

FIG. 1 shows a block diagram of a communications environment wherein a preferred embodiment of the present invention is practiced;

FIG. 2 shows a block diagram which describes various components utilized by the present invention;

FIG. 3 shows cooperation between a user terminal and an authentication module in accordance with the present invention;

FIGS. 4-6 show flow charts of procedures performed at an authentication center in accordance with the present invention;

FIG. 7 shows a block diagram of a user database memory structure utilized by the authentication center in accordance with the present invention;

FIG. 8 shows a block diagram of a log-on message utilized by the present invention;

FIG. 9 shows a flow chart of a procedure performed at user terminals in accordance with the present invention;

FIGS. 10-11 show flow charts of procedures performed at an authentication node in accordance with the present invention; and

FIG. 12 shows a block diagram of a public key list memory structure utilized by the authentication node in accordance with the present invention.

#### DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 shows a block diagram of a communications environment 10 within which the preferred embodiment of the present invention is practiced. Environment 10 includes any number of user terminals 12, base stations 14, and central switching offices 16. Base stations 14 and central switching offices 16 serve as nodes of a communications network 18. Network 18 provides communication services or resources to subscribers through user terminals 12.

In the preferred embodiment, central switching offices 16 are dispersed throughout a wide geographical area. Each central switching office 16 controls its own set of base stations 14 through dedicated communication links 20. Links 20 may be implemented using radio-communication for base stations 14 which are mobile, such as on aircraft, ships, or vehicles, and/or not terrestrially based, such as orbiting satellites. On the other hand, links 20 may be implemented using land-lines for base stations 14 which are stationary and/or terrestrially based. In the preferred embodiment, base stations 14 communicate over radio frequency (RF) links 22 with the user terminals 12 that are located nearby. In addition, base stations 14 communicate with neighboring base stations 14 over links 24, which may be implemented using RF or landlines. Any user terminal 12 or node of network 18 may communicate through network 18 with other user terminals 12 and with other nodes of network 18.

In the preferred embodiment, central switching offices 16 of network 18 couple to the public switched telecommunications network (PSTN) 26. This gives additional routes for communication between nodes of network 18 and permits any user terminal 12 to communicate with any of the multitude of telephone instruments and devices 28 coupled to PSTN 26.

Environment 10 additionally includes an authentication center 30. Authentication center 30 is in data communication with network 18 and all nodes thereof. This data communication may occur through PSTN 26, as shown in FIG. 1, or through a direct link to any node of

network 18 (not shown). While authentication center 30 may be positioned anywhere, it is preferably placed at a permanent location where security measures may be effectively employed at low expense. Due to a desire to maintain inexpensive but effective security, the use of only one authentication center 30 within environment 10 is preferred.

FIG. 2 shows a hardware block diagram which, with minor variations, applies to authentication center 30, to each user terminal 12, and to each node of network 18. Generally speaking, each of authentication center 30, terminals 12, and the nodes of network 18 represents a computer 32. Terminals 12 and the nodes of network 18 represent computers which are dedicated to their respective communication functions and which include additional features not related to the present authentication system. Authentication center 30 is, for example, a general purpose, personal computer.

Computer 32 includes a processor 34 which couples to a memory 36 and an input/output (I/O) interface 38. Memory 36 stores data. Some of this data is stored permanently and other data is stored temporarily. The data include computer programs which instruct computer 32 how to perform the procedures that are discussed below in more detail. Processor 34 communicates data through I/O interface 38. For user terminals 12 and nodes of network 18, interface 38 couples to a link which may be an RF link, such as links 20-24, discussed above in connection with FIG. 1. For certain nodes of network 18 and for authentication center 30, I/O interface 38 couples to a land-line wire or optical link 40, through which data may be communicated as discussed above in connection with FIG. 1. In addition, I/O interface 38 couples to other conventional I/O devices 42. Devices 42 include a wide range of data input devices, such as keyboards, keypads, pointing devices, and the like, and a wide range of data output devices, such as displays, printers, and the like.

For authentication center 30, I/O interface 38 also couples to a conventional programmer 44. Programmer 44 is used for programming authentication block data (discussed below) into an authentication module (AM) 46. Preferably, AM 46 contains a programmable read only memory (PROM) 47 mounted in a small housing 48 having connectors 49 adapted for mating with programmer 44 and with a user terminal 12. The programming of each AM 46 is customized for its own user terminal 12.

As shown in FIG. 3, the physical characteristics of housing 47 of AM 46 are designed in cooperation with user terminal 12 so that AM 46, including memory 47 therein, is removably inserted within user terminal 12. Moreover, each AM 46 is combined with its terminal 12 so that connectors 49 (see FIG. 2) mate with corresponding connectors (not shown) within the terminal 12 and so that memory 47 of AM 46 then serves as a portion of memory 36 (see FIG. 2) for the terminal 12.

Alternatively, AM 46 contains digital circuitry (not shown) that performs addressing of PROM 47. Thus, terminal 12 has no control over the addressing of the information in AM 46 and only requests information from AM 46. The digital circuitry addresses PROM 47 in a predetermined manner and transfers the resultant data to terminal 12. The digital circuitry is configured such that the next request for information will point to the next desired address. The configuration may result in sequentially addressing the PROM (i.e. a sequential