

## PROCESS FOR IMPROVING PUBLIC KEY AUTHENTICATION

United States Patent application entitled "Authentication System" with Ser. No. 795,606, filed Nov. 21, 1991, now U.S. Pat. No. 5,249,230, by the same inventors related.

### FIELD OF THE INVENTION

The present invention relates generally to the provision of services. More specifically, the present invention relates to systems and methods for insuring that services are provided only to legitimate users of the service.

### BACKGROUND OF THE INVENTION

Communication services, whether land-line telecommunication, cellular telecommunication, or other radio-communication services, are offered through the use of automated equipment. Computing services, database services, and various financial services are other examples of automated services. These and other automated services are offered to subscribers by service providers. Typically, subscribers utilize such services through user equipment, and service providers establish and maintain infrastructures which cooperate with the user equipment to provide resources to the subscribers.

The providers of automated services often need to insure that their services are being provided only to legitimate subscribers. When the resources are valuable, such as when communication is involved, piracy of the services can deprive the service provider of revenues, waste scarce resources on users not entitled to receive the resources, reduce availability of resources for legitimate subscribers, and generally increase costs for legitimate subscribers. In other situations, such as in connection with database and financial services, the offered resources are of a sensitive nature wherein serious damage can result from unauthorized tampering.

In order to insure that only legitimate subscribers use available resources, service providers often employ systems to authenticate the users. In accordance with one authenticating system, the service provider supplies both the infrastructure equipment and all the user equipment. The service provider may design the various parts of this equipment to cooperate with one another in accordance with proprietary design parameters. While this system may be effective with a small number of users, legal and economic factors cause it to fail as the number of users increases to mass market proportions. As the number of users grows, additional equipment suppliers desire to serve the marketplace, the design parameters tend to become widely known, and "pirate" equipment tends to appear. Unauthorized users can then gain access to the service through the use of pirate equipment.

Other systems cause the users to take particular actions to gain access to the service. For example, computer and database resources often require users to supply passwords before access to the service is granted. Financial services often require users to supply personal identification numbers (PINs) before access is granted. However, such passwords and PINs are not effective in authenticating users. When passwords and PINs are configured so that they can be easily remembered, they are easily discovered by potential pirates. When passwords and PINs are more complex, legitimate subscri-

ers tend to write them down where they become vulnerable to pirates.

Other systems require legitimate users to carry devices which include complex and occasionally encrypted codes that serve to identify the users. Such devices are often used with PINs to protect against theft of the device. When the devices include encrypted codes, the service providers typically provide elaborate key management procedures making the service more burdensome and driving up the costs for all legitimate users. Furthermore, requiring users to carry devices to access a service is an unwanted burden in many situations.

### SUMMARY OF THE INVENTION

Accordingly, it is an advantage of the present invention that an improved system for authenticating users of a service is provided.

Another advantage is that the present invention effectively authenticates users without requiring a service provider to control user equipment.

Another advantage of the present invention is that users are effectively authenticated without placing a burden on legitimate users of the service.

Another advantage of the present invention is that users are effectively authenticated at minimal cost. Yet another advantage is that the present invention provides services on a priority basis.

The above and other advantages of the present invention are carried out in one form by a method for authenticating users of a service offered by a service provider. The service is accessible through user terminals that have equipment identification data (ID) associated therewith. The equipment ID for one of the user terminals is obtained. An encrypted block of data, which includes the equipment ID and sequence numbers, is then formed. The encrypted block of data is stored in the user terminal, and the user terminal sends a log-on message to the service provider. The log-on message includes the encrypted block and the equipment ID.

The above and other advantages of the present invention are carried out in another form by a method for authenticating user's of a service which is accessible through user terminals that have equipment identification data (ID) and sequence numbers associated therewith. A log-on message is received. The log-on message includes one of a sequence of encrypted blocks of data and an identifying block of data. The encrypted block includes a first equipment ID in an encrypted form and a sequence number. The identifying block includes a second equipment ID. The encrypted block is decrypted to obtain the first equipment ID and sequence number. The sequence number in the encrypted block is compared with the sequence number received in the previous log-on message. Access to the system is denied if the sequence number is equal to or less than the previous one. The first and second equipment IDs are evaluated to detect correspondence therebetween. Access to the service is denied if a correspondence is not detected.

### BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention may be derived by referring to the detailed description and claims when considered in connection with the Figures, wherein like reference numbers refer to similar items throughout the Figures, and: