PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F 12/14, 17/21, 17/60

A1

(11) International Publication Number: **WO 00/57279**

(43) International Publication Date: 28 September 2000 (28.09.00)

(21) International Application Number: PCT/US00/07437

(22) International Filing Date: 21 March 2000 (21.03.00)

(30) Priority Data:
09/274,059 22 March 1999 (22.03.99) US

(71) Applicant: PITNEY BOWES INC. [US/US]; One Elmcroft Road, Stamford, CT 06926 (US).

(72) Inventors: SANSONE, Ronald, P.; 4 Trails End Road, Weston, CT 06883 (US). WILSON, Michael, W.; 74 Rollingwood Drive, Trumbull, CT 06611 (US). COOPER, Michael, B.; 2925 Oxford Court, Aurora, IL 60504 (US). MACDONALD, Marcy, F.; 221 Division Avenue, Shelton, CT 06484 (US). RACITI, Robert, C.; 417 Martling Avenue, Tarrytown, NY 10591 (US). GIFFORD, Nathaniel, M.; 25 Skating Pond Road, Trumbull, CT 06611 (US). ULESKE, Shawn, P.; 51 Brownley Drive, Stamford, CT 06905 (US). MARTIN, Judith, D.; 2121 Long Ridge Road, Stamford, CT 06903 (US). DOEBERL, Terrence, M.; 111 Simpaug Turnpike, West Redding, CT 06896 (US). GREY, Suzanne, N.; 11 Hillcrest Road, New Canaan, CT 06840 (US).

(74) Agent: MEYER, Robert, E.; Intellectual Property & Technology Law, Pitney Bowes Inc., 35 Waterview Drive, P.O. Box 3000, Shelton, CT 06484-8000 (US).

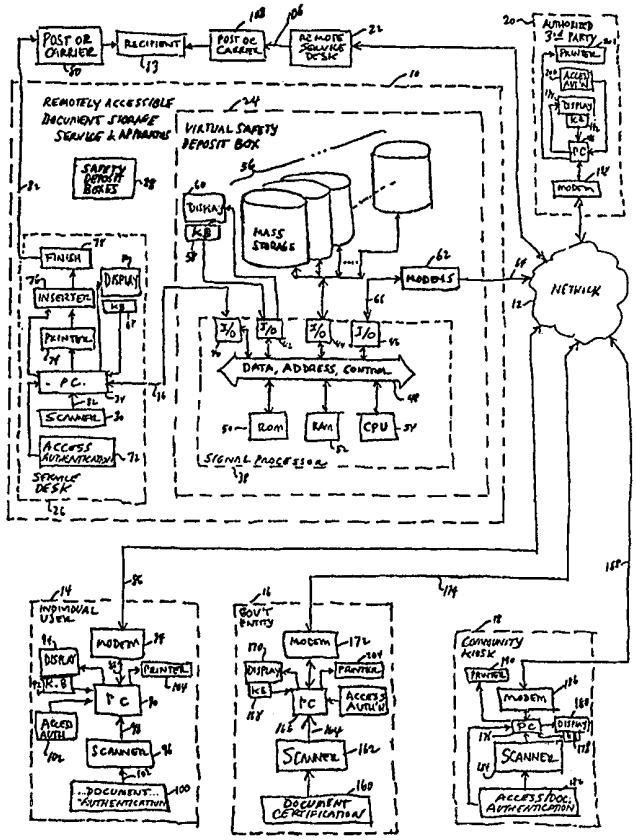
(81) Designated States: AE, AL, AM, AU, AZ, BA, BB, BG, BR, BY, CA, CN, CR, CU, CZ, DM, EE, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, RO, RU, SD, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: REMOTELY ACCESSIBLE LEGACY DOCUMENT STORAGE AND SERVICE APPARATUS

(57) Abstract

A remotely accessible document storage service and apparatus (10) includes a virtual safety deposit box (24) in which legacy documents may be stored in a safe environment for subsequent retrieval by an access device utilizing access authorization. Various access devices may include devices useable by individual users (14), government entities (16), community kiosks (18), or authorized third parties (20). The remotely accessible document storage apparatus may include a service desk (26) for physically receiving documents from users for scanning (30) and for printing (74) and sending documents via post or carrier (80) to a recipient (83) designated by the user. A remote service desk (22) is also contemplated sited near a carrier hub (108) for convenience and efficiency of physical transfer.



FOR THE PURPOSES OF INFORMATION ONLY

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

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

REMOTELY ACCESSIBLE LEGACY DOCUMENT STORAGE AND SERVICE APPARATUS

Background of the Invention

Technical Field

This invention relates to transfer of documents across a network and, more particularly, to a remotely accessible document storage and service apparatus and to various access devices for gaining access thereto.

Discussion of Related Art

Most people keep important and valuable personal and business-related documents such as birth certificates, citizenship papers, baptismal certificates, licenses, deeds, stock certificates, car titles, medical records, passports, school transcripts and admission papers, purchase receipts, military discharge papers, birth, baptismal and death certificates, marriage licenses, divorce papers, contracts, real estate assignments and related papers, insurance policies, banking and financial records, intellectual property transfer agreements and patents, personnel records, court papers, warranties, income tax returns, accounts receivable files, invoices, wills, voice prints, photos, fingerprints, family heirlooms, legal documents, etc. Such documents will be called "legacy" documents hereafter. Legacy documents will include documents originally created in digital form as well as scanned documents. Many people try to keep such important legacy documents in a secure location, such as a strongbox or fire resistant file cabinet in the home or business. It is typically the case, however, that these documents are scattered in the home or business in various "safe" locations. It will often be the case that such documents cannot easily be located when needed. An inventory concerning such legacy documents may not even exist.

Videotapes, digital pictures or negatives and/or detailed lists of valuable personal and/or business assets, such as art, jewelry, furniture, etc.,

may also be stored for insurance purposes and retrieval after a fire, floor, hurricane or other natural disaster.

Summary of the Invention

It is an object of the present invention to provide a remotely accessible document storage service and apparatus for storing legacy documents for users.

It is another object of the present invention to provide various access devices for accessing the remotely accessible document storage service and apparatus.

According to a first aspect of the present invention, an apparatus, accessible over a network by a plurality of users, comprises a mass storage device for storing customer legacy documents and a signal processor connected to said mass storage device for receiving access requests over said network for storing said customer legacy documents received over said network in said mass storage device and for retrieving said customer legacy documents from said mass storage device for sending said legacy documents over said network, wherein each access request includes an access code for authenticating said access request and wherein said signal processor grants or denies said access request according to said access code.

In further accord with the first aspect of the present invention, in a case where an access request is for access to a legacy document in the form of a governmental document stored at a governmental entity which provides electronic access to governmental documents, the signal processor transmits an access request over the network to the governmental entity, wherein the governmental entity retrieves the governmental document and transmits the governmental document over the network with an electronic certification of authenticity to the apparatus or to an access device of a user or an authorized third party requester.

In still further accord with the first aspect of the present invention, the apparatus accessible over the network by a plurality of users further comprises a service desk for receiving actual user legacy documents from

users for scanning said actual user legacy documents and for providing said actual user legacy documents in electronic form as scanned legacy documents for storage in said mass storage device. Moreover, the actual user legacy documents received at the service desk can be received by the service desk for storage in safety deposit boxes rented by said users and located within a facility for said apparatus. Furthermore, the service desk may also include a printer for printing copies of the scanned legacy documents for delivery via post or carrier to a designated recipient.

According still further to the first aspect of the present invention, the access request may be from an authorized third party user (attorneys or agents of the party) for accessing legacy documents of another user.

Still further in accord with the first aspect of the present invention, the access request may be from an access device for an individual user or from a community kiosk access device for use by plural users.

According still further to the first aspect of the present invention, the apparatus is for use in the system including plural access devices including access devices for individual users, government entities, community kiosks and authorized third party users.

In accordance still further with the first aspect of the present invention, the access request may be for the apparatus to transmit a legacy document over the network to a remote service desk for printing and delivery via post or carrier to a designated recipient. In that case, the remote service desk will typically be located at or near a post or carrier hub.

In accordance with a second aspect of the present invention, an access device for accessing an apparatus over a network comprises a computer connected to various input and output devices including means for providing a digitally encoded legacy document, such as a scanner for scanning a legacy document and for providing a scanned legacy document signal to said computer, an access authorization entry means responsive to a user input for providing an access authorization signal to said computer, a communications device, such as a communications device, responsive to an access request signal from said computer for transmitting said access authorization signal and said scanned legacy document via said network to an

apparatus for storing legacy documents of users. The means for providing a digitally encoded legacy document need not be a scanner, but can be any kind of device for receiving or originating a digital signal representation of a legacy document. The access device may further comprise a display or printer for displaying or printing a legacy document retrieved over said network from said apparatus in response to an access request signal from said computer.

The access device may be for use by an individual user, a governmental entity, or a plurality of individual users gaining access at a community kiosk.

In further accord with the second aspect of the present invention, the access device is for use by an authorized third party user for accessing legacy documents of another user.

These and other objects, features and advantages of the present invention will become more apparent in light of the following detailed description of a best mode embodiment thereof, as illustrated in the accompanying drawing.

Brief Description of the Drawings

Fig. 1 illustrates a remotely accessible document storage service and apparatus, according to the present invention, accessible over a network by various access devices.

Fig. 2A shows a flow chart executable in the remotely accessible document storage apparatus of Fig. 1 for receiving and handling a retrieval request.

Fig. 2B shows a flow chart executable in the remotely accessible document storage apparatus of Fig. 1 for receiving and handling a storage request.

Fig. 2C shows a flow chart executable in the remotely accessible document storage apparatus of Fig. 1 for handling an enrollment request.

Fig. 2D shows a flow chart executable in the remotely accessible

document storage apparatus of Fig. 1 for handling a request for a certificate from a government entity.

Fig. 2E shows storage of warranty or service information and notification of timed event information relating thereto to a user.

Detailed Description

Fig. 1 shows a remotely accessible document storage service and apparatus 10, according to the present invention. It is accessible over a network 12 to a plurality of access devices 14, 16, 18, 20, 22 for storing and gaining access to documents stored in the remotely accessible document storage apparatus 10. The network may be any kind of network or combination of networks known in the art.

The remotely accessible document storage apparatus 10 includes a virtual safety deposit box 24, a service desk 26, and a plurality of safety deposit boxes 28. The remotely accessible document storage apparatus 10 may be located at a facility that users may visit for the purpose of having their original legacy documents scanned and stored electronically in the virtual safety deposit box. They may also rent and physically store the original legacy documents in one of the safety deposit boxes 28. An attendant at the service desk enrolls a new user as a user of the virtual safety deposit box and issues the new user an access authentication protocol such as a personal identification number or other method of authentication such as voice print, fingerprint, retinal scan or the like. A given enrolled user will hand over one or more legacy documents to the attendant at the service desk who will then scan the legacy documents using a device 30, such as a scanner, and will categorize the documents according to type. It should be realized that the device 30 need not be a scanner but could be any kind of device for receiving or originating a digital signal representation of a legacy document. The various types available for categorization can be selected from a standard list provided by the service or may be supplied by the user. The digital signal representations, such as scanned documents, are provided in electronic form on a signal line 32 to a personal computer 34 where they are temporarily

stored before being transferred to the virtual safety deposit box 24. Upon receipt of a transfer command, the temporarily stored documents are transferred on a signal line 36 to a signal processor 38 in the virtual safety deposit box. The signal processor includes one or more input/output (I/O) devices 40, 42, 44, 46 connected to a data, address, and control bus 48 which is also connected to a read only memory 50, random access memory 52 and central processing unit 54. This general purpose signal processor 38 is used to receive the documents stored on the PC 34 and transferred on the line 36 via the I/O port 40 and to store same temporarily in the random access memory 52. The user's "legacy" documents are then transferred from the RAM 52 via I/O port 44 to one of a plurality of mass storage devices 56 where they can reside indefinitely in a safe and secure environment. The legacy documents stored on the mass storage device 56 are accessible and locally manageable from a keyboard 58 and display 60 which are connected to the signal processor via the I/O port 42. The virtual safety deposit box 24 is remotely accessible to the access devices 14, 16, 18, 20, 22 by means of one or more communications devices 62 connected to or connectable to the network 12 by one or more signal lines 64. The communications devices 62 are connected to the signal processor 38 via the I/O port 46 by means of a plurality of signal lines 66.

Likewise, the service desk includes a keyboard 68 and display 70 connected to the personal computer 34 by which access to the virtual safety deposit box can be made by the attendant. Once a user has stored a legacy document or a plurality of such documents in the virtual safety deposit box, he or she can return to the service desk at a later time and request the attendant to retrieve one or more of the stored legacy documents after giving the attendant the requisite access authentication. This is symbolized in Fig. 1 by a block 72 connected to the personal computer 34. This may be a fingerprint scanner, a retinal scanner, or may simply constitute a keypad entry or handing over of a personal identification number to the attendant who will then enter same on the keyboard. The user and the attendant can together pinpoint the desired document for retrieval over the line 36 from one of the mass storage devices 56 via the signal processor 38 for printing on a printer

74. The desired document, once printed, can then be handed over to the user. Or, the user can designate a recipient and mailing address to the attendant who can enter same on the keyboard for controlling the printer to provide the printout to an inserter 76 under the control of the personal computer 34 for inserting the printout in an envelope, finishing the envelope for mailing and sending same to a Post Office or carrier by physical transfer thereto as symbolized by a line 82. A recipient 83 at the mailing address receives the printout by post or carrier, as designated. It should be realized that the printer/inserter/finish devices can be located elsewhere than the service desk.

The virtual safety deposit box 24 is remotely accessible to the various access devices 14, 16, 18, 20 and 22 via the network 12 as described below. An individual user access device 14 is shown having a communications device, such as a communications device, 84 connected via line 86 to the network and by a line 88 to a personal computer 90 which may be utilized by the individual user via a keyboard 92 and display 94. The individual user can provide digital signal representations of legacy documents, e.g., by scanning legacy documents using a device 96, such as a scanner, for providing scanned, digitally encoded versions thereof on a signal line 98 to the personal computer 90 for a transfer on the signal line 88 to the communications devices 84 for transfer on the line 86 to the network 12 and on the line 64 to the virtual safety deposit box 24 where it is received and stored in a manner similar to that already described for the service desk. This can be done either automatically as described subsequently in connection with Fig. 2B or it can be done interactively between an attendant using the keyboard 58 and display 60 and the individual user using the access device 14. It should be realized that the device 96 can be any kind of device for receiving or originating a digital signal representation of a legacy document. Before or after providing the digital signal representations of legacy documents, the individual user may apply a selected form of document authentication such as a digital signature or some other form of electronic source certification to the scanned document. Prior to establishing a connection to the virtual safety deposit box, the individual user may enter an access authorization code via

the keyboard 92 or some other form of access authentication entered via an access authentication device 102 connected to the personal computer 90. Such may include voice prints, fingerprints, retinal scans and the like. The purpose of such access authentication is for the apparatus 10 to ensure that access is only granted to authorized users. It may be unidirectional or interactive. The keyboard 92 or access authentication device 102 may also be used for gaining different levels of access via different privilege codes that may be established under the control of the individual user in conjunction with the remotely accessible document storage service and apparatus.

When the individual user subsequently desires to retrieve a legacy document from the virtual safety deposit box 24, access is gained using an access authorization code or access authentication device as described and the requested documents are retrieved from one of the mass storage devices 56 and transferred over the network 12 to the individual user access device 14 and printed on a printer 104. On the other hand, the individual user can direct the remotely accessible document storage service to transfer the retrieved document to another access device such as a remote service desk 22 similar to the service desk 26 except located at or near a central hub of a overnight carrier for example. The remote service desk 22 can then print the document, insert it into an envelope and physically transfer same as indicated on a line 106 to a Post Office or carrier hub 108 for delivery to a recipient 83 designated by the user.

Referring now to Fig. 2A, a series of steps are illustrated for execution by the signal processor 38 of Fig. 1 for handling retrieval requests, storage requests, enrollment requests, and the like from users. It should be realized that the steps shown are merely illustrative of one of many ways to carry out the present invention, and that the various steps shown can be deleted, augmented, rearranged, etc. After entering in a step 110, the signal processor receives an access request from the network on a line 64 via the communications devices 62 and the signal line 66. This will include access authentication such as an access authorization code which is checked in step 114. If not authorized, as determined in a step 116, access is denied in a step 118 and a return is made in a step 120. If authorized, the request is

evaluated in a step 122. One evaluation could be whether the authorized access request authorizes access to all legacy documents of the user or whether the access request is limited by one of a plurality of possible privilege levels with different legacy document categories at each level. Privilege levels can be embedded in access authorization codes to provide limited access to third parties to specified categories of user legacy documents. A step 124 determines if the access privilege is legitimate and if not, access is denied in the step 118 and a return made in step 120. If the access privilege is identified and is satisfactory, a step 126 is executed in which it is determined whether the access request is a retrieval request. If so, a step 128 is executed to retrieve the requested document or documents from storage at the privileged level. A step 130 then determines if there is a print request and if so, it is determined whether the document is to be printed locally, e.g., at the service desk 26 or remotely. If locally, the document is sent to the service desk where it is printed in a step 134 and handled as described above, for example, by insertion 76 and finishing 78 for transfer 82 to a carrier 80 for physical delivery to a designated recipient 83. If the printing is to take place remotely or if the printing is not requested, the retrieved documents may be encrypted as indicated in a step 136 and transferred via the network 12 to the authorized requester as indicated in a step 138. A return is then made in the step 120.

If, on the other hand, the step 126 determines that the access request is not a retrieval request, a series of steps illustrated in Fig. 2B may be executed instead, for a storage request. First, a decision step 140 is executed to determine if the access request is in fact a storage request. If so, the remotely accessible document storage service 10 responds to the authorized user with a request to the user for transfer of electronic versions of legacy document to be stored. Such documents are then sent by the user to the apparatus 10 via the network 12 and received as indicated in the step 142. If encrypted, they are decrypted in a step 144 and stored in one of the mass storage devices 56 and indexed according to the user's preferences as indicated in a step 146 after which a return is made in a step 148. If the access request is determined in the step 140 not to be a storage request, a

series of steps illustrated in Fig. 2C are executed instead, e.g., for an enrollment request. A prospective user can obtain a temporary enrollment access authorization code, e.g., by calling an 800 number of the remotely accessible document storage service 10. A step 150 determines whether the access request is an enrollment request and if so, executes an interactive enrollment process in which the prospective user is given an access authentication methodology to follow such as instructions on using permanent access authorization codes or the like associated with a new account. The user can specify categories of documents to be stored and, once enrolled, a return is made in a step 154 and the enrolled user can now send documents for storage over the network 12 as already described in connection with the individual user access device 14 of Fig. 1.

If the access request evaluated in the decision step 150 is determined not to be an enrollment request, another set of alternative steps as illustrated in Fig. 2D may be executed instead. For instance, a decision step 156 will be executed to determine if the access request is a request from a user for access to a government entity 16 such as illustrated in Fig. 1 for retrieving a certified government document such as a birth certificate from a state government entity established for keeping records of this kind and issuing certificates to persons entitled to receive same. If so, the remotely accessible document storage service 10 contacts the government entity 16 via the network 12 and transmits the access request with authorization according to the protocol established between the government entity 16 and the service 10. For instance, the protocol could require that the service 10 provide the name, date of birth, place of birth, name of parents and a code indicating authorization according to the protocol established between the service 10 and the government entity 16. The government entity can require the service to establish proof of identity of the user during the enrollment process during which various vital statistics of the user are entered into the system. Such could include social security number, photo I.D., electronic fingerprint, retinal scan, palm print, and the like and can likewise require the service 10 to utilize specified access authentication of these kinds for gaining access. In this way, the remotely accessible document storage service 10 can establish with

virtual certainty the identity of various users requesting access to both legacy documents stored in the virtual safety deposit box 24 and/or requested and retrieval from government entities 16. Once an access request with proper access authentication is transmitted to the government entity 16 from the service 10, the government entity 16 retrieves the desired document in electronic form from its own storage system and affixes an electronic form of document certification as indicated in a block 160. If it is not already in electronic form, the certified document is originated, e.g., by scanning, as indicated in a block 160 and transferred on a line 164 to a personal computer 166 where it is temporarily stored prior to certification and transfer via the network 12. An operator at the government entity may use a keyboard 168 and display 170 for interfacing with the personal computer 166 for controlling the certification and transfer process indicated in Fig. 2D. Once the certified document is ready for transfer, the operator controls the transfer from the PC 166 to a communications device 172 which transfers the document or documents on a line 174 to the network 12 and then to the indicated recipient, whether it be an individual user, authorized third party 20, remote service desk 22 or for storage in the virtual safety deposit box 24. The certified document could also be transferred directly to one of the users. In any event, the document or documents are received as indicated in a step 160 in Fig. 2D which assumes that the remotely assessable document storage service and apparatus is the recipient. A determination is then made in a step 162 as to whether the received documents are to be transferred via post or carrier 108 or not. If so, a transfer is made to a local service desk 26 or remote service desk 22 for printout and physical transfer to the designated recipient 83. If not, the step 138 of Fig. 2A may be executed for sending the document or documents to an authorized requestor. On the other hand, as indicated previously, the retrieved document may simply be stored in one of the mass storage devices 56 of the virtual safety deposit box 24 of Fig. 1.

As also indicated previously, various access devices are contemplated according to the present invention. In addition to the individual user access device 14 and the government entity access device 16 already discussed above, additional access devices may be employed as well, including but not

limited to the community kiosk 18 shown in Fig. 1 and the authorized third party user access device 20. These various devices may have a structure similar to that already described in connection with the individual user access device 14 or the government entity access device 16. The community kiosk, for example, may be located in a public building such as a Post Office or a private carrier service or some other publicly accessible facility. The kiosk 18 may have a personal computer 176 having a keyboard 178 and display 180 connected thereto for community use. A user can enter access authentication via the keyboard 178 or via an access authentication device 182 to the PC 176. A scanner 184 may be used to scan legacy documents of a user for electronic storage temporarily in the personal computer 176. Once the user has finished scanning his or her legacy documents, the personal computer 176 transfers them via a communications device 186 over a signal line 188 to the network 12 for transfer on the line 64 to the remotely accessible document storage apparatus. There, the steps already described in connection with Fig. 2B for fulfilling a storage request are executed for storing the legacy documents of the user at the kiosk in one of the mass storage devices 56. On the other hand, a user of the kiosk can request the retrieval of a stored legacy document from the remotely accessible document service and apparatus 10 via the network and the steps 128 et seq. of Fig. 2A can be executed to retrieve and send a requested legacy document to an authenticated requester at the community kiosk 18. Once received by the personal computer 176, it can be printed on a printer 190 for use by the user of the kiosk 18.

Authenticated third parties may use access devices such as the access device 20 shown in Fig. 1 for retrieving legacy documents of other users as authorized by said other users by granting privileged access to selected categories of legacy documents. For instance, a user's attorney may be authorized to access a will of the user for use in drafting a new will or for use after the death of the user for probate. In that case, it is even contemplated that the remotely accessible document storage service 10 can establish protocols with government entities 16, in the form of various Probate Courts for storing wills which will be recognized for purposes of probate upon

retrieval from the virtual safety deposit box. Alternatively, the attorney 20 could utilize a keyboard 192 and display 194 at his location for accessing a personal computer 196 which in turn establishes a connection by means of a communications device 198 to the network 12 for accessing the desired probate document stored in one of the mass storage devices 56 by his client who is a user of the service 10 and who has authorized his attorney to access a category of documents designated as probate documents using an access authorization device 200 or a code entered by means of the keyboard 192 with the appropriate privilege level indicated for that category of documents. The attorney would then print out the will on a printer 202 at his location or direct that it be printed at a printer 204 at the government entity 16, in this case a Probate Court.

Finally, it should be realized that many uses of stored legacy documents can be contemplated beyond simple storage and retrieval. For instance, the legacy document could be warranty information on products purchased by a user, such as warranty card information taken from a paper warranty or encoded on a warranty card provided by the manufacturer and preloaded onto the warranty card. The remotely accessible document storage service could then be used to store proof of purchase and registration information, to maintain warranty files for each user, to inform the user when warranties are about to expire, or to enable the user to schedule maintenance, to apply for extended warranty or other service options and to alert customers to the availability of warranty or service contracts. These various other options can be easily executed within the apparatus 10 of Fig. 1. For instance, instead of branching to a return step from the step 156 of Fig. 2D after it is determined that access to a government entity is not requested, a branch can instead be made to a subroutine illustrated at Fig. 2E, where a check is made that is shown in a step 206 for a need to send a notification to a user, such as a timed event corresponding to expiration of a warranty or service contract. If it is determined that it is time to send such a notification as indicated in a step 208, the notification is sent as indicated in a step 210, after which a return is made in a step 212. If it is not time to send a notification, a step 214 could be implemented to determine if a user is making

an access request to enter timed event or warranty information. If so, a branch can be made to the steps of Fig. 2B to execute storage of such information. If not, a return can be made in the step 212. Thus, based on the storage of documents of various kinds, many useful services can be provided by the remotely-accessible document storage service and apparatus of the present invention.

Although the invention has been shown and described with respect to a best mode embodiment thereof, it should be understood by those skilled in the art that the foregoing and various other changes, omissions and additions in the form and detail thereof may be made therein without departing from the spirit and scope of the invention.

What is claimed is:

1. An apparatus accessible over a network by a plurality of users, comprising:

a mass storage device for storing user legacy documents; and

a signal processor connected to said mass storage device for receiving access requests over said network for storing said user legacy documents received over said network in said mass storage device and for retrieving said user legacy documents from said mass storage device for sending said legacy documents over said network, wherein each access request includes an access code for authenticating said access request and wherein said signal processor grants or denies said access request according to said access code.

2. The apparatus of claim 1, wherein an access request for access to a legacy document is for a governmental document stored at a governmental entity which provides electronic access to governmental documents, wherein said signal processor transmits an access request over said network to said governmental entity, wherein said governmental entity retrieves said governmental document and transmits said governmental document over said network with an electronic certification of authenticity to said apparatus or to an access device of a user or of an authorized third party requester.

3. The apparatus of claim 1, further comprising a service desk for receiving actual user legacy documents from users for scanning said actual user legacy documents and providing said actual user legacy documents in electronic form as scanned legacy documents for storage in said mass storage device.

4. The apparatus of claim 3, wherein said actual user legacy documents are stored in safety deposit boxes rented by said users.

5. The apparatus of claim 3, wherein said service desk is also for printing copies of said scanned legacy documents for delivery via post or carrier to a designated recipient.

6. The apparatus of claim 1, wherein said access request is from an authorized third party user for accessing legacy documents of another user.

7. The apparatus of claim 1, wherein said access request is from a community kiosk for use by plural users.

8. The apparatus of claim 1, wherein said access request is from an individual user.

9. The apparatus of claim 1, wherein said apparatus is for use in a system including plural access devices including access devices for individual users, government entities, community kiosks and authorized third party users.

10. The apparatus of claim 1, wherein said access request is for the apparatus to transmit said legacy documents over said network to a remote service desk for printing and delivery via post or carrier to a designated recipient.

11. The apparatus of claim 1, wherein said legacy documents include warranty or service information and wherein said apparatus transmits reminders and other status information relating thereto to said users.

12. An access device for accessing an apparatus over a network, said access device comprising:

a computer connected to various input and output devices including means for providing a digitally encoded legacy document signal to said computer, an access authorization entry means

responsive to a user input for providing an access authorization signal to said computer, a communications device responsive to an access request signal from said computer for transmitting said access authorization signal and said digitally encoded legacy document signal via said network to an apparatus for storing digitally encoded legacy document signals of users.

13. The access device of claim 12, wherein said access device further comprises a display or printer for displaying or printing a legacy document retrieved over said network from said apparatus in response to an access request signal from said computer.

14. The access device of claim 12, wherein said device is for use by an individual user.

15. The access device of claim 12, wherein said device is for use by a governmental entity.

16. The access device of claim 12, wherein said device is for use by a plurality of individual users.

17. The access device of claim 12, wherein said access device is located in a community kiosk.

18. The access device of claim 12, wherein said device is for use by an authorized third party user for accessing legacy documents of another user.

19. A method for a plurality of users to access documents over a network, said method comprising the steps of:

receiving requests over a network from users to store their legacy documents;

issuing users access codes to store and retrieve legacy documents;

storing users legacy documents;

receiving requests from users over a network for accessing legacy documents;

authenticating the user's access codes;

transmitting the requested legacy document to the user if the user's access code is correct; and

denying the user access to the requested legacy document if the user's access code is incorrect.

20. The method claimed in claim 19, wherein the transmitted legacy document is transmitted over a network.

21. The method claimed in claim 19, wherein the transmitted legacy document is physically delivered to the user requesting the document.

22. The method claimed in claim 19, further including the steps of:

receiving actual legacy documents from users;

scanning the legacy document;

storing the scanned legacy document in electronic form; and

returning the actual legacy document to the user.

23. The method claimed in claim 19, further including the steps of:

receiving actual legacy documents from users;

scanning the legacy document;

storing the scanned legacy document in electronic form;

returning the actual legacy document to the user; and

storing the actual legacy document.

24. The method claimed in claim 23, further including the steps of:

printing copies of the scanned legacy document; and

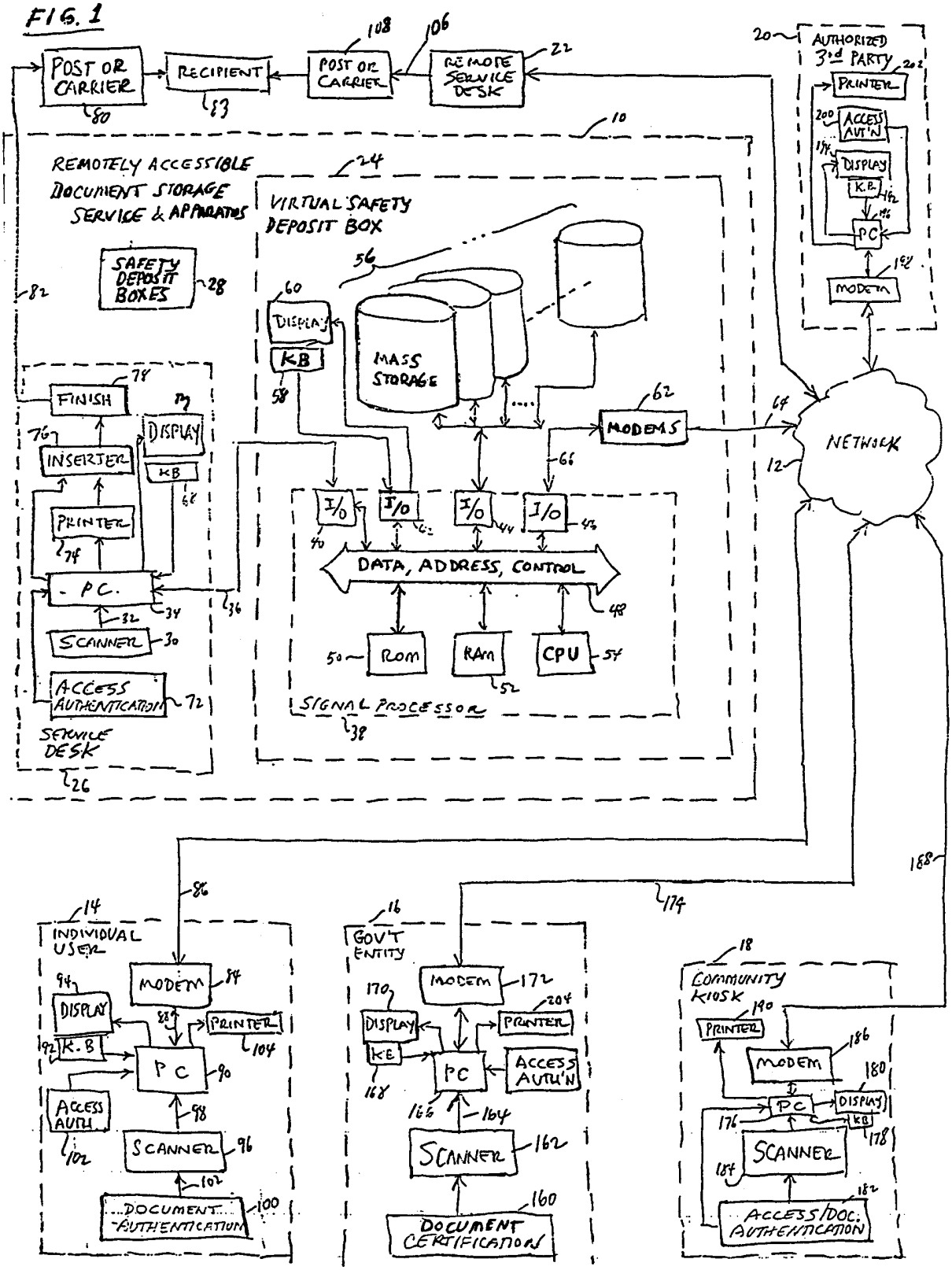
delivering copies of the printing document to user's designated recipients.

25. The method claimed in claim 19, wherein the access report is from an individual user.

26. The method claimed in claim 19, wherein the access request is from a governmental entity.

27. The method claimed in claim 19, wherein the access request is from a corporate user.

FIG. 1


POST OR CARRIER
80
RECIPIENT
83
POST OR CARRIER
108
106
REMOTE SERVICE DESK
22
AUTHORIZED 3rd PARTY
20
PRINTER
202
ACCESS AUT'N
200
DISPLAY
K.B.
PC
MODEM
REMOTELY ACCESSIBLE DOCUMENT STORAGE SERVICE & APPARATUS
10
VIRTUAL SAFETY DEPOSIT BOX
24
SAFETY DEPOSIT BOXES
28
82
56
60
DISPLAY
KB
58
MASS STORAGE
62
MODEMS
64
NETWORK
12
FINISH
74
76
INSERTER
PRINTER
DISPLAY
KB
PC
SCANNER
30
ACCESS AUTHENTICATION
72
SERVICE DESK
26
I/O
DATA, ADDRESS, CONTROL
ROM
RAM
CPU
54
SIGNAL PROCESSOR
38
INDIVIDUAL USER
14
MODEM
DISPLAY
K.B
PRINTER
PC
ACCESS AUTH
SCANNER
DOCUMENT AUTHENTICATION
100
GOV'T ENTITY
16
MODEM
172
DISPLAY
KB
PRINTER
PC
ACCESS AUTH'N
SCANNER
162
DOCUMENT CERTIFICATION
160
COMMUNITY KIOSK
18
PRINTER
MODEM
PC
DISPLAY
KB
SCANNER
ACCESS/DOC. AUTHENTICATION
182
174
188
86

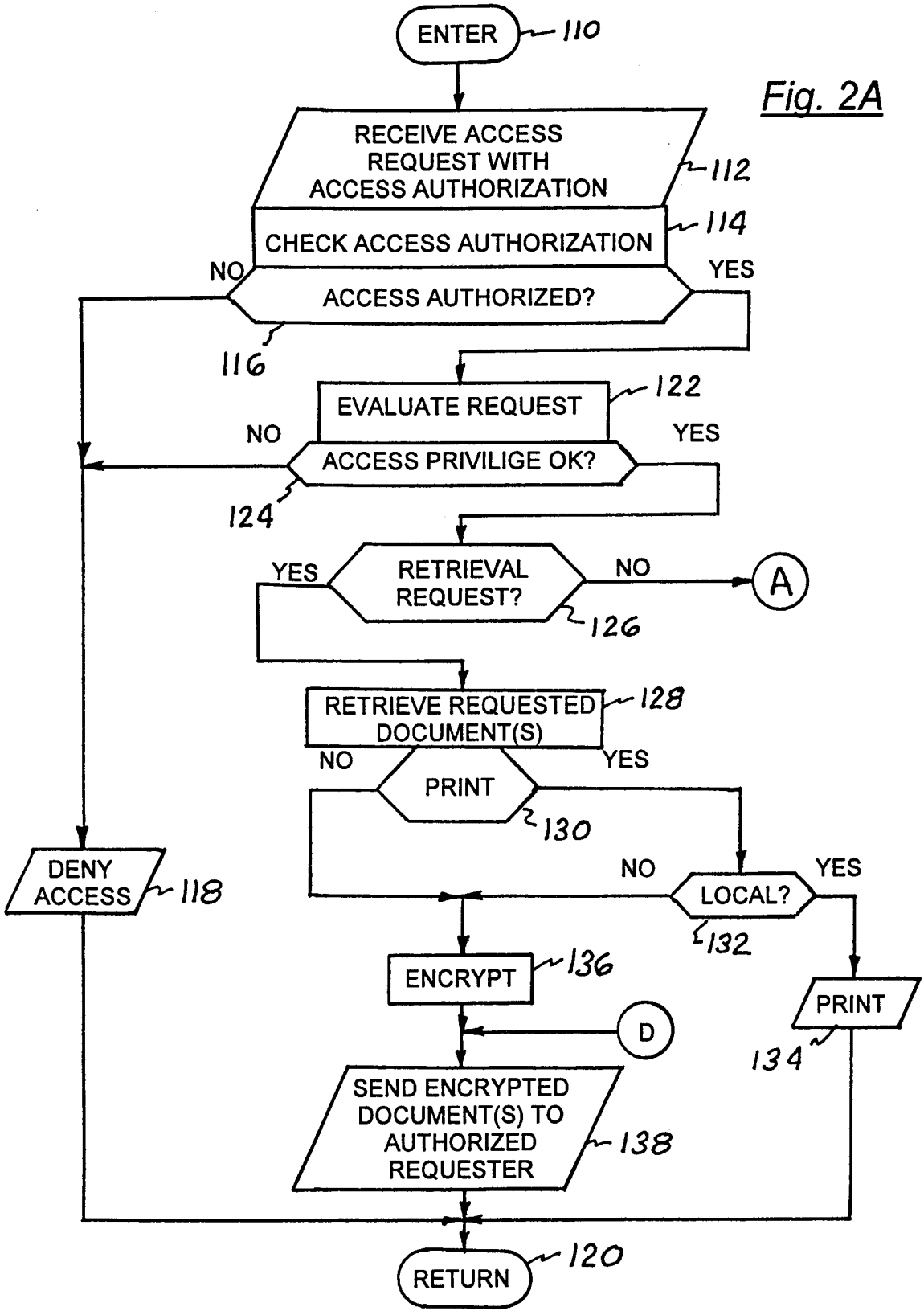

ENTER
110
RECEIVE ACCESS REQUEST WITH ACCESS AUTHORIZATION
112
CHECK ACCESS AUTHORIZATION
114
NO
ACCESS AUTHORIZED?
YES
116
EVALUATE REQUEST
122
NO
ACCESS PRIVILIGE OK?
YES
124
YES
RETRIEVAL REQUEST?
NO
A
126
RETRIEVE REQUESTED DOCUMENT(S)
128
NO
PRINT
YES
130
DENY ACCESS
118
NO
LOCAL?
YES
132
ENCRYPT
136
D
PRINT
134
SEND ENCRYPTED DOCUMENT(S) TO AUTHORIZED REQUESTER
138
RETURN
120

Fig. 2A

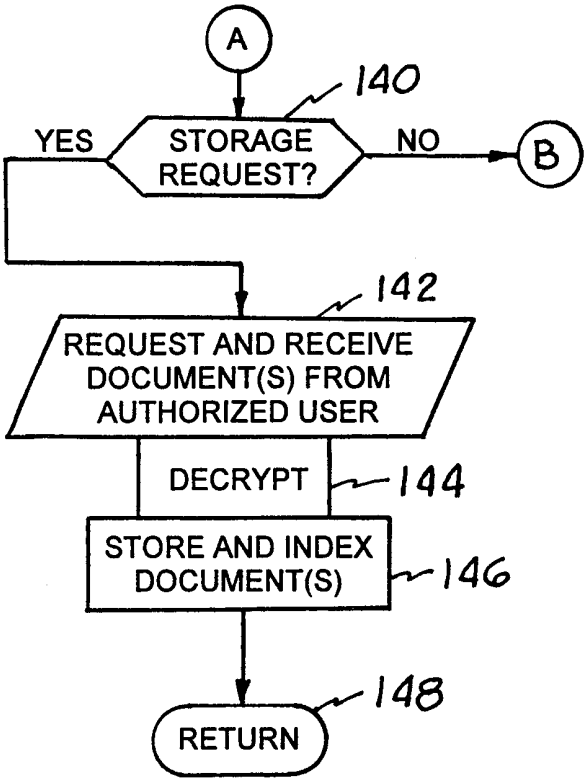

A
140
YES
STORAGE REQUEST?
NO
B
142
REQUEST AND RECEIVE DOCUMENT(S) FROM AUTHORIZED USER
DECRYPT
144
STORE AND INDEX DOCUMENT(S)
146
148
RETURN

Fig. 2B

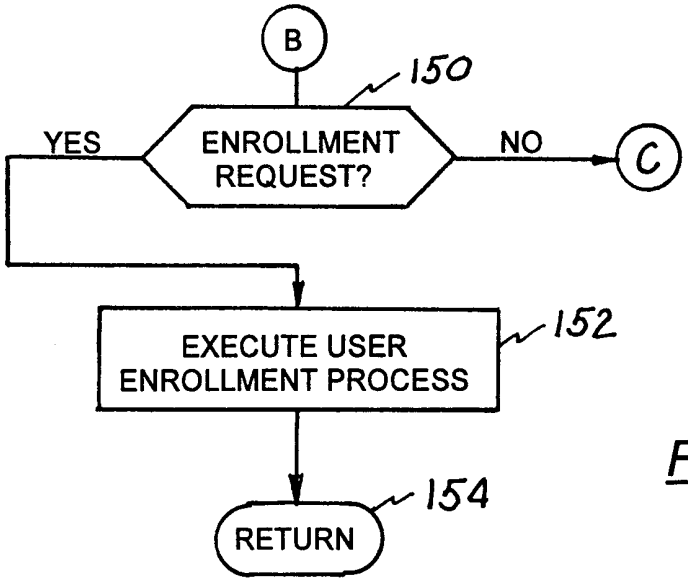

B
150
YES
ENROLLMENT REQUEST?
NO
C
EXECUTE USER ENROLLMENT PROCESS
152
154
RETURN

Fig. 2C

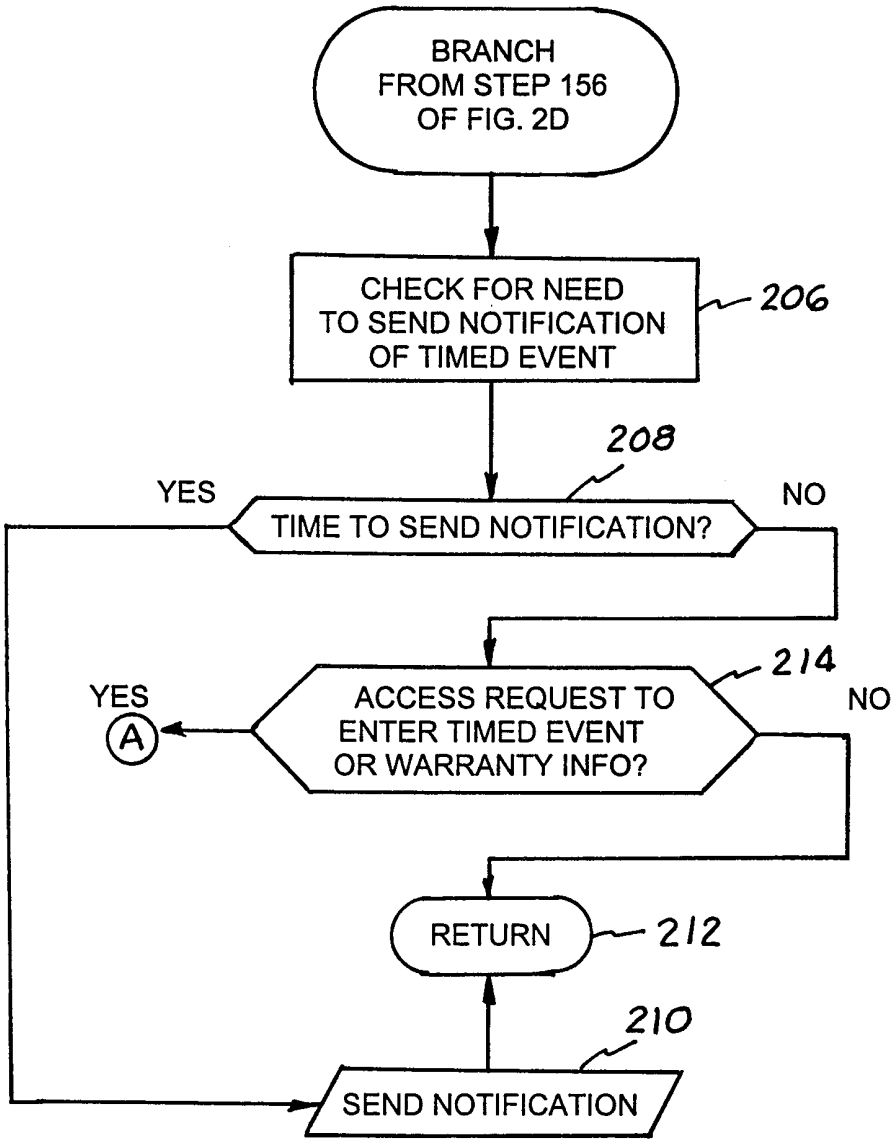

BRANCH FROM STEP 156 OF FIG. 2D
CHECK FOR NEED TO SEND NOTIFICATION OF TIMED EVENT
206
208
YES
TIME TO SEND NOTIFICATION?
NO
214
YES
A
ACCESS REQUEST TO ENTER TIMED EVENT OR WARRANTY INFO?
NO
RETURN
212
210
SEND NOTIFICATION

FIG. 2E

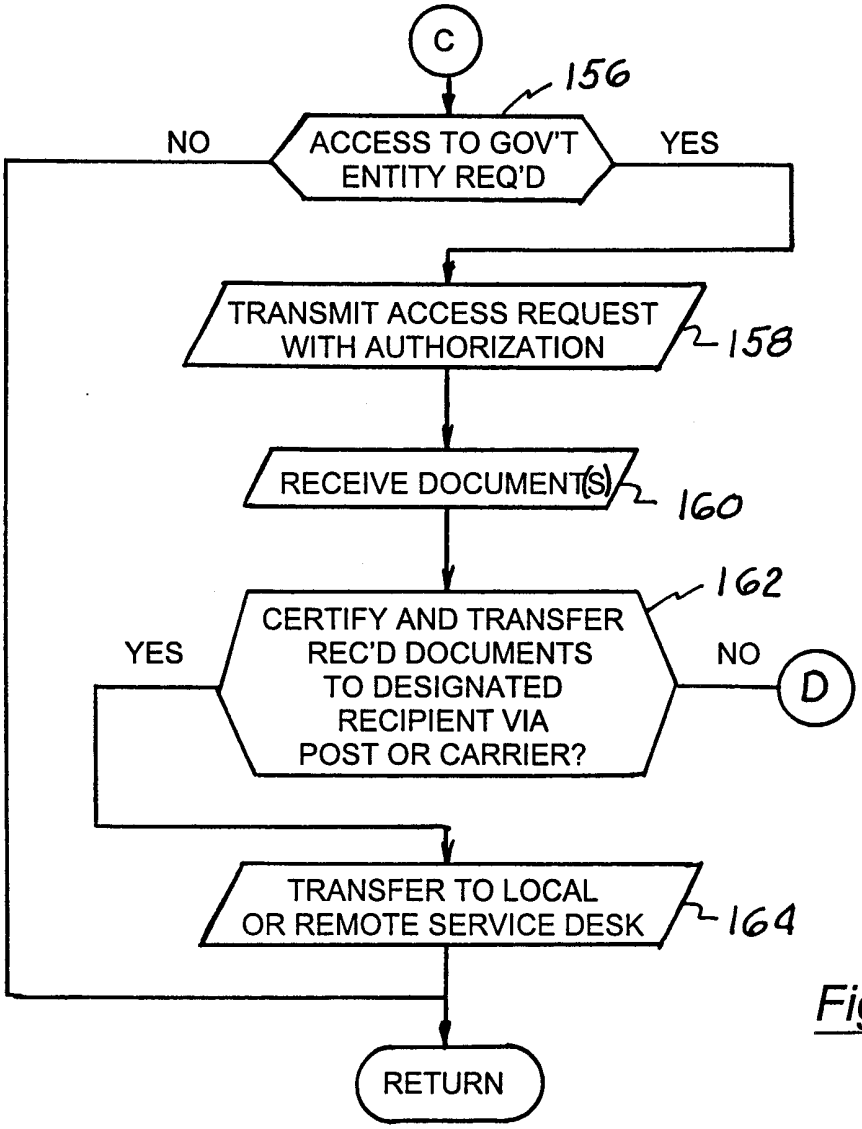

C
156
NO
ACCESS TO GOV'T ENTITY REQ'D
YES
TRANSMIT ACCESS REQUEST WITH AUTHORIZATION
158
RECEIVE DOCUMENT(S)
160
162
YES
CERTIFY AND TRANSFER REC'D DOCUMENTS TO DESIGNATED RECIPIENT VIA POST OR CARRIER?
NO
D
TRANSFER TO LOCAL OR REMOTE SERVICE DESK
164
RETURN

Fig. 2D

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/07437

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G 06 F 12/14; G 06 F 17/21; G06 F 17/60

US CL : 713/189; 705/2, 51; 707/500

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/156, 162, 163, 165, 168, 183, 184, 189, 193; 705/2, 51; 707/500, 526

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P --- Y,P	US 6,018,713 A (COLI et al.) 25 January 2000 (25.01.00), col. 3, lines 6-10 and 46-65, col. 4, lines 36-67, col. 5, lines 7-13 and 58-65, and col. 6, lines 1-17 and 42-65.	1, 3, 6-9, 12, 14-20, 22, 23, 25-27 --- 2, 4, 5, 10, 11, 13, 21, 24
X --- Y	Internet FileZone. Products [online], 27 April 1998 (27.04.98) [retrieved on 2000-06-16]. Retrieved from the Internet: <URL: http://www.i-filezone.com/products.html>, entire document.	1, 3, 6, 7, 8, 12, 14, 16, 17, 18, 19, 20, 25, 27 --- 2, 4, 5, 9, 10, 11, 13, 15, 21, 22, 23, 24, 26
L	Business Wire, "Atrieva Corporation Ships Atrieva Anywhere: Browser-Based File Access for Remote and Mobile Professionals," 27 April 1998 (27.04.98), p. 4271303.	1-27
L	Internet FileZone. About Us [online], 27 April 1998 (27.04.98)[retrieved on 2000-06-16]. Retrieved from the Internet: <URL: http://www.i-filezone.com/about_us/042798pr.html>, entire document.	1-27
Y,P	US 5,982,956 A (LAHMI) 09 November 1999 (09.11.99), col. 1, lines 6-8 and 21-23.	2

☒ 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 application or patent 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
30 June 2000 (30.06.2000)	23 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod R. Swann Telephone No. (703) 305-9700

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/07437

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,852,665 A (GRESSEL et al.) 22 December 1998 (22.12.98), col. 20, lines 66-67, column 21, lines 1-2, and figure 11, step 600.	4
Y,P	US 5,953,392 A (RHIE et al.) 14 September 1999 (14.09.99), col. 1, lines 18-25, col. 4, lines 27-33, and figure 2, items 26, 34.	5, 10, 13
Y	US 5,717,989 A (TOZZOLI et al.) 10 February 1998 (10.02.98), col. 1, lines 5-6, col. 16, lines 12-41, and figure 3B, step 820.	5, 10, 21
Y,P	US 6,014,135 A (FERNANDES) 11 January 2000 (11.01.00), col. 4, lines 17-21, col. 10, lines 29-47, col. 12, lines 57-67, figure 4, item 46E, and figure 5.	24