



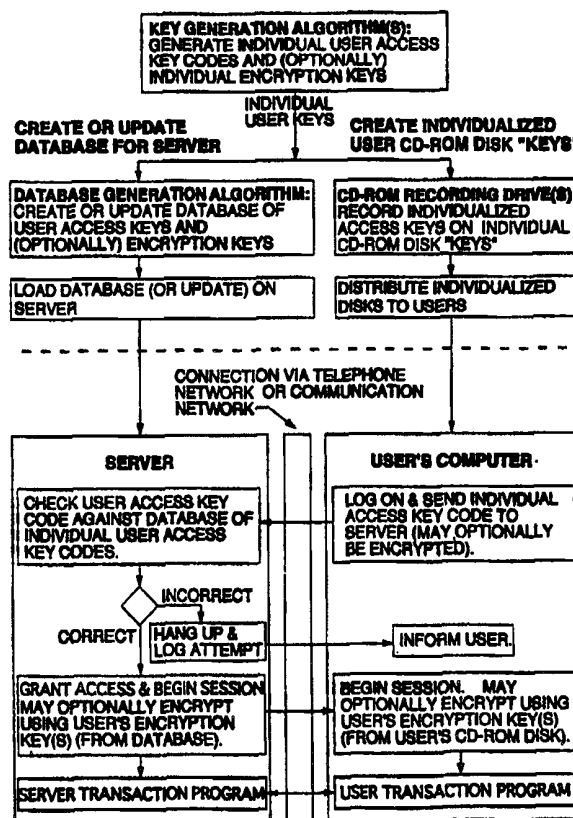
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|--|--|--|
| <p>(51) International Patent Classification ⁶ : G06F 15/20</p> | <p>A1</p> | <p>(11) International Publication Number: WO 99/46691 (43) International Publication Date: 16 September 1999 (16.09.99)</p> |
| <p>(21) International Application Number: PCT/US98/10355 (22) International Filing Date: 22 May 1998 (22.05.98) (30) Priority Data: 09/037,297 9 March 1998 (09.03.98) US (71)(72) Applicants and Inventors: NEWTON, Farrell [US/US]; 8 Brighton 10th Path, Brooklyn, NY 11235 (US). WILLIAMS, Gareth [US/US]; 35-11 85th Street, Jackson Heights, NY 11372 (US). (74) Agent: CORNMAN, Michael, A.; Schweitzer Comman Gross & Bondell LLP, 230 Park Avenue, New York, NY 10169 (US).</p> | <p>(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, 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).</p> <p>Published <i>With international search report.</i></p> | |

(54) Title: INTERNET, INTRANET AND OTHER NETWORK COMMUNICATION SECURITY SYSTEMS UTILIZING ENTRANCE AND EXIT KEYS

(57) Abstract

A security system emphasizing ultra-long keys for restricting access to a host computer or server, through a network such as the internet or an intranet, from a remote computer by the usage of an electronic "double-sided pass key" established on a portable memory medium such as a CD-ROM. The key has ultra-long, constantly revised entrance codes to permit access to the server and ultra-long, constantly revised exit codes to authenticate or to validate the transactions conducted during authorized access and before termination of the authorized connection. If the proper exit code is not received the transactions of the connection are erased, thus aborting a hijacked connection. In addition, the portable memory medium includes defensive tools to thwart trespassing attacks on the security system including electronic dye markers and electronic homing beacons which serve to identify and to locate trespassers.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|-----------|--------------------------|-----------|--|-----------|--|-----------|--------------------------|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakistan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

INTERNET, INTRANET AND OTHER NETWORK COMMUNICATION SECURITY
SYSTEMS UTILIZING ENTRANCE AND EXIT KEYS

BACKGROUND OF THE INVENTION

5 Most security programs for personal computers and
networks rely upon simple user passwords and they are
therefore vulnerable. There are two common methods for
acquiring unauthorized access to a host computer. In the
first method, the intruder improperly obtains and illegally
10 uses the user ID and password of a valid user. The second
method is to steal a valid user session in progress by
switching the connection of the user to the thief's ter-
minal. Without a method to verify the identity of the
user, there is little preventing an intruder from obtaining
unauthorized access to the user's account through a pur-
15 loined user ID and password.

This lack of security has been a shortcoming of
various corporate and other networks including the Internet
and is one factor that has limited commercial use of these
networks.

20 One existing authentication system proposes to add a
card reader to personal computers so that users can verify
their identity with a user identification card, as shown in
U.S. Patent 4,438,824, issued on March 27, 1984, to C.
Mueller-Schloer for an invention entitled "Apparatus and
25 Method for Cryptographic Identity Verification". However,
few users will spend the time and money to install an
expensive card-reader. Furthermore, user identification
cards have very limited storage and usually store a short
identification key. Therefore, the same short identifica-
30 tion key is used during most if not all authentications.

United States Patent 5,371,792, entitled CD-ROM DISK
AND SECURITY CHECK METHOD FOR THE SAME issued on December
6, 1994 to Toshinori Asai and Masaki Kawahori, relates to

CD-ROMs for television game devices. The purpose of the security check is to prevent unlicensed CD-ROM disks from being played on a Sega game machine. The CD-ROM disk identifier disclosed in this patent is not unique to each individual CD-ROM disk, but instead merely indicates a kind of the CD-ROM disk. All CD-ROM disks of the same type have the same disk identifier. In the patent, two kinds of identifiers, "SEGADISKSYSTEM" and "SEGABOOTDISC" are described. The security code indicates that the CD-ROM disk is duly licensed and also contains a program which generates a message displayed on the user's monitor that the disk is licensed.

There have been numerous patents issued for integrated circuit cards and other computerized portable security devices. For example, Beitel et al., U.S. Patent No. 4,430,728, employs a physical security key which is coupled into a connector provided for it at a remote terminal. The key has two access keys which are required to access the central computer. This invention, like the Mueller-Schloer '824 credit card device, requires special hardware to be added to computers and requires costly security keys. Locking the terminal does not prevent intruders from procuring unauthorized access on public networks, since the intruder can use another terminal elsewhere.

SUMMARY OF THE INVENTION

The object of the present invention is to provide a practical and effective security system for secure remote terminal or terminal emulation or computer access to a host computer. This is accomplished by using ultra long passwords and/or ultra large databases of identification keys, i.e., by a CD-ROM disk or other portable large capacity storage medium containing a database of identification keys, long identification keys, or a combination thereof. The subsequent descriptions of the invention will be in

terms of CD-ROM disks, although other portable storage media are contemplated for use, including Zip disks, floppy disks, digital versatile disks (DVD disks), Bernoulli disks, portable hard drives (e.g. PCMCIA hard drives), and portable semiconductor memory units (e.g. PCMCIA memory units). The authentication system further includes a remote terminal with a portable large capacity storage medium reader or connector, and a communications device or system which connects the remote terminal to a host computer which has a large capacity storage medium.

A microprocessor or logic circuitry may be added to the portable memory medium in certain applications to implement additional security features or user features. Moreover the system of the present invention may be incorporated into a portable electronic devices.

In accordance with the invention, the new security system may utilize one or more CD-ROM disks, other portable storage media, other storage devices including redundant arrays of inexpensive disks and hard drives, or any hybrid thereof containing databases of the user identification keys.

The invention also contemplates encryption and other security methods for authenticating the identity of users. Specifically, an enhanced security system entails the use of separate entrance and exit codes at the beginning and end respectively of the communication session, along with multiple authentication codes during each session, as required for super security. The invention also includes means for the tagging or identification of hackers who attempt to penetrate the new system; a programming means for such tagging or identification may be implemented on the portable storage media, in the central computers (servers) of the new system, or both.

DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram of an exemplary preferred embodiment illustrating the various steps required to practice the fundamental security system of the present invention, as well as illustrating the components which
5 comprise the required hardware and software of one CD-ROM-based implementation of the fundamental system itself; and

Fig. 2 is a schematic diagram of an alternate preferred embodiment including a double-sided key or password.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

In general, the new and improved security system of the present invention provides individual users with what are characterized as "ultra long identification keys" which are embodied on a physical object such as a CD-ROM disk which is provided to the authorized individual user. By "ultra long" it is contemplated that the individual user code will comprise at least 20 characters or digits (requiring 20 or 10 bytes, respectively) of information as a bare minimum (it being understood that the typical password employed for consumer credit cards and the like is 16 characters), although the use of a CD-ROM disk "key" enables even passwords of hundreds of characters to be readily employed.

The following describes the use of CD-ROM disks as the portable storage medium; however, it is to be understood that the use of other portable storage media in lieu of CD-ROM disks is within the scope of this disclosure.

The initial step in the new security method is to generate individual user access codes for each and every contemplated user who is to be granted authorized access to a network or a database or source or repository of information which is desired to be protected and which is stored in or in conjunction with a "home" server or base computer. The individual user access key codes are generated using algorithms or circuitry or combinations thereof which may

be optionally provided with means to generate individual encryption keys as well, in accordance with well known methods and industry standards for generating encryption key codes. It is of course to be understood that in accordance with the principles of the present invention, the individual access key code is "ultra long" and is of a length that is otherwise too long and too cumbersome to be conveniently typed into a system by an individual.

A central registry or other compilation of all of the individualized user access codes is established and is optionally encrypted for loading on the home or main computer terminal or server on which the secured database is to be located or in association with which the server is to function as a security mechanism. As a parallel to this step of the development of the security system, each of the individualized user access key codes is separately recorded, for example by ganged optical recording machines of the type known to the art for recording information onto CD-ROM disks. Each disk is in the form of a "CD-ROM key" which is individualized for a particular end user (for example, a customer of a catalog sales organization, a user of a secure database, a customer of a financial institution, etc.).

At this stage of the establishment of the system there is a complete registry of "ultra long" identification key codes stored in a server and there is a distribution of the

physical CD-ROM disk keys to authorized individual users who are to be provided access to a database.

In order to provide authorized access to an authorized user of the database or "transaction program", the user at his remote personal computer terminal which is equipped with a CD-ROM reader, loads the CD-ROM disk into his computer and logs onto an access program or user program (which may optionally be recorded on the CD-ROM disk as well). The user program then transmits the user's individual access key code (which optionally may be encrypted) over a communication network or over a telephone network to the host computer or server, which will be appropriately programmed to check the user's access key code against the registry of stored authorized individual user access key codes. The server program will further include the requisite steps to interdict and end any attempt to gain access to the server or transaction program through a transmitted access code which is not stored in the database of authorized individual user access key codes. The server program will disconnect and may optionally inform the user that an unauthorized key access code has been transmitted.

Alternatively, and assuming the CD-ROM disk was proper and contained an authorized access key code, the communication between the user's remote computer and the host server will continue with the host computer's program including steps to grant access to the user's program and begin the

session. As explained hereinafter, the host computer program or server program and the user program may optionally encrypt the session using the user's encryption key or keys, which are also stored in the server's database and on the individual user's CD-ROM disk. The optional encryption might also include encryption keys which are stored on the user's CD-ROM disk key.

At this stage, access to the secured database or "secured server transaction program" can proceed with the authorized user communicating through his own personal computer with the host server to conduct whatever "transaction" he may wish to effect, ranging from the simple ordering of merchandise, to the conduct of financial transactions, to conduct of research into a secured database, or any other type of two-way communication which is capable of being conducted between a remote computer terminal and a host computer over a communication network or a telephone network. It is to be understood that a level of security heretofore unavailable to remote consumers communicating with a host computer is provided by the new system which utilizes ultra long identification key codes typically impressed upon or otherwise recorded upon "large keys" in the form of a CD-ROM disk or the like. The ultra long identification keys are checked and approved through databases of such identification keys which are stored in a remote host computer or server.

Security may also be enhanced by providing multiple keys or a database or table of keys (which may be a one-time pad of keys) on each user's CD-ROM disk.

The user program may provide the keys in sequence or according to a pre-arranged pattern or algorithm, or from a location requested by the server. The server might request the keys in sequence or from random locations; i.e. in a random order, or according to some other algorithm. It is important to note also that the user program may provide or the server may request more than one key or multiple keys at different times during the session. As hereinafter described, the use of a one-time pad of keys also insures that no key is transmitted twice; hence intercepting or decrypting a key will not allow an attacker to gain access to the system.

In some applications, the key generation algorithm will run on the server itself or even on the users' computers; in the latter case, means to avoid generating duplicate keys is required (e.g. by a randomization function in the key generation algorithm or circuitry, plus a check for duplicate keys whenever a new key is added to the database).

Numerous other variants will also readily be apparent to those skilled in the art.

In a preferred embodiment, each user is issued a unique CD-ROM disk containing one or more unique identification keys. An individual user inserts his CD-ROM

disk "key" into a computer connected via a network or other communications device to a host computer; also referred to herein as a server. An access program on the CD-ROM "key" connects to and forwards the unique identification key from the CD-ROM disk key to the host computer in encrypted form. 5 A security authentication program stored on the server then decrypts the identification key, compares the identification key with an identification key from the database of user identification keys located on a large capacity storage device connected to the host computer, and verifies 10 the user's identity. The host computer or the user's access program may include a program or routine which will also demand that the user type in a password. If the identification key matches the identification key in the host computer's database of user identification keys and if 15 the user enters the correct password, the host computer, through its programming, will grant access to the user.

The host computer (server) may be further programmed to require or challenge the user's remote access terminal program to re-authenticate itself at regular intervals or 20 from time-to-time during the communication session. Or, the user's program may so reauthenticate itself and the host computer may be programmed to expect such reauthentication. This helps defend against hackers who try to capture an identification key en route to the host computer 25 or who misappropriate or steal a user's connection. Unless a hacker has the user's unique CD-ROM "key", he would be

unable to use his unauthorized access for longer than the time between requested re-authentications. Means to insure that an intercepted identification key or message cannot be re-used by an attacker are discussed below.

5 Similarly, the user's program may require the host computer (server) to reauthenticate itself at regular intervals or from time-to-time during a communication session. Or, the server program may so re-authenticate itself and the user program may include code to expect such
10 re-authentication. This helps defend against hackers who attempt to impersonate the host computer (server). Alternatively, the host computer and remotely accessed terminal program may request or expect identification keys periodically from each other.

15 It should be noted that such re-authentication may optionally be required at critical points in a communication session, e.g. to complete a transaction or to access a database. Such reauthentication may be required before, to initiate the action; or after, to validate the action;
20 or both.

 To insure that an intercepted identification key or message cannot be re-used by an attacker, defensive methods have been developed including the use of multiple, different identification keys; encrypting the identification
25 keys or messages, ideally by time-dependent means, e.g. by combining the identification keys with time-of-day information, then encrypting.

Another defensive method for authenticating a user to the host computer and the host computer to the user with the identification keys is the exchange of identification keys one digit at a time. In a typical implementation of this method, the user's access program (running on the user's terminal or computer) transmits the first digit of its identification key to the host. The host computer determines whether the digit transmitted was correct. If the digit is correct, the host computer transmits the first digit of its identification key to the user's terminal or computer. The user's access program determines whether the digit returned by the host is correct. This process continues until either the user program and host computer have given each other all the digits of their respective identification keys or until an incorrect digit is received by the host computer or user's access program.

Any attempt by a hacker to mimic either the host computer or the user terminal or computer most probably will fail on the first digit; if so, the hacker will get only one digit of the user password or host computer password. Thus, this technique provides additional security against "man in the middle" attacks aimed at illicitly obtaining a user or host password. Alternatively, several digits of the identification keys may be exchanged at each iteration, or single bits can be exchanged at each iteration, etc.

Although individual identification keys are contemplated, in some applications, some or all of these identification keys may be shared among a class or subclass of users.

5 In another embodiment, the host computer is programmed to send an encryption key to the remote terminal. The terminal program executing on the remote terminal uses the encryption key to encrypt the unique identification key on the CD-ROM disk. Then the encrypted identification key is
10 sent to the host computer for verification. If the encryption means is a public key encryption algorithm with a sufficiently long key, a third party would have great difficulty extracting the unencrypted identification. A variation to this method is to have part of the encryption
15 key contained on the user's CD-ROM "key" with the other part sent from the host computer. The host computer always has access to a complete database of all the encryption keys and identification keys. Without the portion of the encryption key from the CD-ROM or host computer, the remote
20 terminal program is unable to decrypt messages. If the encryption key from the host computer is varied with time, selected randomly, or unique to each user session, the user's computer will essentially never transmit the same encrypted identification key twice.

25 The remote terminal program may pad the identification key with random, null, or nonsense prefixes or suffixes or interpolated characters. To help insure that the same

identification message is not sent twice, the encryption algorithm is preferably provided with good diffusion (wherein a change in any character in the plain text changes many or all of the characters in the encrypted text). The pad will preferably be specified by the host computer so that previously used encrypted identification keys do not repeat.

The pad may vary in a pre-determined manner with time. For example, the pad may be the day, hour, and minute clock. The host computer will then be programmed to check that the pad is correct based upon the day, hour, and minute. The pad may also vary with each logon. Additionally, the user ID or user number may be padded as discussed above.

In another embodiment, the encryption key is included on the user's CD-ROM key disk and is never transmitted. The remote terminal program may pad the identification key as previously discussed. The host computer will be programmed to look up the encryption key for the user's claimed identity in a stored database of encryption and identification keys. Then the host computer will decrypt the unique identification key, remove the padding, and compare the decrypted key with the key retrieved from the host computer database, thereby verifying the user's identity. Again, when the encryption algorithm has good diffusion, the added characters will insure that the user's

computer will essentially never transmit the same identification key twice.

In another embodiment, the central server selects the encryption key of the moment from a table on the user's CD-ROM; a copy of the table being in the central server. This
5 avoids transmitting the encryption key over the connection; all that is transmitted is which entry in the key table is to be used, not the encryption key itself.

In another embodiment, the remote terminal transmits
10 to the host computer a plain text or encrypted user ID or identification key from an identification key database on the user's CD-ROM key. A second encrypted identification key is sent from the remote terminal to the host computer. The first identification key is used by the host computer
15 to look up a unique encryption key for that user. The second identification key is then decrypted using the unique encryption key and the user's claimed identity. If the decrypted identification key is correct, the user's claimed identity is then verified. The encryption key is
20 never transmitted since both the remote terminal and the host computer have the encryption key stored locally.

In addition, other parts of the transmission, or the entire transmission or session may be encrypted using a unique user-specific encryption key on the user's CD-ROM
25 disk. When the server is aware of the user's identity, it will look up the key in its own table; hence the key need never be transmitted between user and server or vice-

versa. Again, techniques such as padding would typically be used. This embodiment not only provides additional security, it also securely authenticates the host computer to the remote terminal program. An "imposter" server would
5 lack the database of user encryption keys and would be unable to decrypt the remote terminal's messages and accordingly would be unable to respond plausibly to the remote terminal.

Alternatively, a one-time pad stored on both the
10 user's CD-ROM disk key and the host computer may be used as the encryption means or key to encrypt the user's identification key to provide additional security. After receiving the encrypted identification key, the host computer is programmed to look up the one-time pad under
15 the user's claimed identity in a database of one-time pads. After decrypting the identification key, the host computer will authenticate the user's identity.

Alternatively, a one-time pad of unique identification keys may be stored on each user's CD-ROM key disk. The
20 central server would then demand a new key every time, and verify the new key against its own copy of that user's one-time pad of ID keys. The central server can keep track of which one-time-pad keys have been used to prevent re-use. If the user's portable storage medium is writable, the user
25 terminal software or access software may be used to keep a usage record or table on the portable storage medium, or the user may overwrite the keys that have been used. If

the user only accesses the server from the one terminal, the user may keep a usage record or table on the user terminal, e.g. on the hard drive.

5 Preferably, usage records may be kept in both the central server and on the user's portable storage medium or terminal, and any discrepancy between the usage records on the user's portable storage medium or terminal and on the server would suggest an attempt by a third party to illicitly gain access. Such a discrepancy will be indicated by any attempt by either the user program or the server to re-use a one-time-pad key or one-time-pad entry that has already been used with the server or user program respectively. Such a discrepancy will also be indicated by any attempt to use a key or pad entry out-of-sequence or any other "out-of-synch episode".

10

15

Both one-time pad arrangements also avoid transmitting the same user authentication key or message twice.

Furthermore, the one-time pad can be used to encrypt other important information communicated. For example, with use of a 250 kilobyte user-specific one-time pad (e.g. in conjunction with a consumer catalog) to encrypt the user's credit card number, assuming that one byte is used to encrypt each digit, then a sixteen digit credit card number would use 16 bytes of the 250 kilobyte one-time pad.

20

25 Assuming the user performed ten transactions a day, the 250 kilobyte one-time pad would last more than four years.

For any of the aforementioned identification techniques, the terminal program and the host computer also may be programmed to demand that the user enter by typing (through a keyboard) a password previously specified. The password will be compared with the user passwords stored on the CD-ROM or host computer corresponding to the user ID.

All of the above-described encryption methods can also be used to encrypt important information transmitted.

All of the above-described authentication methods can also be used in reverse to authenticate the host computer to the remote terminal program, as will be readily understood.

The most secure encryption techniques, such as public key encryption, can take up to 1000 times longer to process than more routine encryption methods, unless a special-purpose processor for the particular algorithm is added to the user's computer. One method to increase speed is to use the most secure means to encrypt only the most sensitive portions of the transmission and use faster encryption methods for less critical portions of the transmission. Because of the large capacity and speed of a CD-ROM, databases of encryption keys for each encryption method and host computer can be easily stored and accessed. Portions of the transmission that are common and do not need to be protected can be transmitted as plain text. Repeated text or graphics which all users will view can optionally be stored on the CD-ROM to decrease the amount

of information transmitted from the host computer to the remote terminal.

A special encryption device may be attached to the host computer in order to expedite encryption and decryption of transmitted data. Since the host computer will most likely service many users, the encryption device should prove very economical when amortized over the large number of users. The cost of having extremely large keys and databases of keys is the cost of the space on a CD-ROM which is not available for other information and the space needed to store these keys on the computer host. Since the cost of producing CD-ROM disks is modest, the use of CD-ROM disks has become quite economical. Thus the new authentication system of the invention is more economical and more effective than the prior art systems.

Additionally, a user's CD-ROM key according to the invention may contain different identification keys or tables or databases of identification keys for use with different servers or to provide access to different databases or services on any individual server. For example, in an application wherein several catalogs of different vendors are contained on or accessed by one CD-ROM key, different databases of identification keys and encryption keys would be allocated to provide access to each vendor's host computer or database.

Also, a user's CD-ROM key according to this invention may contain different identification keys or tables or

databases of identification keys to provide different levels of access to one or more host computers. Or, the host computer may be programmed to grant different access privileges to different users. For example, in a corporate network, the president's CD-ROM key would grant maximum access to all information on the host computer, while a clerk's CD-ROM key would only grant limited access to specific data. Similarly, in a consumer application, different consumers might have different credit limits. The requisite privilege or privilege level might either be encoded on the CD-ROM or, preferably, would be included in a database on the host computer.

It will also be apparent that a single authorization server or set of authorization servers can be used to authorize access to many other servers or to many different databases or services. In this case, the table of what is authorized for a given user would typically be kept in the single server or set of servers for ease of updating, although it could be kept on the users' portable storage media (e.g. the user's CD-ROM disk) or on the central computer (server) or divided between the two.

If the user program contacts the other servers directly, the other servers can access the single server or set of servers to obtain the authorization; alternatively, the user program might contact the other servers through the single server or set of servers (e.g. if the authoriza-

tion server function is implemented by an Internet service provider's server).

If a single server or set of servers is used to authorize access to other servers or to different databases or servers, new servers or databases or services can be authorized for a given user by simply updating the table of what is authorized for the user. Typically, the table or the portion of the table being updated would be in the single server or set of servers. However, if the user's portable storage medium is writable, an authorization table on the portable storage medium could be updated in the same fashion. Thus, the user will be able to use an existing CD-ROM or other portable storage medium to access new servers, databases or services.

It is also desirable to allow existing CD-ROM keys to be used to access new servers or databases or servers when the different host computers authorize access, as an alternative to or in lieu of referring access requests to a central server or set of servers per above. To do so, each CD-ROM disk would include identification keys or tables or databases of identification keys that are initially not assigned to any server or database or service. These would then be assigned later to access new servers, computers, programs, databases or information functions or services. This arrangement averts the need for distributing new CD-ROM disks whenever a new server is added.

Information about the new server or database or service, such as its name,, network address, and telephone number, along with the identification of the database of keys on the CD-ROM disk assigned to the new server must be added to the user's access program. For example, if 200 keys or key tables or one-time-pads of keys are already assigned to existing servers, the 201st key might be assigned to a new server. This information would be included (in either encrypted or unencrypted form) on an update floppy disk or other portable medium, posted on a bulletin board or server, or updated automatically by the remote terminal access program during a subsequent communication session. Such information is typically the same for all users being granted access to the new server.

If the user key is on a writable portable storage medium, the update information would typically be written directly to the portable storage medium.

If the portable storage medium is not writable, as with a conventional CD-ROM disk, the user's access program would typically store the update information for the new servers in a small file on the user's hard drives. If the users have a writable CD-ROM drive, the information could be added to the CD-ROM disk key. If the information about each server comprises no more than 50 characters, a 10 kilobyte disk file could contain information on at least 100 new servers. A file a few megabytes in size would allow a short description of each server.

Eventually, the new servers would be included on updated CD-ROM disk keys distributed to all users.

Informational, transactional, and promotional databases and services are all of ever-increasing commercial interest. Access can be controlled, verified, or tabulated by the CD-ROM key of the invention. In addition, the individual CD-ROM disks may be provided with all or portions of these databases. The portions of the databases that change infrequently might be encoded on the users' CD-ROM disks and updated when new disks are produced, whereas variable portions might typically be stored on the server.

The response speed of the user authentication system may be increased if the server or host computer being accessed begins the communication session in parallel with checking the user identification key from the user program against the database of user identification keys to authorize the user. This may be advantageous if the database of keys has a slow response time, e.g. during peak usage hours. It may also be advantageous if the server or host computer being accessed must take the time to contact another server or set of servers to check the database and obtain authorization, as discussed hereinbefore.

In such a case, it may be advantageous for the host computer being accessed to run a fast key-check algorithm to check whether the user identification key is a valid key, and whether or not it belongs to the particular user. In some applications, the server being accessed could use

this validity check and then grant a provisional or limited access, pending checking of the user identification key against the database.

In addition, in certain applications, provisional initiation of the transaction upon receipt of a valid identification by the host computer might be permitted, but the transaction is completed only when the ID is verified in the server's database. This arrangement further improves response time for the user and reduces the speed requirements on the storage means. For example, a credit card transaction could be started upon receipt of a valid ID but not completed until after the ID has been checked with the database and approved.

In one such key-check technique, the CD-ROM key of the invention may contain both unencrypted and encrypted versions of one or more identification keys. The encryption is done before or as the disk is imprinted using a key and encryption method unknown to the user and using encryption means that are ideally unknown to the user. For user authentication purposes, the host computer, which has the key, would be programmed to demand both the unencrypted version of the identification key and the encrypted version of the key. The host computer then would be programmed to decrypt the encrypted version of the key and compare it with the unencrypted version. If the two keys are the same, then the user identification key is virtually certainly a valid key. For example, if the encryption were

the inverse of a long-key public-key encryption, the public key would be held by the host computer only (and the inverse or private key would be held by the disk maker only). An intruder would have to generate a counterfeit identification with the corresponding encrypted version, which would require the inverse or private key. Obtaining the key would be virtually impossible, even if the would-be counterfeiter obtained huge numbers of different user disks. Since the server does not have the private key, even illicitly accessing the server would not allow a counterfeiter to make new counterfeit user identification keys. Accordingly, counterfeiting of valid user identification numbers cannot be done.

A further security measure includes appending the encrypted version of the identification key to the unencrypted version to form a single longer key. Alternatively, the final key may comprise two different encrypted versions of the unencrypted key. Alternatively, the final key may be a function of both the unencrypted version and of a parity, hash, encryption function, or other function of the unencrypted version.

Such key-validity-check algorithms help protect against attempts to counterfeit or simulate user disks or portable storage media; they do not protect against the use of stolen user disks or portable storage media to gain at least provisional or limited access to the server.

One method to help protect against the use of stolen user disks or portable storage media to gain at least provisional or limited access in the above system is to provide each server with a list or database of known stolen
5 keys; this database is much smaller than the complete database of user keys; it also can be checked more rapidly.

Unlike a human user, the computer does not make mistakes in entering an identification key. Accordingly, unless line disruption is indicated, the preferred software
10 implementation will disconnect the user after only one attempt using any invalid CD-ROM identification key. This allows speedy rejection of attempts by hackers or other transgressors and avoids tying up the system with their illicit attempts. By disconnecting after one attempt,
15 hackers cannot rapidly try multiple identification keys.

The host computer's database of user identification keys is well protected against attempts to steal or copy it. Nevertheless, it is advantageous to protect against attempts to steal or copy the server's database of user
20 identification keys or user access keys and thereby counterfeit or mimic the users' unique CD-ROMs. Accordingly, the server database of a preferred implementation of the invention contains an encrypted or otherwise altered version of the user identification keys. The server of the
25 invention employs a trap-door authentication algorithm to compare the user ID or access key recovered from the incoming data stream with the altered version in the

server's own database for that user's claimed identity. The trap-door authentication algorithm authenticates the user if and only if the encrypted identification key in the server's database represents the same identification key as the one embedded or encrypted in the incoming data stream. 5 The trap-door authentication algorithm is impractical to be used to recover the actual identification key from the encrypted key in the host computer's database. Since the server database does not contain the actual identification keys, and the trap-door authentication function is of no 10 help in recovering them, mere possession of the host computer's database is not sufficient to recover the identification keys. Thus, stealing or copying the host computer's database of identification keys will not allow a thief to counterfeit the users' unique CD-ROM key access 15 disks and thus will not allow the thief to access the system as a legitimate user.

One such trap door authentication algorithm is implemented as follows. When preparing the users' CD-ROMs and the database for the host computer, the users' unique 20 identification keys are encrypted with a difficult-to-decrypt long-key code. The encrypted key is copied into the host computer's database and the un-encrypted identification key is written onto the user's CD-ROM key. In use, the host computer takes the identifica- 25 tion key recovered from the incoming data stream from the user, encrypts it with the same means used to encrypt the

database, and compares the encrypted key with the database entry for that user. If the keys are identical, the user is authenticated and access is granted.

Another class of trapdoor authentication algorithms go directly from the encrypted version of the password embedded in the data stream from the user to the other encrypted version in the server's database. Accordingly, the unencrypted version of the password never exists on the server and cannot be tapped or recorded by any illicit program or virus on the server.

In a yet further embodiment, each CD-ROM key is provided with multiple databases of identification and encryption keys. The server or host computer is programmed to use or have access only to one database. The copies of the other databases on the user's CD-ROM are stored in a vault. If the host computer's identification keys were ever stolen, the host computer can simply be loaded with one of the user databases from the vault and use the new identification keys. Since the user already has the new database of his new keys on his CD-ROM, there is no need to provide a new CD-ROM to all the users, and the thief remains locked out of the host computer. In addition, if only part of the server's database is copied or stolen, then only a portion of the database need be changed and only the corresponding users' CD-ROM disks need use an alternative identification database.

In one implementation, the server then simply requests the new or different keys from the users' program rather than requesting the previously used keys; the users' programs access a different location on the users' CD-ROM keys or portable storage medium keys. If the users have individual databases or one-time pads of keys, the users' programs then access a different database on the users' CD-ROM keys or portable storage medium keys. The server might also transmit a re-authentication code to access any key or database of keys or one-time-pad of keys.

Preferably, a secure means to direct the users' computers to use a different database of identification keys on the CD-ROM is used. Any of the previously described authentication algorithms can be used for this purpose. One technique is for the server to encrypt by private key the message with a time-dependent pad. The user program on the CD-ROM then uses the public key, which is also stored on the CD-ROM, to decrypt the message, then checks that the time-dependent pad is correct and switches to an alternate user ID or identification key database. The private key and the replacement database are given to the host computer at the same time.

The host computer may be provided with multiple databases wherein a specific combination is required to access any identification keys. For example, in one embodiment, one database contains a one-time pad and the other contains the database of identification keys encrypt-

ed using the one-time pad. A thief who stole or copied only the database would be unable to recover any keys.

In corporate applications, where the user CD-ROM keys will be used only or primarily on the company's own computers, the change to another user ID can be made permanent by recording a word in a small file on the hard drive. Once the file is altered on all of the company's computers, the change is complete. This could be done at the next log-on for each user.

In yet a further implementation, the host computer can use an array of inexpensive CD-ROM drives to store the database of identification keys. Advantages of this novel CD-ROM array approach include that the cost per megabyte is comparable to or less than that of magnetic disk drives, and that a drive failure almost always leaves the recorded data intact. The CD-ROM disk can simply be changed to another drive. In addition, there is the security advantage that the written data is in permanent form.

As an occasional delay in a transaction is tolerable, magnetic tape can optionally be used as a back-up means or as a redundant storage means for use in regenerating data, or to store user keys or portions of the users' key tables or databases that are not yet needed. The storage means then comprises a fast storage means (e.g. CD-ROM disks or hard disk drives) that stores data that is apt to be needed in the near future, and a slow storage means with

larger capacity and lower cost (the magnetic tape) to store keys that are not yet needed.

The users' CD-ROM disks may also contain a network access program, encryption routines, and other data and programs of utility to the users.

The portable large storage media may contain a read-only portion and a read-write portion, typically a write-once read-many portion or a write few, read many portion. (For the case of CD-ROM disks with writable portions, see, for example, the disks illustrated and described in U.S. patents 5,287,335 and 5,206,063, the disclosure of which is incorporated by reference herein.) The read-only portion would typically contain programs or information common to many users, e.g. network access programs and/or encryption routines and/or other data or programs of utility to many users. For example, in consumer applications, the read-only portion might include catalogs, advertising, or other commercial information. The read-write portion or write-once read-many portion would typically contain the unique user access key codes and unique user encryption keys (if used) and any other information unique to the particular user.

In a CD-ROM implementation, the read-only portion of the users' disks could be imprinted quickly and economically by pressing. The individualized portion, typically a write-once, read-many portion, would then be quickly recorded on an appropriate recording CD-ROM drive. This

approach may prove advantageous in a variety of high-volume applications.

If the user's portable storage medium key according to the present invention is re-writable, the medium may be "recharged" with new keys. Examples of such media keys are semiconductor memory units or cards, rewritable CD-ROM disks, floppy disks, and the like. In one implementation, a user key comprising a portable storage medium with less capacity can be "recharged" from another user key comprising a portable storage medium of greater capacity. For example, a user's memory card key could be re-charged from that user's CD-ROM key. Alternatively, a portable storage medium key can be re-charged at a secure computer, workstation, terminal, or facility. A yet further alternative is an exchange program wherein a user's used-up portable storage medium is exchanged for a re-charged or fresh storage medium with a new supply of keys. Other methods will be readily apparent to those skilled in the art. Conventional authentication means or any of the authentication means of the invention can be used to insure that only the proper user with the proper storage key can re-charge same.

Additionally, if the portable storage medium key of the invention is also used as a credit or debit disk or unit or card or the like, it may be re-charged with additional funds or the like. In addition, transaction information could be logged onto the portable storage

medium, either as verification, or for later down-loading; e.g. if the card or portable storage medium is used with systems that do not contact the server of the secure system of the invention; e.g. systems that are not connected to a
5 network.

The present invention may also be incorporated in a portable electronic device. The portable electronic device may comprise portable storage media for storing the ultra-long identification keys and/or database of identification keys. A microprocessor and/or logic circuitry,
10 hereinafter referred to as a microprocessor, may be incorporated in the portable electronic device. For many forms of memory IC, a simple microprocessor can be fabricated on the same IC at small or negligible cost. If the portable
15 storage medium is a portable hard disk drive, the microprocessor or logic functions can typically be implemented by adding additional code or programming to the microprocessor already present in the hard disk drive; again the cost would be negligible.

The microprocessor can provide additional security functions. Additionally, it can implement any of the security functions we have discussed as being implemented by a user terminal program or user access program running on the user's terminal or PC, either to off-load these
20 functions from the user's PC and thereby improve speed or simplify the software, or to provide additional assurance
25

that these functions will be performed and not defeated, e.g. by a rogue program or virus on the user's PC.

Conversely, any of the tasks described here as being performed by the microprocessor and/or clock of a portable electronic device may be performed by the microprocessor
5 and/or clock of the remote terminal.

Additionally, the microprocessor can be programmed to "re-charge" the storage medium with new keys, per above, including the relevant security precautions. Additionally,
10 ly, the microprocessor can be programmed to log transaction information, per above, e.g. for stand-alone use in situations where the user uses the portable electronic device to conduct transactions without access to a PC. In many implementations of such portable electronic devices, the
15 microprocessor will provide additional security to prevent unauthorized individuals or software from accessing or copying or using the identification keys on the portable storage medium.

For example, the microprocessor may be programmed to
20 request a password from the user whenever the user attempts to access the identification keys on the portable storage medium. In order to access the identification keys on the portable storage media, the user must enter his or her appropriate user identification password. The user may
25 enter the password through the remote terminal or a keypad on the portable storage media.

The microprocessor may refuse access to the identification keys on the portable storage medium for a fixed period of time if several incorrect user passwords are typed in consecutively. For example, the microprocessor
5 may prevent access to the identification keys on the portable storage media for an hour when three incorrect user identification passwords are typed in consecutively.

The portable electronic device may further comprise a
10 clock. The clock could be used, for example, to time the duration for which the microprocessor refuses access to the portable storage medium, as described hereinabove. Alternatively, the duration of refusal could be timed by a software timing loop or by keeping a running sum of the
15 (known) execution times of each of the functions executed by the microprocessor. Clock circuits are inexpensive, and use little power. They can readily be powered for years by a small watch battery or the like. If the portable storage medium is a semiconductor memory, a clock
20 circuit can readily be incorporated on the same IC as the memory and microprocessor.

Additionally or alternatively, the microprocessor may disable access to the portable storage medium if multiple incorrect user passwords are typed in consecutively. For
25 example, the microprocessor may disable access when ten incorrect user passwords are typed in consecutively. Re-enabling the system might require human intervention from

the central server or provision of a special password or erasure of the contents of the portable storage medium.

5 Additionally or alternatively, the microprocessor may limit the number of passwords or one-time-pad entries accessed from the portable storage device in any pre-
specified amount of time. This would prevent rapid copying of the identification keys stored on the portable storage medium. Again, a timing function, such as a clock or a software timing loop or running sum of execution times
10 is required. For example, the microprocessor may be programmed to limit the number of identification keys or one-time-pad entries or the like accessed from the portable storage device in a given number of seconds, minutes, hours or days. Alternatively, the microprocessor could prevent
15 accessing identification keys or one-time-pad entries at a rate faster than they would be used by the user's terminal program, or could prevent accessing one-time-pad keys at a rate faster than the maximum transmission rate between the remote terminal and the host computer. Other desirable
20 rate limitations will readily be apparent to those skilled in the art.

Alternatively or additionally, the microprocessor may be programmed to output a time-dependent identification key or one-time-pad entry or the like; i.e. it may output a
25 number that depends upon the time-of-day (including date) from the clock as well as upon the contents of the portable storage device. For example, the memory location or key

accessed might depend upon the time-of-day, rather than the memory locations or keys being accessed in sequential order; i.e. the microprocessor selects the appropriate number or key from the portable storage medium based upon
5 the current time. If desired, the microprocessor may combine the entry accessed from the portable storage medium with time-of-day information. For example, the keys could be added or concatenated and the result encrypted by the microprocessor and sent from the portable electronic
10 device. Other time-dependent key techniques will readily be apparent to those skilled in the art. For any time-dependent key technique, the host computer (server) would correspondingly be programmed to expect the result to be used as an identification key or as an encryption means;
15 accordingly, the number outputted by the portable electronic device would be usable only at the time it was obtained.

The time-dependent key techniques can be used with any portable storage medium to produce keys that are only valid when produced; if the portable storage medium does
20 not have its own local microprocessor, the above algorithms or similar algorithms can be implemented on the processor in the user's terminal or PC. They can also be used on the host computer or server; with the above algorithms or similar algorithms being implemented by the server or an
25 outboard microprocessor, possibly associated with the key storage means. Accordingly, the above time-dependent key techniques can be operated in reverse to authenticate the

server to the user in addition to authenticating the user to the server.

Additionally or alternatively, the microprocessor may be programmed to access the portable storage medium only if the user terminal is running on the user's machine. For example, the microprocessor can require an access protocol or password (possibly incorporating time-of-day information).

Additionally or alternatively, the microprocessor may be programmed to access the portable storage medium only if the user terminal is accessing the host computer. For example, it might require an encrypted time-of-day function from the host computer. In addition to limiting access to the portable storage medium to legitimate requests, this authentication function would typically be made available to the user's terminal program.

There are many ways to connect peripheral devices or electronic storage media to a terminal or computer. Accordingly, an electronic portable storage medium or a portable electronic device, in accordance with the principles of the invention, may further comprise a PCMCIA interface or a serial port or a parallel port or SCSI port or "Firewire" port or infrared link or radio link or a "memory reader" or any other port or communication means capable of enabling it to pass information to and receive information from the user's terminal or computer. Preferably, for a portable electronic device or memory medium

which communicates with the remote terminal via an infrared link or radio link, the transmissions between the portable electronic device and the remote terminal are encrypted. The processor and/or logic circuitry in the portable electronic device may also optionally handle communication with the user's computer or PC.

In another embodiment, the portable electronic device may additionally record which identification keys and/or one-time-pad entries or the like have been previously accessed, hence presumably used; rather than the user's terminal program or access software performing this function. If the portable storage medium is rewritable, the identification keys, one-time-pads, and the like, may be overwritten once used. Alternatively, if the portable storage medium is writable, a usage record, table or list may be kept. Alternatively, e.g. if the portable storage medium is read-only, the portable storage device may further comprise a secondary writable portable storage medium, and a usage record, table or list may be kept there. This prevents an identification key or one-time-pad entry or the like from being used more than once.

Usage records can be alternatively kept in the server or host computer. Preferably usage records can be kept in both places and any discrepancy between usage records on the user's portable storage medium and on the server would suggest an attempt by a third party to illicitly gain access. Again, such a discrepancy might be indicated by

any attempt by either the user program or the server to re-use a one-time-pad key or one-time-pad entry that has already been used with the server or user program respectively. Such a discrepancy may also be indicated by any attempt to use a key or pad entry out-of-sequence or any other "out-of-synch episode".

Anything that suggests an attempt to gain illicit access either to the contents of the storage medium or anything that suggests an attempt to illicitly gain authorization with the server or anything that suggests a "man in the middle attack" by either counterfeiting the server to the user or the user to the server might be detected either by the portable electronic device or user program or by the server. Such suggestive incidents include those discussed above; e.g. repeated incorrect passwords typed in by the user, an attempt to access too many keys from the portable storage medium, an attempt to use a time-sensitive key at a later time, any failure to authenticate the user to the server or vice-versa, an attempt by either the alleged user or alleged server to re-use a one-time password or any other "out-of-synch" episode, and the like. Additionally, any attempt to use a known stolen user key or invalid or counterfeit user key suggests an attack, as does a usage pattern that suggests a user key may be stolen. In one implementation, if the incident is detected by the portable electronic device or the user program, either or both may be programmed to contact or otherwise to notify the server.

If the incident is detected by the server, the server may be programmed to contact the portable electronic device or user program.

Procedures for dealing with a suspected attack include but are not limited to: blocking access to the portable memory medium or portable electronic device for a set time; disabling access to the portable memory unit or portable electronic device (especially if the incident suggests that the unit or device has been stolen); blocking access by that device or unit or user to the server, either for a set time or until the situation is resolved (e.g. by the server operator); notifying the true user (e.g. by E-mail or telephone to the true user); or notifying the server operator.

In another embodiment, the portable electronic device comprises a portable storage media, a microprocessor, and a modem. The microprocessor may handle the authentication protocols with the server. Additionally, the microprocessor may handle all encryption of information transmitted by the remote terminal via the modem and all decryption of information received from the host computer by the remote terminal via the modem. Including a modem also allows the microprocessor to be programmed to allow the user to conduct stand-alone transactions via the network and without later downloading when the user does not have access to a regular terminal or PC.

There are a variety of additional techniques and embodiments of the present invention that can be implemented using a CD-ROM key or any portable storage medium key or a portable electronic device key, per above.

5 For example, in another embodiment of the present invention, the host computer (server) may request an identification key from a random location on the user's CD-ROM or portable storage medium. The remote terminal or portable electronic device would read the identification
10 key from the appropriate location in the memory medium and it would be transmitted to the host computer.

The present security system, in a most preferred embodiment, entails the use of a "double-sided" key technique comprising the use of separate entrance and exit keys
15 at the beginning and end respectively of the communication session. In this method, the remote terminal program (or portable electronic device) transmits an identification key to the host computer (server) at the beginning of the communication session, thereby authenticating itself to
20 gain access. The remote terminal (or portable electronic device) transmits a second identification key to the server at the end of the communication session; typically, this can be used to validate the session. For example, the server is programmed such that it will not process the
25 information transmitted unless both identification keys are correct; e.g. in a transaction system, the user transactions would be received by the server during the session,

but not accepted or validated or processed unless or until
a valid exit key is received at the end of the session.
Thus, the first key functions to grant provisional access;
the second key functions to provide the final authorization
5 for the transactions.

In order to authenticate the server to the user's
terminal program (or portable electronic device), the
server would transmit to the user separate entrance and
exit keys in a directly analogous manner; one would typi-
10 cally then have an exchange of identification keys between
the user program and the server at both the beginning and
the end of the communication session. Additionally, the
identification keys may be time-dependent, e.g. using the
techniques described hereinabove.

15 Authenticating the user and server to each other at
the beginning and end of the session blocks attempts to
simply "hijack" the communication session. However, it
does not block attempts to insert information into or
delete information from otherwise valid sessions. The use
20 of time-dependent identification keys imposes the further
constraint that any tampering must be done in real time,
and also blocks attempts to obtain valid entrance and exit
keys, e.g. by using "man in the middle" techniques, and use
them later. Thus authentication means to authenticate the
25 entire session, or at least authenticate critical portions
of the session, such as transaction information or transac-

tion requests should always be included for maximizing security.

To authenticate a session or the critical portions thereof, the session or critical portions thereof may be encrypted. An unbroken encryption technique will serve to authenticate the encrypted messages or information. Thus, for example, encrypting the critical portions of the session using a one-time-pad stored on the portable storage medium key and in the central server will authenticate that information

Another technique to authenticate a session or the critical portions thereof is to calculate one or more check-sums or check-functions (hereinafter called check-functions) using means whereby it is (a) difficult or impossible to counterfeit the check-functions, and (b) difficult or impossible to fabricate spurious messages with the same check-function(s) as intercepted legitimate messages.

With the double-sided key technique, such check-functions can be included in or combined with the above-discussed end-of-session key. The end-of-session key will not only authenticate the user or server but it will also authenticate the contents of the session. For example, if the check-function(s) from the user to the server include the transaction information from the user, it authenticates that transaction information; if it includes the relevant messages from the server as well, it authenticates those as

well; thus confirming that the user received the messages sent by the server. Moreover, if the check-function includes the entire session, it authenticates the entire session. If the check-function(s) include time-of-day
5 information, either for the communication session or for individual messages, it authenticates that time-of-day information as well.

It is preferable to combine the check-function(s) with the end-of-session key using a combining function that has
10 good "diffusion", so that an attacker cannot separate the check-functions from the end-of-session key and attack them separately. Note, for example, that simply adding (without carries or with) the check-function to the end-of-session key cannot be reversed by an attacker if the latter
15 is from a one-time key-pad. Other techniques include convolution or encrypting the combination of the two, using an encryption algorithm with good diffusion.

It is preferable that the combining function(s) have good "diffusion" so that it is not possible for a hacker to
20 discover that some bits involve only the password, some bits involve only the checksum(s) and some bits only involve the time-of-day information; a combining function with good diffusion helps scramble them all together. Good diffusion may be achieved by simply adding the check-sums
25 or functions to part or all of the exit signature, or convolve them or use other algorithms that mix the information. Yet another means would be to encrypt the two

together with an encryption function that has good diffusion.

There are many different ways to calculate check-functions that are difficult to counterfeit and where
5 spurious messages with given check-functions are also difficult to counterfeit, or equivalently, spurious messages with the same check-functions as an intercepted message are difficult to counterfeit. For example, one may assign different parts or characters or pieces of the
10 transmission different weights; e.g. depending on a key or random number from our portable storage medium or from the server.

There are various ways to combine a weight function with the messages or portions thereof; one way is to binary
15 add without carrying on a bit-by-bit basis; another way is to group and multiply or group and add, typically throwing away the higher-order bits. One then typically sums the results of these operations. The checksum or check function typically would either be that sum, or, preferably,
20 the lower-order digits or bits of that sum.

In addition or alternatively, one may use changing, unique, or one-time weight functions. For example, one may have a region of the user's one-time-pad (or a separate
25 pad) set aside for use as a weight function, and vary the starting point, or the order in which the entries are taken, or both from session to session. One way of doing so is to have the starting point or order or both depend

upon a number taken from a one-time-pad or provided by the server or user program or calculated from time-of-day information, etc. Since there are $N!$ orderings for a set, the same pad can (optionally) be re-used at little risk
5 (especially if only the lower-order bits of the sum are used, per above). Yet another way to calculate a check-function is to encrypt the message(s) locally, then calculate the checkfunction on the encrypted messages.

Alternatively or in addition, the checksum or check-
10 function may be combined with or include time-of-day information or (better) a function computed from time-of-day information.

The double-sided key or password technique of the invention can use keys or passwords from our portable storage medium, or from an algorithm or from a string sent
15 out by the server, or by any other means of generating passwords. For example, the double-sided keys could be implemented by a unique algorithm for each user; for example, by encrypting the time-of-day with a key unique to
20 each user.

The second password can come from the same database or circuit or algorithm as the first, or from a separate database or circuit or algorithm than the first. Note also that we can use two or more passwords, either from a single
25 portable storage medium, database, circuit or algorithm, or from two or more algorithms, or two or more circuits or ICs.

Alternatively, in lieu of a second key or password, the key or password is divided; one part is sent at the beginning of the session and the second part is sent at the end of the session.

5 The double-sided key technique conserves keys and therefore is particularly suitable for implementations of the new security system invention using semiconductor memory keys or portable electronic device keys with semiconductor memories, and for other implementations of the
10 invention using portable memory media of limited capacity.

In addition, any of the techniques to detect and foil an illicit attack, including attempts to break into the system or steal identification keys or hijack a communication session may be combined with a program to create an
15 entrapment session to keep the attacker or intruder linked or on the line to allow his call to be traced with a view to identifying or apprehending him. The entrapment session might also include programming to elicit additional
20 information from the attacker or intruder or his computer or from servers along the way.

Additionally, any of the portable storage means of the present invention, including portable electronic devices, might also comprise programming to plant a "cookie" or
25 information packet or a covert program or "identification virus" on an attacker's computer to facilitate subsequent

identification of the attacker or at least of the computer
he or she used. The cookie or covert program would be
planted upon detection of an illicit attack by any of the
means described above. Such programming may be a part of
5 any user terminal program or user access program on the
portable storage means or needed to run the portable
storage means; it may also be a part of any software
drivers needed to access same, or of any other user program
included on or with our system. (The only function of the
10 "identification virus" is detection and identification of
hackers; it is a totally benign virus. It should be
programmed to be non-executing unless queried or activated,
e.g. by a server.)

Alternatively, upon detection of an illicit attack,
15 the server will plant the cookie or covert program in the
attacker's computer, using means well-known to those
skilled in the art (conventional cookies are normally
planted by central servers and not by programming on the
user's computer) .

20 Alternatively, a service provider's computer may be
programmed to plant such a cookie or covert program upon
detection of an illicit attack; the new security program
would thus enable service providers to police their ser-
vices. The cookie would be routinely asked for or
25 searched for by other programs that link to the computer or
by Internet service providers or by the secured servers.
Similarly, the covert program would routinely be activated

or searched for or queried by other programs that link to the computer or by service providers or by the secured servers of the invention.

The covert program might also include means to capture the attacker's true identity; e.g. when the attacker uses it to access the Internet. Such an ID program could additionally search out identifying information on the hacker's system, including but not limited to: name(s), software serial numbers, hardware identifying or serial numbers, account numbers, log-on information (e.g. user names, but preferably not passwords), or any other number or character string that is unique or associated with the owner or user(s) of the computer or with the computer itself. If the covert program is successful while the attacker is linked to the server (e.g. while the attacker is tied up with a dummy session as mentioned above), it could then send the information to the server immediately.

Additionally, the covert program or identifying program or "identification virus" would typically include means to covertly access the central or host computer to permit the call to be traced, or means to send a covert E-mail to the server, along the lines "Here I am, come and get me.", or other means to contact the central or host computer.

Accordingly, the covert program would act as a "hacker homing device" or Internet dye marker, analogous to the dye markers used by banks.

Additionally, any such covert program or cookie might record specific actions taken by the attacker, particularly actions that indicate criminal intent or intent to defraud. Alternatively, it could record the entire illicit access attempt(s). In addition, to provide for the case where the hacker is using a legitimate user's machine, the system of the invention can include means to record the hacker's session, plus other sessions immediately after (e.g. in case the hacker uses the legitimate user's machine for something else; e.g. to send an E-mail.)

A particular advantage of the "identification virus" approach is that it is typically attached to an existing program and is not detectable as a separate file. Similarly, the tracer cookie of the invention might be appended to an existing cookie. Alternatively, other means to hide the covert program or cookie or the like may be used; these include but are not limited to creating one or more hidden files, masquerading as a system or application file, marking it's block on the disk as "unusable" (and reversing same when one attempts to read it) and the like. A virus might be non-executing unless queried or except under other restricted circumstances.

Additionally, such "cookies" or markers or programs could be planted in any of the intermediate servers or machines along the way; for example, this would allow the maintainers or operators of the servers to notify an

Internet service provider that the service is being attacked.

The means discussed herein for securing and controlling access to a host computer or server can also be implemented on an auxiliary or dedicated processor or computer such as a "firewall processor", or on a network processor, router, or switching system, instead of the host computer or server. An auxiliary or dedicated processor or computer eliminates the need for the host computer to perform the authentication, decreasing the processing load of the host computer.

The CD-ROM or the other portable storage medium can be used to control access to, through, or under the control of, any stored-program processor capable of directly or indirectly accessing storage capacity sufficient to hold the requisite database of user key codes. Indirect access may comprise remote access via a network or may comprise access from another processor or memory system.

It will also readily be apparent to those skilled in the art that the means described herein for providing secure access to a host computer or server or to databases or transaction processing systems implemented on same can also be used to control access to other computers, or to networks, or to databases or transaction processing systems or other programs or information functions implemented on or accessed through same. The read-write portion or write-once read-many portion would typically contain the unique

user access key codes and unique user encryption keys (when used) and any other information unique to the particular user.

5 In a CD-ROM implementation, the read-only portion of the users' disks could be imprinted quickly and economically by pressing. The individualized portion, typically a write-once, read-many portion, would then be quickly recorded on an appropriate recording CD-ROM drive. This approach may prove advantageous in a variety of high-
10 volume applications.

Although the foregoing description has been given by way of preferred embodiments, it will be understood by those skilled in the art that other forms of the invention falling within the ambit of the following claims is contemplated. Accordingly, reference should be made to the
15 following claims in determining the full scope of the invention.

We claim:

1 1. A method of providing user identification and
2 authentication using ultra long identification key codes
3 and/or ultra large databases of identification key codes in
4 a manner providing secure access from a remote computer
5 terminal to a database or server transaction program stored
6 on a host computer, comprising the steps of:

7 (a) utilizing key generation algorithms to generate
8 individual, class specific, or both user access key codes
9 which may optionally contain individual encryption keys;

10 (b) utilizing key generation algorithms to generate
11 one or more media access codes;

12 (c) creating a database or otherwise updating an
13 existing database comprising a compilation of each of said
14 individualized and class specified user access key codes
15 which have been generated for predetermined authorized
16 users of the server transaction program;

17 (d) recording, on separate individual portable
18 storage media directly compatible with and readily insert-
19 able and removable from said remote computer terminal, each
20 of said individualized and class specified user access key
21 codes, along with the optional individual encryption keys,
22 and the media access codes;

23 (e) loading or providing the server serving as the
24 host computer with a complete registry or compilation of
25 each individualized and class specified access key code and

26 any optional individual encryption keys which have been
27 generated by the key generation algorithms;

28 (f) providing each authorized user with said port-
29 able storage medium containing the authorized user's
30 individual or class specified access key code;

31 (g) providing the server with computer programming
32 including steps for comparing individual and class speci-
33 fied access key codes transmitted over telephone networks
34 or communication networks from a user's remote computer
35 terminal against the stored compilation of authorized
36 access key codes and permitting correct matches to have
37 access to said server transaction program while denying
38 access to unauthorized access key codes;

39 (h) providing users' remote computer terminals with
40 programming including the steps for comparing media access
41 codes entered by the user against media access codes stored
42 on the portable storage medium and permitting correct
43 matches to have access to the individual or class specified
44 access key codes stored on the portable storage medium;

45 (i) providing users' remote computer terminals with
46 programming to permit connection to said server through a
47 communication network or telephone network and to transmit
48 individual and class specific access key codes through said
49 remote computer terminal utilizing readers for the portable
50 storage medium to said server for the purposes of gaining
51 access to said server transaction database; and

52 (j) conducting a communications session between the
53 user's remote computer terminal and said server trans-
54 action program through said telephone or communication net-
55 work.

1 2. A method of providing user identification and
2 authentication using ultra long identification key codes
3 and/or ultra large databases of identification key codes in
4 a manner providing secure access from a remote computer
5 terminal to a database or server transaction program stored
6 on a host computer, comprising the steps of:

7 (a) utilizing key generation algorithms to generate
8 individual, class specific, or both user key codes which
9 may optionally contain individual encryption keys;

10 (b) creating a database or otherwise updating an
11 existing database comprising a compilation of each of the
12 access key codes which have been generated for predeter-
13 mined authorized users of the server transaction program;

14 (c) recording, on separate individual portable
15 storage media directly compatible with and readily insert-
16 able and removable from said remote computer terminal, each
17 of said individualized and class specified user access key
18 codes along with the optional individual encryption keys;

19 (d) loading or providing the server serving as the
20 host computer with a complete registry or compilation of
21 each individualized and class specified access key code and

22 any optional individual encryption keys which have been
23 generated by the key generation algorithms;

24 (e) providing each authorized user with said port-
25 able storage medium containing the authorized user's
26 individual or class specified access key code;

27 (f) providing the server with computer programming
28 including steps for comparing individual and class speci-
29 fied access key codes transmitted over telephone networks
30 or communication networks from a user's remote computer
31 terminal against the stored compilation of authorized
32 access key codes and permitting correct matches to have
33 access to said server transaction program while denying
34 access to unauthorized access key codes;

35 (g) providing users' remote computer terminals with
36 programming to permit connection to said server through a
37 communication network or telephone network and to repeated-
38 ly or periodically transmit individual and class specific
39 access key codes through said remote computer terminal
40 utilizing readers for the portable storage medium to said
41 server for the purposes of gaining access to said server
42 transaction database; and

43 (h) conducting a communications session between the
44 user's remote computer terminal and said server trans-
45 action program through said telephone or communication net-
46 work.

1 3. A method of providing user identification and
2 authentication using ultra long identification key codes
3 and/or ultra large databases of identification key codes in
4 a manner providing secure access from a remote computer
5 terminal to a database or server transaction program stored
6 on a host computer, comprising the steps of:

7 (a) utilizing key generation algorithms to generate
8 individual, class specific, or both user key codes which
9 may optionally contain individual encryption keys;

10 (b) creating a database or otherwise updating an
11 existing database comprising a compilation of each of the
12 access key codes which have been generated for predeter-
13 mined authorized users of the server transaction program;

14 (c) recording, on separate individual portable
15 storage media directly compatible with and readily insert-
16 able and removable from said remote computer terminal, each
17 of said individualized and class specified user access key
18 codes along with the optional individual encryption keys;

19 (d) loading or providing the server serving as the
20 host computer with a complete registry or compilation of
21 each individualized and class specified access key code,
22 the location on the portable storage media where each
23 individualized and class specified access key code is
24 stored, and any optional individual encryption keys which
25 have been generated by the key generation algorithms;

26 (e) providing each authorized user with said port-
27 able storage medium containing the authorized user's
28 individual or class specified access key code;

29 (f) providing the server with computer programming
30 including steps for

31 (i) requesting one or more individual and class
32 specified access key codes from a specific location on the
33 portable storage media, and

34 (ii) comparing individual and class specified
35 access key codes transmitted over telephone networks or
36 communication networks from a user's remote computer
37 terminal against the stored compilation of authorized
38 access key codes and permitting correct matches to have
39 access to said server transaction program while denying
40 access to unauthorized access key codes;

41 (g) providing users' remote computer terminals with
42 programming to permit connection to said server through a
43 communication network or telephone network and to transmit
44 individual and class specific access key codes through said
45 remote computer terminal utilizing readers for the portable
46 storage medium to said server for the purposes of gaining
47 access to said server transaction database;

48 (h) conducting a communications session between the
49 user's remote computer terminal and said server trans-
50 action program through said telephone or communication net-
51 work.

1 4. A method of providing user identification and
2 authentication using ultra long identification key codes
3 and/or ultra large databases of identification key codes in
4 a manner providing secure access from a remote computer
5 terminal to a database or server transaction program stored
6 on a host computer, comprising the steps of:

7 (a) utilizing key generation algorithms to generate
8 individual, class specific, or both user key codes which
9 may optionally contain individual encryption keys;

10 (b) creating a database or otherwise updating an
11 existing database comprising a compilation of each of the
12 access key codes which have been generated for predeter-
13 mined authorized users of the server transaction program;

14 (c) recording, on separate individual portable
15 storage media directly compatible with and readily insert-
16 able and removable from said remote computer terminal, each
17 of said individualized and class specified user access key
18 codes along with the optional individual encryption keys;

19 (d) loading or providing the server serving as the
20 host computer with a complete registry or compilation of
21 each individualized and class specified access key code and
22 any optional individual encryption keys which have been
23 generated by the key generation algorithms;

24 (e) providing each authorized user with said port-
25 able storage medium containing the authorized user's
26 individual or class specified access key code;

27 (f) providing the server with computer programming
28 including steps for comparing individual and class speci-
29 fied access key codes transmitted over telephone networks
30 or communication networks from a user's remote computer
31 terminal against the stored compilation of authorized
32 access key codes and permitting correct matches to have
33 access to said server transaction program while denying
34 access to unauthorized access key codes;

35 (g) providing users' remote computer terminals with
36 programming to permit connection to said server through a
37 communication network or telephone network and to transmit
38 individual and class specific access key codes through said
39 remote computer terminal utilizing readers for the portable
40 storage medium to said server for the purposes of gaining
41 access to said server transaction database;

42 (h) providing users' remote computer terminals with
43 programming to permit copying of information or one or more
44 programs from the server or the portable storage medium to
45 the remote computer terminals; and

46 (i) conducting a communications session between the
47 user's remote computer terminal and said server trans-
48 action program through said telephone or communication net-
49 work.

1 5. A method of providing user identification and
2 authentication as described in claim 2, wherein in said
3 step of providing users' remote computer with programming,

4 individual and class specific key codes are transmitted at
5 the beginning and end of the communications session.

1 6. A method of providing user identification and
2 authentication as described in claim 2, further comprising
3 the steps of:

4 (a) counting the information transmitted from
5 the remote terminal to the server according to a pre-
6 determined algorithm;

7 (b) transmitting the count to the server
8 whenever individual and class specific access key codes are
9 transmitted to the server.

1 7. A user identification authentication system
2 using ultra long identification keys and/or ultra large
3 databases of identification keys for secure remote com-
4 puter terminal access to a host computer comprising:

5 (a) a host computer having a compiled database of
6 pre-authorized user access key codes of ultra long length;

7 (b) a series of individual portable storage media
8 directly compatible with and readily insertable and remov-
9 able from said remote computer terminal, each containing

10 (i) a unique or class unique access key code
11 distributed among authorized users of a server transaction
12 program, and

13 (ii) one or more media access codes;

14 (d) a remote terminal with programing to compare
15 entered media access codes with the media access codes
16 stored on the portable storage media and to deny access to
17 the access key codes stored on the portable storage media
18 to any unauthorized media access codes but to permit access
19 to any user entering an authorized media access code;

20 (e) a server with programming to compare received
21 access key codes with stored authorized access key codes
22 and to deny access to the server transaction program to any
23 user transmitting an unauthorized key code but to permit
24 access to any user transmitting an authorized access key
25 code;

26 (f) each of said access key codes being ultra long
27 and comprising at least 20 characters or digits (requiring
28 20 or 10 bytes, respectively).

1 8. A method of providing user identification and
2 authentication using ultra long identification key codes
3 and/or ultra large databases of identification key codes in
4 a manner providing secure access from a remote computer
5 terminal to a database or server transaction program stored
6 on a host computer, comprising the steps of:

7 (a) utilizing key generation algorithms to generate
8 individual, class specific, or both user key codes which
9 may optionally contain individual encryption keys;

10 (b) creating a database or otherwise updating an
11 existing database comprising a compilation of each of the

12 access key codes which have been generated for predeter-
13 mined authorized users of the server transaction program;

14 (c) recording, on separate individual portable
15 storage media directly compatible with and readily insert-
16 able and removable from said remote computer terminal, each
17 of said individualized and class specified user access key
18 codes along with the optional individual encryption keys;

19 (d) loading or providing the server serving as the
20 host computer with a complete registry or compilation of
21 each individualized and class specified access key code and
22 any optional individual encryption keys which have been
23 generated by the key generation algorithms;

24 (e) providing each authorized user with said port-
25 able storage medium containing the authorized user's
26 individual or class specified access key code;

27 (f) providing the server with computer programming
28 including steps for comparing individual and class speci-
29 fied access key codes transmitted over telephone networks
30 or communication networks from a user's remote computer
31 terminal against the stored compilation of authorized
32 access key codes and permitting correct matches to have
33 access to said server transaction program while denying
34 access to unauthorized access key codes;

35 (g) providing users' remote computer terminals with
36 programming to permit connection to said server through a
37 communication network or telephone network and to transmit
38 individual and class specific access key codes through said

39 remote computer terminal utilizing readers for the portable
40 storage medium to said server for the purposes of gaining
41 access to said server transaction database; and

42 (h) conducting a communications session between the
43 user's remote computer terminal and said server trans-
44 action program through said telephone or communication net-
45 work.

1 9. A user identification authentication system
2 using ultra long identification keys and/or ultra large
3 databases of identification keys for secure remote com-
4 puter terminal access to a host computer comprising:

5 (a) a host computer having a compiled database of
6 pre-authorized user access key codes of ultra long length;

7 (b) a series of individual portable storage media
8 directly compatible with and readily insertable and remov-
9 able from said remote computer terminal, each containing a
10 unique or class unique access key code distributed among
11 authorized users of a server transaction program;

12 (c) a server with programming to compare received
13 access key codes with stored authorized access key codes
14 and to deny access to the server transaction program to any
15 user transmitting an unauthorized key code but to permit
16 access to any user transmitting an authorized access key
17 code;

18 (d) each of said access key codes being ultra long
19 and comprising at least 25 characters or 25 bytes.

1 10. A method of providing user identification and
2 authentication as described in claim 8, further comprising:

3 (a) an algorithm which generates one time pads;

4 (b) said one time pads are stored on a CD-ROM which
5 is said portable storage medium and said pads are loaded or
6 provided to the server; and

7 (c) the one time pads are used to encrypt the user
8 access key codes by the remote computer terminal access
9 program before being transmitted to the host computer.

1 11. The method of claim 10, further including the
2 step of:

3 (a) providing additional programming on said CD-
4 ROM.

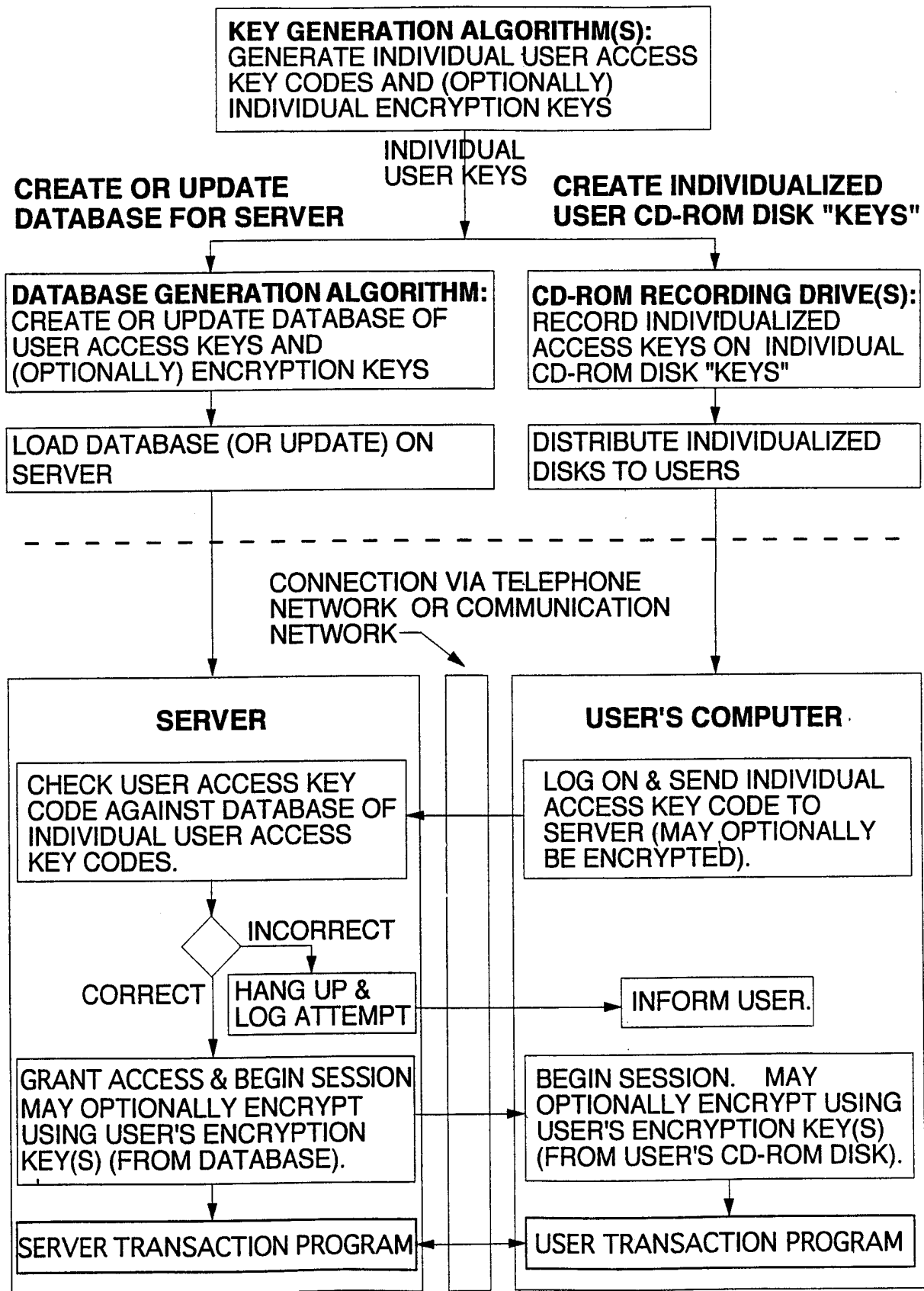


FIG. 1

2/2

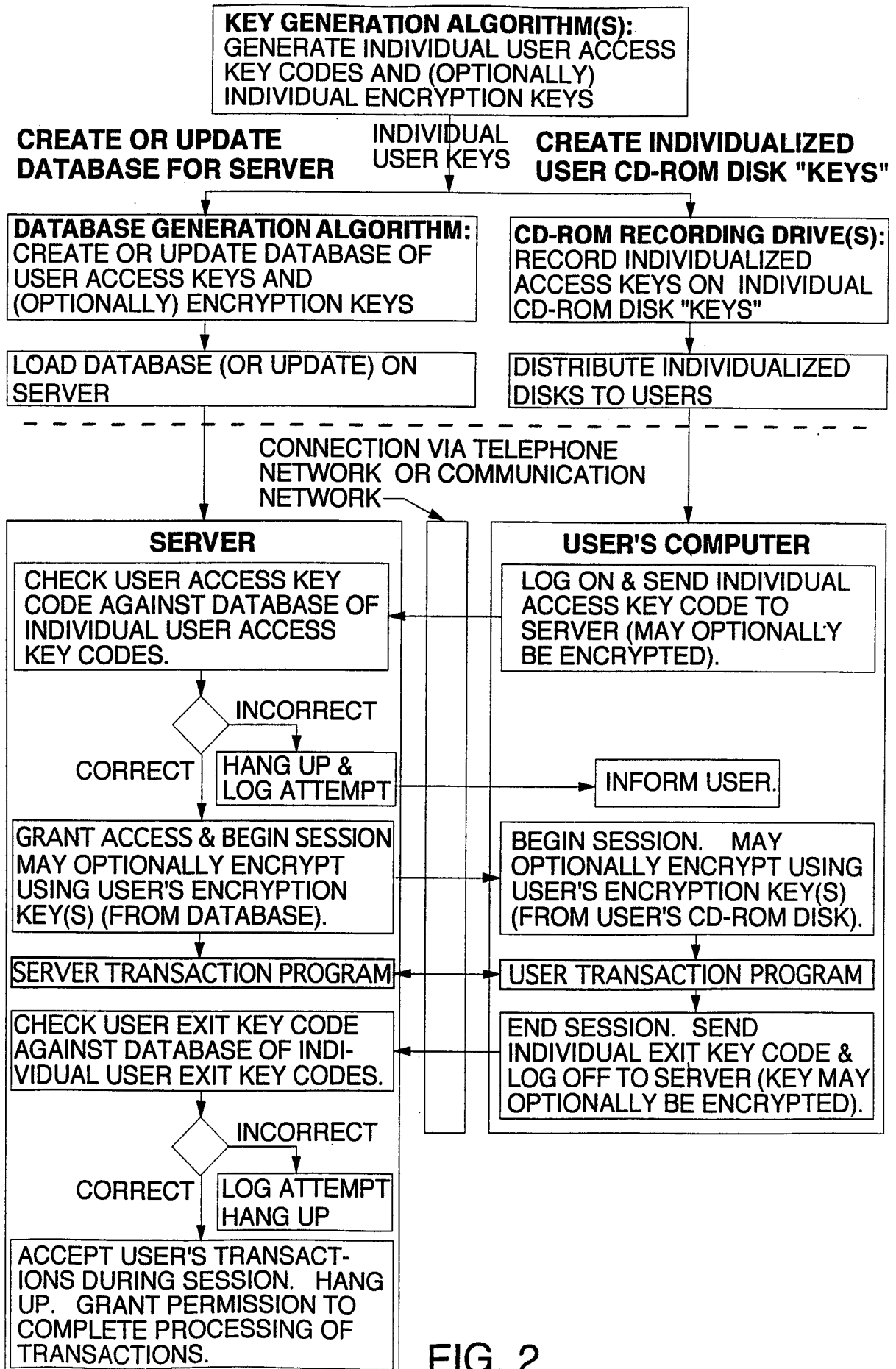



FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/10355

| A. CLASSIFICATION OF SUBJECT MATTER IPC(6) : GO6F 15/20 US CL : 380/009 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) U.S. : 380/009, 025, 003, 004, 025, 45; 395/186, 187.01; 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 practicable, search terms used) APS: TOKEN, PORTABLE MEMORY, SMART CARD, CD ROM, ENCRYPT, PASSWORD, PIN, PERSONAL IDENTIFICATION NUMBER, ACCESS CODE, TERMINAL, SERVER. | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | |
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| X ----- Y | US 5,677,953 A [DOLPHIN] 14 OCTOBER 1997, COLUMN 9, LINES 19-23, COLUMN 14 LINES 16-23, LINES 57-61, COLUMN 7, LINES 11-26, COLUMN 5, LINES 31-37, COLUMN 2, LINES 59-68, COLUMN 3, LINES 7-10 | 1,2,3,4,8 ----- 7,9-10 |
| Y | US 5,282,247 A [McLEAN] 25 JANUARY 1994, COLUMN 6, LINES 36-38 | 7,9-10 |
| A | US 5,272,754 A [BOERBERT] 21 DECEMBER 1993, COLUMN 5, LINES 40-48 | |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex. | | |
| * *A* *E* *L* *O* *P* | Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance earlier document published on or after the international filing date 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) document referring to an oral disclosure, use, exhibition or other means document published prior to the international filing date but later than the priority date claimed | *T* *X* *Y* *&* 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 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 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 30 SEPTEMBER 1998 | | Date of mailing of the international search report 02 NOV 1998 |
| Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230 | | Authorized officer GAIL HAYES  Telephone No. (703) 305-3900 |

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/10355

| C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT | | |
|---|--|-----------------------|
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| Y | US, 5,282,247 A [MCLEAN] 25 January 1994, column 6, lines 36-38 | 7,9-10 |