(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2008 (24.01.2008)

PCT

(10) International Publication Number
WO 2008/009915 A1

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/GB2007/002689

(22) International Filing Date: 17 July 2007 (17.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/831.859 18 July 2006 (18.07.2006) US

(71) Applicant *(for all designated States except US)*: **HES LTD**; P.O Box 119, Martello Court, Admiral Park, St. Peter Port GY1 3HB (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KORNBLUTH, Elaine** [GB/GB]; 15 Raleigh Close, London NW4 2SX (GB). **KORNBLUTH, Jul** [GB/GB]; 15 Raleigh Close, London NW4 2SX (GB). **KUMAR, Akiva Anthony** [IN/LV]; Vilandes Lela 16, Dz 2B, LV-1010 Riga (LV).

(74) Agent: **WHITE, Duncan**; Marks & Clerk, 90 Long Acre, London WC2E 9RA (GB).

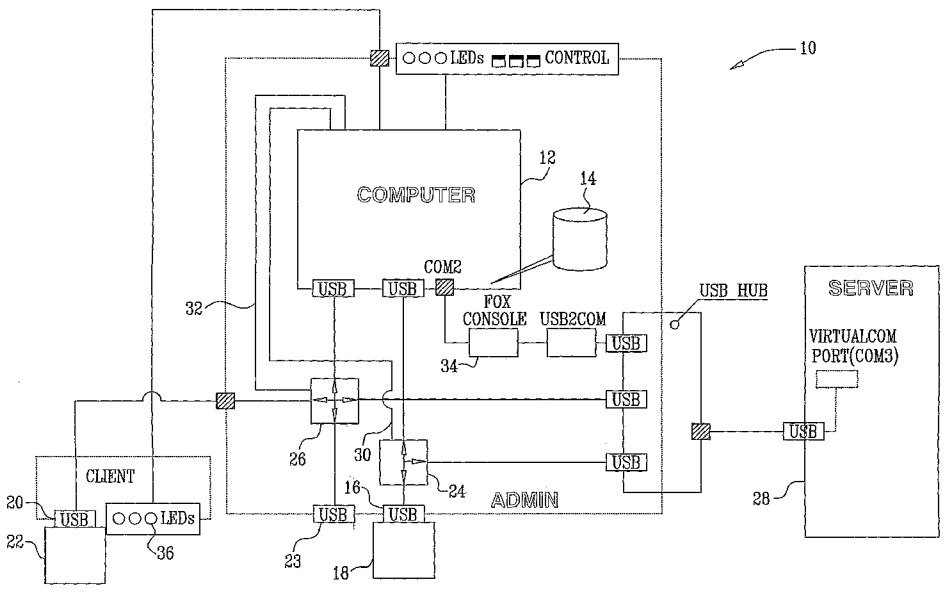
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

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

(54) Title: MEDICAL DATA PROTECTION AND TRANSMISSION SYSTEM



(57) Abstract: Methods and systems are provided for storage of medical information including a port- able user-retained storage device (22) and a portable master storage device (18), both connectable to a host computer (12). Using password protection, the host computer is cooperative with the storage devices when connected thereto to read an encryption key from the master storage device, to encrypt a medical record using an encryption algorithm and the encryption key, and to store the encrypted medical data on the user-retained storage device. The user-retained storage device can be independently connected to another computer to decrypt and display the medical data using a second password.

WO 2008/009915 A1

Medical Data Protection and Transmission System

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application 60/831,859, filed July 18, 2006, which is herein incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention.

[0002] This invention relates to data security. More particularly, this invention relates to data security for medical data.

2. Description of the Related Art.

[0003] PCT Publication No. WO2005/076191 by Willems, describes a system for storing and exchanging medical information using a plurality of portable electronic storage devices. Each storage device has an interface and one or more data carriers on which are stored medical data representative of the health of at least one individual and a computer program. The system also includes a data processing device having a second interface for connecting the data processing device to at least one of the portable electronic storage devices and a display device for displaying processed medical data.

[0004] U.S. Patent Application Publication No. 2005/0125678 by Shaw et al., describes a system for storing and reading digital identifications and permissions with an access rights management component that protects the privacy and integrity of the data stored. The use of smart cards is proposed for storage applications such as air travelers' identities, medical information such as history and prescriptions, and secure employee access cards. Multiple levels of security are permitted to ensure that users of the data, programs, and other resources stored on the card may access only that data for which they have been authorized. The use of a single card for multiple user roles may be used in conjunction with multiple access methods.

SUMMARY OF THE INVENTION

[0005] Embodiments of the present invention provide a medical information system based on a local client-to-client data transfer architecture running at a medical facility, such as a clinic or surgery, which can export a medical record of a patient, sometimes referred to herein as a "user", to a portable storage device, e.g., a flash drive, upon request. The system

includes two different portable storage devices, one for use by the medical facility and one retained in possession of the user. In some embodiments of the invention, an additional portable storage device, which provides additional security protections, is used by an issuance office.

[0006] An embodiment of the invention provides a data processing system for storage of medical information including a portable user-retained storage device, and a portable master storage device having master software stored thereon. The user-retained storage device and the master storage device are connectable to a host computer. The master software, when accessed by the host computer, causes the host computer to accept an administrative pass phrase, and to validate the administrative pass phrase. Thereafter, the host computer is operative to read an encryption key from the master storage device, to encrypt a medical record using an encryption algorithm and the encryption key to produce an encrypted medical record, and to store the encrypted medical record on the user-retained storage device.

[0007] According to a further aspect of the data processing system, the user-retained storage device has user software stored thereon, and is connectable to a user computer. The user software, when accessed by the user computer, causes the user computer to accept a user pass phrase, to derive from the user software a decryption key, to validate the user pass phrase, and thereafter to decrypt with the decryption key the encrypted medical record to thereby generate a decrypted medical record and to display the decrypted medical record.

[0008] According to one aspect of the data processing system, the host computer is operative to scan the user-retained storage device to detect unauthorized software and to inactivate the unauthorized software.

[0009] Other embodiments of the invention provide methods for carrying out the functions of the above-described data processing system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] For a better understanding of the present invention, reference is made to the detailed description of the invention, by way of example, which is to be read in conjunction with the following drawings, wherein like elements are given like reference numerals, and wherein:

[0011] Fig. 1 is a block diagram of a data processing system in which the invention may be implemented;

[0012] Fig. 2 is a block diagram of a user token shown in Fig. 1, in accordance with a disclosed embodiment of the invention;

[0013] Fig. 3 is a block diagram of a master token shown in Fig. 1, in accordance with a disclosed embodiment of the invention;

[0014] Fig. 4 is a block diagram of an exemplary office token, in accordance with a disclosed embodiment of the invention;

[0015] Fig. 5 is a flow chart illustrating a method of securely transmitting medical data to the user token of Fig. 2, in accordance with a disclosed embodiment of the invention;

[0016] Fig. 6 is a flow chart illustrating a method of displaying the data stored on the user token of Fig. 2, in accordance with a disclosed embodiment of the invention;

[0017] Fig. 7 is a flow diagram showing a procedure for changing the user pass phrase of the user token of Fig. 2, in accordance with a disclosed embodiment of the invention; and

[0018] Fig. 8 is a block diagram illustrating the use of one-time unlock keys in accordance with a disclosed embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0019] In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art, however, that the present invention may be practiced without these specific details. In other instances, well-known circuits, control logic, and the details of computer program instructions for conventional algorithms and processes have not been shown in detail in order not to obscure the present invention unnecessarily.

[0020] Software programming code, which embodies aspects of the present invention, is typically maintained in permanent storage, such as a tangible readable medium. In a client/server environment, such software programming code may be stored on a client or a server. The software programming code may be embodied on any of a variety of known media for use with a data processing system, such as a diskette, or hard drive, or CD-ROM. The code may be distributed on such media, or may be distributed to users from the memory or storage of one computer system over a network of some type to other computer systems for use by users of such other systems.

Overview

[0021] A medical record is provided to a user by a medical facility on a portable storage device, referred to herein as a "user token", in a secure manner, allowing the user to read it as necessary at different locations. The user token may be accessed using a compatible computing device, e.g., a personal computer, personal digital assistant, and the like. The location

may be insecure, e.g., an Internet Café or a computer booth at an airport or railway station. Therefore, while the information on the user token is viewable, it is also non-modifiable and non-cacheable; security provisions are provided to prevent relay of the medical record to other computer programs resident on the host device.

[0022] Additional security provisions assure that medical information on the user token can only be updated under control of a privileged user, e.g., an authorized medical caregiver, who requires access to a second portable storage device, referred to herein as a "master token", which is typically located at the medical facility. Furthermore, there are safeguards to prevent uploading of unauthorized software from the portable storage device to the medical facility's computer. The user token is authenticated and the master token is time-stamped for every update session at the medical facility to prevent or track illicit attempts to tamper with the user token.

[0023] In one aspect of the invention, medical data export functionality is separated from other programs, which may run on the medical facility's computer. The medical record of a user is typically exported as a text file and transferred to the user's portable storage device by a computer other than the medical facility's computer in a secure manner.

[0024] In some embodiments of the invention, an additional portable storage device, referred to herein as an office token, is used by a token issuance office to provide additional security protections. In other embodiments of the invention, the medical facility itself functions as the issuance office, in which case the office token is not required.

[0025] There is one office token per issuance office, one master token per medical facility, and one user token per user.

System Architecture.

[0026] Turning now to the drawings, reference is initially made to Fig. 1, which is a block diagram of an exemplary data processing system 10 in which the invention may be implemented. System 10 comprises a computer 12. Computer 12 may comprise specialized hardware, for example a Linux® embedded system based on an ETRAX™ LX100 MCM 4+16 processor with a MMU (Memory Management Unit), available from Axis Communications AB, Emdalavägen 14, SE-223 69 Lund, Sweden. Alternatively, computer 12 may comprise a general purpose computer. Computer 12 is provided with a memory 14 for storage of executables and data. Memory 14 is typically realized as a hard disk. Alternatively, com-

puter 12 may use other known types of integral or distributed memory alone or in combination with the hard disk as memory 14.

[0027] Computer 12 is provided with a port 16 for reading and writing to a master token 18, which is a storage device, described in further detail herein below. Computer 12 is further provided with a port 20 for reading and writing to a user token 22, another storage device described below. Conventional smart cards adapted to the ports 16, 20 may also be used for these tokens. An additional port 23 is provided for backup purposes. Typically, ports 16, 20, 23 are Universal Serial Bus (USB) ports, and tokens 18, 22 are USB flash drives. Alternatively, some or all of the storage devices may be removable media, e.g., high capacity floppy discs, which may be inserted into drives that are permanently plugged into ports 16, 20, 23. Alternatively the linkages between the tokens 18, 22 and the ports 16, 20, 23 may be wireless connections. In such case, the flash drives are compliant with a wireless communications protocol, e.g. WiFi, and have suitable reception and transmission facilities.

[0028] Port 16 is connected to computer 12 via a switch 24. Similarly, ports 20, 23 are connected to computer 12 via a switch 26. Switch 24 is connected to a server 28 so that, depending on the position of switch 24, port 16 may be actively linked to at least one of the computer 12 or server 28. The position of switch 24 is controlled by computer 12 using a control line 30. Switch 26 is connected to server 28 so that, depending on the position of switch 26, port 20 or port 23 may be actively connected to at least one of the computer 12 or server 28. The position of switch 26 is controlled by computer 12 using a control line 32.

[0029] Computer 12 is connected to a console 34 for text input and display of output. In Fig. 1, console 34 is shown also connected to server 28, via a USB-COMM connector. In other embodiments of the invention, computer 12 and server 28 may have separate consoles.

[0030] A number of LEDs (light emitting diodes) are connected to computer 12 to provide visual indicators of hardware and software events, including a green LED 36 to indicate that processing is complete.

[0031] Reference is now made to Fig. 2, which is a block diagram of user token 22, in accordance with a disclosed embodiment of the invention. User token 22 includes medical information about a user, and has an associated pass phrase, called the "user pass phrase", known only to the user. User token 22 comprises:

[0032] a software component 105;

[0033] a field 106 containing a random block of text;

[0034] a field 107 containing the text from field 106, encrypted using the user pass phrase;

[0035] a text file 110 containing medical data of the user, which is encrypted, as described below;

[0036] a field 120 containing a unique identifier;

[0037] a field 125 containing a private key for asymmetric encryption;

[0038] a field 130 containing a public key for asymmetric encryption;

[0039] a field 135 containing a key for symmetric encryption; and

[0040] a field 140 containing a number (typically 10) of randomly generated pass phrases.

[0041] Software component 105 comprises executable code that is invoked by a host computer, which can be the user's personal computer, when connected to token 22 (Fig 1). Typically, software component 105 comprises different modules, for example a security module for handling encryption and decryption, a viewer module for handling display of medical information and a module for interfacing with computer 12 (Fig. 1) Typically, software component 105 enables the user to view the medical information stored on the user token from locations such as a place of residence. It also enables the user to change the user pass phrase. These tasks are described in detail hereinbelow.

[0042] Field 106 contains an unencrypted block of text, which is stored, typically encrypted using the key for symmetric encryption from field 135, in field 107. This is used to verify that the user has entered the user pass phrase correctly.

[0043] Text file 110 is encrypted using a symmetric encryption algorithm (i.e., the same key, sometimes referred to as a symmetric key, is used for encryption and decryption), which can be AES (Advanced Encryption Standard) using at least a 256 bit key. The key is generated randomly each time that text file 110 is exported to user token 22. Alternatively, text file 110 may be encrypted using any encryption algorithm that can be decrypted using the user pass phrase.

[0044] The encryption key (also referred to as a master key or master AES key) used to encrypt text file 110 is itself encrypted using an asymmetric encryption algorithm (i.e., one key is used for encryption and another key is used for decryption). The result of the encryption is stored in field 135. The asymmetric encryption algorithm can be the well-known RSA algorithm, using at least 1024 bit keys, and preferably at least 4096 bit keys. The public key, used for encryption, and the private key, used for decryption, are derived from the user pass phrase.

[0045] The private key is stored, encrypted using the key for symmetric encryption from field 135 in field 125.

[0046] The public key is stored, unencrypted in field 130.

[0047] The identifier in field 120 is generated when the user token is initialized, and stays constant during further updates. It is stored unencrypted and is used in the first step of the user and token identification process.

[0048] In some embodiments of the invention, randomly generated pass phrases are stored scrambled in field 140. These are one-time card unlock keys, which become invalid following a single use. They allow the user token to be unlocked by medical staff when the user is not in a position to unlock it, or if the user's current pass phrase has been forgotten. This is accomplished during generation of the master AES key for symmetric encryption while developing new instances of the user token 22. The master AES key is encrypted 10 times, and stored as encrypted one-time unlock keys on a remote site, e.g., an office token, using an algorithm such as AES256. In one embodiment, a card unlock key consists of 10 symbols (numbers from 0-9 and Upper Case letters from A-Z). Digests of the one-time unlock keys are stored on the user token 22. In the event that a patient is unable to provide a pass phrase for the user token 22, one of the encrypted one-time unlock keys is retrieved from its remote site, using suitable authorization and authentication procedures. Reference is now made to Fig. 8, which is a block diagram illustrating the operation of encrypted one-time unlock keys in accordance with a disclosed embodiment of the invention. An encrypted one-time unlock key 802 unlocks an encrypted master AES key 807 just as would user pass phrase 812. As noted the unlock key 802 provides a new valid user pass phrase. Thus, both the user pass phrase 812 and the one-time unlock keys unlock the master AES key 807, not the data itself. Unlocked master AES key 817 is then used to decrypt a medical record 822, retrieved from encrypted storage 827 as described above. Decrypted medical data 832 can then be viewed.

Example.

[0049] Use of the one-time unlock keys is demonstrated by the following scenario. A patient, who has forgotten the pass phrase, calls a Health eCard Customer Call Center. When a patient/medical personnel wants to gain access to the patient card (user token 22, Fig. 1) and does not possess the patient's pass-phrase, a card unlock key (CUK) dialogue is invoked, and asks for a random key number e.g., CUK #4. The patient (or medical personnel) requests that particular key number from a call center operator. The call center operator follows a predeter-

mined authentication procedure to identify the caller, and then asks for the CUK number shown on the CUK dialogue, i.e., CUK #4. The call center operator then dictates the key corresponding to CUK #4 from the 10 available card unlock keys. After receiving and correctly entering the CUK, the card holder is prompted to choose and confirm a new pass-phrase. There are only three attempts allowed to enter the correct CUK, which is compared with the pre-stored digests. The new pass phrase gives the holder complete access to the medical data on the card. The CUK #4 used to unlock the card cannot be used again and will be deleted from the office card for that patient. Since the unlock keys are valid for a single use only, knowledge of a CUK by an outsider does not result in immediate access to patient data.

[0050] Other techniques that may be used for implementing one-time unlock keys are known, for example, from U.S. Patent Application Publication No. 20020040438, entitled "Method to Securely Load and Manage Multiple Applications on a Conventional File System Smart Card".

[0051] In some embodiments of the invention, at least a portion of memory space on user token 22 is pre-reserved for use by software component 105, shown as memory 108. Memory 108 is pre-reserved, e.g., by write-protection to prevent installation of unauthorized data or programs. The pre-reserved memory 108 can only be written to by specific host applications, and then only when authorized by the medical facility, for example using an office token or master token 18.

[0052] In a current embodiment, memory reservation is accomplished by establishing a single file that occupies the entire memory space of a patient card (user token 22, Fig. 1). This file encapsulates the directory structure currently in use. This is similar to known compound document technology, e.g., COM/OLE, available from the Microsoft Corporation, Redmond, Washington. In other words, a single file is used to emulate a file system.

[0053] Reference is now made to Fig. 3, which is a data diagram of master token 18, in accordance with a disclosed embodiment of the invention. Master token 18 includes information about all the patients registered at a medical facility, and has an associated pass phrase, called the "administrative pass phrase", known to an administrator of the medical facility, and another associated pass phrase, called the "master pass phrase", known to a higher level supervisor of the administrator. Master token 18 comprises:

[0054] a software component 205;

[0055] a field 206 containing a random block of text;

[0056] a field 207 containing the text from field 206, encrypted as described below;

[0057] a field 208 containing a key for symmetric encryption;

[0058] a field 210 containing an unencrypted name of master token 18;

[0059] records 215 (one for each user registered with this medical facility), described below;

[0060] a field 218 containing the key for symmetric encryption from field 208, encrypted using the master pass phrase; and

[0061] a field 219 containing a public key.

[0062] Software component 205 comprises executable code that is invoked by a host computer, typically server 28 (Fig. 1), when connected to master token 18. Typically, software component 205 comprises different modules, for example a security module for handling encryption and decryption, a viewer module for viewing and modifying records 215, a parsing and pre-processing module for conversion of data into a XML format, and a module for interfacing with computer 12. Typically, software component 205 enables the administrator to update text file 110 (Fig. 2) with medical report data, or to browse or modify records 215. Software component 205 also enables the supervisor (but not the administrator) to change the administrative pass phrase. This prevents a disgruntled employee from locking master token 18 with a new pass phrase. These tasks are described in detail hereinbelow.

[0063] Field 206 contains an unencrypted block of text, which is stored, encrypted using the key for symmetric encryption from field 208, in field 207. This is used to verify that the administrator has entered the administrative pass phrase correctly.

[0064] The encryption key used to encrypt field 207 and records 215 is itself encrypted using an asymmetric encryption algorithm and stored as a data string in field 208. The asymmetric encryption algorithm can be the RSA algorithm, as described above. The public key, used for encryption, and the private key, used for decryption, are derived from the administrative pass phrase.

[0065] The encryption key used to encrypt field 207 and records 215 is additionally encrypted using an asymmetric encryption algorithm and stored as a data string in field 218. The asymmetric encryption algorithm can be the RSA algorithm, as described above. The public key, used for encryption, and the private key, used for decryption, are derived from the master pass phrase.

[0066] The name contained in field 210 need not be unique. Field 210 can store one or more descriptors that are meaningful to the user, e.g., a GP (General Practitioner), medical facility. Field 210 is provided for identification purposes only.

[0067] The public key stored in field 219 is used to verify the validity of a new token digitally signed by an office.

[0068] Field 207 and records 215 are encrypted using a symmetric encryption algorithm, typically the same algorithm as is used to encrypt text file 110 (Fig. 2). The key for symmetric encryption is itself encrypted and stored in fields 208, 218, as described above. Each of records 215 comprises:

[0069] a field 220, containing the unique identity stored in field 120 (Fig. 2) of user token 22 (Fig. 2) for the user;

[0070] a field 225, containing verifiable identification data, e.g., social security number, of the user;

[0071] a field 230 containing the user's name;

[0072] a field 235 containing the user's address;

[0073] a field 240 containing the user's date of birth;

[0074] a field 245 containing optional comments about the user;

[0075] a field 250 containing the user's MIS (Medical Information System) number, a unique patient number in a medical system registry, entered by medical facility personnel when the patient registers for the first time;

[0076] a field 255 containing a time stamp of the last time that a medical record was exported to user token 22;

[0077] A field 257 containing a time stamp of when the user first registered at the medical facility;

[0078] a field 260 containing the public key stored in field 130 (Fig. 2); and

[0079] a field 265 containing a checksum (typically using the SHA1 hashing algorithm) of the medical data exported to user token 22 (Fig. 2). The checksum is used to verify data integrity the next time that the user's medical record is downloaded from the medical facility.

[0080] In some embodiments of the invention, all of the memory space on master token 18 is pre-reserved for use by software component 205. This prevents users storing stray files on master token 18, which may contain malicious software designed to infect medical facility computers or other host computers.

[0081] Reference is now made to Fig. 4, which is a data diagram of an office token 302, in accordance with a disclosed embodiment of the invention. Office token 302, like the tokens 18, 22 (Fig. 1), is realized as a portable storage device, such as a flash drive,

adapted to plug into a port of a host device, e.g., a USB port. The office token 302 includes a database containing information about all instances of the master token 18 issued throughout a medical care system, and has an associated pass phrase, called the "office pass phrase", known to a clerk at the office. Office token 302 comprises:

[0082] a software component 305;

[0083] a field 306 containing a random block of text;

[0084] a field 307 containing the text from field 306, encrypted using the office pass phrase;

[0085] a field 308 containing a key for symmetric-encryption;

[0086] a field 310 containing an unencrypted name of office token 302; and

[0087] records 315 (one for each medical facility registered with the office), described below.

[0088] Software component 305 comprises executable code that is invoked by a host computer when connected to a storage device, on which office token 302 is stored. Typically, software component 305 comprises different modules, for example a security module for handling encryption and decryption, and a viewer module for viewing and modifying records 315. Typically, software component 305 enables the clerk to change the office pass phrase. It also enables the clerk to browse or modify records 315.

[0089] Field 306 contains an unencrypted block of text, which is stored, encrypted using the key for symmetric encryption from field 308, in field 307. This is used to verify that the clerk has entered the office pass phrase correctly.

[0090] The encryption key used to encrypt field 307 and records 315 is itself encrypted using an asymmetric encryption algorithm and stored as a data string in field 308. The asymmetric encryption algorithm can be the well-known RSA algorithm, using at least 1024 bit keys, and preferably at least 4096 bit keys. The public key, used for encryption, and the private key, used for decryption, are derived from the office pass phrase.

[0091] The name contained in field 310 may or may not be unique, and could identify the organization. Field 310 is provided for identification purposes only.

[0092] Field 307 and records 315 are encrypted using a symmetric encryption algorithm, typically the same algorithm as is used to encrypt text file 110 (Fig. 2). The key for symmetric encryption is itself encrypted and stored in field 308 as described above. Each of records 315 comprises:

[0093] a field 320, containing a unique identity of the medical facility;

[0094] a field 325 containing the public key stored in field 219 (Fig. 3);

[0095] a field 330 containing a private key;

[0096] a field 335 containing the master pass phrase stored in field 217 (Fig. 3);

[0097] a field 340 containing a name of the medical facility;

[0098] a field 345 containing an address of the medical facility;

[0099] a field 350 containing optional additional details of the medical facility;

[0100] a field 355 containing a name of the GP; and

[0101] a field 360 containing optional additional details of the GP.

[0102] The private key stored in field 330 is used to digitally sign user token 22 when it is issued.

[0103] Using the office token 302, it is possible to issue or recall instances of the master token 18.

[0104] In some embodiments of the invention, all of the memory space on office token 302 is pre-reserved for use by software component 305, indicated as memory 304. This prevents users storing stray files on office token 302, which may contain malicious software designed to infect medical facility computers or other host computers.

Operation.

[0105] Reference is now made to Fig. 5, which is a flow chart of a method of securely transmitting medical data to user token 22, in accordance with a disclosed embodiment of the invention. The steps of the method are shown in an exemplary sequence in Fig. 5 for clarity of presentation. However, it will be evident to those skilled in the art that many of them can be performed in parallel, asynchronously, or in different orders. The method begins at initial step 410. There is an active connection between computer 12 (Fig. 1) and port 16 (Fig. 1).

[0106] Next, at step 415, an administrator at the medical facility inserts master token 18 (Fig. 1) into port 16 (Fig. 1). Computer 12 mounts file system information stored on master token 18.

[0107] Next, at decision step 420, computer 12 (Fig. 1) determines whether master token 18 is genuine, by calculating a checksum of software component 205 and comparing this with a value known to computer 12. A suitable checksum for this purpose is the well-known MD5 (Message Digest Algorithm 5).

[0108] If the determination at decision step 420 is negative, control proceeds to final step 425. Typically, computer 12 generates an audible or visible alert, and port 20 (Fig. 1) may be powered off.

[0109] If the determination at decision step 420 is affirmative, control proceeds to decision step 430. It is determined whether unauthorized software other than software component 205 (Fig. 3) are found on master token 18 (Fig. 3). If the determination at decision step 430 is negative, control proceeds to step 435 described below.

[0110] If the determination at decision step 430 is affirmative, control proceeds to step 440. Computer 12 inactivates the unauthorized software, typically by renaming or deleting it.

[0111] In some embodiments of the invention, at least a portion of the memory space on master token 18 is pre-reserved for use by software component 205, shown as optional memory segment 209. This prevents the storage of unauthorized software on master token 18. For these embodiments, decision step 430 and step 440 are omitted.

[0112] Next, at step 435, the user inserts user token 22 (Fig. 1) into port 20. In some embodiments, the user pass phrase (or a one-time unlock key) is applied to the user token 22.

[0113] Next, at decision step 445, computer 12 (Fig. 1) determines whether user token 22 is genuine, by calculating a checksum, of software component 105 and comparing this with a value known to computer 12. A suitable checksum for this purpose is the above-noted MD5.

[0114] If the determination at decision step 445 is negative, control proceeds to final step 425, as described above.

[0115] If the determination at decision step 445 is affirmative, control proceeds to decision step 450. It is determined whether unauthorized software other than software component 105 (Fig. 2) are found on user token 22 (Fig. 2). If the determination at decision step 450 is negative, control proceeds to step 455 described below.

[0116] If the determination at decision step 450 is affirmative, control proceeds to step 460. In embodiments not employing reliably reserved memory, computer 12 inactivates the unauthorized software, typically by renaming or deleting it.

[0117] In some embodiments of the invention, all of the memory space on user token 22 is pre-reserved for use by software component 205. This prevents the storage of unauthorized software on user token 22. For these embodiments, decision step 450 and step 460 may be omitted.

[0118] Control now proceeds to step 455. Referring again to Fig. 1, computer 12 uses control line 32 to adjust switch 26, in order to connect user token 22 to server 28.

[0119] Referring again to Fig. 5, control now proceeds to step 465, where the administrator at the medical facility enters the administrative pass phrase at console 34.

[0120] Next, at decision step 470, it is determined whether the pass phrase is valid. This is done by first deriving from the pass phrase a private key, which is then used to decrypt the encrypted key for symmetric encryption stored in field 208 (Fig. 3), to produce a key for symmetric encryption, which is then used to encrypt the text block stored in field 206 (Fig. 3), and finally comparing the result with the encrypted text in field 207 (Fig. 3).

[0121] If the determination at decision step 470 is negative, control proceeds to final step 475. Typically, computer 12 generates an audible or visible alert and port 16 (Fig. 1) may be powered off.

[0122] If the determination at decision step 470 is affirmative, control proceeds to step 480. Referring again to Fig. 1, computer 12 uses control line 30 to adjust switch 24, in order to connect master token 18 to server 28.

[0123] Referring again to Fig. 5, control proceeds to decision step 485, where it is determined whether user token 22 is valid, using a RSA digital handshake. If the determination at decision step 485 is negative, then control proceeds to final step 425, described above.

[0124] If the determination at decision step 485 is affirmative, then control proceeds to step 490. Server 28 (Fig. 1) generates a random key for symmetric encryption. This key is encrypted using the user's public encryption key, stored in field 260 (Fig. 3). The resulting data string is copied to field 135 (Fig. 2) on user token 22. The user's medical record is encrypted using the key for symmetric encryption to produce another data string, which is stored in text file 110 (Fig. 2). A checksum of the medical record is stored in field 265 (Fig. 3) and the current data and time are stored in field 255 (Fig. 3).

[0125] Control now proceeds to final step 495. Server 28 sends a message to computer 12. Typically, computer 12 may emit an audible alert and green LED 36 flashes to signal the completion.

[0126] Reference is now made to Fig. 6, which is a flow chart illustrating a method of displaying the data stored on user token 22 (Fig. 2), in accordance with a disclosed embodiment of the invention. At initial step 560, the user inserts user token 22 into a suitable port on a general purpose computer, for example a personal computer. The general purpose computer mounts file system information stored on user token 22.

[0127] Next, at step 565, the user enters the user pass phrase (or a one-time unlock key) at the general purpose computer's terminal.

[0128] Next, at step 568, the pass phrase entered at step 565 is used to derive a private key. This private key is then used to decrypt the encrypted key for symmetric encryption stored in field 135 (Fig. 2), to produce a key for symmetric encryption.

[0129] Control passes to decision step 570, where it is determined whether the pass phrase entered is valid. This is done by encrypting the text block stored in field 106, using the key for symmetric encryption obtained at step 568, and comparing the result with the encrypted text in field 107. If the determination at decision step 570 is negative, then control proceeds to final step 575 and the method ends.

[0130] If the determination at decision step 570 is affirmative, then control proceeds to step 585. The encrypted text stored in text file 110 is decrypted using the key for symmetric encryption obtained at step 568, to produce the medical record.

[0131] The medical record is displayed at final step 590.

[0132] Reference is now made to Fig. 7, which is a flow diagram showing a procedure for changing the user pass phrase of user token 22 (Fig. 2), in accordance with a disclosed embodiment of the invention. The procedure may be executed using software component 105 (Fig. 2).

[0133] At initial step 610, the user connects token 22 to a suitable computing device, for example a personal computer.

[0134] Next, at step 615, the user types in the current user pass phrase.

[0135] Next, at step 618, the pass phrase entered at step 615 is used to derive a private key, which is then used to decrypt the encrypted key for symmetric encryption stored in field 135 (Fig. 2), to produce a key for symmetric encryption.

[0136] Control now proceeds to decision step 620, where it is determined if the pass phrase entered is valid. This is done by encrypting the text block stored in field 106, using the key for symmetric encryption obtained at step 618, and comparing the result with the encrypted text in field 107.

[0137] If the determination at decision step 620 is affirmative, then control proceeds to step 625, described below.

[0138] If the determination at decision step 620 is negative, then control proceeds to decision step 630, where it is determined if a threshold of allowable pass phrase errors has been exceeded. In some embodiments, the threshold is zero, i.e., the determination is always

affirmative. In other embodiments, there is no threshold and the determination is always negative.

[0139] If the determination at decision step 630 is affirmative, then control proceeds to final step 635, and the procedure ends.

[0140] If the determination at decision step 630 is affirmative, then control returns to step 615.

[0141] Step 625 is performed if the determination at decision step 620 is affirmative. The user enters a new user pass phrase.

[0142] Next, at step 640, the user enters a new user pass phrase.

[0143] Control passes to decision step 645, where it is determined if the pass phrases entered at step 625 and step 640 are identical. If the determination at decision step 645 is negative, then control returns to step 625.

[0144] If the determination at decision step 645 is affirmative, then control proceeds to final step 655. The new user pass phrase is used to derive a new public key and a new private key. The new private key is stored, encrypted using the key for symmetric encryption obtained at step 618, in field 125. The new public key is stored in field 130. The key for symmetric encryption derived at step 618 is encrypted using the new public key and stored in field 135. Upon completion of final step 655, the private key remains unchanged, and a new AES key has been generated, based on changes in the pass phrase.

[0145] The procedure described above, with modifications as described below, is also used as part of software component 205 (Fig. 3) for changing the administrative pass phrase. In this case, the actions are performed by the supervisor at the medical facility.

[0146] At initial step 610, the computing device is typically server 28 (Fig. 1).

[0147] At step 615, the supervisor types in the current master pass phrase.

[0148] At step 618, the pass phrase entered at step 615 is used to derive a private key, which is then used to decrypt the encrypted key for symmetric encryption stored in field 218 (Fig. 3), to produce a key for symmetric encryption.

[0149] At decision step 620, it is determined if the pass phrase entered is valid by encrypting the text block stored in field 206 (Fig. 3), using the key for symmetric encryption obtained at step 618, and comparing the result with the encrypted text in field 207 (Fig. 3).

[0150] At step 625 the supervisor enters a new administrative pass phrase.

[0151] At step 640, the supervisor re-enters a new administrative pass phrase.

[0152] At final step 655, a new private key is derived from the new administrative pass phrase, and is used to encrypt the key for symmetric encryption derived at step 618, the result of which is stored in field 208 (Fig. 3).

[0153] The procedure described above, with modifications as described below, is also used by software component 305 (Fig. 4) for changing the office pass phrase. In this case, the actions are typically performed by a clerk at the office.

[0154] At step 615, the clerk types in the current office pass phrase.

[0155] At step 618, the pass phrase entered at step 615 is used to derive a private key, which is then used to decrypt the encrypted key for symmetric encryption stored in field 308 (Fig. 4), to produce a key for symmetric encryption.**[0156]** At decision step 620, it is determined if the pass phrase entered is valid by encrypting the text block stored in field 306 (Fig. 4), using the key for symmetric encryption obtained at step 618, and comparing the result with the encrypted text in field 307 (Fig. 4).

[0157] At step 625 the clerk enters a new office pass phrase.

[0158] At step 640, the clerk re-enters a new office pass phrase.

[0159] At final step 655, a new private key is derived from the new office pass phrase, and is used to encrypt the key for symmetric encryption derived at step 618, the result of which is stored in field 308 (Fig. 4).

[0160] It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof that are not in the prior art, which would occur to persons skilled in the art upon reading the foregoing description.

Claims:

1. A data processing system for storage of medical information comprising:

a portable user-retained storage device; and

a portable master storage device having master software stored thereon, said user-retained storage device and said master storage device being connectable to a host computer, wherein said master software, when accessed by said host computer, causes said host computer to accept an administrative pass phrase, to validate said administrative pass phrase, thereafter read an encryption key from said master storage device, to encrypt a medical record using an encryption algorithm and said encryption key to produce an encrypted medical record, and to store said encrypted medical record on said user-retained storage device.

2. The data processing system according to claim 1, wherein said user-retained storage device has user software stored and is connectable to a user computer, wherein said user software, when accessed by said user computer, causes said user computer to accept a user pass phrase, to derive from said user software a decryption key, to validate said user pass phrase, and thereafter to decrypt with said decryption key said encrypted medical record to thereby generate a decrypted medical record and to display said decrypted medical record.

3. The data processing system according to claim 2, wherein said encrypted medical record comprises first data and second data, said first data having medical information encrypted therein, and said second data comprising an encrypted symmetric key, and wherein said user computer is operative to decrypt said encrypted symmetric key using said decryption key and an asymmetric decryption algorithm to generate a decrypted symmetric key, and said user computer is operative to use said decrypted symmetric key and a symmetric decryption algorithm to decrypt said first data, thereby generating said decrypted medical record from said first data.

4. The data processing system according to claim 1, 2, or 3, wherein said user-retained storage device stores a plurality of one-time unlock keys that are accessible by a third party, each of said one-time unlock keys being valid only for a single use thereof.

5. The data processing system according to any one preceding claim, wherein said user-retained storage device comprises a reserved memory.

6. The data processing system according to any one preceding claim, wherein said encryption algorithm comprises a symmetric algorithm and an asymmetric algorithm, and said encryption key comprises a symmetric key and an asymmetric key and said host computer is operative to encrypt said medical record using said symmetric algorithm and said symmetric key to produce first data, to encrypt said symmetric key using said asymmetric algorithm to produce second data, and to combine said first data and said second data to produce said encrypted medical record.

7. The data processing system according to claim 6, wherein said symmetric algorithm comprises an AES (Advanced Encryption Standard) algorithm with a key length of at least 256 bits.

8. The data processing system according to claim 6 or 7, wherein said asymmetric algorithm comprises a RSA algorithm with a key length of at least 1024 bits.

9. The data processing system according to any one preceding claim, wherein said host computer is further operative to store a checksum of said encrypted medical record on said master storage device.

10. The data processing system according to any one preceding claim, wherein said host computer is operative to scan said user-retained storage device to detect unauthorized software and to inactivate said unauthorized software.

11. A data processing system for storage of medical information comprising:

a host computer;

a portable user-retained storage device; and

a portable master storage device having master software stored thereon, said user-retained storage device and said master storage device, wherein said master software, when accessed by said host computer causes said host computer to accept an administrative pass phrase, to validate said administrative pass phrase, thereafter to read an encryption key from said master storage device, to encrypt a medical record using an encryption algorithm and said encryption key to produce an encrypted medical record, and to store said encrypted medical record on said user-retained storage device.

12. The data processing system according to claim 11, wherein said user-retained storage device has user software stored and is connectable to a user computer, wherein said user software, when accessed by said user computer, causes said user computer to accept a user pass phrase, to validate said user pass phrase, to derive from said user software a decryption key, and thereafter to decrypt with said decryption key said encrypted medical record to thereby generate a decrypted medical record and to display said decrypted medical record.

13. The data processing system according to claim 11 or 12, wherein said host computer is operative to scan said user-retained storage device to detect unauthorized software and to inactivate said unauthorized software.

14. The data processing system according to claim 11, 12 or 13, further comprising a user switch and a master switch linked to an external server on which said medical record is stored, said host computer controlling said user switch and said master switch to connect said user-retained storage device to said server via said user switch and to connect said master storage device via said master switch.

15. The data processing system according to any one of claims 11 to 14, further comprising a portable office storage device connectable to said host computer having a database of a plurality of master storage devices stored therein.

16. A method for securely transmitting medical information comprising the steps of:

providing a portable user-retained storage device and a portable master storage device;

connecting said user-retained storage device and said master storage device to a host computer;

accepting and validating an administrative pass phrase;

thereafter reading an encryption key from said master storage device using said host computer;

encrypting a medical record on said host computer using an encryption algorithm and said encryption key to produce encrypted medical data; and

storing said encrypted medical data on said user-retained storage device.

17. The method according to claim 16, wherein said user-retained storage device stores a plurality of one-time unlock keys that are accessible by a third party, each of said one-time unlock keys being valid only for a single use thereof.

18. The method according to claim 16 or 17, further comprising the steps of:

connecting said user-retained storage device to a user computer,

accepting in said user computer a user pass phrase;

deriving from said user pass phrase a decryption key;

validating in said user computer said user pass phrase;

decrypting using said decryption key said encrypted medical data to thereby generate decrypted medical data; and

displaying said decrypted medical data.

19. The method according to claim 18, wherein said encrypted medical data comprises first data and second data, said first data having medical information encrypted therein, and said second data comprises an encrypted symmetric key, further comprising the steps of using said user computer to decrypt said encrypted symmetric key using said decryption key and an asymmetric decryption algorithm to generate a decrypted symmetric key, and with said decrypted symmetric key and a symmetric decryption algorithm to decrypt said first data, thereby generating said decrypted medical data from said first data.

20. The method according to any one of claims 16 to 19, wherein said encryption algorithm comprises a symmetric algorithm and an asymmetric algorithm, and said encryption key comprises a symmetric key and an asymmetric key and said step of encrypting a medical record comprises using said symmetric algorithm and said symmetric key to produce first data, to encrypt said symmetric key using said asymmetric algorithm to produce second data, and to combine said first data and said second data to produce said encrypted medical data.

FIG. 1

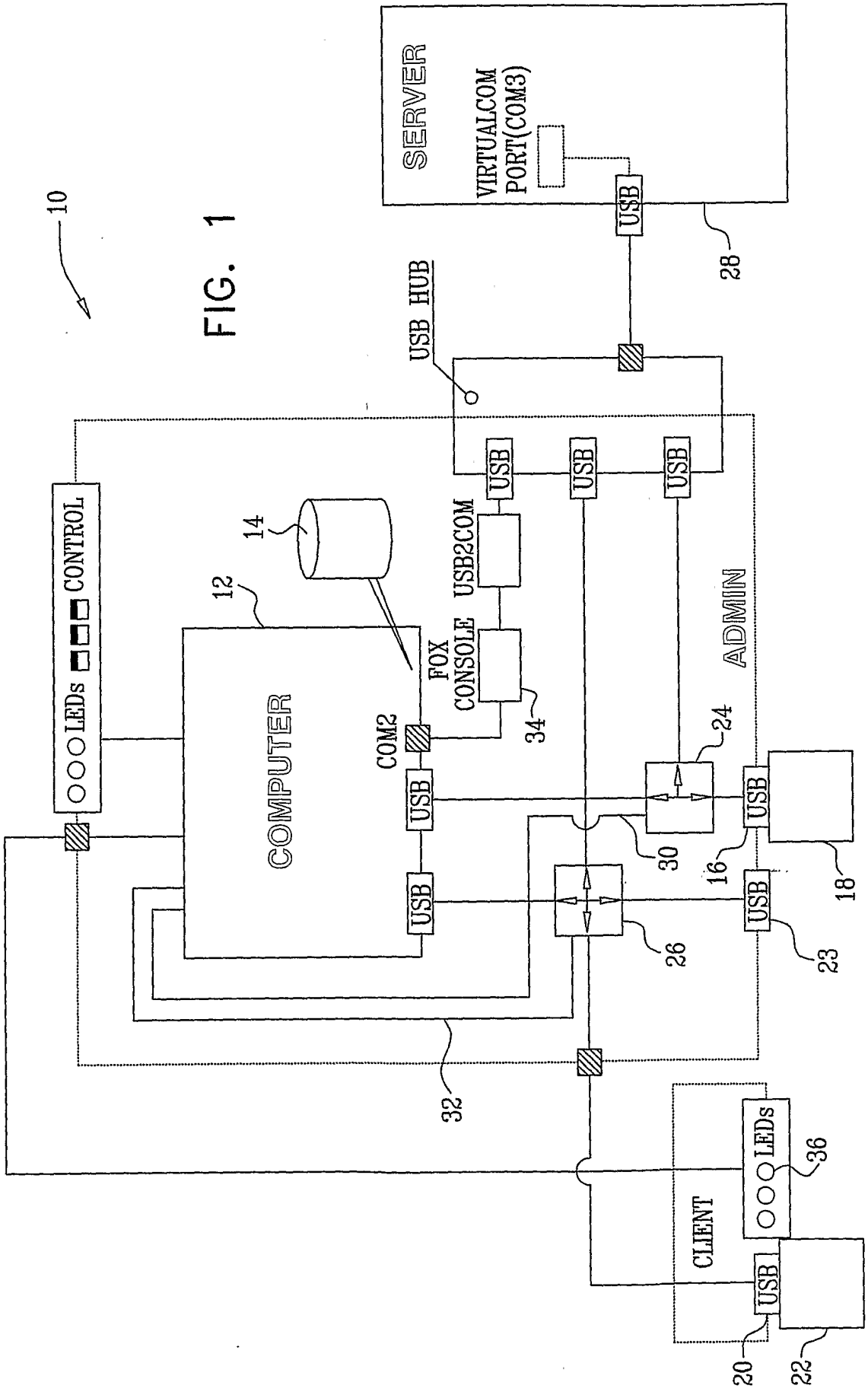

10
SERVER
VIRTUALCOM PORT(COM3)
USB
28
USB HUB
USB
USB
USB
USB2COM
FOX CONSOLE
34
14
12
COMPUTER
COM2
USB
USB
CONTROL
LEDs
24
30
16
18
ADMIN
USB
USB
26
23
32
CLIENT
LEDs
36
USB
20
22

FIG. 2

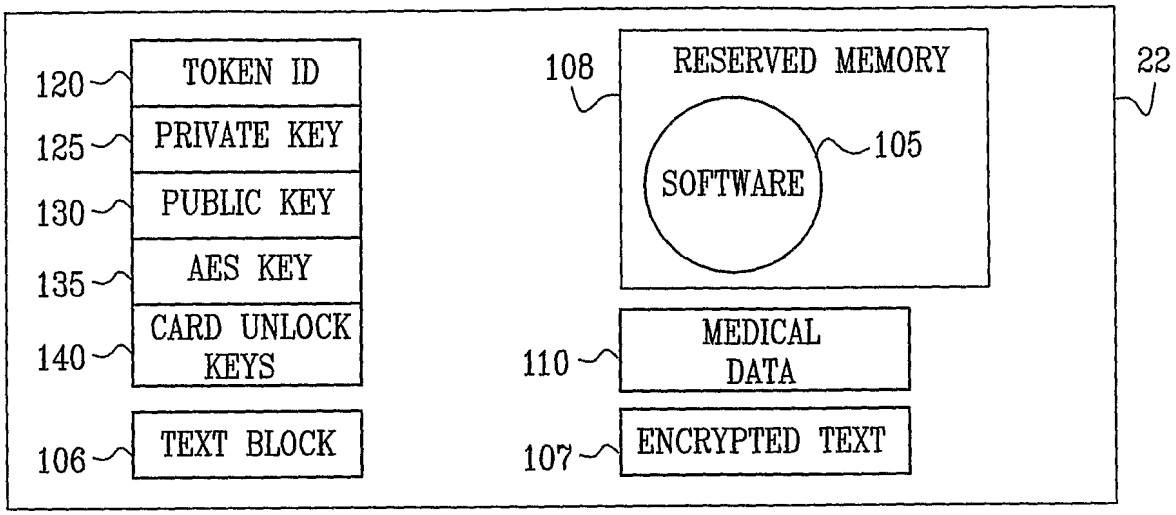

120
TOKEN ID
125
PRIVATE KEY
130
PUBLIC KEY
135
AES KEY
140
CARD UNLOCK KEYS
106
TEXT BLOCK
108
RESERVED MEMORY
SOFTWARE
105
22
110
MEDICAL DATA
107
ENCRYPTED TEXT

FIG. 3

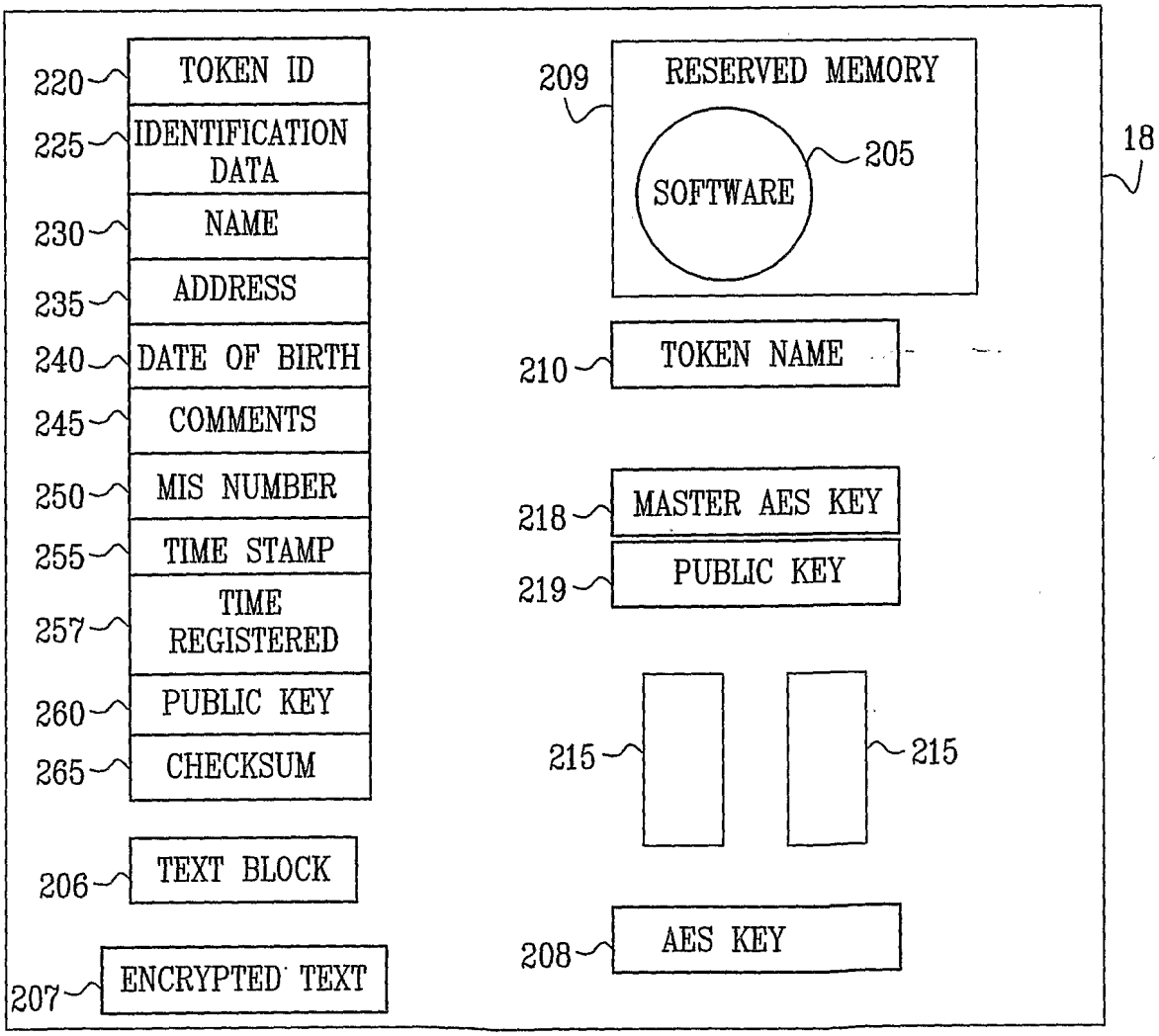
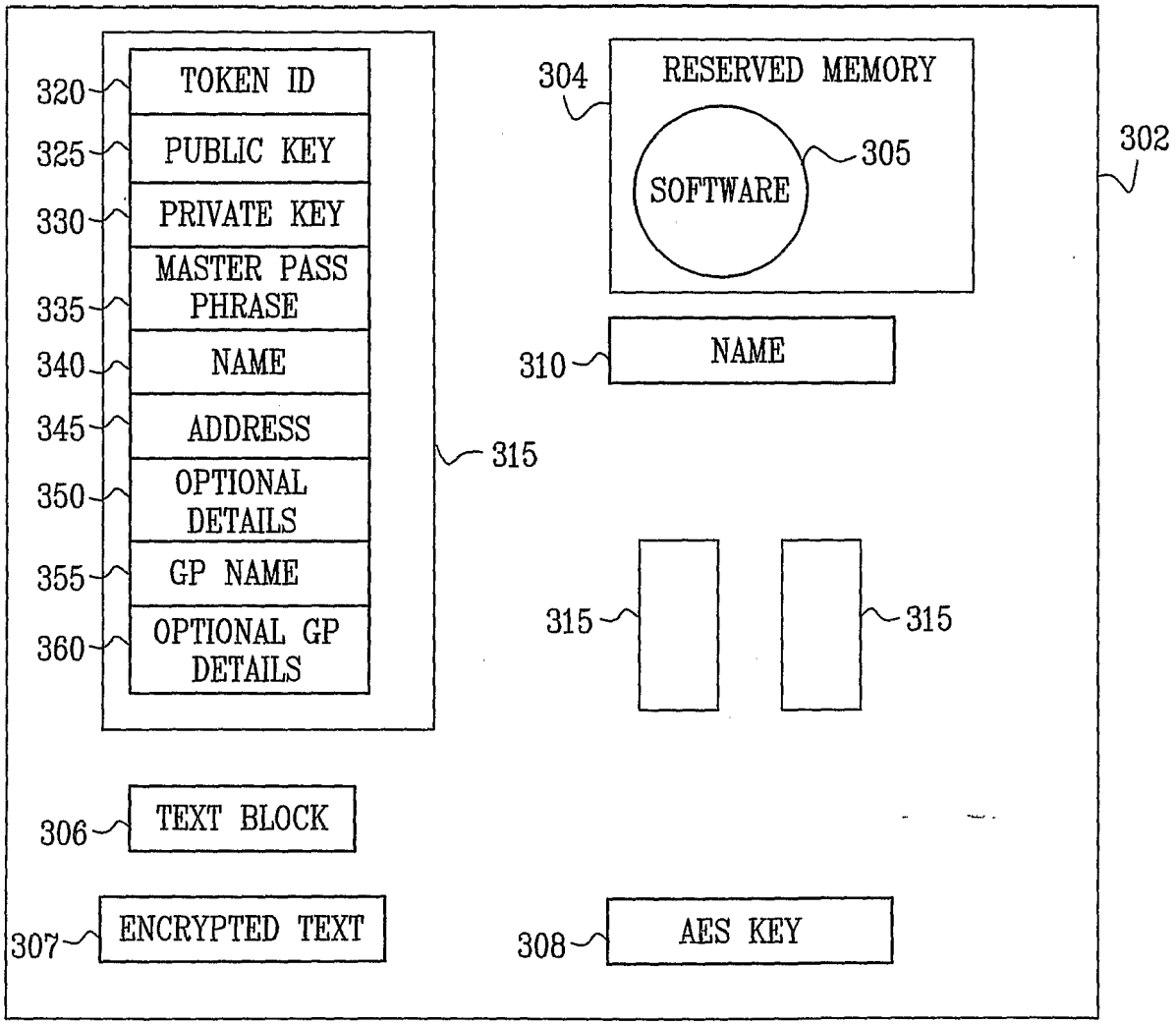

220
TOKEN ID
225
IDENTIFICATION DATA
230
NAME
235
ADDRESS
240
DATE OF BIRTH
245
COMMENTS
250
MIS NUMBER
255
TIME STAMP
257
TIME REGISTERED
260
PUBLIC KEY
265
CHECKSUM
206
TEXT BLOCK
207
ENCRYPTED TEXT
209
RESERVED MEMORY
SOFTWARE
205
18
210
TOKEN NAME
218
MASTER AES KEY
219
PUBLIC KEY
215
215
208
AES KEY

FIG. 4


320
TOKEN ID
325
PUBLIC KEY
330
PRIVATE KEY
335
MASTER PASS PHRASE
340
NAME
345
ADDRESS
350
OPTIONAL DETAILS
355
GP NAME
360
OPTIONAL GP DETAILS
315
304
RESERVED MEMORY
SOFTWARE
305
302
310
NAME
315
315
306
TEXT BLOCK
307
ENCRYPTED TEXT
308
AES KEY

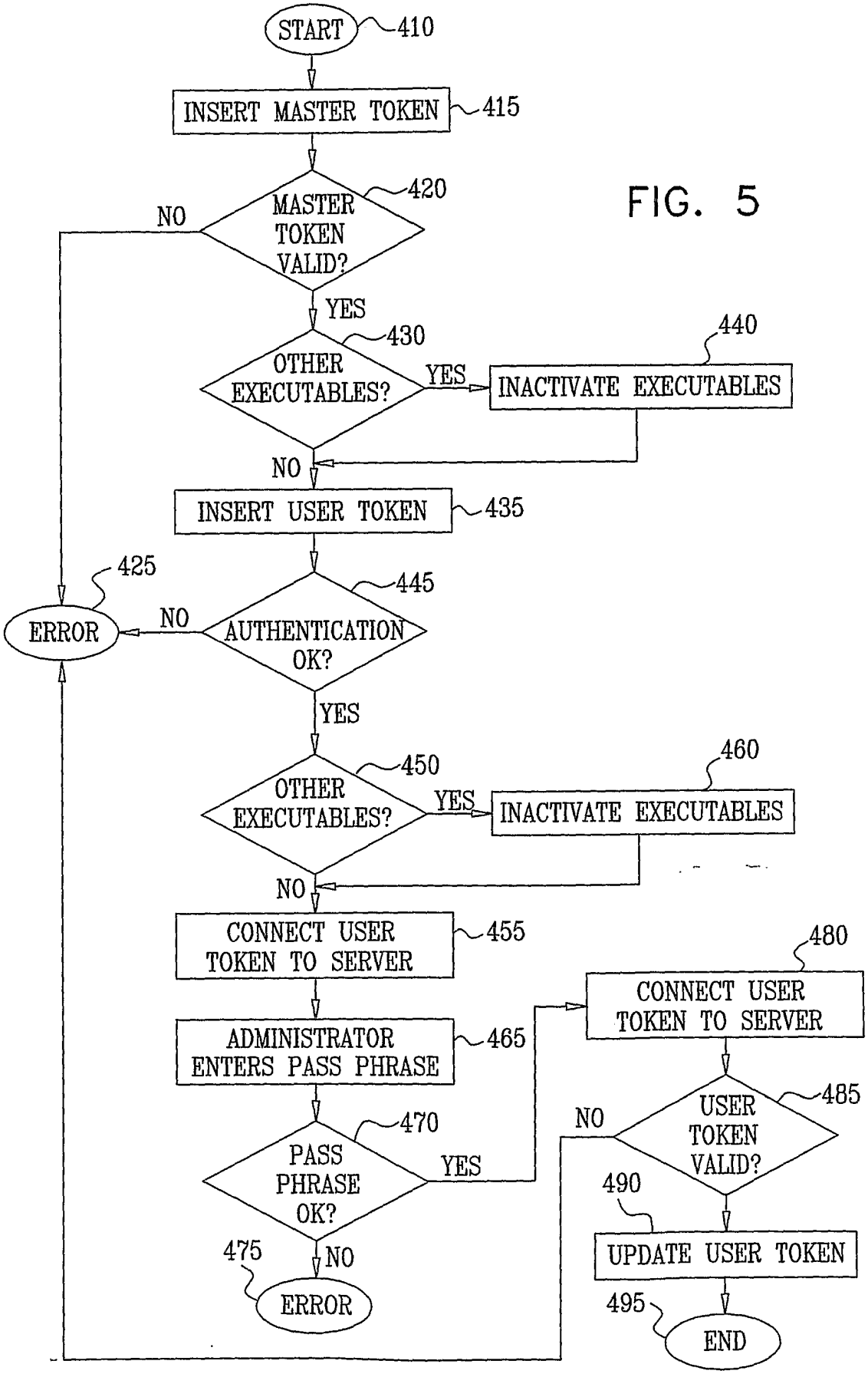

START
410
INSERT MASTER TOKEN
415
MASTER TOKEN VALID?
420
NO
YES
OTHER EXECUTABLES?
430
YES
INACTIVATE EXECUTABLES
440
NO
INSERT USER TOKEN
435
ERROR
425
NO
AUTHENTICATION OK?
445
YES
OTHER EXECUTABLES?
450
YES
INACTIVATE EXECUTABLES
460
NO
CONNECT USER TOKEN TO SERVER
455
ADMINISTRATOR ENTERS PASS PHRASE
465
PASS PHRASE OK?
470
YES
NO
ERROR
475
CONNECT USER TOKEN TO SERVER
480
USER TOKEN VALID?
485
NO
UPDATE USER TOKEN
490
END
495

FIG. 5

FIG. 6

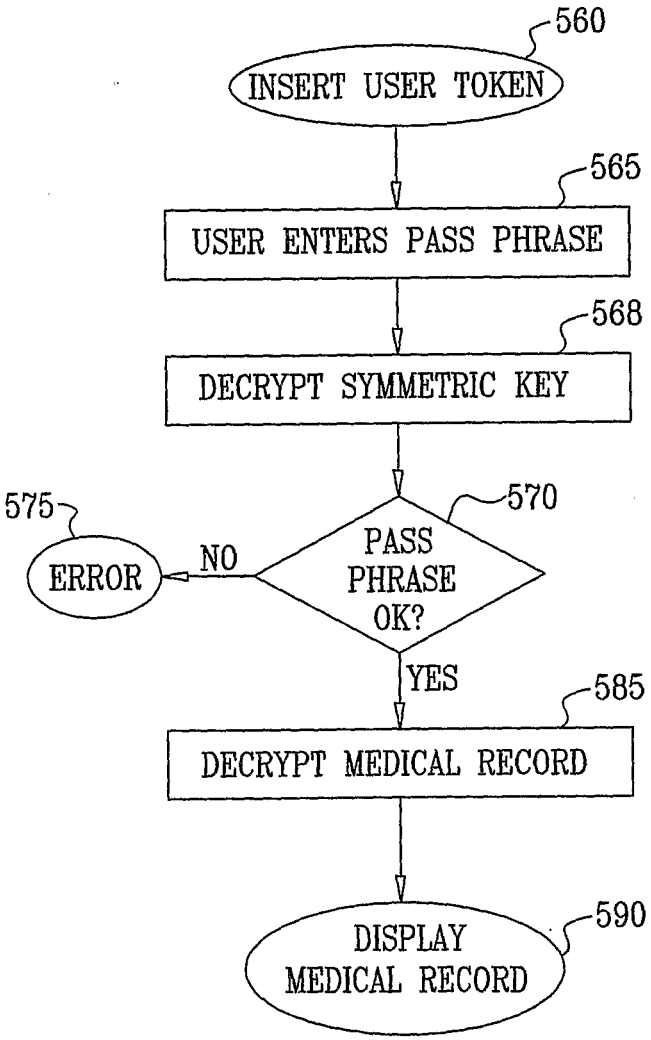

560
INSERT USER TOKEN
565
USER ENTERS PASS PHRASE
568
DECRYPT SYMMETRIC KEY
570
PASS PHRASE OK?
NO
575
ERROR
YES
585
DECRYPT MEDICAL RECORD
590
DISPLAY MEDICAL RECORD

FIG. 7

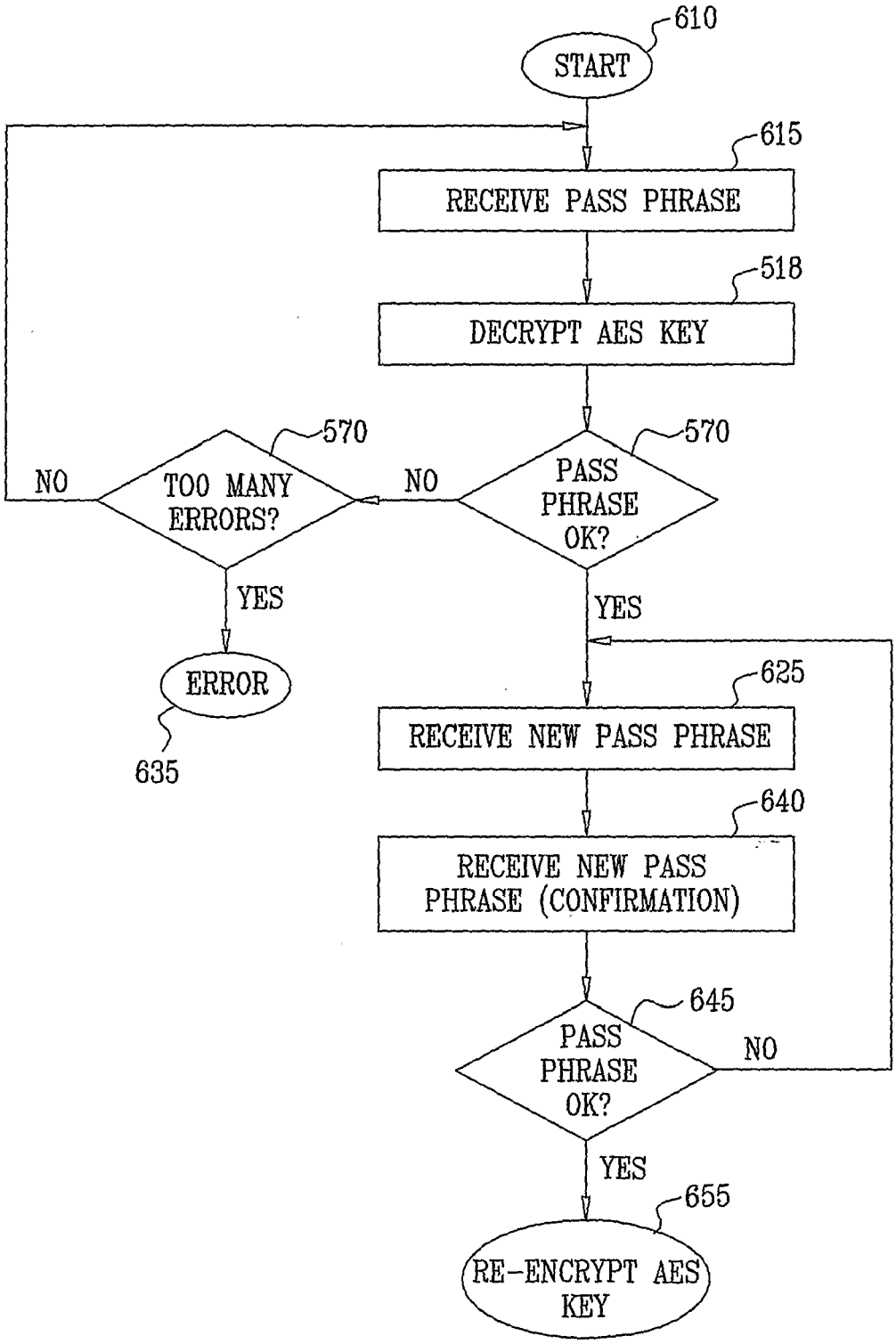
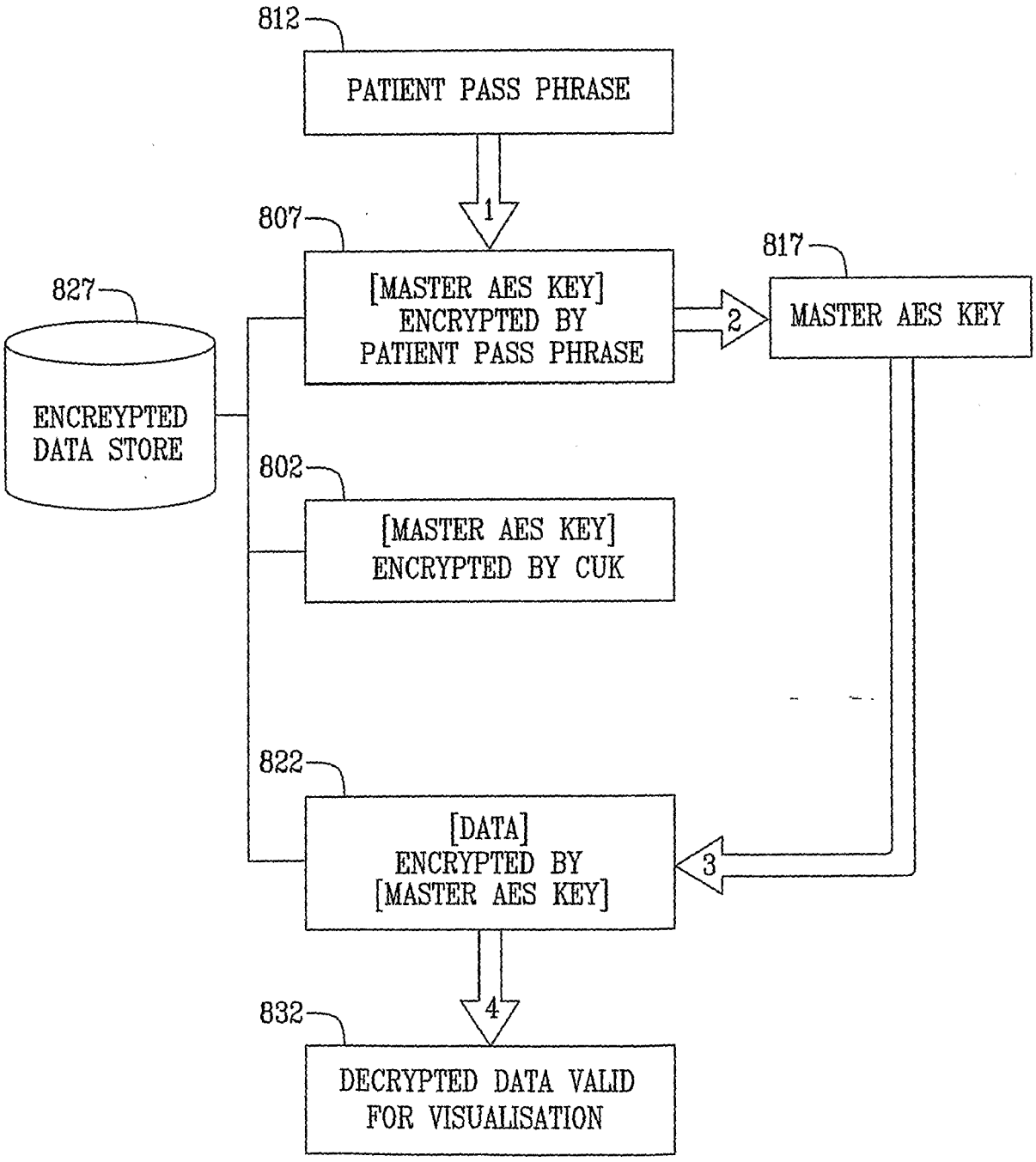

610
START
615
RECEIVE PASS PHRASE
518
DECRYPT AES KEY
570
PASS PHRASE OK?
NO
570
TOO MANY ERRORS?
NO
YES
YES
ERROR
635
625
RECEIVE NEW PASS PHRASE
640
RECEIVE NEW PASS PHRASE (CONFIRMATION)
645
PASS PHRASE OK?
NO
YES
655
RE-ENCRYPT AES KEY

FIG. 8


812
PATIENT PASS PHRASE
1
807
[MASTER AES KEY]
ENCRYPTED BY
PATIENT PASS PHRASE
2
817
MASTER AES KEY
827
ENCREYPTED
DATA STORE
802
[MASTER AES KEY]
ENCRYPTED BY CUK
822
[DATA]
ENCRYPTED BY
[MASTER AES KEY]
3
4
832
DECRYPTED DATA VALID
FOR VISUALISATION

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2007/002689

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/24

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)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/186746 A1 (ANGST WENDY P [US] ET AL) 23 September 2004 (2004-09-23) paragraph [0015] - paragraph [0024]	1-20
A	US 2004/010699 A1 (SHAO ZHIMIN [CN] ET AL) 15 January 2004 (2004-01-15) paragraph [0017] - paragraph [0059]	1-20
A	WO 02/056154 A (RAINBOW TECHNOLOGIES B V [NL]) 18 July 2002 (2002-07-18) the whole document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 October 2007	07/11/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pinto, Raúl

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2007/002689

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004186746 A1	23-09-2004	WO 2004084610 A2	07-10-2004
US 2004010699 A1	15-01-2004	GB 2385157 A	13-08-2003
WO 02056154 A	18-07-2002	AU 2002228039 A1	24-07-2002