consists of, for instance,

a password followed by a fingerprint scan. As such, the operating system may require both the password and a BIR. Thus, software of the present invention works within and complements the HA-API to transparently associate, retrieve and present the password associated with the BIR enrollment data of the
5 accessing user along with the capture BIR data.

More specifically, the password associated with the stored BIR data is retrieved from cached memory and sent to the operating system. In this manner, the programming requirements of the operating system and biometric vendor are fulfilled without burdening the accessing user with conventional
10 password requirements. The invention in its broader aspects is, therefore, not limited to the specific details, representative apparatus and method, and illustrative examples shown and described. Accordingly, departures may be made from such details without departing from the spirit or scope of the general inventive concept.

15 Having described the invention, what is claimed is:

Claims

1. A method of biometrically controlling a user's access to a computer adapted to communicate with a network having at least one server associated therewith, comprising:

storing at the server, enrollment BIR data correlated with a privileged user;

causing an accessing user to provide capture BIR data to the computer and causing the computer to communicate with the server via the network; and

evaluating the capture BIR data with the enrollment BIR data to determine whether the accessing user is to be given access to the network as the privileged user via the computer, and if so, thereafter storing a copy of the enrollment BIR data in the computer for later use.

2. The method according to claim 1, further comprising retrieving the enrollment BIR from the server.

3. The method according to claim 1, further comprising encrypting the enrollment BIR data at the computer.

4. The method according to claim 1, further comprising encrypting the enrollment BIR data at the server.

5. The method of claim 1, further comprising:
after storing the copy of the enrollment BIR data at the computer, and
thereafter, while the computer is not communicating with the network, causing the accessing user to provide the captured BIR data to the computer; and
evaluating the capture BIR data and the stored copy of the enrollment BIR data to determine whether the accessing user is to be given access to the computer as the privileged user.

6. The method according to claim 5, further comprising granting the privileged user access to the computer in response to determining a match between the capture BIR data and the stored copy of the enrollment BIR data.

7. The method according to claim 5, further comprising storing at the computer an ID of at least one previous user of the computer.

8. The method according to claim 7, further comprising storing the enrollment BIR data in such a manner as to be associated with the ID stored on the computer.

9. The method according to claim 5, further comprising storing at the computer a password of at least one previous user of the computer.

10. The method according to claim 9, further comprising storing the enrollment BIR data in such a manner as to be associated with the password stored on the computer.

11. The method according to claim 7, further comprising displaying the ID to the accessing user.

12. The method of according to claim 11, further comprising enabling the accessing user to select the displayed ID.

13. The method of according to claim 12, further comprising retrieving the enrollment BIR data associated with the accessing user in response to the selected ID.

14. The method according to claim 12, further comprising associating a preferred BIR device with the selected ID.

15. The method according to claim 14, further comprising associating the preferred BIR device with the accessing user.

16. The method according to claim 14, further comprising verifying the availability of the preferred BIR device on the computer.

17. The method according to claim 14, further comprising prompting the user to enter the password in response to the preferred BIR device being unavailable.

18. The method according to claim 14, further comprising selecting the preferred BIR device according to a setting selected from a group consisting of: user, computer, global, and some combination thereof.

19. The method of claim 1, wherein the accessing user normally has to provide at the computer an ID and the capture BIR data to access the network, further comprising:

after storing the copy of the enrollment BIR data, on a subsequent attempt by the accessing user to gain access via the network, causing the accessing user to provide the capture BIR data to the computer without providing the ID; and

evaluating the capture BIR data against the stored enrollment BIR data to determine whether the accessing user is to be given access to the computer as the privileged user.

20. The method according to claim 19, further comprising granting the privileged user access to the computer in response to determining a match between the capture BIR data and the stored copy of the enrollment BIR data.

21. The method according to claim 19, further comprising associating the enrollment BIR data with the ID.

22. The method according to claim 21, further comprising retrieving the ID in response to receiving the capture BIR data.

23. The method according to claim 19, further comprising associating the enrollment BIR data with the password.

24. The method according to claim 23, further comprising retrieving the ID in response to receiving the capture BIR data.

25. The method according to claim 19, further comprising verifying the computer is configured to allow access to the privileged user absent the ID.

26. The method according to claim 19, further comprising determining the preferred biometric login device.

27. The method according to claim 26, wherein the preferred biometric enrollment device is determined according to the machine setting.

28. The method according to claim 26, further comprising determining whether the preferred biometric enrollment device is available on the computer.

29. The method according to claim 26, further comprising determining if the computer is configured to allow access using the preferred biometric enrollment device absent the ID.

30. The method according to claim 29, further comprising causing the user to provide the ID in response to the preferred biometric enrollment device being unavailable.

31. The method according to claim 29, further comprising determining a second preferred biometric enrollment device.

32. The method according to claim 19, further comprising scrambling the ID.

33. The method according to claim 19, further comprising storing the ID of the accessing user for later recall.

34. A method of biometrically controlling a user's access to information retrievable via a computer, wherein the user normally has to provide at the computer both an ID and capture BIR data to gain access to the information, further comprising:

after storing a copy of enrollment BIR data, on a subsequent attempt by the accessing user to gain access to the information, causing the user to provide the capture BIR data to the computer without providing the ID;
and

evaluating the capture BIR data against the stored enrollment BIR data to determine whether the user is to be given access to the information.

35. The method according to claim 34, further comprising granting the user access to the information in response to determining a match between the capture BIR data and the stored copy of the enrollment BIR data.

36. The method according to claim 34, further comprising associating the enrollment BIR data with the ID.

37. The method according to claim 34, further comprising retrieving the ID in response to receiving the capture BIR data.

38. The method according to claim 34, further comprising associating the enrollment BIR data with the password.

39. The method according to claim 34, further comprising retrieving the ID in response to receiving the capture BIR data.

40. The method according to claim 34, further comprising verifying the computer is configured to allow access to the user absent the ID.

41. The method according to claim 34, further comprising determining a preferred biometric login device.

42. The method according to claim 41, wherein the preferred biometric enrollment device is determined according to a machine setting.

43. The method according to claim 34, further comprising determining whether the preferred biometric enrollment device is available on the computer.

44. The method according to claim 34, further comprising determining if the computer is configured to allow access using the preferred biometric enrollment device absent the ID.

45. The method according to claim 34, further comprising causing the user to provide the ID in response to the preferred biometric enrollment device being unavailable.

46. The method according to claim 34, further comprising determining a second preferred biometric enrollment device.

47. The method according to claim 34, further comprising encrypting the ID.

48. The method according to claim 34, further comprising storing the ID of the accessing user for later recall.

49. An apparatus, comprising:

a memory;

a database resident within the memory, the database storing enrollment BIR data retrieved from a network and correlated with a privileged user;

a program configured to prompt an accessing user to provide capture BIR data to the computer and the computer to communicate with the network; and initiates an evaluation of the capture BIR data with the enrollment BIR data to determine whether an accessing user is to be given access to the network as the privileged user via the computer, and if so, configured to thereafter store a copy of the enrollment BIR data in the database for later use.

50. The apparatus according to claim 49, wherein the database maintains an ID associated with the enrollment BIR data.

51. The apparatus according to claim 49, wherein the database maintains a password associated with the enrollment BIR data.

52. The apparatus according to claim 49, wherein the program initiates retrieving the enrollment BIR from the network.

53. The apparatus according to claim 49, wherein the program initiates encrypting the enrollment BIR data at the computer.

54. The apparatus according to claim 49, wherein the program initiates encrypting the enrollment BIR data at the server.

54. The apparatus according to claim 49, wherein after storing the copy of the enrollment BIR data at the computer, and thereafter, while the computer is not communicating with the network, the program further causes the accessing user to provide the captured BIR data to the computer; and initiates the evaluation of the capture BIR data and the stored copy of the

enrollment BIR data to determine whether the accessing user is to be given access to the computer as the privileged user.

55. The apparatus according to claim 54, wherein the program grants the privileged user access to the computer in response to determining a match between the capture BIR data and the stored copy of the enrollment BIR data.

56. The apparatus according to claim 54, wherein the program initiates storage at the computer of an ID of at least one previous user of the computer.

57. The apparatus according to claim 54, wherein the program initiates storage of the enrollment BIR data in such a manner as to be associated with the ID stored on the computer.

58. The apparatus according to claim 51, wherein the program initiates storage at the computer of the password of at least one previous user of the computer.

59. The apparatus according to claim 51, wherein the program initiates storing the enrollment BIR data in such a manner as to be associated with the password stored on the computer.

60. The apparatus according to claim 56, wherein the program initiates displaying the ID to the accessing user.

61. The apparatus according to claim 60, wherein the program enables the accessing user to select the displayed ID.

62. The apparatus according to claim 60, wherein the program initiates retrieval of the enrollment BIR data associated with the accessing user in response to the selected ID.

63. The apparatus according to claim 60, wherein the program initiates associating a preferred BIR device with the selected ID.

64. The apparatus according to claim 63, wherein the program initiates associating the preferred BIR device with the accessing user.

65. The apparatus according to claim 63, wherein the program initiates verifying the availability of the preferred BIR device on the computer.

66. The apparatus according to claim 63, wherein the program initiates prompting the user to enter the password in response to the preferred BIR device being unavailable.

67. The apparatus according to claim 63, wherein the program initiates selecting the preferred BIR device according to a setting selected from a group consisting of: user, computer, global, and some combination thereof.

68. The apparatus according to claim 49, wherein the accessing user normally has to provide at the computer both an ID and the capture BIR data to access the network, after initiating storage of the enrollment BIR data and on a subsequent attempt by the accessing user to gain access via the network, the program causes the accessing user to provide the capture BIR data to the computer without providing the ID; and causes the evaluation of the capture BIR data against the stored enrollment BIR data to determine whether the accessing user is to be given access to the computer as the privileged user.

69. The apparatus according to claim 68, wherein the program initiates granting the privileged user access to the computer in response to determining a match between the capture BIR data and the stored copy of the enrollment BIR data.

70. The apparatus according to claim 68, wherein the program initiates associating the enrollment BIR data with the ID.

71. The apparatus according to claim 68, wherein the program initiates retrieving the ID in response to receiving the capture BIR data.

72. The apparatus according to claim 68, wherein the program initiates associating the enrollment BIR data with the password.

73. The apparatus according to claim 68, wherein the program initiates retrieving the ID in response to receiving the capture BIR data.

74. The apparatus according to claim 68, wherein the program initiates verifying the computer is configured to allow access to the privileged user absent the ID.

75. The apparatus according to claim 68, wherein the program initiates determining the preferred biometric login device.

76. The apparatus according to claim 75, wherein the preferred biometric enrollment device is determined according to the machine setting.

77. The apparatus according to claim 75, wherein the program initiates determining whether the preferred biometric enrollment device is available on the computer.

78. The apparatus according to claim 75, wherein the program initiates determining if the computer is configured to allow access using the preferred biometric enrollment device absent the ID.

79. The apparatus according to claim 78, wherein the program initiates causing the user to provide the ID in response to the preferred biometric enrollment device being unavailable.

80. The apparatus according to claim 68, wherein the program initiates determining a second preferred biometric enrollment device.

81. The apparatus according to claim 68, wherein the program initiates encryption of the ID.

82. The apparatus according to claim 68, wherein the program initiates storing the ID of the accessing user for later recall.

83. An apparatus for biometrically controlling access of a user to information retrievable via a computer, wherein the user normally has to provide at the computer both an ID and capture BIR data to gain access to the information, comprising:

a memory;

a database resident within the memory, the database storing enrollment BIR data correlated with a privileged user;

a program configured to, after storing a copy of enrollment BIR data and on a subsequent attempt by the accessing user to gain access to the information, cause the user to provide the capture BIR data to the computer without providing the ID; and to initiate an evaluation of the capture BIR data against the stored enrollment BIR data to determine whether the user is to be given access to the information.

84. The apparatus of claim 83, wherein the program grants the user access to the information in response to determining a match between the capture BIR data and the stored copy of the enrollment BIR data.

85. A program product, comprising:

a program configured to prompt an accessing user to provide capture BIR data to a computer, wherein memory of the computer stores enrollment BIR data retrieved from a network and correlated with a privileged user, and to cause the computer to communicate with the network; and further to initiate an evaluation of the capture BIR data with the enrollment BIR data to determine whether an accessing user is to be given access to the network as the privileged user via the computer, and if so, configured to thereafter store a copy of the enrollment BIR data in the database for later use; and

a signal bearing medium bearing the program.

86. The program product of claim 85, wherein the signal bearing medium includes at least one of a recordable medium and a transmission medium.

87. A program product, comprising:

a program configured to cause an accessing user to provide capture BIR data to a computer without providing an ID, wherein a copy of an enrollment BIR data was stored on a previous attempt by the accessing user to gain access via a network, and to evaluate the capture BIR data against the stored enrollment BIR data to determine whether the accessing user is to be given access to the computer as the privileged user; and

a signal bearing medium bearing the program.

88. The program product of claim 87, wherein the signal bearing medium includes at least one of a recordable medium and a transmission medium.

1/4

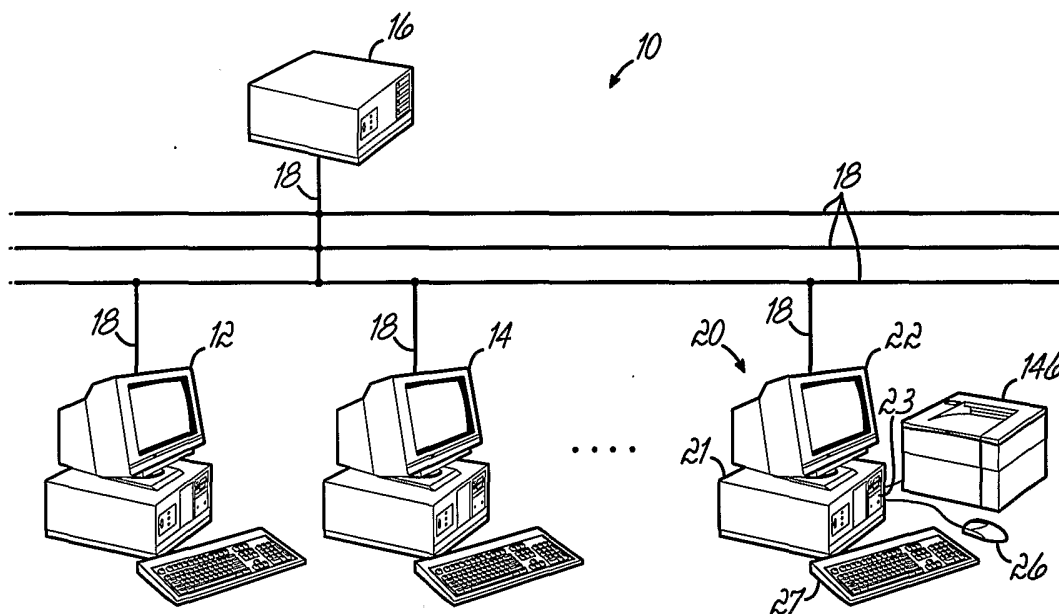


FIG. 1

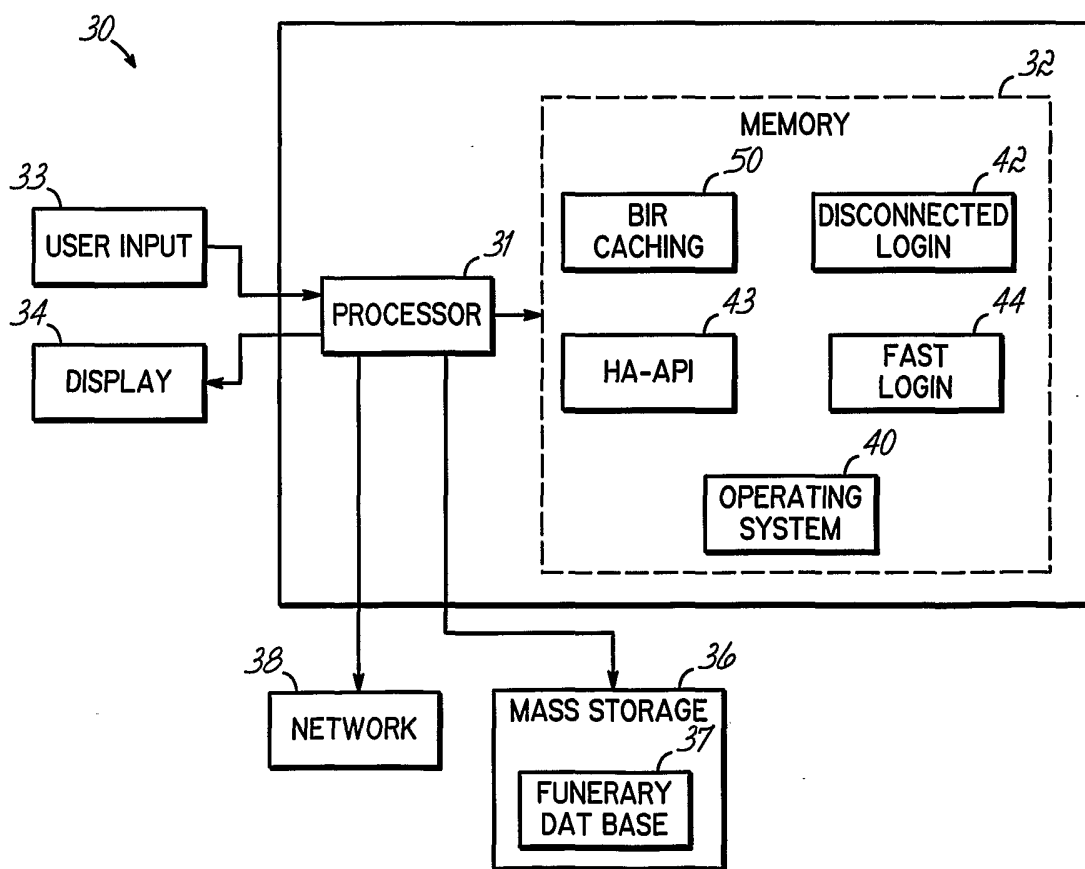


FIG. 2

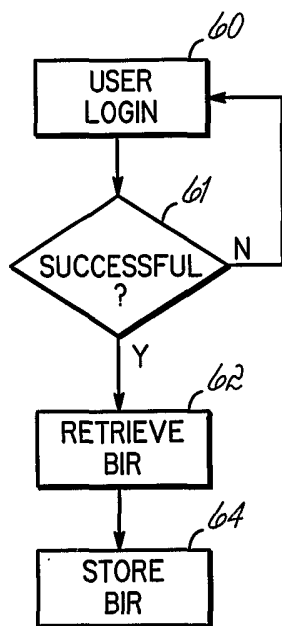


FIG. 3

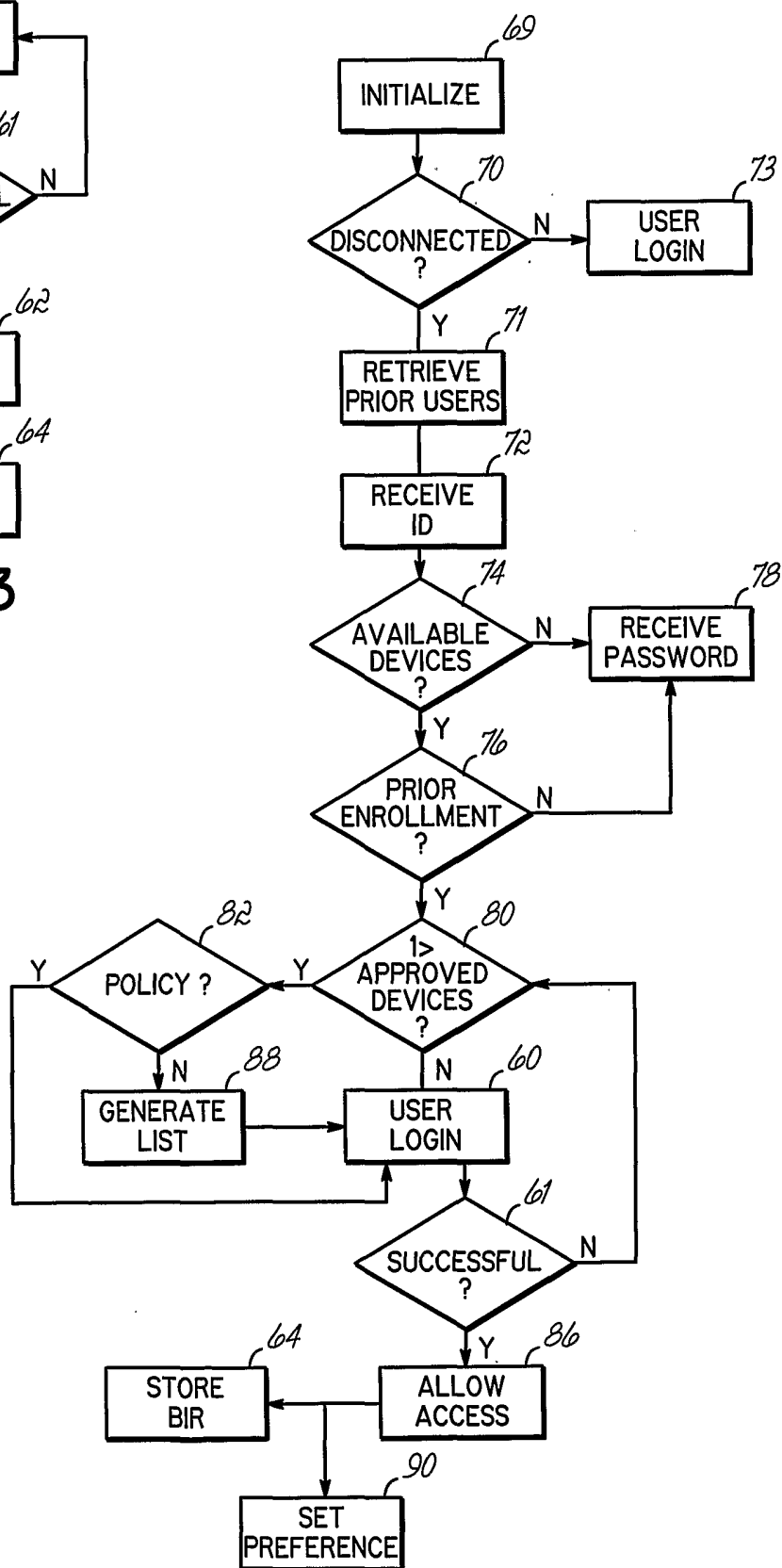
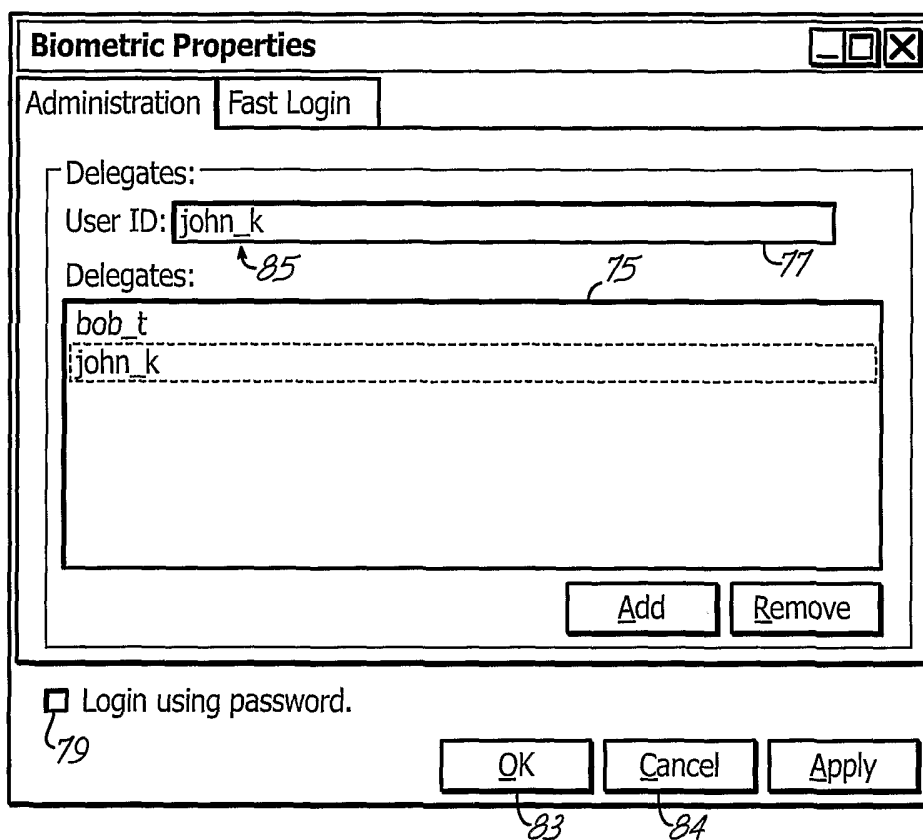


FIG. 4



The dialog box is titled "Biometric Properties" and has two tabs: "Administration" and "Fast Login". The "Fast Login" tab is selected. It contains a "Delegates:" label, a "User ID:" text box with "john_k" entered, and a list box with "bob_t" and "john_k". There are "Add" and "Remove" buttons below the list box. At the bottom, there is a checkbox labeled "Login using password." and three buttons: "OK", "Cancel", and "Apply".

Delegates:

User ID: john_k

Delegates:

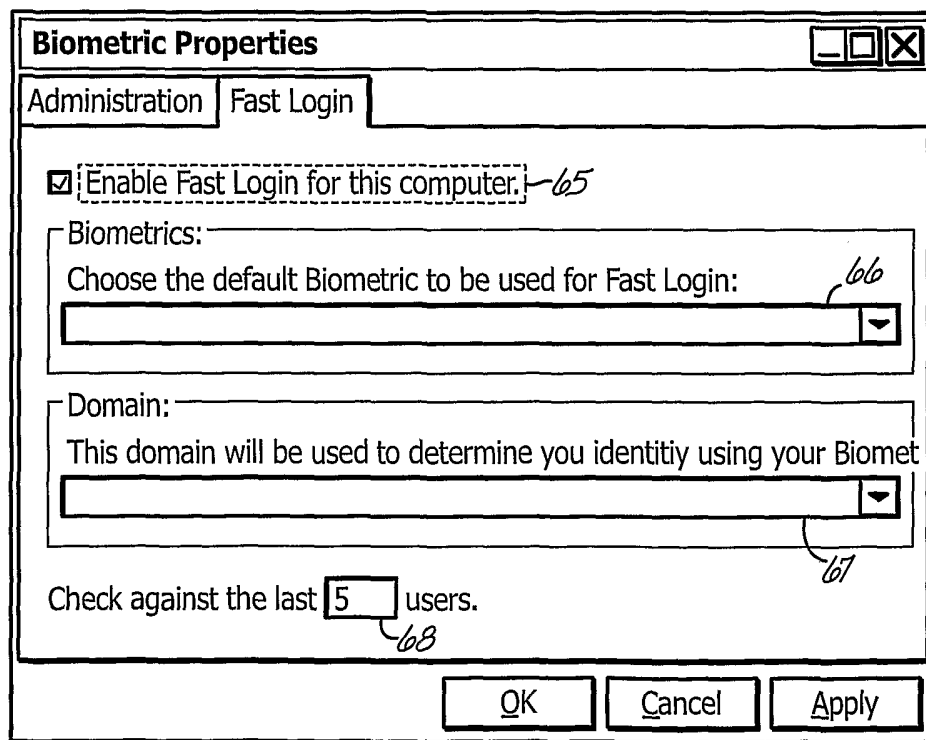
- bob_t
- john_k

Add Remove

☐ Login using password.

OK Cancel Apply

FIG. 5



The dialog box is titled "Biometric Properties" and has two tabs: "Administration" and "Fast Login". The "Fast Login" tab is selected. It contains a checkbox labeled "Enable Fast Login for this computer.", a "Biometrics:" label, a text box for "Choose the default Biometric to be used for Fast Login:", a "Domain:" label, a text box for "This domain will be used to determine your identity using your Biometric", and a text box for "Check against the last 5 users.". There are "OK", "Cancel", and "Apply" buttons at the bottom.

Enable Fast Login for this computer.

Biometrics:

Choose the default Biometric to be used for Fast Login:

Domain:

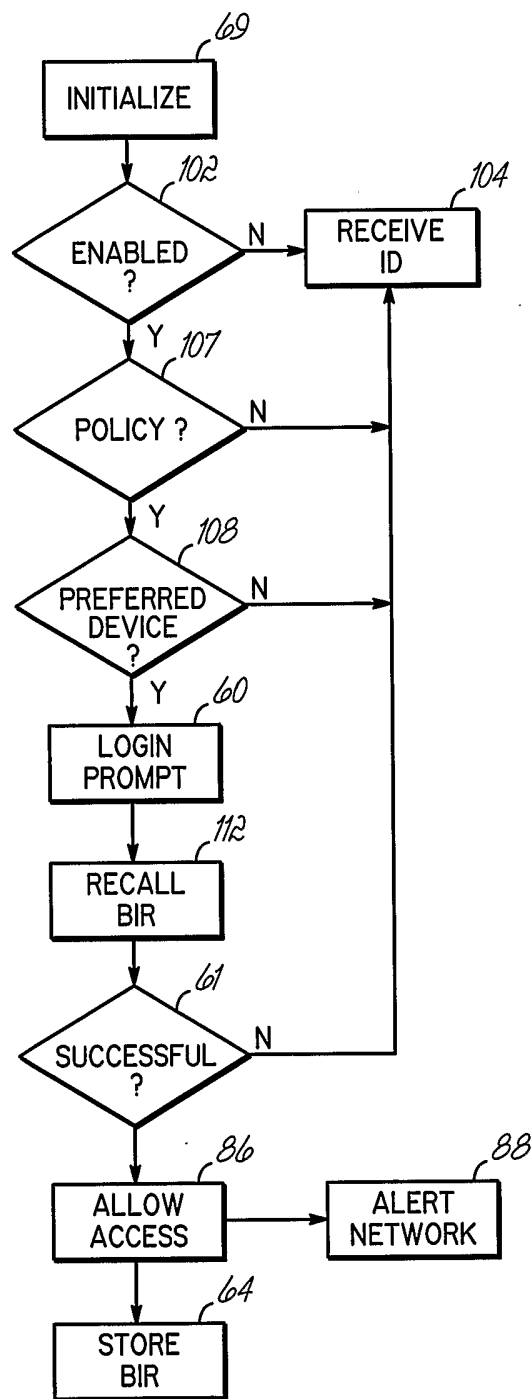
This domain will be used to determine your identity using your Biometric

Check against the last 5 users.

OK Cancel Apply

FIG. 7

4/4

**FIG. 6**

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 01/30458

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

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

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

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 167 517 A (GILCHRIST GARY ET AL) 26 December 2000 (2000-12-26) column 5, line 51 -column 6, line 65 figure 3	1, 2, 19, 33-39, 48-52, 54, 55, 68-74, 83-88
Y	WO 01 48674 A (LINK PLUS INC; YOO CHIN WOO (KR)) 5 July 2001 (2001-07-05) page 9, line 6 -page 10, line 20 page 17, line 20 -page 19, line 1 -/--	1, 2, 19, 33-39, 48-52, 54, 55, 68-74, 83-88



Further documents are listed in the continuation of box C.



Patent family members are listed in 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 claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

29 May 2002

Date of mailing of the international search report

05/06/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sigolo, A

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/30458

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 182 076 B1 (YU YUAN-PIN ET AL) 30 January 2001 (2001-01-30) abstract; figure 5 column 13, line 1 - line 58 -----	3, 4, 53, 54

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 01/30458

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 6167517	A	26-12-2000	NONE	
WO 0148674	A	05-07-2001	AU 2233601 A	09-07-2001
			WO 0148674 A1	05-07-2001
			US 2001056487 A1	27-12-2001
US 6182076	B1	30-01-2001	US 5930804 A	27-07-1999
			US 2001000045 A1	15-03-2001
			EP 0923756 A1	23-06-1999
			WO 9857247 A1	17-12-1998
			JP 2000516746 T	12-12-2000