US006259909B1

(12) **United States Patent**
**Ratayczak et al.**

(10) **Patent No.: US 6,259,909 B1**
(45) **Date of Patent: Jul. 10, 2001**

(54) **METHOD FOR SECURING ACCESS TO A REMOTE SYSTEM**

(75) Inventors: **Georg Ratayczak**, Gangelt; **Norbert Niebert**, Aachen, both of (DE)

(73) Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/111,868**

(22) Filed: **Jul. 8, 1998**

(51) **Int. Cl.**$^7$ .................................................... **H04M 1/66**
(52) **U.S. Cl.** ........................... **455/411**; 455/410; 455/414
(58) **Field of Search** .................................... 455/410, 411, 455/414; 379/188

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,668,875 | * | 9/1997 | Brown et al. | 380/23 |
| 5,745,559 | * | 4/1998 | Weir | 455/411 |
| 5,774,525 | * | 6/1998 | Kanevsky et al. | 379/188 |
| 5,907,597 | * | 5/1999 | Mark | 379/188 |
| 5,991,617 | * | 11/1999 | Powell | 455/410 |
| 6,091,945 | * | 7/2000 | Oka | 455/410 |
| 6,091,946 | * | 7/2000 | Ahvenainen et al. | 455/411 |
| 6,112,078 | * | 8/2000 | Sormunen et al. | 455/411 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| 92/04671 | 3/1992 | (WO) . |

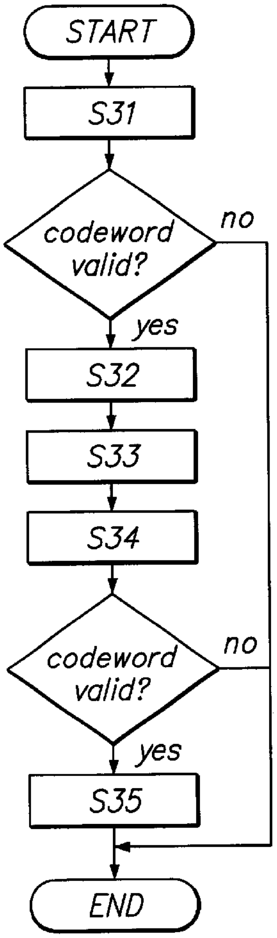
* cited by examiner

*Primary Examiner*—Daniel Hunter
*Assistant Examiner*—Thuan T. Nguyen
(74) *Attorney, Agent, or Firm*—Burns, Doane, Swecker & Mathis, L.L.P.

(57) **ABSTRACT**

Method for secure user access to a remote system using a communications device. Access to the system is released only after the input of valid code words via independent communications devices. One of the communications devices may be a data processing unit and the second communications device may be a mobile telephone.

**27 Claims, 2 Drawing Sheets**



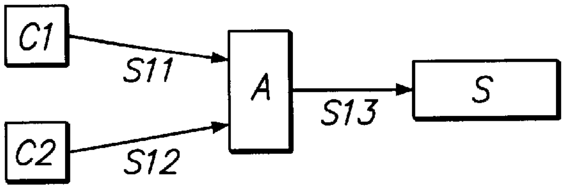


FIG. 1

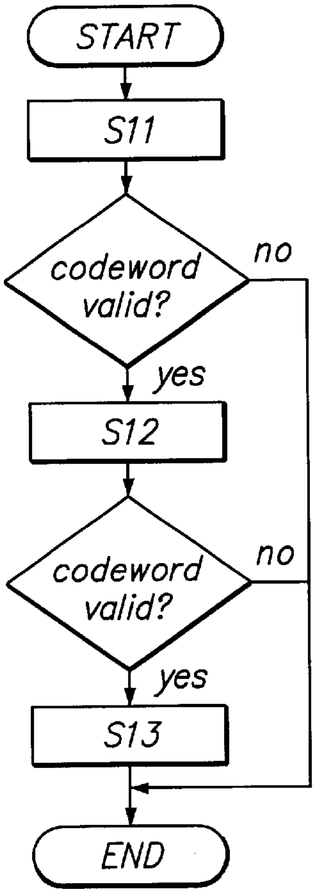


FIG. 2

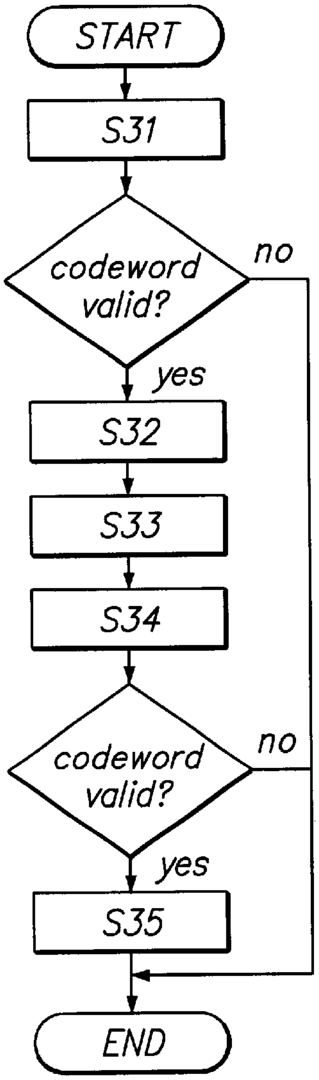


FIG. 4

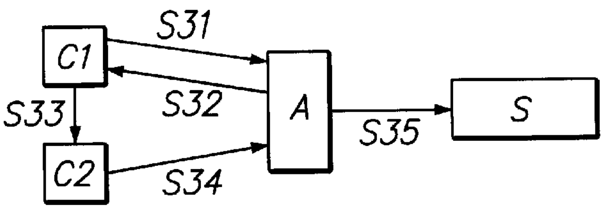


FIG. 3

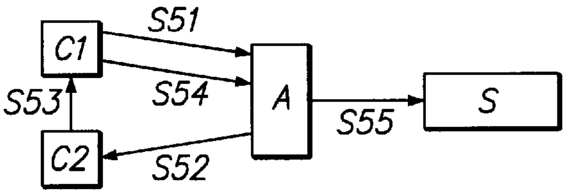


FIG. 5

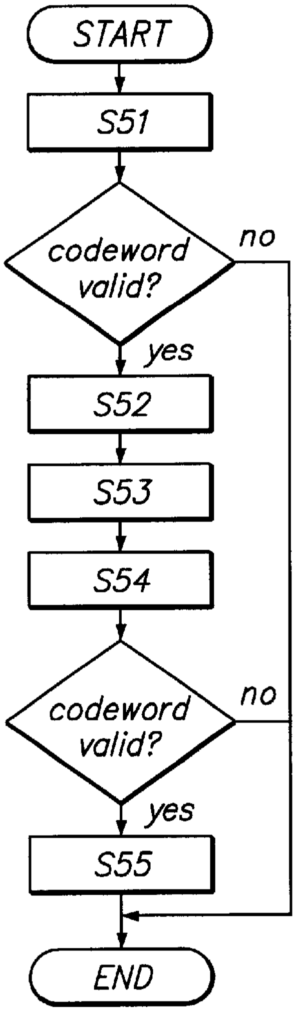


FIG. 6

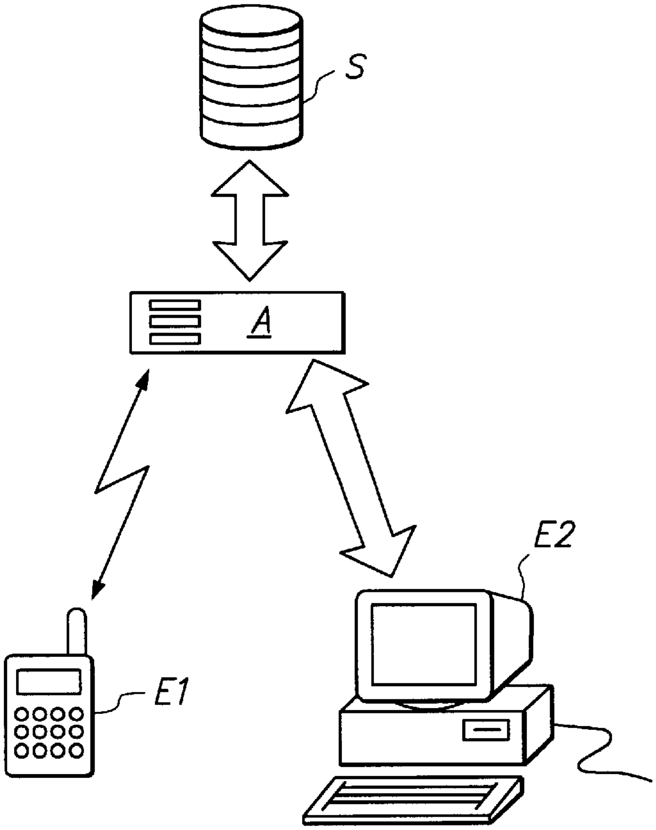


FIG. 7

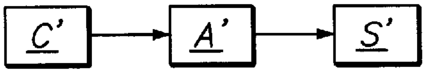


FIG. 8
PRIOR ART

# METHOD FOR SECURING ACCESS TO A REMOTE SYSTEM

The present invention relates to a method for securing access to a system. In particular, the invention relates to a method for securing access to data of a remote system using a communications apparatus.

Because of the increasingly widespread deployment and use of data networks, security aspects are becoming increasingly important in various applications. These may be applications in which secret information is transferred between data processing devices via a data network, e.g. in electronic payments transactions, electronic “shopping” and the like. Most importantly, security requirements include, apart from secure transmission of data via the network, the identification of an authorized user. In particular, when an authorized user wishes to access, via a publicly accessible data network, to a system and/or to data stored there and associated with it, it must be ensured by specific arrangements, that only the authorized user can access associated data.

For example, the data network can be an internet, comprising a large number of computers are connected with each other to form a generally accessible network. Since in such a network there are no secure data transmission lines, other ways are required to secure data and to identify an authorized user.

In general, a secure unit requests the input of a code word for authenticating a user, thus clearly identifying the user.

This process of securing access from a communications device to a remote system is generally known. An example is shown in FIG. **8**. C' marks a communications device, A' an access device and S' the system. Access from the communications device to the system is cleared as follows: in a first step, a code word is entered at the communications device C'. It is then transmitted to the access device A' where it is checked for validity. In case the code word is determined to be valid, the access device releases access to the system by the communications device C'.

A large number of such processes, identifying a subscriber by means of such code word, are known. However, like the example described above, they do have the disadvantage that the knowledge of the code word allows an unauthorized user to, e.g., access data of another user or to otherwise take not allowed influence on the system.

It is therefore object of the invention to provide a method for securing access to data allowing greater security in authenticating an authorized user wishing to access said data.

This object of the present invention is solved methods with the features of claims **1**. The method with the features of claim 1 advantageously allows the secure identification of a user, by using two individual connections between a first and a second communications device and a determining device, in order to transmit a first and a second code word to the determining device for checking.

The problem of the present invention is furthermore solved by a method with the features of patent claim **3**. The method in accordance with claim **3** permits improved security of access to the system due to the fact that after the transmission and checking of a first code word by the determining device, a second code word is transmitted to the second communications device, for input into the first communications device and transmission from the first communications device and the transmission device for checking.

In an advantageous embodiment of the invention, a data processing device can be used as one of the two communications devices, connected to the determining device via a data network. A telephone can be used as the second communications device, connected to the determining device via a telephone line.

The connections can particularly advantageously be established via an Internet and/or via a mobile radio network. In this connection it is possible that after establishing the connection between the data processing device and the determining device and after input of the code word by depressing one or more keys on the mobile telephone, access to the system and/or to subscriber data stored in a data memory of the system is released. By use of a mobile telephone allocated to a subscriber, a secure identification of the subscriber can be carried out.

In a further advantageous embodiment of the method in accordance with the invention, the transmission device may generate a code word using a secret algorithm. The code word may be transferred to one of the communications devices for input into the other one of the two communications devices, and for subsequent retransmission to the access device for investigation. This allows a further enhanced security.

In addition, one of the code words can be used to carry out data encoding of data transmitted between one or both of the communications devices and the determining device. In general, a code word may be derived from predetermined subscriber data, the date or the time. Further, the code word may be valid for only one access procedure.

For the implementation of the method for securing access to a system, advantageously an access device may be used, which on the one hand is connected with the system and on the other is connected, via separate communication paths, with two communication devices for the transmission of code words and for access to the system, preferably a data processing unit and a telephone/mobile telephone.

Further embodiments and advantageous modifications of the method become obvious with the subclaims.

## BRIEF DESCRIPTION OF THE FIGURES

FIG. **1** shows a schematic illustration of an embodiment of the method in accordance with the invention for securing access to a remote system;

FIG. **2** shows a flow diagram of the embodiment of the method in accordance with the invention of FIG. **1**;

FIG. **3** shows a schematic illustration of a further embodiment of the method in accordance with the invention;

FIG. **4** shows a flow diagram of the embodiment of the method in accordance with the invention of FIG. **3**;

FIG. **5** shows a schematic illustration of another embodiment of the method in accordance with the invention;

FIG. **6** shows a flow diagram of the embodiment of the inventive method in accordance with FIG. **5**;

FIG. **7** shows a block diagram of a device for carrying out the method in accordance with the invention; and

FIG. **8** shows a schematic illustration of a known access procedure.

In the following, the invention is described with respect to the figures.

FIG. **1** shows a first embodiment of the method in accordance with the invention, wherein individual process steps are illustrated using arrows. FIG. **1** shows first communications device C**1**, a second communications device C**2** as well as an access device A and a system S, to which access is to be obtained. Further devices, such as for example communications lines, data transmission devices and the like are not shown. Reference numerals S**11**, S**12** and S**13** denoting the arrows illustrate process steps which are carried out successively in the embodiment of the method in accordance with the invention.

FIG. **2** shows a flow diagram of the embodiment shown in FIG. **1** to further clarify the process in accordance with the invention for securing access to a remote system.

In the following, steps for executing the procedure in accordance with FIGS. **1** and **2** will be described. At first, the step denoted S**11** is carried out. In step S**11**, a first connection is established from the communications device C**1** to an access device A and, besides identifying a user, a first code word is transmitted from the first communications device C**1** to the access device A. The first code word is received by the access device A and it is compared with authentication data stored in access device A. The comparison can be a known procedure for the verification of a transmitted code word. For example, in access device A, a copy of the first code word could be stored and it could be determined by comparison, whether the code word which was transmitted is the requisite code word. It could also be determined by a mathematical operation whether the first code word is correct, by checking a particular relationship to the authentication data which are stored in access device A. If the first code word is determined as being incorrect, the execution of the process proceeds to the end point of the flow diagram shown in FIG. **2**. If the first code word is found to be correct, the process moves on to a step S**12**.

In step S**12**, a connection is established from the second communications device C**2** to access device A. A second code word is transmitted via this connection to the access device. This second transmitted code word is received at the access device and is authenticated, as was already described in step S**11**. The code word can be a fixed sequence of signs, which identify the user and a code portion which is known only to the user. But identification of the user may also be carried out in a differently. If no user assigned code word has been transmitted, the process moves on to the end point shown in the flow diagram of FIG. **2**. If the second code word is determined to be correct, the process moves on to step S**13**.

In step S**13**, access to the system S is released by the access device A from one or both of the communications devices C**1**, C**2**. This access to system S may be such that data can be transferred to system S and/or data can be retrieved from system S via one or both of the communications devices C**1**, C**2**. In addition, it is possible that the authorized user can trigger certain functions of the system S via one or both of the communications devices C**1**, C**2**. In the embodiment described, process steps are carried out in sequence, preferably in the sequence S**11**–S**13**. However, modifications of this sequence or partial steps are possible.

As in the case of a device described in more detail later with reference to FIG. **7**, in a second embodiment a data processing unit can be used as the first communications device C**1** and wherein the connection between this data processing unit and the access device A is established via a data processing network.

The data processing unit may be constituted by a personal computer available on the market, which is equipped with a suitable modem. The connection between the personal computer and the access device A may be established via a data network, for example the Internet. The provision of a connection from a computer via an internet to the access device A, which may also be constituted by a computer or a server, optionally with special functions and features, is well known and will not be further explained at this point.

In addition, in the second embodiment, the second communications device C**2** may be constituted by a telephone and the connection between the telephone and the access device A may be established via a telephone network. In this connection, the telephone network may preferably be a mobile radio network or a conventional fixed telephone network and/or PSTN.

Thereby it is possible that the connections between the first and/or second communications devices C**1**, C**2** and the access device A may be established via separate communications routes independent from each other.

Furthermore, in the second embodiment, the system S to be accessed, may be a mobile radio network and/or a memory device of the mobile radio network, in which specific subscriber-related data are stored, but in particular a telephone network in accordance with the GSM standard. In case of a GSM network, the access device may advantageously be an expansion of the HLR (home location register) which forms a unit with a server of the worldwide web (WWW) and/or of the Internet. In this embodiment, access is advantageously controlled to the HLR (home location register) by the access device A. In thie HLR register, subscriber-specific data are stored, for example for services such as forwarding of calls or other configuration settings which concern the subscriber. The above described embodiment enables a subscriber a secure access to the communication network or to subscriber data associated with him stored in the HLR register.

Therefore the user may alter in a particularly convenient way, for example, configuration settings, activate certain services and deactivate them and may retrieve, change or store information and data. The communication between the user and the system, necessary for transmission of the code words, may be carried out, inter alia, via USSD (unstructured supplementary service data).

Access to subscriber-specific data stored in the HLR register in this embodiment may be carried out as follows when relying on the method in accordance with the invention shown in FIGS. **1** and **2**.

A subscriber wishing access to the subscriber data in the HLR register associated with him, establishes a connection between a data processing unit constituting one of the communications devices and which is connected by the internet (WWW client) to access device A. In this case, this is an internet server forming a unit with an expansion of the HLR. Authentication of the user and/or subscriber is carried out by the transmission and validation of the first code word in step S**11**, shown in FIGS. **1** and **2**, to access device A. Here, the communication between the data processing unit and the access device A may be performed in accordance with a so-called TCP/IP protocol.

If the access device A determines the user as being authorized, access device A awaits an input of a second code word via a second communications device, in this case the mobile telephone or a fixed network telephone (step S**12**). In further embodiments, access device A may transmit a request for an input of the second code word (step **12**) via an interface to the GSM network of the mobile telephone or of a fixed network telephone. The input of the code word may be carried out using a telephone keyboard by pressing a single key, for example the call demand key, or by pressing a sequence of keys.

After authorization of the second code word and therefore of the subscriber at access device A, the access device allows access to system S (step S**13** in FIGS. **1** and **2**).

This may be access to subscriber-specific data stored in the memory device of the HLR register or it may be an

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

### FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

### E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.