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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2015 (29.01.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/013328 A2

(51) International Patent Classification:
G06F 21/31 (2013.01)

(21) International Application Number:
PCT/US2014/047689

(22) International Filing Date:
22 July 2014 (22.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/856,986 22 July 2013 (22.07.2013) US

(71) Applicant: **MOBEHR CORPORATION** [US/US]; 405 SE Osceola Ave, #207, Ocala, Florida 34471 (US).

(72) Inventor: **NARINS, Joshua**; 405 SE Osceola Ave, #207, Ocala, Florida 34471 (US).

(74) Agent: **NORANBROCK, Randy A.**; Lowe Hauptman & Ham LLP, 2318 Mill Road, Suite 1400, Alexandria, Virginia 22304 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2015/013328 A2

(54) Title: A COMPUTER-IMPLEMENTED INFORMATION PROCESSING SYSTEM FOR SECURE ACCESS TO DATA

(57) Abstract: A computer-implemented information processing system for limiting access of data to an authorized user, the authorized user being authorized to allow access to at least one computer file is disclosed. The system includes a user device (UD) including an electronic storage device containing the at least one computer file and a first copy of a verification information file (VID) and a Bluetooth Access Point (BTAP) device communicatively coupled to the UD. The system also includes a central server (CS) having a second copy of the VID and a clerk device (CD) configured to display the first copy of the VID and the second copy of the VID and to transmit to the CS either a confirmation signal or a denial signal.

Attorney Docket No. 5703-001PCT

A COMPUTER-IMPLEMENTED INFORMATION PROCESSING SYSTEM FOR SECURE ACCESS TO DATA

By Joshua Simeon Narins

Cross Reference to Related Applications

[0001] The present application claims priority to U.S. Provisional Patent Application Ser. No. 61/856,986, filed on July 22, 2013, the entire contents of which are hereby incorporated herein by reference.

Field of Invention

[0002] One or more embodiments of the present invention relate to a process to authenticate and/or provide access to electronically stored data in an electronic storage device.

Definitions

[0003] Computer file refers to electronically processable information including data or computer (or processor or controller or the like) executable instructions stored (and/or storable) in an electronic storage which can be processed by a computer for the purpose of operating a device associated with a computer including, for example a display device, a printer, a

modem, another processor, or any other device that can be operated by a computer.

[0004] Image file as used herein refers to a computer file including electronic information that can be processed or interpreted by a computer and based on which the computer can operate a display device to render an image for observation.

[0005] Data file as used herein refers to a computer file including electronic information representing data.

[0006] Text file as used herein refers to a computer file including electronic information that can be processed by a computer and based on which a computer can operate a display device to display text for observation.

[0007] Audio file as used herein refers to a computer file including electronic information that can be processed by a computer to operate a sound reproduction device such as a loudspeaker.

[0008] Program, app or application as used herein refers to a computer file containing computer executable and/or interpretable instructions for execution and/or interpretation by a computer to perform at least one computer related task.

Background

[0009] Mobile computing devices such as laptops, tablet computers, and smart cell phones are well known.

[0010] A mobile computing device typically includes an electronic memory for storage of computer file(s), a processor for executing a program, a display for displaying text and images, one or more speakers for rendering audio, and an input device to receive input from a user (e.g. a keyboard). Mobile computing devices have been configured (programmed) to perform many electronic transactions such as, for example, credit card transactions or keeping a patient's medical records up to date.

[0011] In a typical application, an electronic transaction through a mobile computing device may be authorized when the operator of the device provides the appropriate authorization for the transaction. For example, a password, biometric information, such as fingerprints or iris scans, are provided by the operator of the mobile computing device in order to enable the transaction to proceed. In another conventional process, an image of the person whose identity is to be authenticated is displayed for authentication. While this process may help to confirm the identity of a person who is seeking authentication of his/her identity, it is insufficient in many circumstances.

[0012] Brief Description of the Figures

[0013] Fig. 1 is a diagram of a system configured to carry out a process for providing secure access to data, in accordance with some embodiments.

[0014] Fig. 2 is a diagram illustrating display of security information for providing secure access to data, in accordance with some embodiments.

[0015] Figs. 3A-3F illustrate steps in a process for configuring a system for providing secure access to data, in accordance with some embodiments.

[0016] Figs. 4A-4D illustrate steps in a process for providing secure access to data, in accordance with some embodiments.

[0017] Detailed Description

[0018] The following disclosure provides many different embodiments, or examples, for implementing different features of the provided subject matter. Specific examples of components and arrangements are described below to simplify the present disclosure. These are, of course, merely examples and are not intended to be limiting. For example, the formation of a first feature over or on a second feature in the description that

follows may include embodiments in which the first and second features are formed in direct contact, and may also include embodiments in which additional features may be formed between the first and second features, such that the first and second features may not be in direct contact. In addition, the present disclosure may repeat reference numerals and/or letters in the various examples. This repetition is for the purpose of simplicity and clarity and does not in itself dictate a relationship between the various embodiments and/or configurations discussed.

[0019] Further, spatially relative terms, such as "beneath," "below," "lower," "above," "upper" and the like, may be used herein for ease of description to describe one element or feature's relationship to another element(s) or feature(s) as illustrated in the figures. The spatially relative terms are intended to encompass different orientations of the device in use or operation in addition to the orientation depicted in the figures. The apparatus may be otherwise oriented (rotated 90 degrees or at other orientations) and the spatially relative descriptors used herein may likewise be interpreted accordingly.

[0020] A computer-implemented process for secure access to data is described herein. Prior processes are insufficient to authenticate the authority of the authenticated person to allow

access to a device and/or computer file(s) residing on the device.

[0021] In these known processes, any operator whose identity can be authenticated can authorize a transaction (e.g. a person who knows the right password or the person whose image is displayed). Thus, in a typical process the authority to enable an electronic transaction is assumed as long as the operator can be authenticated. Clearly, such processes cannot prevent unauthorized access to a device and/or computer files residing on a device when the association of the device with the operator is not authenticated. Thus, conventional processes can be compromised to allow unauthorized access to a device and/or computer file(s) residing on a device.

[0022] In some embodiments, a process is disclosed herein to ensure that an authenticated and authorized person is allowed to enable an electronic transaction.

[0023] In some embodiments, a process is disclosed herein to ensure that an authenticated and authorized person is allowed to permit access to computer files residing on a mobile computing device.

[0024] In some embodiments, a process is disclosed herein to manage selective access to computer files residing on a mobile computing device.

[0025] In some embodiments, a process is disclosed herein to manage selective access to computer files residing on a mobile computing device based on the physical, geographic location of a mobile computing device.

[0026] In some embodiments, a process is disclosed herein to manage authority to modify computer files residing on mobile computing devices, especially where the list of authorized modifiers does not include the mobile device owner.

[0027] In some embodiments, an authentication system secures documents from alteration by the device owner, or hackers, such that a pharmacist fills a prescription based on the data on the user's device, a doctor treats a patient based on the health record contained on the user's device, a retailer counts on money represented on the device actually is valid, and/or a banker pays out, in cash, based on electronic money contained on the device. Because of the legal requirements of HIPAA, or the privacy desires of individuals, the actual health records or wallet contents do not need to be known to the owner of the central server.

[0028] Other features and advantages of the present invention will become apparent from the following description of the invention, which refers to the accompanying drawings.

[0029] Fig. 1 illustrates a system 10 configured to carry out a process according to one or more embodiments of the present invention.

[0030] System 10 includes a user device (UD) 12, which can be any mobile computing device such as a laptop, a tablet computer, or a smart phone. In some embodiments, UD 12 includes at least one non-volatile electronic memory device for storage of computer files, a computer processor for executing computer executable code from a program, a display device for displaying images, an input device for receiving operator input (e.g. a physical or virtual keyboard or its equivalent) such as data or instructions, and suitable hardware for near-field, wireless communication (e.g. hardware for wireless communication using Bluetooth). In some embodiments, UD 12 includes a user device identification (UDID) which is electronically stored data representing a series of numbers and/or letters (e.g. a serial number provided by the manufacturer of the UD) that uniquely identifies UD 12. In some embodiments, the UDID represents a series of characters including at least numbers and/or letters.

[0031] System 10 further includes a near field communication access point, such as a Bluetooth Access Point (BTAP) 14, to enable wireless communication with UD 12. BTAP 14 may further include suitable hardware to report its geographic position

electronically (e.g. by sending electronic data representative of its geographic position). For example, BTAP 14 may include hardware that can report the geographic position of BTAP 14 through use of a global positioning system (GPS). BTAP 14 may also include a BTAP device identification (BTAPID), which may be electronically stored data representing a series of numbers and/or letters (e.g. a serial number provided by the manufacturer of the BTAP) that uniquely identifies the BTAP 14. BTAP 14 may also include suitable hardware and/or software to produce an RSA token, such as the SecurID authentication token by RSA Security LLC, a division of EMC Corporation.

[0032] System 10 further includes a central server (CS) 16, which is a computer. CS 16 is in communication with UD 12 through, for example, a communication network 18. In one embodiment, CS 16 is in communication with UD 12 via a publicly accessible network of computers such as the Internet, although it should be understood that a system for carrying out a process according to the present invention is not limited to the use of a computer network to enable communication.

[0033] System 10 further includes a clerk device 20. Clerk device 20 is not limited to any particular computing device and in some embodiments is a PC, a laptop, a tablet computer, a smart phone or any other suitable device. In some embodiments, CD 20

includes a non-volatile electronic memory device for storage of computer files, a computer processor for executing computer executable code in the form of a program, a display device for displaying images, an input device to enable the operator of CD 20 to input data/instructions into CD 20.

[0034] CD 20 is in communication with CS 16 via a communication network 22, which, in some embodiments, is a publicly accessible network of computers such as the Internet, although it should be understood that a system 10 for carrying out a process according to one or more embodiments of the present invention is not limited to communication through a computer-based communication network. CD 20 may be integrated with BTAP 14, so that they are one physical device.

[0035] To carry out a process according to an embodiment of the present invention UD 12, BTAP 14, CS 16, and CD 20 has residing thereon computer files including text files, image files, data files as well as programs. Thus, UD 12, BTAP 14, CS 16, and CD 20 are configured to perform the functions necessary for carrying out a process according to an embodiment of the present invention.

[0036] A process according to one or more embodiments of the present invention requires a computer file or computer files (referred to herein as verification information file (VID). The

VID contains information for the identification of the authorized operator of UD 12. The authorized operator as referred to herein refers to a person authorized to allow access to at least one of the computer files residing in UD 12 (e.g. in one or more memory locations in electronic memory device of UD 12).

[0037] The VID, for example, includes text file(s) based on which a computing device can display text representing the user's personal information (e.g. name, age, address, height, weight, eye color, hair color, etc.) and/or image file(s) based on which a computing device can display images (e.g. personal images such as the operator's face in different orientations, biometric images like fingerprints or iris scans, or other graphical images). In some embodiments, the VID also includes an audio file based on which a computing device can reproduce a sample of the voice of the operator of UD 12 through an associated sound reproduction device.

[0038] In a process according to at least one embodiment of the present invention, the VID resides at least in one or more memory locations in CS 16. In one embodiment, the VID also resides in at least one memory location in UD 12. In another embodiment, the VID also resides in one or more memory locations in CD 20. A VID may be configured by the authorized operator of UD 12 and an authorized operator of CD 20 in a set

up/initialization process. Thus, referring to Figs. 3A and 3B, UD 12 may be provided with an initialization program to allow for the configuration of a VID (S10). In one embodiment, the initialization program displays a user interface to the operator (S12). In some embodiments, the user interface includes a form that allows the operator to enter personal information such as name, address, date of birth, height, weight, hair color, eye color, etc. In some embodiments, personal information regarding the operator's physical characteristics is provided as images. For example, an image file to display an image of the operator's iris is provided to represent the operator's eye color. Similarly, an image file to display an image of a portion of the operator's face (e.g. the operator's cheek) is usable to represent the operator's skin tone on an objective basis. In some embodiments, the initialization program also provides the operator with a user interface that allows the operator to associate image file(s) and/or an audio file(s) with the personal information received by UD 12 (S16). The image file(s) and/or audio file(s) are then associated with the personal information to form a VID. Thereafter, the initialization program associates the VID with the UDID (S18) for transmission to CS 16, where the VID will be stored and associated with the UDID. In some embodiments, the initialization program also allows for the

creation of a password, or recording of biometric information, to restrict access (S22) to the program that allows UD 12 to carry out its part of a process according to an embodiment of the present invention. Thereafter, UD 12 establishes communication with an access point (this can be a BTAP 14 or CD 20 with the required NFC facilities) and retrieves(S34) the ID of the BTAP 14, the RSA token, and any GPS information available (S30, S32, S33). UD 12 then begins the process of configuration of the information, and sending the VID and information from BTAP 14, to CS16 (S35.1). It should be noted that, in some embodiments, the operator moves the operator's hands out of the range of the access point to ensure that a hidden device is not placed in communication with the access point (S25). At this point, UD 12 begins displaying the information contained in the VID in a manner consistent with Fig. 2 (S35.2).

[0039] CS 16 then stores the information received as the VID in association with the UDID (S36). In one embodiment, the non-VID portions of the bundle (the BTAP 14 ID and GPS information) are also stored.

[0040] In at least some embodiments, CD 20 that is associated with CS 16 is then operated to view the information. Thus, CD 20 may request the VID information from CS 16 (S38).

[0041] Referring to Fig. 3D, the information in the VID is then displayed by the display associated with CD 20 (S40). CS 16 may then receive a confirmation message(s) from the operator of CD 20. Thus, the application on CD 20 receives input from the operator of CD 20 confirming that the VID information received by CS 16 matches the VID information in UD 12 (S42) by comparing the VID information displayed at CD 20 with the information displayed by UD 12 and the personal identity information provided in the VID matches those of the operator of UD 12 (S44).

[0042] Referring to Fig. 3E, the confirmation process may include comparing each image reproduced based on the image file (s) in the VID to the operator of UD 12 (S46), and comparing the personal information reproduced based on the information in the VID with, for example, a government issued ID (S48). Then, the operator of CD 20 may cause the confirmation/denial message to be sent to CS 16 by first accessing CD 20 (S50) and causing a confirmation or a denial message to be sent to CS 16 (S52) from CD 20.

[0043] Thereafter, if confirmation of the identity and the accuracy of the VID information is received from CD 20, CS 16 creates a repository for the VID information (S54), store checksums associated with the repository (S56), and return the checksums and CS 16's unique ID for the repository to UD 12

(S58). In at least some embodiments, UD 12 then creates a duplicate of the set of checksums (S60), which resides in UD 12.

[0044] In one embodiment, CS 16 and UD 12 both have a copy of the VID stored thereon. Also, in one embodiment, UD 12 is programmed to display the displayable information (e.g. personal information and the images) with its display. Fig. 2 illustrates an example of how information from a VID is displayed. Thus, in section 22 the personal information is displayed textually and in another section 24, preferably adjacent to section 22, image(s) 26 is displayed. In one embodiment, more than one image 26 is displayed in section 24. For example, several images are sequentially displayed (rotated). The displayed personal information includes basic ID card information provided by CS 16. In some embodiments, images 26 include an image of an official seal of the authorizing body (e.g. the image of the seal of the Bureau of Consular Affairs of the State Department of the United States would be appropriate if the authentication of the initialization process was performed by that agency). Section 24 may also indicate the type of document being represented, e.g., what government issued the ID. Section 24 may also include an authorizer section 28 and CS section 30, each for displaying information. In at least some embodiments, the information presented in 28 authorizer section is provided in real time by a

system associated with the authorizer (not shown) in order to, for example, confirm that the ID has not been revoked. In some embodiments, the authorizer's systems and CS 20 are also in communication about revocations and other updates through, for example, time-delayed "batch" job processing. Background image(s) 26 could indicate what sort of ID is being displayed (e.g., an image may indicate to an operator of a CD 20 that the displayed ID indicates a diver's license because the seal of the State of New York is shown). Authorizer section 28 may display live valid/invalid indicators, and may display "subtype" information. Examples of subtype information include information used for further classification. For example, if the ID is a driver's license, the subtype information indicates whether the driver's license is class "C" or "D", or if the ID is just an ID, and not a license to drive. Subtype information may not be relayed to all CDs 20. For example, someone checking ID at the entrance to a building might be satisfied with a state issued ID, and does not need to know what driving classifications, if any, the bearer has. This feature may also make it easier for people who have an unusually large number of driving qualifications. Gun, pet, fishing, hunting, campground, and various other licenses, qualifications and identity cards, can also be represented in the same way. In some embodiments, these licenses and qualifications

are also represented by icons in authorizer section 28 or are shown in more detail if the area represented by authorizer section 28 is selected (clicked) by the operator of CD 20.

[0045] In some embodiments, data from CS 16 (CS section 30) includes meta data about the authorization, for example, the age of CS's knowledge of the owner of UD 12, the number of successful and unsuccessful uses of the VID, and codes and data indicating the status of the authorizer.

[0046] An image or sequence of images (still images or video, each appearing for around a second or two) from the VID would appear over the images provided by the authorizing party (e.g. images of the seal). The images might include: a portrait image of the user, a profile image of the user, a video taken, circling the head, so the head can be seen from 360 degrees, a video taken, circling the body, so the body can be seen from 360 degrees. The audio file containing a sample of the voice of the operator may be selected to play the sample of the voice of the operator.

[0047] In at least some embodiments, the operator of CD 20 also has a way to indicate whether the information in the VID sent by CD 16 matches the information in the VID residing on UD 12, and is able to enter a password to send a confirmation message to CS 16.

[0048] CS 16 is programmed to recognize the location and authorities implied by BTAP 14 based on BTAPID. In some embodiments, the location of BTAP 14 is assumed to be the general location of CD 20. Thus, for example, the BTAPID indicates that the BTAP 14 is located in a pharmacy, and its location is assumed to be the same as the location of a CD 20 at the pharmacy. In one embodiment, based on the location and authorities of BTAP 14, CS 16 is programmed to indicate to the operator of UD 12 that the operator of CD 20 requests access to one or more computer files residing in UD 12, or, in emergencies, allow access to one or more computer files residing in UD 12. In a process according to an embodiment of the present invention, the BTAPID and, optionally, the location of CD 20, configuration of CS 20 associated with CD 20, configuration of CS 20 and the identity of the operator of CD 20 associated CS 16, or the use of an override password entered into the BTAP are used to determine the scope of access to a computer file residing on UD 12.

[0049] Referring now to Figs. 4A-4D, in a process according to an embodiment of the present invention, UD 12 includes a program to facilitate a process according to an embodiment of the present invention. Thus, the operator of UD 12 first activates the program (S62), and, if required, provides a password to UD 12 in order to begin the operation (S64). UD 12 will be positioned at

a location near a BTAP 14 in order to establish communication between the two devices (S66). In at least some embodiments, the operator of UD 12 moves outside the range of BTAP 14 (S68) in order to ensure that a hidden device is not being placed in communication with BTAP 14. Thereafter, the operator will cause UD 12 to transmit the UDID to BTAP 14 (S70). UD 12 may display information from the VID (S72). BTAP 14 receives the UDID from UD 12, adds its BTAPID (S74), an RSA Token (S77) and optionally its geographic location (e.g. GPS information) (S76) to the UDID and sends this information back to UD 12 (S78) which then sends it on to CS 16 (S79). CS 16 receives the UDID, BTAPID, the RSA token, and the information related to the geographic location of BTAP 14. Based on the information received, CS 16 may first determine whether there is a CD 20 authorized to communicate with CS 16. If not, CS 16 may send a message via BTAP 14 to UD 12 indicating that there is no authorization to further proceed. If so, CS 16 transmits the VID associated with UD 12 to CD 20 (S80). CD 20 receives the VID and displays the personal information as well as the images based on the information in the VID (S82). Thus, the VID information displayed by UD12 (S72) and the information from VID displayed by CD 20 are compared. Optionally, if there is an audio file, CD 20 may be configured to play the audio file.

[0050] In some embodiments, the operator of CD 20 then studies the displayed information, and compares the same to the operator of UD 12 to confirm that the operator of UD 12 is the authorized user, which confirms the authenticity of UD 12 (S84, S86). Thereafter, the operator of CD 20 may input a password into CD (S88) and then causes CD 20 to transmit a confirmation message (S90) to CS 16 indicating that the identity of the operator of UD 12 has been confirmed as the authorized user. CS 16 then receives the confirmation message and the operator of UD 12 can then retrieve their mobile device, and indicate that they are ready for the next step, at which point a message is sent to CS 16. CS 16 returns a session key to UD 12 (S92) to prompt the operator to allow send data files, or to authorize the completion of a transaction, between UD 12 and CD 20.

[0051] According to an embodiment of the present invention, the applications on CS 16 and UD 12, and the operator of UD 12, control the level of access granted to CD 20. In at least some embodiments, CS 16 is programmed to limit access by CD 20 to computer file(s) residing on UD 12 based on BTAPID and configuration of BTAP 14. For example, each BTAP 14 may be associated with a CD 20 with certain access rights. In other words, the BTAP 14 and its associated CD 20 determine the level of access granted to CD 20 to access computer file(s) residing on

UD 12. Thus, CD 20 may be a computer accessible to a receptionist at a doctor's office, in which case, access may be limited to non-confidential information health information residing on UD 12. Or, CD 20 may be a computer at a pharmacy, in which case, once the clerk has verified the VID, the operator of UD 12 will be prompted to share some or all of their prescription information.

[0052] The level of access may be changed. For example, in an emergency paramedics may be given full access to medical information residing on UD 12.

[0053] In an embodiment, UD 12 may have stored thereon a file containing an electronic health record (EHR) of the authorized user of UD 12. In some embodiments, the EHR contains many pieces of information. By law, depending on who is viewing the information, full access to all the information is not permissible. For example, a physician may review all the information and may change the information, while the patient (the authorized user) may not be allowed to review some of the information or change any of the information. CS 16 may be programmed to control the scope of access to the information in the EHR based on the location of CD 20, which is determined from the BTAPID of BTAP 14 that is associated with CD 20. For example, the operator of CD 20 may be identified as a Registered Nurse

(RN) who may be authorized to review, edit or even change any medical information in the EHR. However, when CD 20 is identified as associated with a billing specialist, access to EHR may be limited to insurance information, billing history, and current account sections.

[0054] Note that, in an emergency (e.g. when the user is not able to operate UD 12) an override password may be entered manually into BTAP 14 via any suitable input device such as a keyboard, keypad, or some other input device. An override password may be generated periodically (e.g. on a daily basis) for each location that handles emergency matters. For example, an emergency room may be provided with an override password privilege to access medical records residing on a UD 12. Alternatively, to enable the process to proceed in an emergency, biometric information may be used. For example, the user's fingerprint information may be transmitted to CS 16 for authentication. If authenticated, CS 16 may open a session between CD 20 and UD 12 to allow access to the EHR residing on UD 12.

[0055] A process according to an embodiment of the present invention may be implemented with GIT. GIT is a known software development platform.

[0056] In an implementation with GIT, CS 16 saves the computer files and directories on a disk (e.g. a hard drive), and creates a new git repository out of them. The git repository is the backup and audit log of changes to a secure computer file, like an EHR. Multiple types of checksums may be used as confirmation for each computer file and directory, and kept near the git repository. The root directory of each git repository will include a directory, or directories, containing all the items from the VID, directories for each applications, and directories for application vendors. CS 16 can send a confirmation message to UD 12 once the VID is received and properly stored. CS 16 also sends the VID to CD 20 for display of information contained in the VID. In at least some embodiments, CD 20 stores a copy of the VID. If there is more than one image file in the VID, the images may be rotated and displayed alongside of the displayed personal information. A virtual button may be provided which allows the operator of CD 20 to cause the audio file to be played, when an audio file is sent with the VID.

[0057] A further example of a process according to an embodiment of the present invention is the secure access by a pharmacist to a prescription in an EHR residing on a UD 12. At the pharmacy, UD 12 will be placed on a BTAP 14. The operator of UD 12 may enter a password to start the program residing on UD

12. Thereafter, UD 12 will transmit its UDID to BTAP 14. Once BTAP 14 at the pharmacy receives the UDID, the BTAP 14 returns its BTAPID, RSA Token, and possibly GPS information to UD 12. UD 12 then transmits the UDID along with information from BTAP 14 to CS 16, then CS 16 can send the VID associated with the UD 12 to a CD 20 at the pharmacy. In some embodiments, the CD 20 stores a copy of each VID it has seen, indexed by UDID, so repeat visits do not require the entire VID be transmitted from CS 16 to CD 20. When the operator of the CD 20 (e.g. the pharmacist) confirms the authenticity of UD 12 and the identity of the operator of UD 12 as the authorized user, then UD 12 is prompted to share the EHR residing on UD 12 with CD 20. It should be noted that CS 16 will limit access only to the prescription information in the EHR, not all the information therein. Moreover, the access may be a read-only access (i.e., with no right to edit or change the information in the EHR). Finally, CD 20 will calculate checksums of the prescription information, these checksums are then sent from CD 20 to CS 16, which will confirm or deny that the prescription information may have been altered in any way. It should be noted that CS 16 may not store the data residing on UD 12, but may only store the checksums. In some embodiments, the data and the checksums will be stored, except when prohibited by law.

[0058] Another example may involve a visit to a doctor by a patient (authorized user and operator of UD12) who visits multiple doctors, whose information systems are not configured to automatically exchange health care information. When the patient visits one of these doctors, and they subsequently update their local EHR data, the next time the operator of UD 12 uses the device the operator is prompted to accept the changes, and the UD 12 copy of the EHR will be updated. Thus, after the identity of the operator of UD 12 is authenticated, any pending changes to the EHR that is made available to CS 16 may be synched with the EHR on UD 12, and then the information residing on CS 20 at the doctor's office may be synched to the newly up-to-date EHR. Updates can be checked for authenticity by comparing the checksums of the files and directories involved at CD 20. After the visit, if the doctor has changed the EHR (e.g. the doctor has changed the chart), UD 12 could be authenticated again. At this point, the authorized user could select to sync updates to the EHR from CD 20 at the doctor's office. First, CD 20 will send updates to CS 16. CS 16 will handle the merging of the data, possibly with GIT. New checksums will be derived. During the sync, updates and checksums then travel from CS 16 to UD 12. Thus, through the process, the EHR residing on UD 12 will remain updated. The next time the operator of UD 12 visits a new doctor,

all available updates can be shared, using the same process. A CD 20 at a doctor's office can notify CS 16 of changes as they occur regardless of whether UD 12 is currently engaged. The updates are synched to UD 12 when a session is started via authentication through a BTAP 14. CS 16 would have the updates, and can provide the updates on behalf of the doctor who had updated the note. The following is an example. Doctor 1 is a Primary Care Physician. Doctor 1 has an up to date copy of the patient's EHR, on a CD 20, from the last time the patient visited. The patient visits Doctor 2, who prescribes a new medicine. This could be in the patient's EHR by the time the patient leaves the office, and will be in the patient's EHR after the sync after the doctor completes the note. That evening, Doctor 2 adds some notes, e.g., about a new diagnosis. When the doctor saves the notes, in one embodiment, the notes will be sent to CS 16 and will be queued for synchronization. The next time UD 12 engages a BTAP 14, the user is given the option to update the EHR. If so, all the checksums are updated, and changes are relayed to UD 12. After this, the EHR may be synched from UD 12 to CD 20. In addition to providing a secure access to an EHR, there are many other applications for a process according to an embodiment of the present invention.

[0059] For example, UD 12 may include an image file which can display an image of the authorized user with a child who is being picked up at school, or at other public (e.g., swimming pool) or private (e.g., summer camp) locations, in order to ensure that a stranger is not picking the child up. Thus, for example, when a child is picked up, the person picking up the child may be verified through a process according to an embodiment of the present invention, and their authority to pick up the child in question can be verified through an extra image, stored on UD 12 and whose checksum is stored at CS 16.

[0060] One UD 12 can exchange a VID with another UD 12 through a CS 16. In this example, each UD 12 may include its own BTAP 14, RSA Token generator, and a device to report GPS information at the time of exchange of the VID. This way, one may receive identity information from a stranger for added peace of mind and security. For example, if the operator of one UD 12 is leaving a bar with a relative stranger operating another UD 12, the relative stranger can cause the transmission of a VID from CS 16 to the operator of the first UD 12 for identity verification. The same process may apply to picking up a hitch-hiker or being picked up as a hitch-hiker. In this example, the receiving UD 12 would be serving as a CD 20. The identity of the operator (authorized user) of UD 12 could be stored at CS 16 and retrieved

at a later date, in the event the operator of UD 12 cannot be located.

[0061] In another application, UD 12 may be used as an identification card. UD 12 may be, for example, used to limit an employee's access to different parts of a building at the employee's place of employment. For example, UD 12 could lock and flash red if UD 12 is at a BTAP 14 located in a place forbidden to the authorized user of UD 12. A map of the areas allowed to the user residing on the user's UD 12 could be viewed by the operator of CD 20 (e.g., a security guard) through a process according to an embodiment of the present invention.

[0062] A potential application is cash or credit transactions. In this example, a bank clerk operating a CD 20 at a bank could effect an electronic deposit of cash or credit into a computer file residing in UD 12. The computer file residing in UD 12 would then include the information relating to the transferred cash or credit. At this point, only UD 12 would certainly know about the amount of money represented on the device. CS 20 would only definitely have knowledge of the checksum of the file representing that amount. This form of electronic money is more like cash, because once it leaves the bank, only the owner is keeping track of it. In such cases, the operator of UD 12 will likely want a backup of their money files. The electronic cash or

electronic credit can be moved from one UD 12 to another device, or to another CD 20 (e.g., a CD 20 located at a vendor). UD 12 would include a computer file indicating the amount of cash/credit after each transaction. In yet another application, a file containing an image of an officer of the state, and a charge of the state, would reside on a UD 12, whereby the officer and his/her UD 12 could be authenticated and legal files associated with the charge (e.g., prisoner) and residing on the officer's UD 12 could be securely accessed during, for example, a transfer.

[0063] It should be noted that, in a process according to an embodiment of the present invention, a UD 12 is first subjected to the initialization/set up process for any or all of these applications. Thus, for example, an EHR is transferred onto a UD 12 after it has gone through the initialization/set up process. This way, an operator cannot establish authority to allow access to files on a UD 12 by initializing UD 12 after transferring files to UD 12. Thus, for example, the operator could not first transfer a computer file containing a prescription for painkillers to a UD 12, and then establish authority to provide access to UD 12 in order to fill the prescription. Therefore, in at least one embodiment, UD 12 is set up, UD 12 is verified through a process according to an embodiment of the present invention and then a restricted computer file is transferred to

UD 12. The computer file so transferred may be identified/marked by, for example, CS 16 as having been transferred after confirming the authentication of UD 12 for added security.

[0064] Furthermore, operator of UD 12 may be provided only limited access to authorized computer files residing on UD 12. For example, the operator of UD 12, even when authorized, may only be granted access to view some of the information in the EHR, and allowed no rights to edit any of the information in that computer file.

[0065] It should be noted that while Fig. 1 shows UD 12 and CD 20 in direct communication with CS 16 each via an independent path, Fig. 1 is only an illustration of one example of a system for carrying out a process according to an embodiment of the present invention. A person of ordinary skill in the art would understand that UD 12 can be in communication with CS 16 through a local server that also enables communication between CD 20 and CS 16. Thus, Fig. 1 should not be interpreted to require the system to be implemented through direct and independent lines of communication. Moreover, while BTAP 14 may be a physically independent device, BTAP 14 may also be part of CD 20. For example, if CD 20 is a mobile computing device (e.g. a tablet), its BTAP 14 may serve the function of a BTAP 14 in a system as illustrated in Fig. 1.

[0066] Furthermore, while Fig. 1 illustrates a system with one BTAP 14 and one CD 20, one should not understand the embodiments of the present invention to be limited to such a system architecture. That is, a system for implementing a process according to an embodiment of the present invention could include, one BTAP 14 and multiple authorized CDs 20 associated with that BTAP 14, one authorized CD 20 and multiple BTAPs 14 associated with that one CD 20, or multiple BTAPs 14 and multiple authorized CDs 20, each CD 20 in the group of CDs 20 being associated with all BTAPs 14 in the group of BTAPs 14 and each BTAP 14 in the group of BTAPs being associated with each CD 20 in the group of CDs 20. Thus, CS 16 may be programmed to associate multiple BTAPIDs with one CD 20, a single BTAPID with multiple CDs 20 or, multiple BTAPIDs with multiple CDs 20. For example, when there are multiple BTAPs 14 and multiple CDs 20 at one site, the operator of CD 20 could use any one of BTAPs 14, and authority could be issued to all authorized CDs 20 to further proceed in the process. The authorized operator of any one of the authorized CDs 20 could then access, for example, a listing of names or pictures of persons who have just used a BTAP 14 at the site in order to establish communication with CS 16, but use a different BTAP 14 at the site to obtain access to the computer files in UD 12. In other words, the same BTAP 14 does not need

to be used for all steps in a process according to an embodiment of the present invention, but different BTAPs 14 or different authorized CDs 20 may be used without deviating from the embodiments of the present invention.

[0067] Although one or more embodiments of the present invention have been described in relation to particular embodiments thereof, many other variations and modifications and other uses will become apparent to those ordinarily skilled in the art.

[0068] Some embodiments disclose a system to secure documents from alteration by the device owner, or hackers, such that a pharmacist can fill a prescription based on the data on the user's device, a doctor could treat a patient based on the health record contained on the user's device, a retailer could count on money represented on the device actually is valid, or a banker could pay out, in cash, based on the electronic money contained on the device. Because of the legal requirements of HIPAA, or the privacy desires of individuals, the actual health records or wallet contents do not need to be known to the owner of the central server.

[0069] Some embodiments disclose a computer-implemented information processing system for limiting access of data to an authorized user, the authorized user being authorized to allow

access to at least one computer file. The system includes a user device (UD) including an electronic storage device containing the at least one computer file and a first copy of a verification information file (VID)and a Bluetooth Access Point (BTAP) device communicatively coupled to the UD. The system further includes a central server (CS) having a second copy of the VID and a clerk device (CD) configured to display the first copy of the VID and the second copy of the VID and to transmit to the CS either a confirmation signal or a denial signal.

[0070] Some further embodiments disclose a computer-implemented information processing system for limiting access of data to an authorized user, the authorized user being authorized to allow access to at least one computer file. The system includes a user device (UD) including an electronic storage device containing the at least one computer file and a verification information file (VID), the user device capable of displaying the VID and a Bluetooth Access Point (BTAP) device communicatively coupled to the UD. The system further includes a central server (CS) having a second copy of the VID and a clerk device (CD) configured to transmit to the CS either a confirmation signal or a denial signal.

[0071] Some still further embodiments include a computer-implemented information processing system for limiting access of

data to an authorized user, the authorized user being authorized to allow access to at least one computer file. The system includes a user device (UD) including an electronic storage device containing the at least one computer file and a first copy of a verification information file (VID)and a Bluetooth Access Point (BTAP) device communicatively coupled to the UD, the BTAP device having an RSA token, wherein the RSA token is passed to the UD. The system further includes a central server (CS) having a second copy of the VID and a clerk device (CD) configured to display the first copy of the VID and the second copy of the VID and to transmit to the CS either a confirmation signal or a denial signal.

WHAT IS CLAIMED IS:

1. A computer-implemented information processing system for limiting access of data to an authorized user, the authorized user being authorized to allow access to at least one computer file, comprising:

a user device (UD) including an electronic storage device containing the at least one computer file and a first copy of a verification information file (VID);

a Bluetooth Access Point (BTAP) device communicatively coupled to the UD;

a central server (CS) having a second copy of the VID; and

a clerk device (CD) configured to display the first copy of the VID and the second copy of the VID and to transmit to the CS either a confirmation signal or a denial signal.

2. The computer-implemented information processing system of claim 1 wherein the VID includes data representing a physical attribute of the authorized user.

3. The computer-implemented information processing system of claim 1 wherein the physical attribute of the authorized user includes at least one of name, age, address, height, weight, eye color or hair color of the authorized user.

4. The computer-implemented information processing system of claim 1 wherein the VID includes biometric information.

5. The computer-implemented information processing system of claim 11 wherein the biometric information includes at least one of fingerprint or iris scan.

6. The computer-implemented information processing system of claim 1 wherein the VID includes image information.

7. The computer-implemented information processing system of claim 11 wherein the image information includes at least one of an image of the authorized user's face or an official seal of an authorizing body.

8. The computer-implemented information processing system of claim 1 wherein the VID includes an audio file.

9. A computer-implemented information processing system for limiting access of data to an authorized user, the authorized user being authorized to allow access to at least one computer file, comprising:

a user device (UD) including an electronic storage device containing the at least one computer file and a verification information file (VID), the user device capable of displaying the VID;

a Bluetooth Access Point (BTAP) device communicatively coupled to the UD;

a central server (CS) having a second copy of the VID; and

a clerk device (CD) configured to transmit to the CS either a confirmation signal or a denial signal.

10. The computer-implemented information processing system of claim 9 wherein the transmission of either the confirmation signal or the denial signal corresponds to an operator's comparison of a government-issued identification card (ID) with the VID.

11. The computer-implemented information processing system of claim 9 wherein the VID includes data representing a physical attribute of the authorized user.

12. The computer-implemented information processing system of claim 11 wherein the physical attribute of the authorized user includes at least one of name, age, address, height, weight, eye

color or hair color of the authorized user.

13. The computer-implemented information processing system of claim 9 wherein the VID includes biometric information.

14. The computer-implemented information processing system of claim 13 wherein the biometric information includes at least one of fingerprint or iris scan.

15. The computer-implemented information processing system of claim 9 wherein the VID includes image information.

16. The computer-implemented information processing system of claim 15 wherein the image information includes at least one of an image of the authorized user's face or an official seal of an authorizing body.

17. The computer-implemented information processing system of claim 9 wherein the VID includes an audio file.

18. A computer-implemented information processing system for limiting access of data to an authorized user, the authorized user being authorized to allow access to at least one computer

file, the processing system comprising:

a user device (UD) including an electronic storage device containing the at least one computer file and a first copy of a verification information file (VID);

a Bluetooth Access Point (BTAP) device communicatively coupled to the UD, the BTAP device having an RSA token, wherein the RSA token is passed to the UD;

a central server (CS) having a second copy of the VID; and

a clerk device (CD) configured to display the first copy of the VID and the second copy of the VID and to transmit to the CS either a confirmation signal or a denial signal.

19. The computer-implemented information processing system of claim 18 wherein the UD displays an image of the authorized user's face to a CD operator.

20. The computer-implemented information processing system of claim 18 wherein the BTAP device includes global positioning system (GPS) hardware to indicate the geographic position of BTAP device.

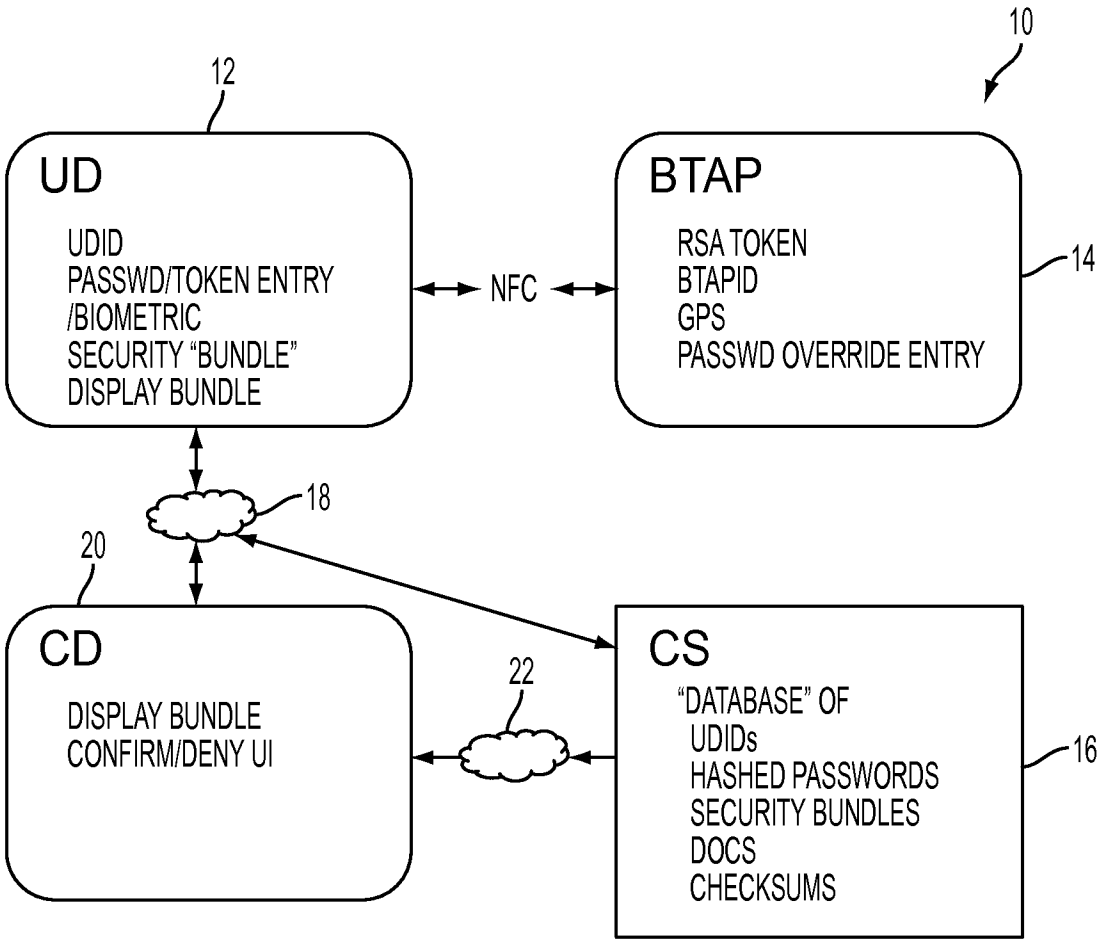
10
12
UD
UDID
PASSWD/TOKEN ENTRY
/BIOMETRIC
SECURITY "BUNDLE"
DISPLAY BUNDLE
NFC
BTAP
RSA TOKEN
BTAPID
GPS
PASSWD OVERRIDE ENTRY
14
18
20
CD
DISPLAY BUNDLE
CONFIRM/DENY UI
22
CS
"DATABASE" OF
UDIDs
HASHED PASSWORDS
SECURITY BUNDLES
DOCS
CHECKSUMS
16

FIG. 1

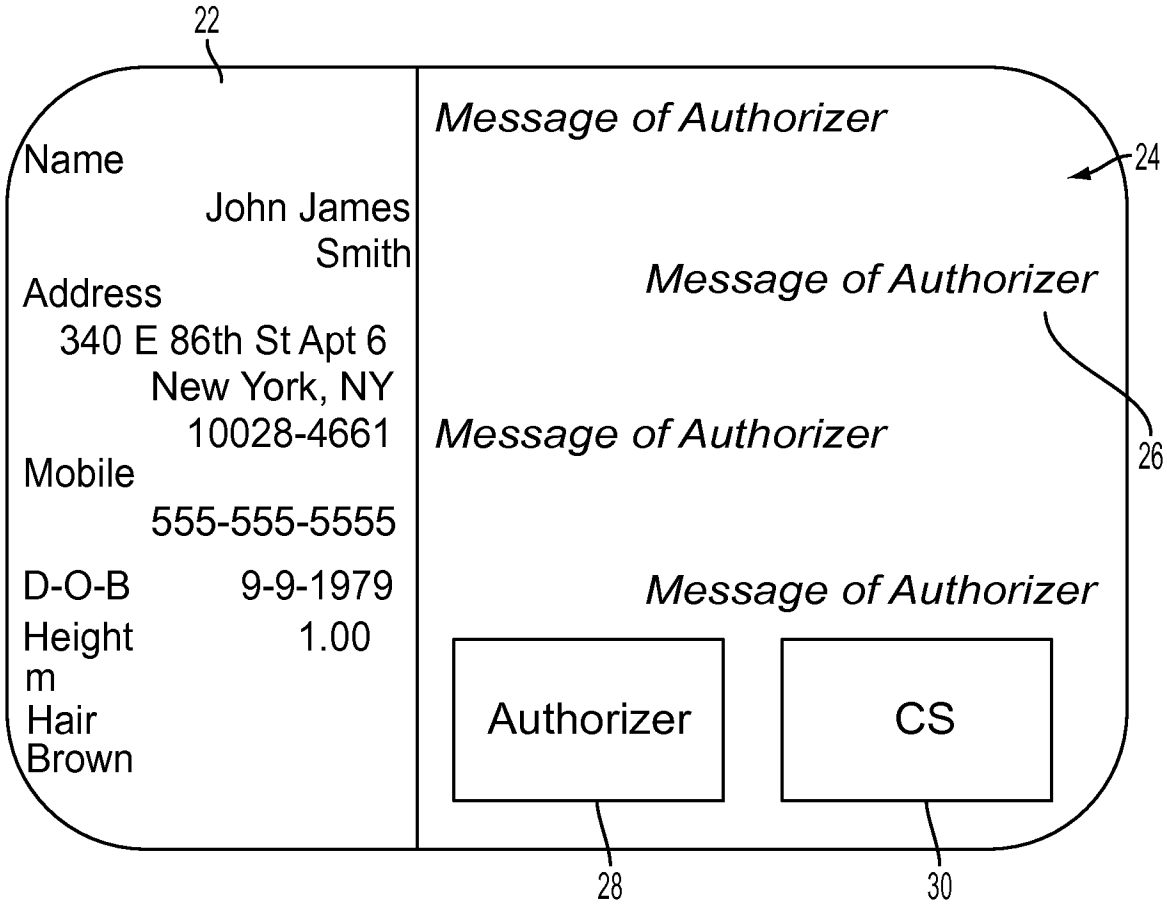
22
Name
John James Smith
Address
340 E 86th St Apt 6
New York, NY
10028-4661
Mobile
555-555-5555
D-O-B 9-9-1979
Height 1.00 m
Hair Brown
Message of Authorizer
24
Message of Authorizer
Message of Authorizer
26
Message of Authorizer
Authorizer
CS
28
30

FIG. 2

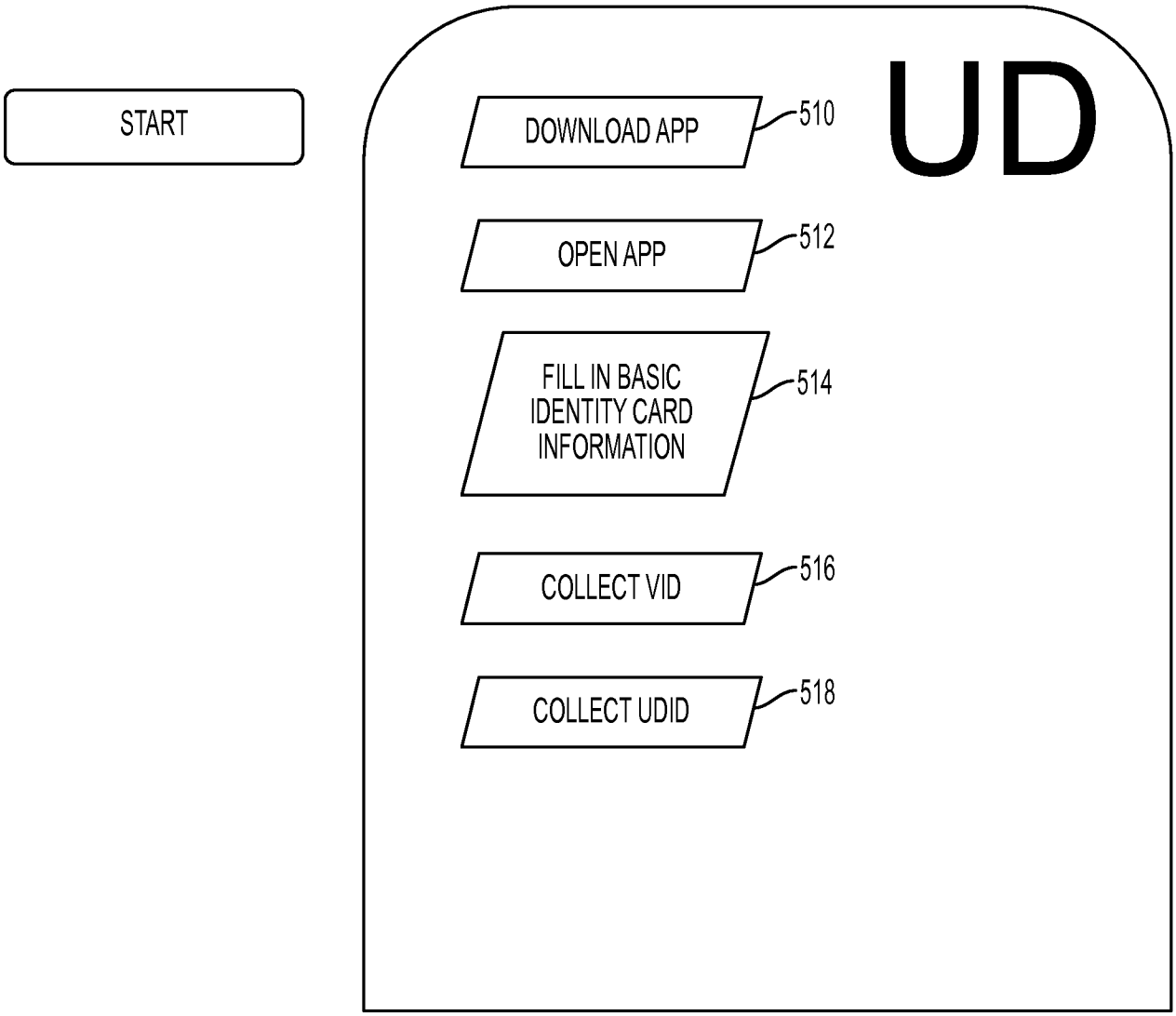
START
UD
DOWNLOAD APP
510
OPEN APP
512
FILL IN BASIC IDENTITY CARD INFORMATION
514
COLLECT VID
516
COLLECT UDID
518

FIG. 3A

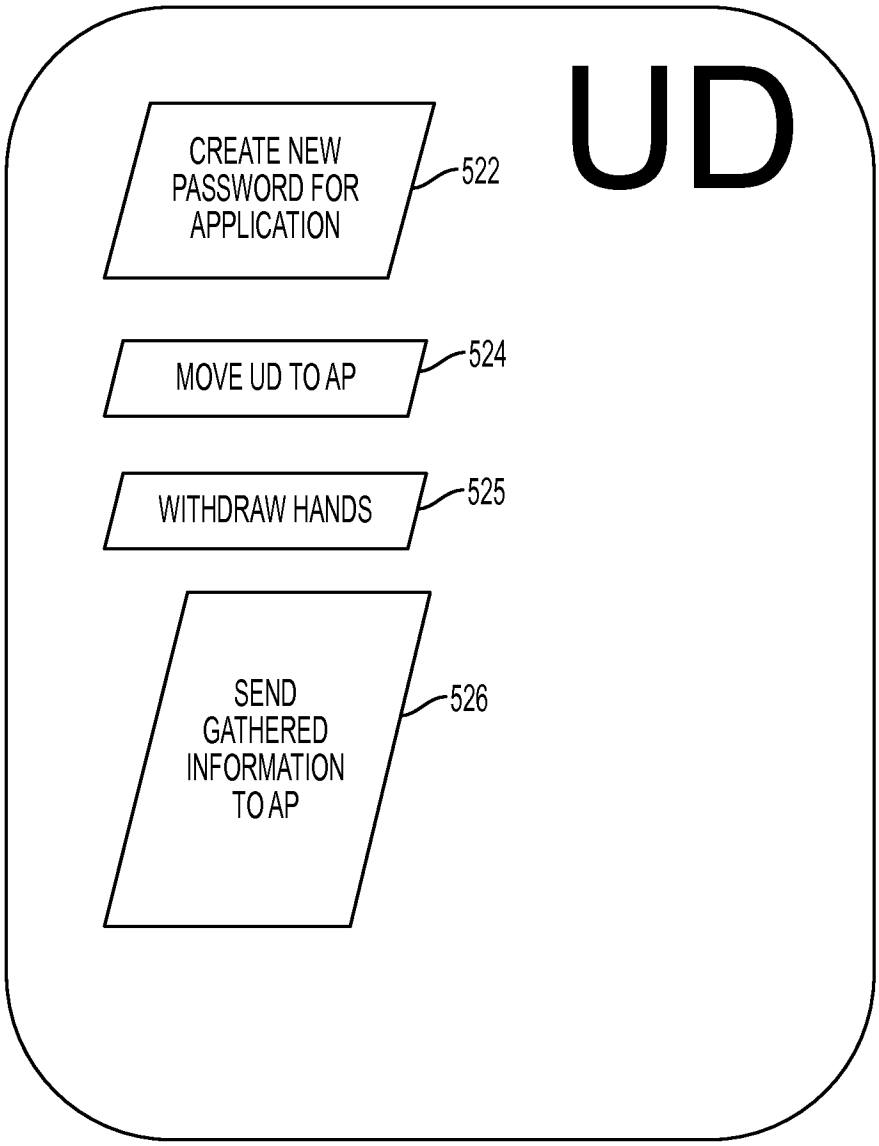
UD
CREATE NEW PASSWORD FOR APPLICATION
522
MOVE UD TO AP
524
WITHDRAW HANDS
525
SEND GATHERED INFORMATION TO AP
526

FIG. 3B

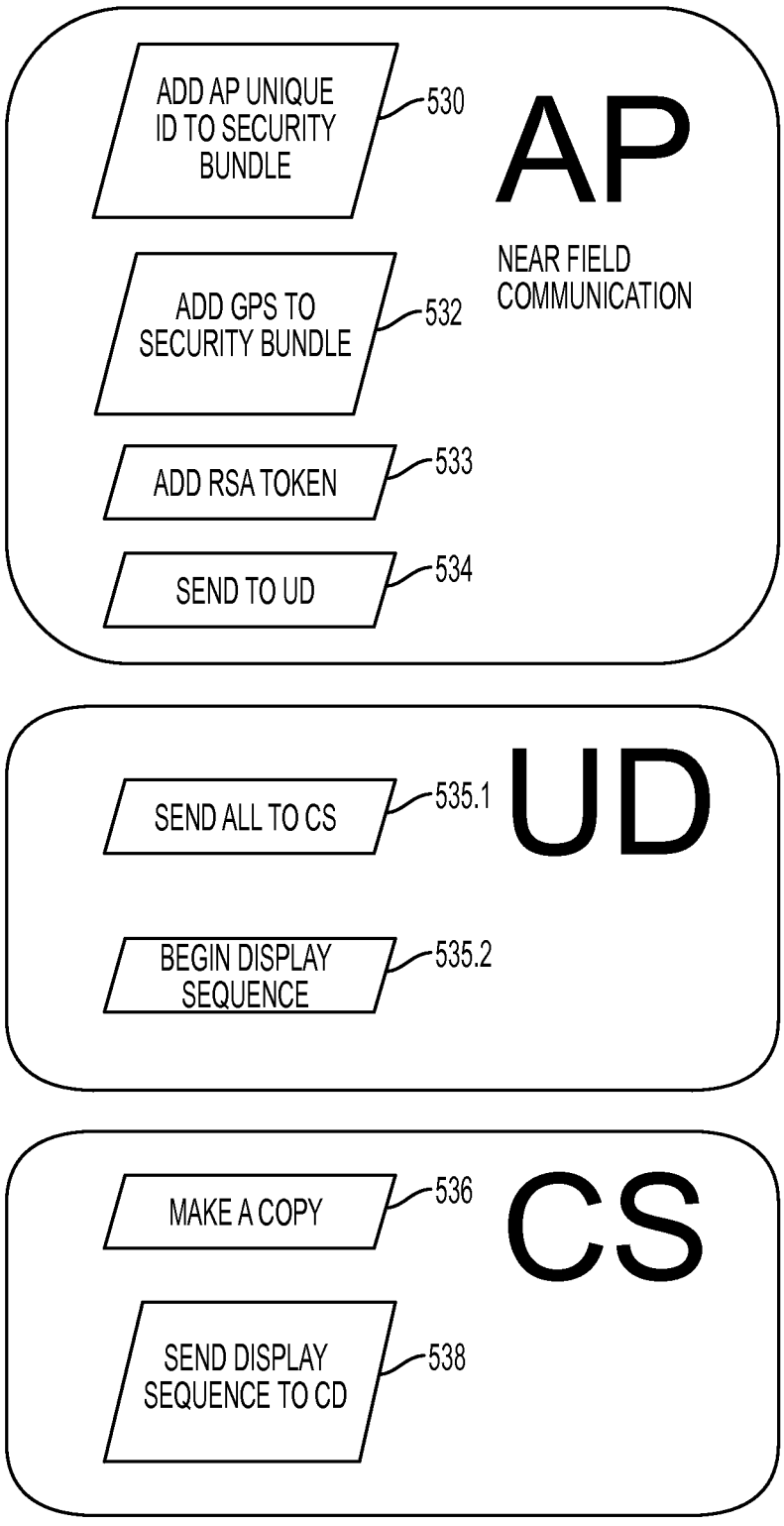
ADD AP UNIQUE ID TO SECURITY BUNDLE
530
AP
NEAR FIELD COMMUNICATION
ADD GPS TO SECURITY BUNDLE
532
ADD RSA TOKEN
533
SEND TO UD
534
SEND ALL TO CS
535.1
UD
BEGIN DISPLAY SEQUENCE
535.2
MAKE A COPY
536
CS
SEND DISPLAY SEQUENCE TO CD
538

FIG. 3C

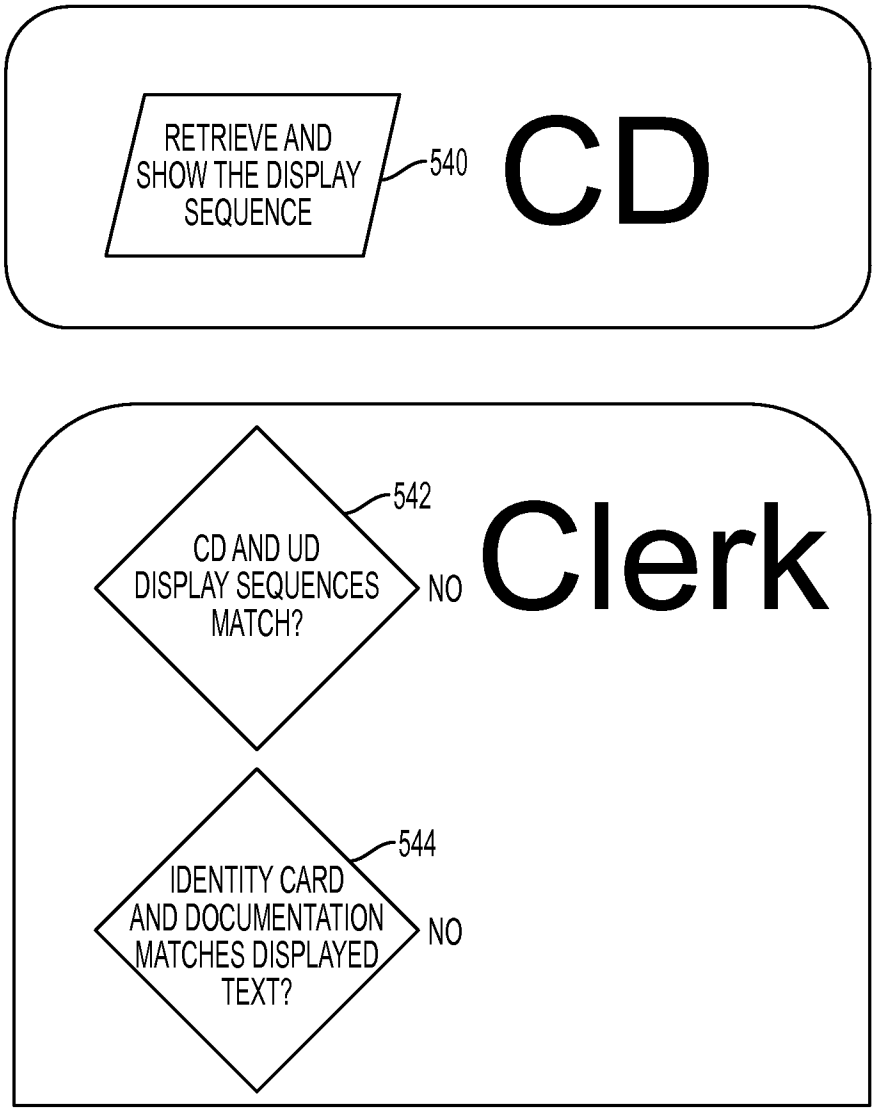
RETRIEVE AND SHOW THE DISPLAY SEQUENCE
540
CD
542
CD AND UD DISPLAY SEQUENCES MATCH?
NO
Clerk
544
IDENTITY CARD AND DOCUMENTATION MATCHES DISPLAYED TEXT?
NO

FIG. 3D

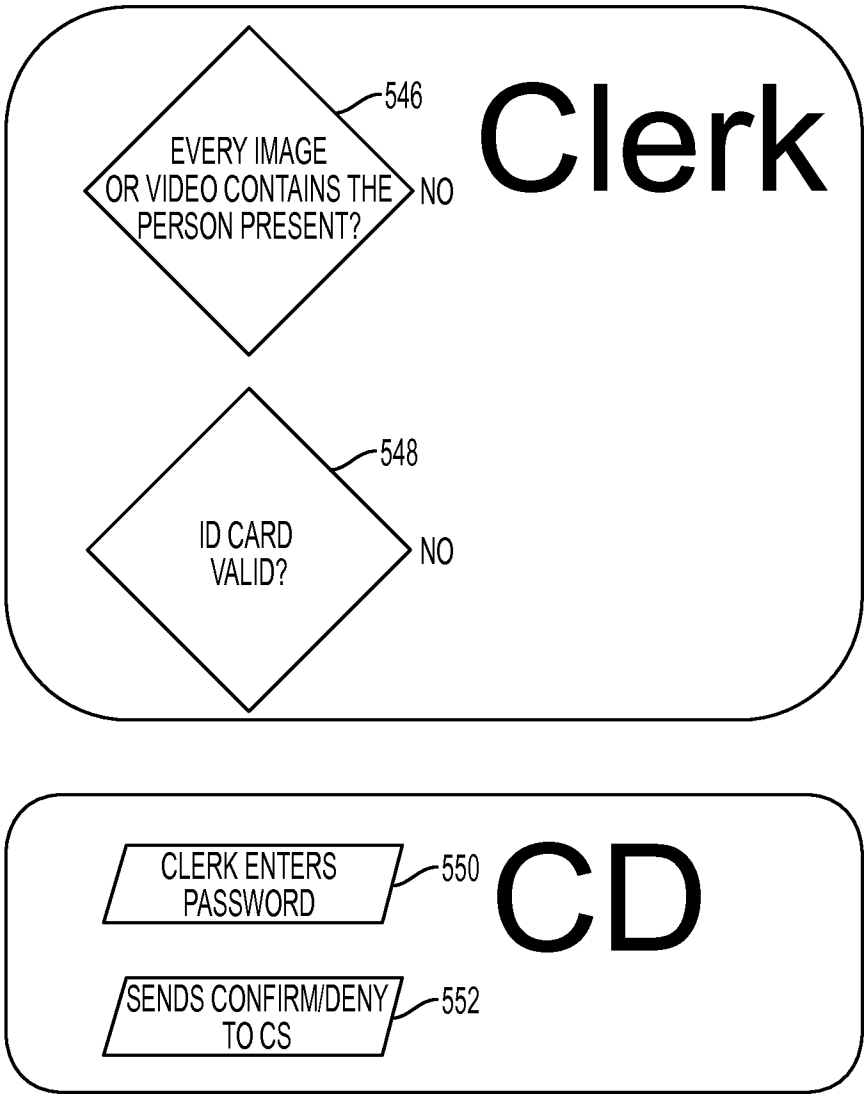
Clerk
546
EVERY IMAGE OR VIDEO CONTAINS THE PERSON PRESENT?
NO
548
ID CARD VALID?
NO
CD
CLERK ENTERS PASSWORD
550
SENDS CONFIRM/DENY TO CS
552

FIG. 3E

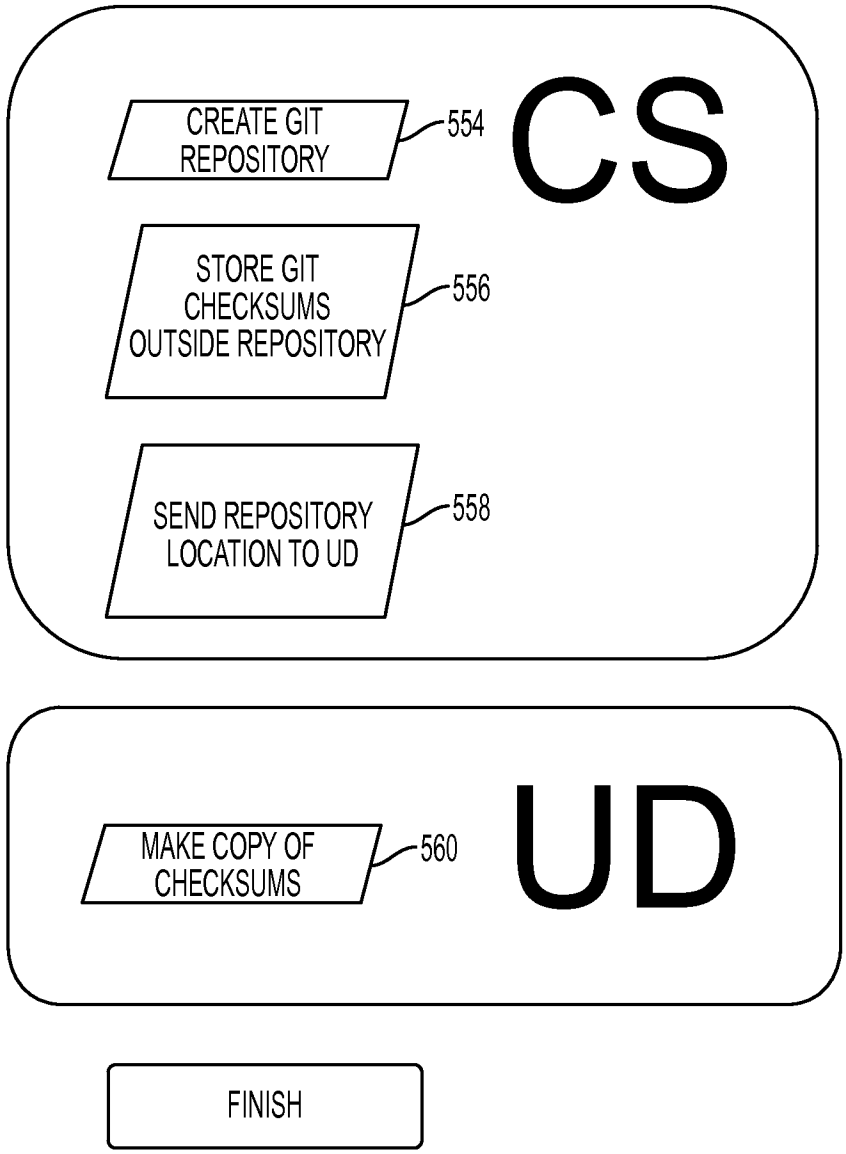
CS
CREATE GIT REPOSITORY
554
STORE GIT CHECKSUMS OUTSIDE REPOSITORY
556
SEND REPOSITORY LOCATION TO UD
558
UD
MAKE COPY OF CHECKSUMS
560
FINISH

FIG. 3F

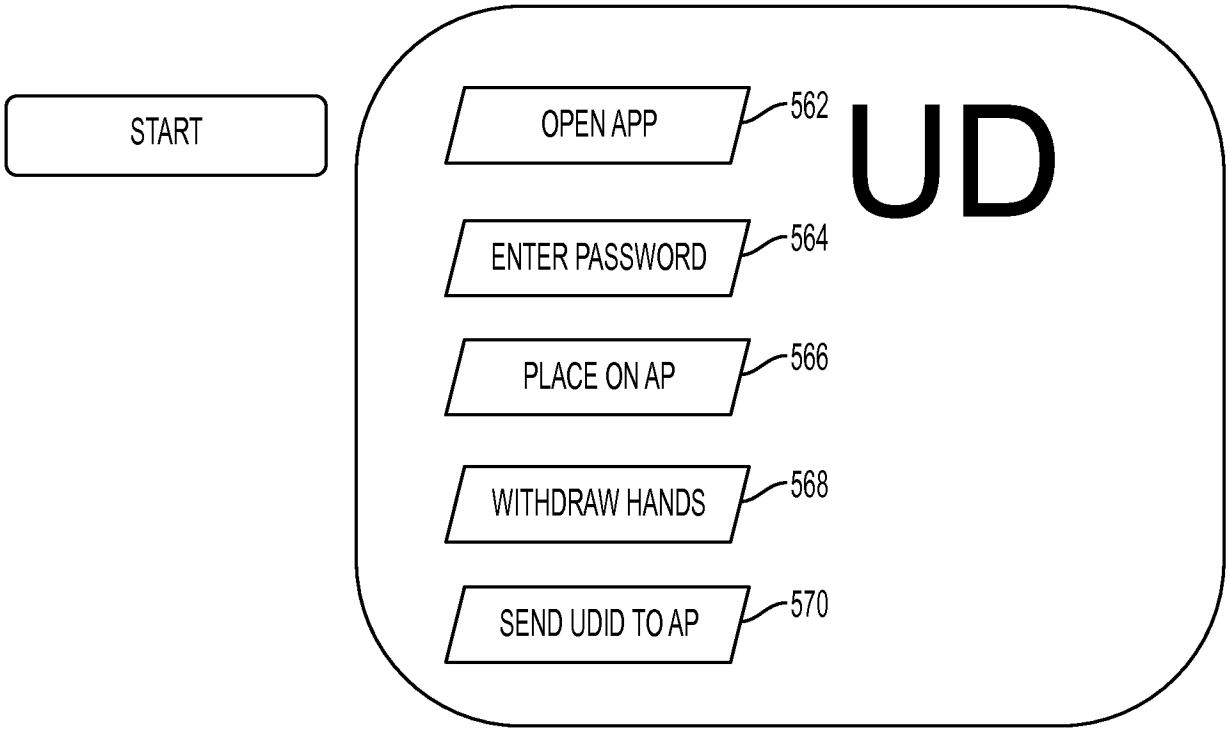
START
OPEN APP
562
UD
ENTER PASSWORD
564
PLACE ON AP
566
WITHDRAW HANDS
568
SEND UDID TO AP
570

FIG. 4A

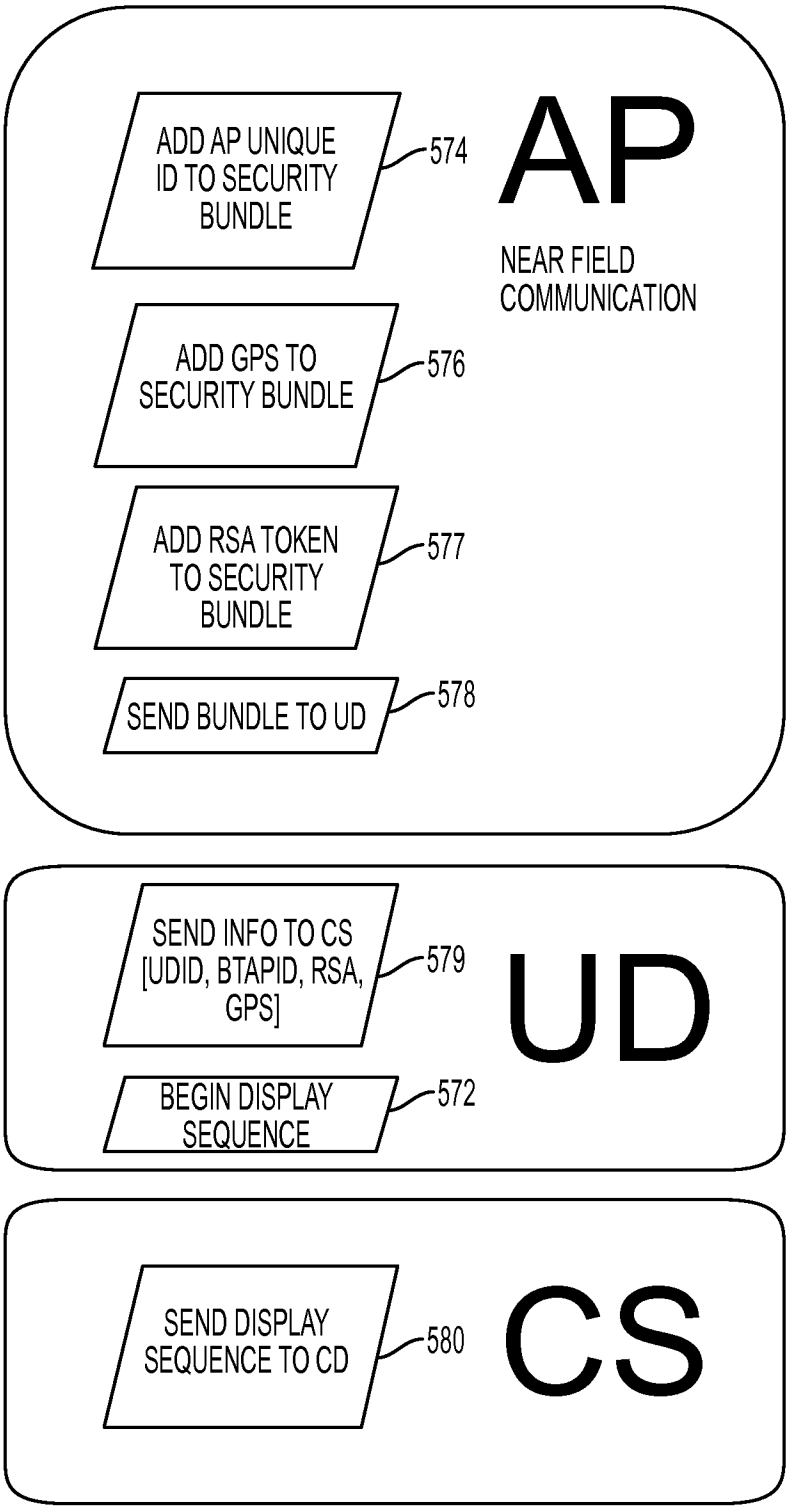
ADD AP UNIQUE ID TO SECURITY BUNDLE
574
AP
NEAR FIELD COMMUNICATION
ADD GPS TO SECURITY BUNDLE
576
ADD RSA TOKEN TO SECURITY BUNDLE
577
SEND BUNDLE TO UD
578
SEND INFO TO CS [UDID, BTAPID, RSA, GPS]
579
UD
BEGIN DISPLAY SEQUENCE
572
SEND DISPLAY SEQUENCE TO CD
580
CS

FIG. 4B

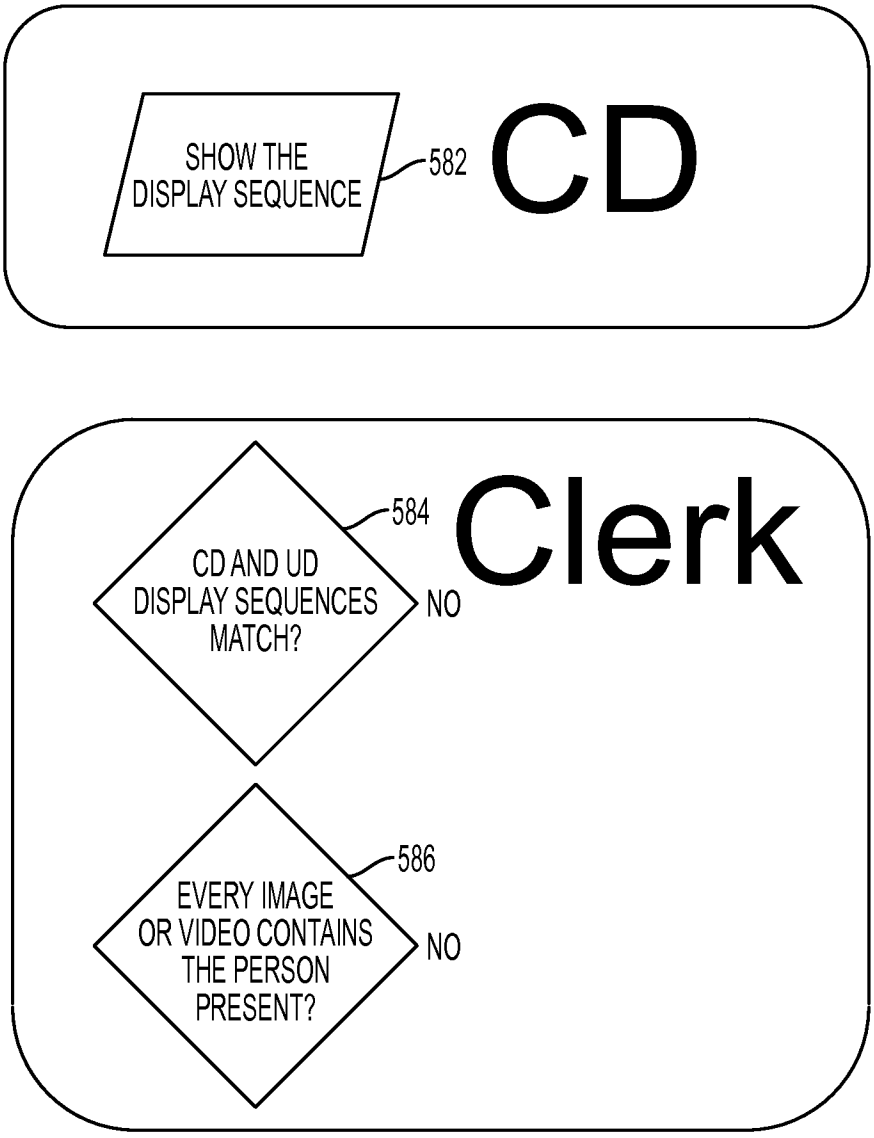
SHOW THE DISPLAY SEQUENCE
582
CD
584
CD AND UD DISPLAY SEQUENCES MATCH?
NO
Clerk
586
EVERY IMAGE OR VIDEO CONTAINS THE PERSON PRESENT?
NO

FIG. 4C

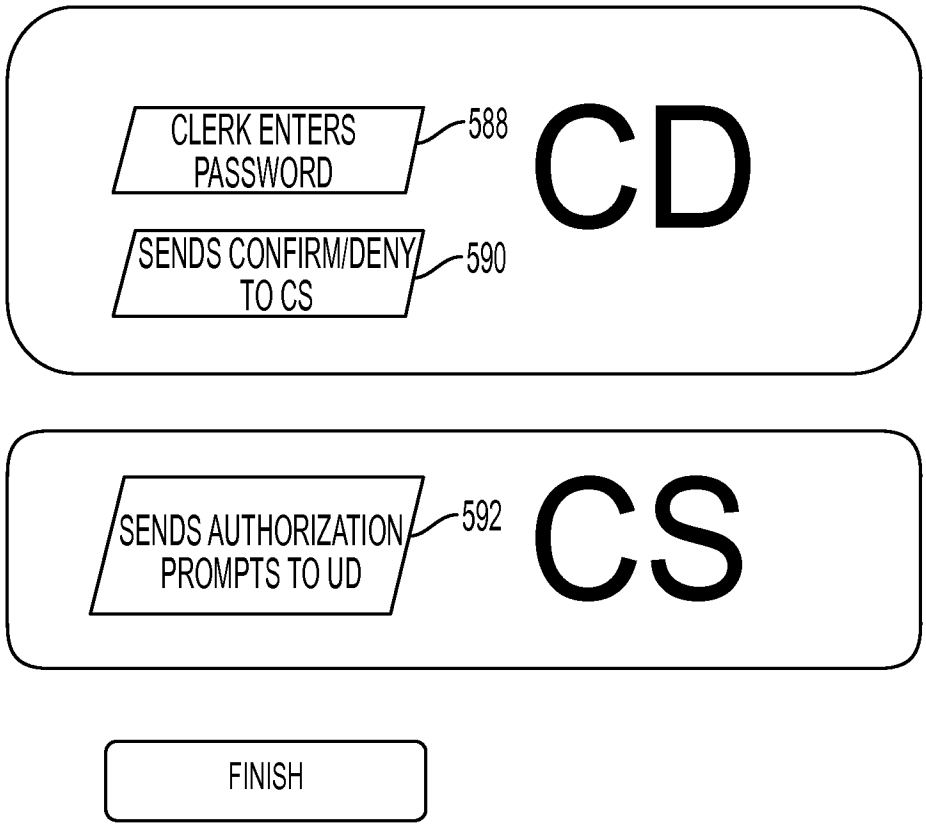
CLERK ENTERS PASSWORD
588
CD
SENDS CONFIRM/DENY TO CS
590
SENDS AUTHORIZATION PROMPTS TO UD
592
CS
FINISH

FIG. 4D