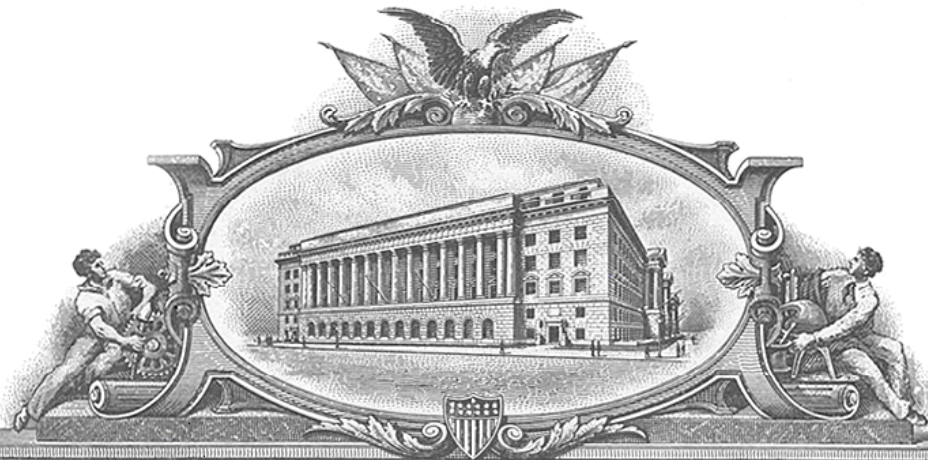


7402753



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

February 18, 2013

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: *09/182,342*
FILING DATE: *October 29, 1998*
PATENT NUMBER: *6370629*
ISSUE DATE: *April 09, 2002*



Certified by

David J. Kappas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

A

FISH & RICHARDSON P.C.

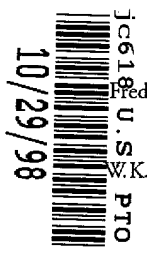
225 Franklin Street
Boston, Massachusetts
02110-2804

Telephone
617 542-5070

Facsimile
617 542-8906

Web Site
www.fr.com

U.S. PTO
09/182342



Frederick P. Fish
1855-1930
W.K. Richardson
1859-1951

October 29, 1998

Attorney Docket No.: 06175/006001

Box Patent Application

Assistant Commissioner for Patents
Washington, DC 20231

Presented for filing is a new original patent application of:

Applicant: THOMAS MARK HASTINGS, MICHAEL E. MCNEIL,
TODD S. GLASSEY AND GERALD L. WILLETT
Title: CONTROLLING ACCESS TO STORED INFORMATION

Enclosed are the following papers, including those required to receive a filing date under 37 CFR §1.53(b):

	<u>Pages</u>
Specification	13
Claims	7
Abstract	1
Declaration	2
Drawing(s)	6

Enclosures:

- Small entity statement. This application is entitled to small entity status.
- Assignment cover sheet and an assignment, 4 pages, and a separate \$40.00 fee.
- New disclosure information, including:
Information disclosure statement, 1 pages.
PTO-1449, 1 pages.
References, 4 items.
- Postcard.

"EXPRESS MAIL" Mailing Label Number EM5291829205

Date of Deposit OCTOBER 29, 1998
I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office To Addressee" with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Ambrose Meau
Ambrose Meau

BOSTON
NEW YORK
SILICON VALLEY
SOUTHERN CALIFORNIA
TWIN CITIES
WASHINGTON, DC

FISH & RICHARDSON P.C.

October 29, 1998

Page 2

Basic filing fee	395.00
Total claims in excess of 20 times \$11.00	88.00
Independent claims in excess of 3 times \$41.00	82.00
Fee for multiple dependent claims	0.00
Total filing fee:	\$ 565.00

A check for the filing fee is enclosed. Please apply any other required fees or any credits to Deposit Account No. 06-1050, referencing the attorney docket number shown above.

If this application is found to be incomplete, or if a telephone conference would otherwise be helpful, please call the undersigned at 617/542-5070.

Kindly acknowledge receipt of this application by returning the enclosed postcard.

Please send all correspondence to:

David L. Feigenbaum
Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804

Respectfully submitted,



David L. Feigenbaum
Reg. No. 30,378

Enclosures

330306.B11

BOSTON ATTORNEYS

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: CONTROLLING ACCESS TO STORED INFORMATION

APPLICANT: THOMAS MARK HASTINGS, MICHAEL E. MCNEIL, TODD S. GLASSEY AND GERALD L. WILLETT

"EXPRESS MAIL" Mailing Label Number EM529182192US

Date of Deposit OCTOBER 29, 1998
I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office To Addressee" with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Ambrose Mema
AMBROSE MEMA

36507 248260

CONTROLLING ACCESS TO STORED INFORMATION

Background

5 This invention relates to controlling access to stored information.

Data distribution media, such as a CD-ROM, can store a large number of files. The producer of the CD-ROM may wish to control access by users to particular files, either
10 because they are confidential or because access is subject to payment by the user.

Access may be controlled by requiring a user to enter a password obtained from the CD-ROM producer. Different passwords may unlock different files or different
15 subsets of files. The files may be cryptographically signed and for added protection, may be encrypted. In the scheme discussed in U.S. Patent 5,646,992, incorporated herein by reference, each file is encrypted by the producer with a unique key known only to the producer. The user receives
20 the encrypted items and, after his request for access is processed by the producer, also receives decryption keys, i.e., passwords, which are used to decrypt the respective encrypted files. The passwords unlock only those files for which access has been requested.

25 Summary

In general, in one aspect of the invention, the invention features controlling access to stored information by determining an actual geographic position where the stored information is located based on signals received at a
30 receiver supplying reliable position information. The actual geographic position is then compared with a geographic region within which access to the stored

SECRET

information is authorized. The user is permitted access to the stored information if the actual geographic position is located within the authorized geographic region.

Embodiments of the invention include the following features. The receiver that supplies the position information can receive the position information from a satellite-based location determination system or an inertial navigation system. The information can be stored on a computer-readable medium, such as a high-capacity disk. The stored information includes files and each of these files has an associated geographic region within which access is permitted. The user has access to a specific file or files if the actual geographic position is located within the authorized geographic region for this file. The stored information can be encrypted, and the user has access to the decryption key only if the actual geographic position is located within the authorized geographic region. The stored information can also be divided into subsets of information and wherein at least one the subsets has a different authorized region from the other subsets. The association of the files with the authorized geographic regions can be stored as a policy file together with the stored information.

In general, in another aspect, the invention features determining an actual date or time at the location of the stored information based on signals received at a receiver supplying reliable time information. The actual date or time is compared with a predetermined date or time interval at which access to the stored information is authorized. The user can access the stored information if the actual date or time occurs within the authorized date or time interval.

In general, in another aspect, the invention includes a receiver supplying reliable position information for determining an actual geographic position where the stored information is located. A computer receives the position information with a geographic region within which access to the stored information is authorized and permits access to the stored information if the actual geographic position is located within the authorized geographic region.

Embodiments of the invention include the following features. The receiver includes a receiver encryption mechanism for cryptographically signing the actual geographic position with a receiver encryption key and verifying the receiver signature with a receiver decryption key before the actual geographic position is compared with the authorized geographic region.

In general, in yet another aspect, the invention includes a reader with a corresponding receiver decryption key for verifying the cryptographically signed actual position.

Embodiments of the invention include the following features. The reader generates an initialization vector providing a position offset which is transmitted to the receiver and added to the actual geographic position. The reader cryptographically signs the position offset with a reader encryption key. The receiver verifies the position offset signature with a corresponding reader decryption key before the position offset is added to the actual geographic position.

In general, in another aspect, the invention features forming a policy associating the information with authorized geographic regions and authorized time intervals and cryptographically signing the policy and the information. The signed policy is stored together with the

SECRET

signed information. The user obtains from the producer a password for unlocking the policy and obtains access to the stored information if the actual geographic position and actual time falls within the authorized geographic regions and authorized time interval of the policy.

Among the advantages of the invention are one or more of the following.

A producer of stored information can restrict use of that information to designated geographic regions or can exclude designated regions where use is not permitted. For example, a service manual for an automobile stored on a CD-ROM may contain differnt sections of information which are applicable to corresponding specific countries and/or regions. A user may be permitted to see only the portion of the information which is applicable to his current geographic location. Likewiese, access to a sensitive corpoarte report may be limited to specific plant location. Access to time-sensitive information may be denied before or after a certain date or limited to a permitted period. By associating information about authorized geographic regions and time intervals with policy files stored on the CD-ROM and accessed with a user password, the CD-ROM producer can issue a new password to permit the user to access a particular set of policy files, and therefore the information authorized, for a corresponding region and date/time.

Other advantages and features will become apparent from the following description and from the claims.

Description

FIG. 1 is a perspective view of a computer system;
FIG. 2 is a block diagram of a computer-based system for controlling access to stored information;

FIGS. 3 through 5 are flow diagrams;

FIG. 6 is a block diagram of cryptographic elements.

As seen in FIGS. 1 to 3, access to information which is stored on a portable computer-readable CD-ROM which

5 serves as a data distribution media 35, may be controlled based on an actual geographic position of a computer system 10 on which the information is to be accessed and the time when it is to be accessed.

10 In computer system 10, a computer 20 is connected to a keyboard 50, a mouse 60, a monitor 40, and a CD-ROM drive 30. A GPS receiver 70 serves as a source of reliable position and time information. The receiver 70 is located at the actual geographic position of the computer system 10 and receives signals 75 from orbiting GPS satellites 90
15 (only one shown). The receiver 70 converts the received signals 75 to geographic position data 71 to an accuracy of several meters in longitude, latitude and height and to date/time data 71 to an accuracy of microseconds. The data 71 are transmitted to the computer 20 via a device driver
20 72.

A receiver crypto-board 80 may contain a public-key certificate 81 signed by the producer and a corresponding private key 82, as shown in FIG 6. The geographic position and date/time data 71 may then be signed with the private
25 key 82 to authenticate the data.

The CD-ROM drive 30 may also include encryption and signature capabilities (decoder 32) which may be implemented either in hardware or in software. The decoder 32 includes a crypto-board public-key certificate 83 which is identical
30 to certificate 81, a producer certificate 84 for verification of the producer's identity, and a distribution media policy decryption key 86 signed by the producer, as shown in FIG. 6. The crypto-board certificate 83 verifies

the signature of the crypto-board 80 signed with the private key 82. The policy decryption key 86 decrypts the access policy 155 stored on the CD-ROM 35.

5 The computer system 10 can have several levels of security, such as Level 1 and Level 2, described in the following examples.

10 In a system with Level 1 security, the receiver 70 communicates with the computer 20 via a conventional device driver 72 and the CD-ROM drive 30 is a conventional CD-ROM. Neither the receiver 70 nor the CD-ROM drive 30 have additional encryption/decryption capabilities. For increased security, the computer 20 in a Level 1 system can be a "trusted" computer which can authenticate and/or encrypt data. In a more secure, Level 2 system, the receiver 70 may include a crypto-board 80 and the CD-ROM drive 30 may include a decoder 32. The Level 2 system is designed to provide data authentication and encrypted data transmission between the receiver 70 and the decoder 32. The computer 20 can then be any commercial computer without data authentication and encryption.

20 Data entered via the keyboard 50 and mouse 60 may include typical command and data input 130 entered via a user interface 95 (provided by an application program 34) and one or more passwords 130 that permit a user to gain access to information stored on the data distribution media 35.

30 The CD-ROM 35 stores different types of information, such as files with information 144, a list 150 of authorized geographic regions, a list 154 of authorized date/time intervals, one or more file decryption key files 146, one or more policy files 152 and a signature 147 for the entire CD-ROM 35. As seen in FIG. 3, the files 144, 146, 150, 152, 154 and 155 may be signed and encrypted.

The files 144 may be grouped in subsets 141, 142 and 143. Files may belong to more than one subset. (In the following discussion, the term file refers to both files and subsets of files.) Each file 141, 142 and 143 may be

5 encrypted with a unique file encryption key 51 (E_1, E_2, E_3). The corresponding file decryption keys 52 (K_1, K_2, K_3) are stored on the CD-ROM 35 in the file decryption key file 146. Additional information about the decryption keys and the decryption key file are found in U.S. Patent 5,646,992.

10 Each file 141, 142 and 143 on the CD-ROM 35 is associated with zero, one or more of the authorized geographic regions stored in the list 150 of authorized geographic regions. For example, a region may be bordered by latitudes and longitudes corresponding to the extent of

15 the Empire State Building in New York City and an altitude of between 50 and 60 meters, so that the file associated with that region can only be opened if the receiver 70 is located in a certain office area inside the Empire State Building.

20 Likewise, each file 141, 142 and 143 is associated with zero, one or more of the authorized date/time intervals stored in the list 154 of authorized date/time intervals.

Each GPS satellite 90 maintains an extremely accurate clock. The receiver 70 receives the GPS clock

25 signals as part of signals 75, or a local atomic clock can provide similar clock signals. The clock signals enable control of access to the information based on the actual time when access to the information is attempted. For example, the producer can specify that access is to be

30 granted only (1) before a predetermined date/time; (2) after a predetermined date/time; or (3) only during a predetermined date/time period.

The producer can associate the files 141, 142 and 143 with specific items in the lists 150 and 154 via a password 130 which the user enters via keyboard 50. The password 130 can be a user password valid for more than one access, or can be a one-time password. Alternately, the producer can associate specific geographic region/date/time information of lists 150 and 154 with the files 141, 142 and 143 via the policy files 152. A valid user password 130 may unlock one or more policy files 152. If the user's actual geographic position and the current date and time are within the authorized geographic region and the authorized date/time corresponding to the user password 150, then the user can access the selected files via the user interface 95. The selected information is then displayed on output device 40.

Table 1 shows, as an example, how five encrypted files, A to F, stored on the CD-ROM 35 and associated with corresponding authorized geographic regions and dates/times, can be accessed. Each file is associated with one of four different file decryption keys K1 to K4. L1 and L2 are two different authorized geographic regions and T1, T2 and T3 are three different authorized date/time intervals. The user who is in possession of the file decryption key K1, e.g., a password, can decrypt Manual A within the geographic regions L1 and L3 at time T1. The same user can also decrypt Manual D at the same time T1 in regions L2 and L3, but not within region L1. Likewise, the user who has key K2 can decrypt Image B and Image E within the region L2, but not at the same time. Drawing C can be decrypted with key K3 at any location, but only at time T3, while the Business Report F requires key K4 and can be decrypted at any time, but only within the region L1.

Table 1

Encrypted File	File Decryption Key	Authorized Geographic Regions	Authorized Date/Time Intervals
Manual A	K1	L1, L3	T1
Image B	K2	L2	T1, T3
Drawings C	K3	--	T3
Manual D	K1	L2, L3	T1
Image E	K2	L2	T2
Report F	K4	L1	--

As shown in FIG. 3, for purposes of cryptographic signature with optional encryption, the producer selects source files 144' to be written on the CD-ROM 35 and specifies a list of authorized geographic regions 150' and a list of authorized date and time intervals 154'. The producer associates (as shown in Table 1) each file or subset of files with zero, one or more geographic regions 150' and zero, one or more date/time intervals 154' and stores this association in a policy file 152'. Each of the files 144', 150', 152', 154' can be signed and encrypted in steps 53, 340, 350 and 360 with corresponding encryption keys 51, 345, 355 and 365, respectively. The corresponding encrypted files 150, 152 and 154 are then stored together on the CD-ROM 35 as a signed, encrypted region/time/file access policy 155. Also stored on the CD-ROM 35 are, as mentioned above, the signed/encrypted files 144, the signed/encrypted symmetric file decryption key file 146 and the signature 147 used by the producer to sign the entire CD-ROM 35.

As seen in FIGS. 4 and 5, to gain access to the signed/encrypted files 144, the user obtains a password 130

(FIG. 2) from the producer (step 400), and enters the password 130 via the keyboard 50 (step 410). The password 130 is assumed to be a one-time password, although user passwords valid for more than one session can also be used.

5 As seen in FIG. 4, the early portions of the process flow for Level 1 and Level 2 are almost identical.

Step 420 checks the password 130 and the process then executes either 440 (for Level 1, with no additional security) or to 450 (for Level 2, with receiver/CD-ROM drive security), depending on the system configuration. Details
10 of steps 440 and 450 are shown in FIG. 5 and will now be discussed.

As seen in FIG. 5, in process 440 the user password 130 is sent to the device driver 72 (step 510). In response
15 to the one-time password 130, the device driver 72 generates from the user's password 130 its own one-time password (step 520) and verifies (step 530) that the user did indeed enter a correct one-time password 130, thus authenticating the user for the interactive session (step 532). Otherwise,
20 access is denied (step 535).

Once the password 130 has authenticated the user, the device driver 72 interrogates the receiver 70 for the current position and date/time (step 540). The device driver 72 then compares the time and position data returned
25 by the receiver 70 with the policy 155 which applies to the files 144 or a subset 141, 142 and 143 of files (step 460). If the user is authorized to access the files 144, then the data is unlocked, decrypted (step 470, FIG. 3) with decryption keys 52 (step 480) and supplied to the user's
30 application program 34 (step 490) and displayed.

In a Level 2 system, the receiver 70 includes the cryptographic receiver board 80, hereafter referred to as "crypto-board". As mentioned before, crypto-board 80 can

sign and encrypt/decrypt messages. The CD-ROM drive 30 includes decoder 32 to decode the position data signed by and received from the crypto-board 80.

As seen in FIG. 5, in process 450, the user's password 130 is sent to the device driver 72, which accepts the password 130 and passes it through unaltered to the decoder 32 (step 550). The driver 32 then internally generates with the private key 86 its own one-time password corresponding to the user's password (step 560) and verifies (step 570) that the correct password 130 was communicated by the device driver 72, thus authenticating the user for the interactive session (step 572). Otherwise, access is denied (step 575).

Once the encryption circuit 32 has authenticated the user, the driver 32 interrogates the crypto-board 80 via the device driver 72 for the current time and position information from receiver 70 (step 580). The decoder unit 30 provides the crypto-board 80 with a signed random or other bit pattern to form an "initialization vector" (step 590), i.e., a position offset, which the device driver 72 passes through the crypto-board 80 along with the request for the time and position (step 590).

The crypto-board 80 responds by preparing a packet according to a pre-established data format which includes the current time and the actual geographic position in latitude and longitude and altitude (step 600). Also included may be information identifying the satellites transmitting the position data as well as other data necessary for the computations. The crypto-board 80 also stores the provided initialization vector at a known offset within the packet and applies a cryptographic signature to the contents of the packet. The cryptographic signature can be, for example, a message digest/hash of the packet data,

SECRET

plus an encryption of the message digest according to some predetermined key, and may be symmetrical or asymmetrical, depending on the key or certificate stored on the crypto-board 80.

5 The crypto-board 80 then transmits (step 605) the signed time/location packet to the device driver 72 which relays the packet to the decoder 32/CD-ROM drive 30. The decoder 32 compares the signature of the packet received from the crypto-board 80 with a signature stored in the
10 decoder 32 (step 610). If the signature verifies properly (step 620), the initialization vector within the packet is examined to determine if the initialization vector is indeed the same initialization vector which the decoder 32 provided to the crypto-board 80 in step 590. If this is the case,
15 then the packet received by the decoder 32 is recent and genuine, and the time and position data are accepted as valid.

 Once the packet from the crypto-board 80 is authorized based on the signature and the initialization
20 vector, the decoder 32 compares the time and position data received from the crypto-board 80 with the policy 155 which applies to the files 144 or to a subset of files 144 (step 460). If the user is authorized to access the files 144, then the data is unlocked (step 470), decrypted with
25 decryption keys 52 (step 480) and supplied to the user's application program 34 and displayed (step 490).

 Other embodiments are within the scope of the following claims. For example, the GPS receiver need not be located at the exact position of the data distribution media
30 reader but could be in a known location (such as a room containing a control server providing computer service to a local area network in a building) relative to the reader.

The policy files 152' may also designate geographic regions where access to certain files 144 is denied.

Control over access to files need not be limited to the use of passwords provided by the producer and entered
5 via a keyboard. For example, certain biometric attributes, such as facial features, finger prints and/or voice prints may be substituted for or used in addition to passwords.

What is claimed is:

SECRET

1 1. A method for controlling access to stored
2 information comprising:
3 determining an actual geographic position where said
4 stored information is located based on signals received at a
5 receiver supplying reliable position information;
6 comparing said actual geographic position with a
7 geographic region within which access to said stored
8 information is authorized; and
9 permitting access to said stored information if said
10 actual geographic position is located within said authorized
11 geographic region.

1 2. The method of claim 1, wherein said receiver
2 comprises a GPS receiver.

1 3. The method of claim 1, wherein said information
2 is stored on a computer-readable medium.

1 4. The method of claim 3, wherein said computer-
2 readable medium is portable.

1 5. The method of claim 3, wherein said computer-
2 readable medium comprises a high-capacity disk.

1 6. The method of claim 1, wherein said stored
2 information comprises files and each of said files has an
3 associated geographic region within which access is
4 permitted, and further permitting access to said file if
5 said actual geographic position is located within said
6 authorized geographic region for said file.

SECRET

1 7. The method of claim 6, further comprising
2 denying access to said stored information if said actual
3 geographic position does not match said authorized
4 geographic region.

1 8. The method of claim 1, further comprising:
2 encrypting said stored information using an
3 encryption key; and
4 providing a decryption key which permits decryption
5 of said stored information if said actual geographic
6 position is located within said authorized geographic
7 region.

1 9. The method of claim 1, further comprising:
2 cryptographically signing said actual geographic
3 position with a receiver encryption key; and
4 verifying the receiver signature with a receiver
5 decryption key before the actual geographic position is
6 compared with said authorized geographic region.

1 10. The method of claim 1, wherein said stored
2 information is divided into subsets of information and
3 wherein at least one the subsets has a different authorized
4 region from the other subsets, so that access is authorized
5 to the subset whose authorized geographic region is located
6 within the actual geographic position, but not to the
7 subsets whose authorized geographic region is not located
8 within the actual geographic position.

1 11. The method of claim 6, wherein said association
2 of the files with the authorized geographic regions is
3 stored as a policy file together with said stored
4 information.

1 12. Apparatus for controlling access to stored
2 information comprising:
3 a receiver supplying reliable position information
4 for determining an actual geographic position where said
5 stored information is located; and
6 a computer for comparing said actual geographic
7 position with a geographic region within which access to
8 said stored information is authorized,
9 wherein said computer permits access to said stored
10 information if said actual geographic position is located
11 within said authorized geographic region.

1 13. The apparatus of claim 12, wherein said
2 receiver is a GPS receiver.

1 14. The apparatus of claim 12, the receiver further
2 comprising a receiver encryption mechanism providing a
3 receiver encryption key for cryptographically signing the
4 actual geographic position.

1 15. The apparatus of claim 14, further comprising a
2 reader for reading said stored information wherein said
3 reader comprises a receiver decryption key for verifying
4 said cryptographically signed actual position.

1 16. The apparatus of claim 15, wherein said reader
2 generates an initialization vector providing a position
3 offset which is transmitted to the receiver and added to the
4 actual geographic position.

1 17. The apparatus of claim 16, further comprising a
2 reader encryption mechanism providing a reader encryption
3 key for cryptographically signing the position offset,

4 wherein said position offset signature is verified by the
5 receiver with a corresponding reader decryption key before
6 the position offset is added to the actual geographic
7 position.

1 18. A method for controlling access to a subset of
2 files belonging to a larger set of files of stored
3 information comprising:

4 associating a unique file encryption key with each
5 file from the larger set of files and encrypting the files
6 using the associated encryption keys;

7 associating each of the files from the larger set of
8 files with at least one authorized geographic region within
9 which access to said stored information is authorized;

10 determining an actual geographic position where said
11 stored information is located based on signals received at a
12 receiver supplying reliable position information;

13 comparing said actual geographic position with said
14 authorized geographic region; and

15 providing a file decryption key which authorizes
16 access to and permits decryption of said files belonging to
17 said subset of files, provided that the actual geographic
18 position is located within the authorized geographic region
19 for the files belonging to said subset of files.

1 19. The method of claim 18, wherein said
2 association of the files with the authorized geographic
3 regions is stored as a policy comprising policy files
4 wherein each policy file is accessible with a user password
5 and authorizes, if the user password is valid, access to the
6 files listed in said policy file, if the actual geographic
7 position which is located within the authorized geographic
8 region associated with the files.

1 20. The method of claim 19, wherein said policy is
2 stored with the stored information.

1 21. A method for controlling access to stored
2 information comprising:
3 determining an actual date or time at the location
4 of said stored information based on signals received at a
5 receiver supplying reliable time information;
6 comparing said actual date or time with a
7 predetermined date or time interval at which access to said
8 stored information is authorized; and
9 permitting access to said stored information if said
10 actual date or time occurs within said authorized date or
11 time interval.

1 22. The method of claim 21, further comprising
2 denying access to said stored information if said actual
3 date or time does not occur within said authorized date or
4 time interval.

1 23. The method of claim 21, wherein said
2 information comprises files and each of said files has an
3 associated authorized date or time interval within which
4 access is permitted, and further permitting access to said
5 file if said actual date or time occurs within said
6 associated authorized date or time interval.

1 24. The method of claims 21, wherein said stored
2 information is divided into subsets of information and
3 wherein at least one of the subsets has a different
4 authorized date or time interval from the other subsets, so
5 that access is authorized to the subset whose authorized
6 date or time interval matches the actual date or time, but

7 not to the subsets whose authorized date or time interval
8 does not match the actual date or time.

1 25. A method for controlling access to stored
2 information comprising:
3 forming a policy associating said information with
4 authorized geographic regions and authorized time intervals;
5 cryptographically signing said policy and said
6 information;
7 storing said signed policy together with said signed
8 information;
9 providing a password for unlocking said policy; and
10 determining an actual geographic position where said
11 stored information is located based on signals received at a
12 receiver supplying reliable position information;
13 determining an actual time;
14 comparing said actual geographic position and said
15 actual time with said authorized geographic regions and
16 authorized time interval of said policy; and
17 permitting access to said stored information if said
18 actual geographic position and actual time falls within said
19 authorized geographic regions and authorized time interval
20 of said policy.

1 26. The method of claim 1, wherein said source of
2 reliable position and time is a Global Orbiting Navigational
3 Satellite System.

1 27. The method of claim 1, wherein said source of
2 reliable position and time is a inertial navigation system.

1 28. The method of claim 1, wherein said source of
2 reliable position and time is a satelllite based location
3 determination system.

SECRET

CONTROLLING ACCESS TO STORED INFORMATION

Abstract

Access to stored information by a user is controlled by comparing an actual geographic position and/or an actual date/time with a geographic region and/or a date/time interval within which access to the stored information is authorized. The actual geographic position where the stored information is located, and the actual date/time can be determined, for example, based on signals received at a receiver supplying reliable position and time information, such as a GPS receiver. Access to the stored information is authorized if the actual geographic position and/or date/time falls within the authorized geographic region and/or date/time interval. The position and date/time information supplied by the receiver may be cryptographically signed and encrypted.

318943.B11

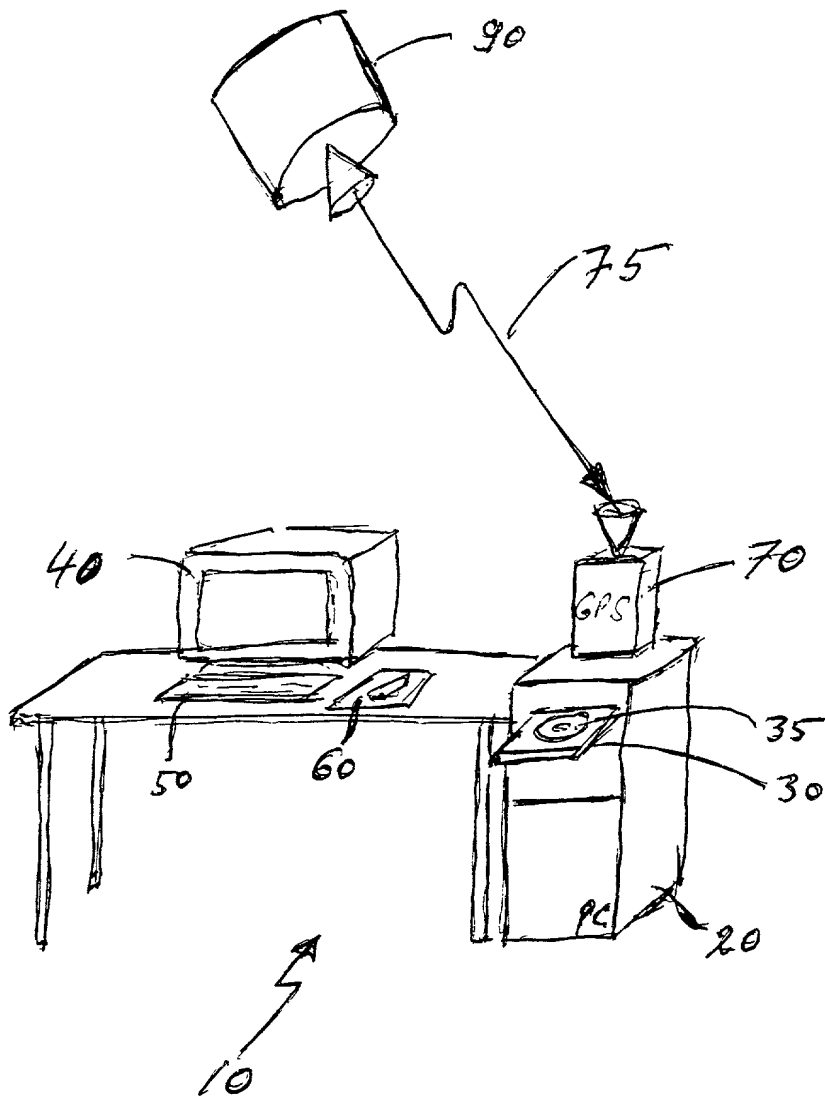
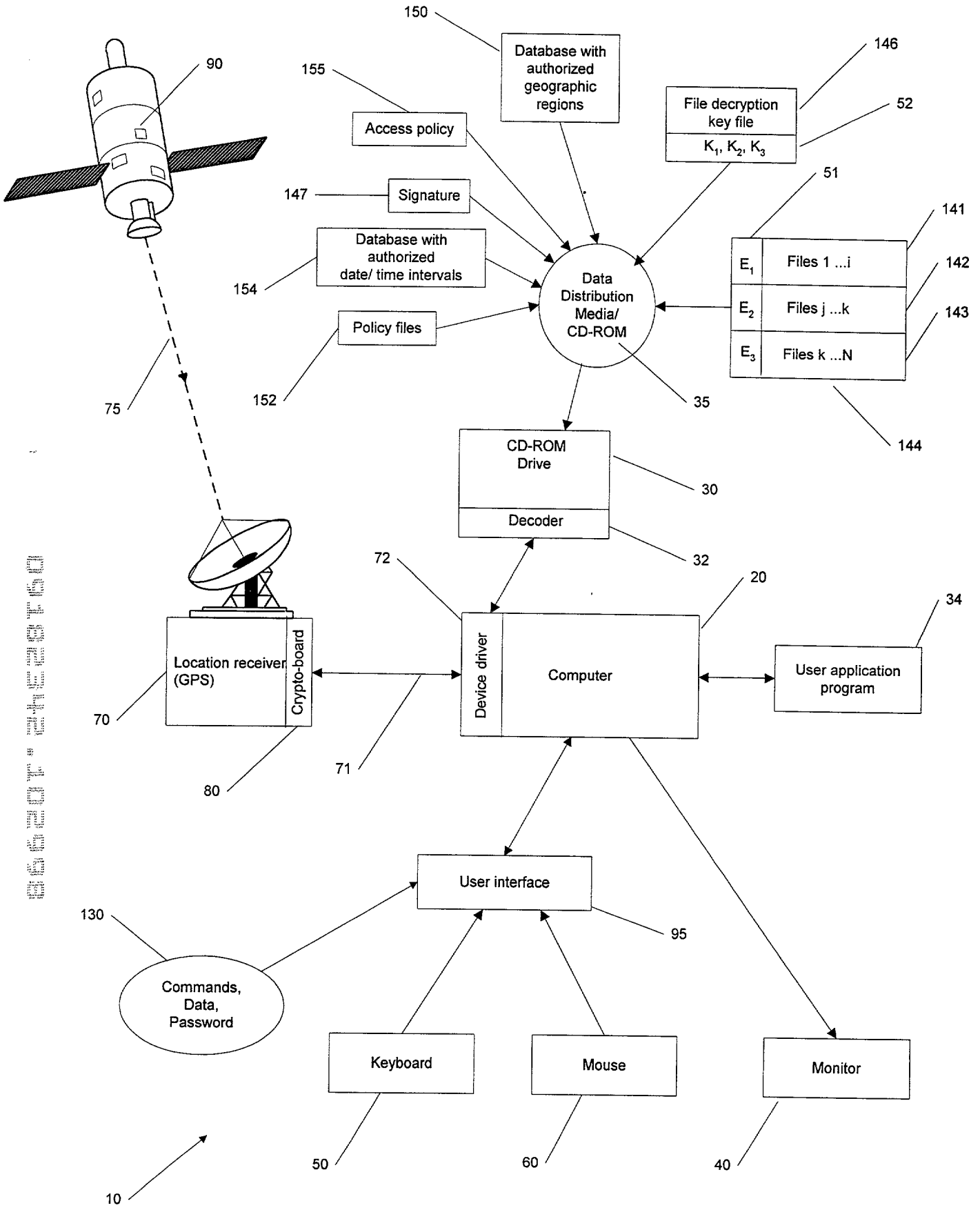


Fig. 1



SECRET

FIG. 2

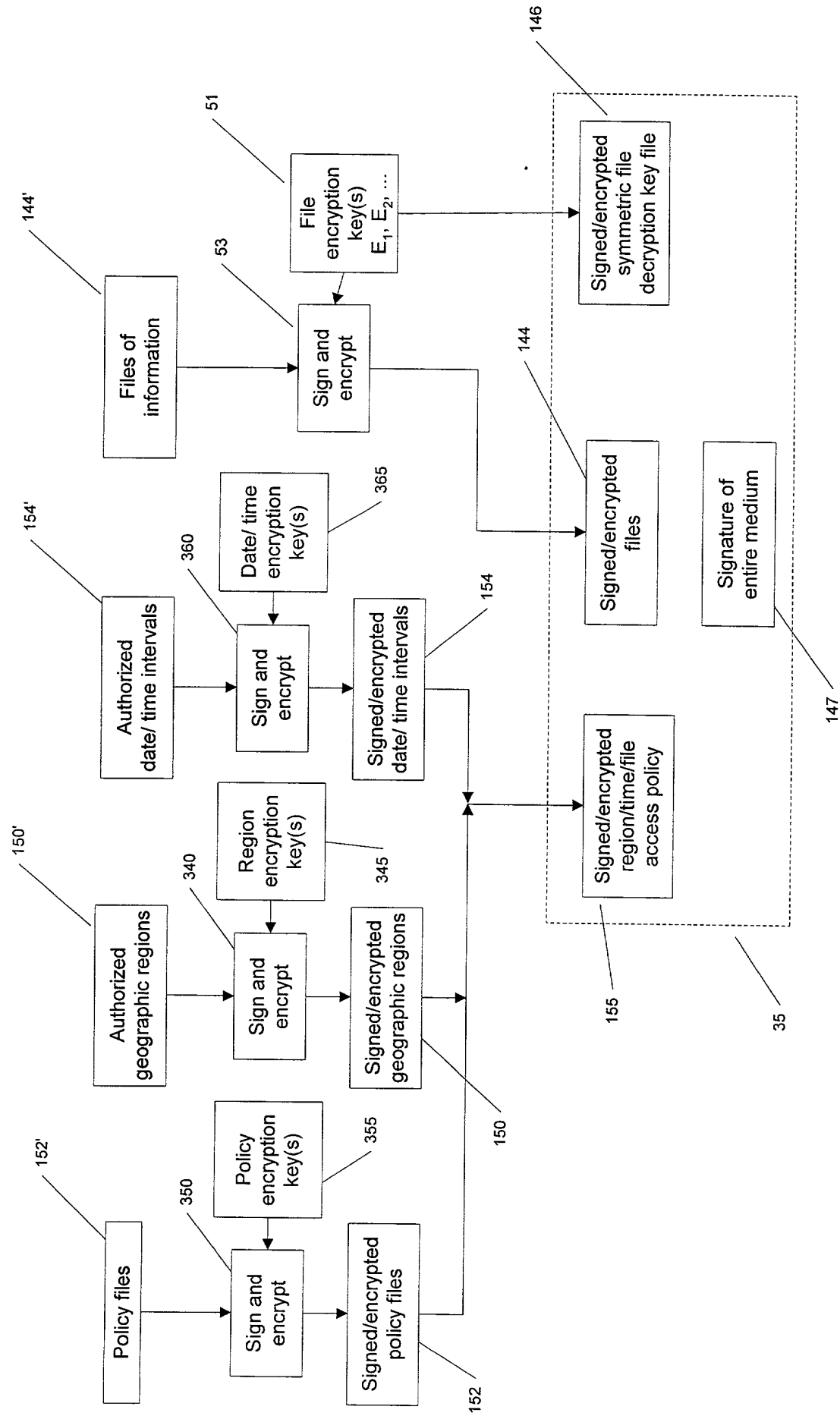


FIG. 3

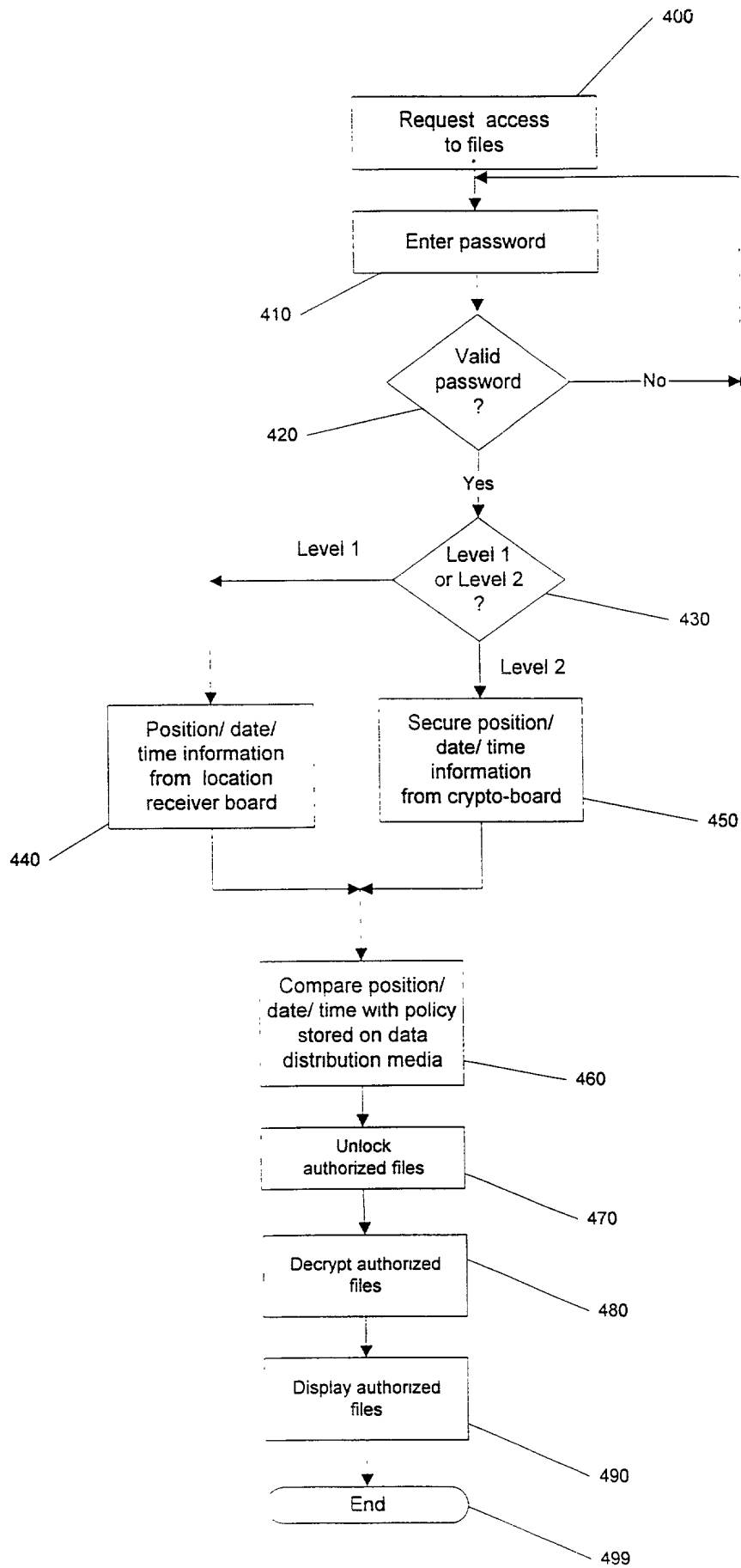
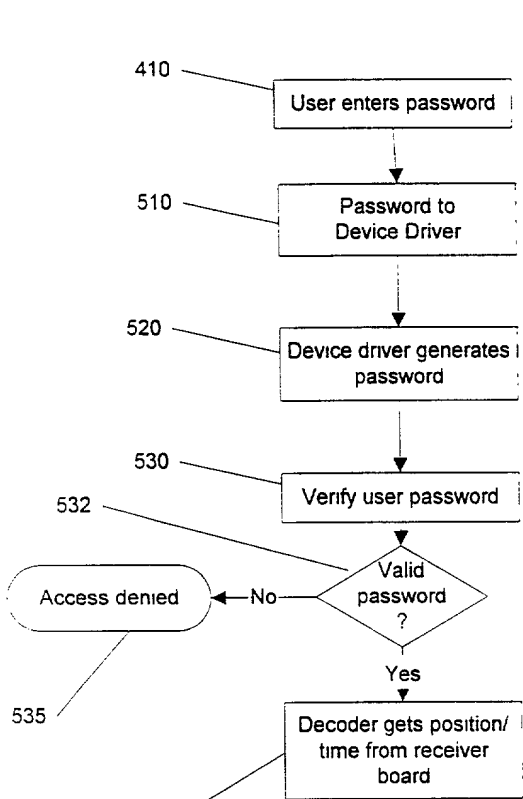


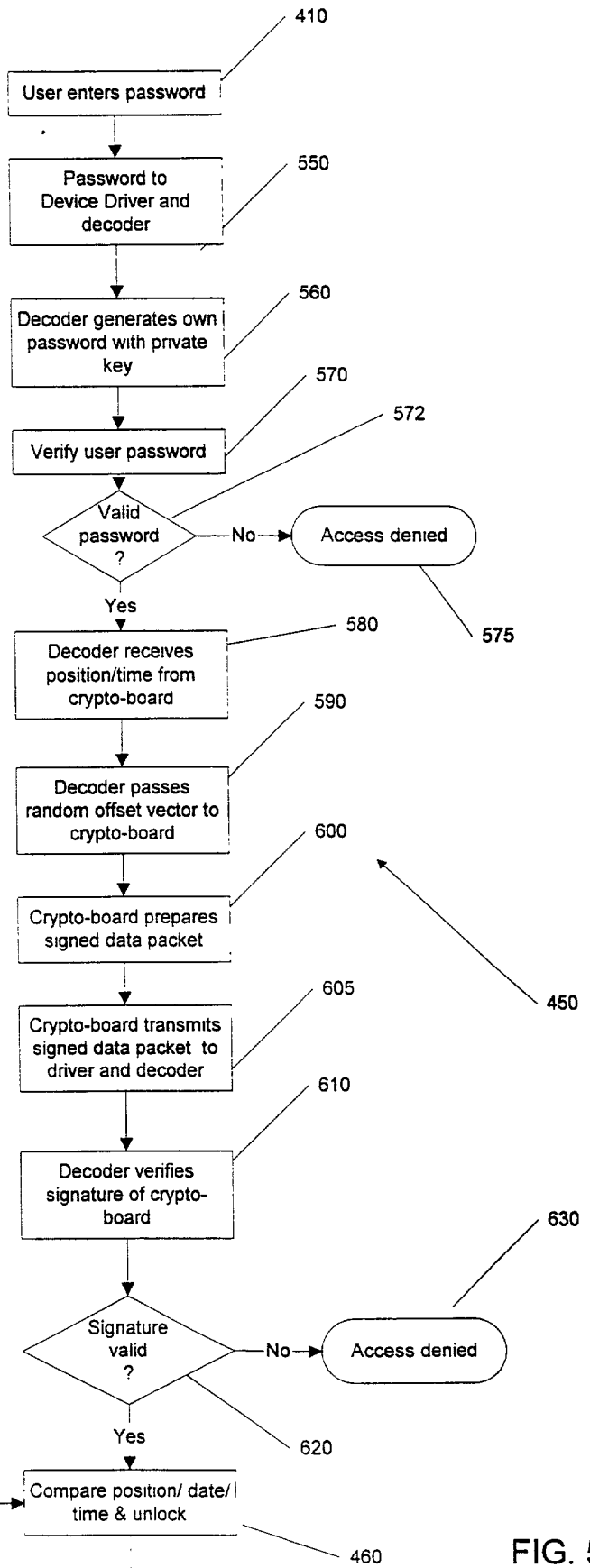
FIG. 4

SECRET

Level 1



Level 2



SECRET

FIG. 5

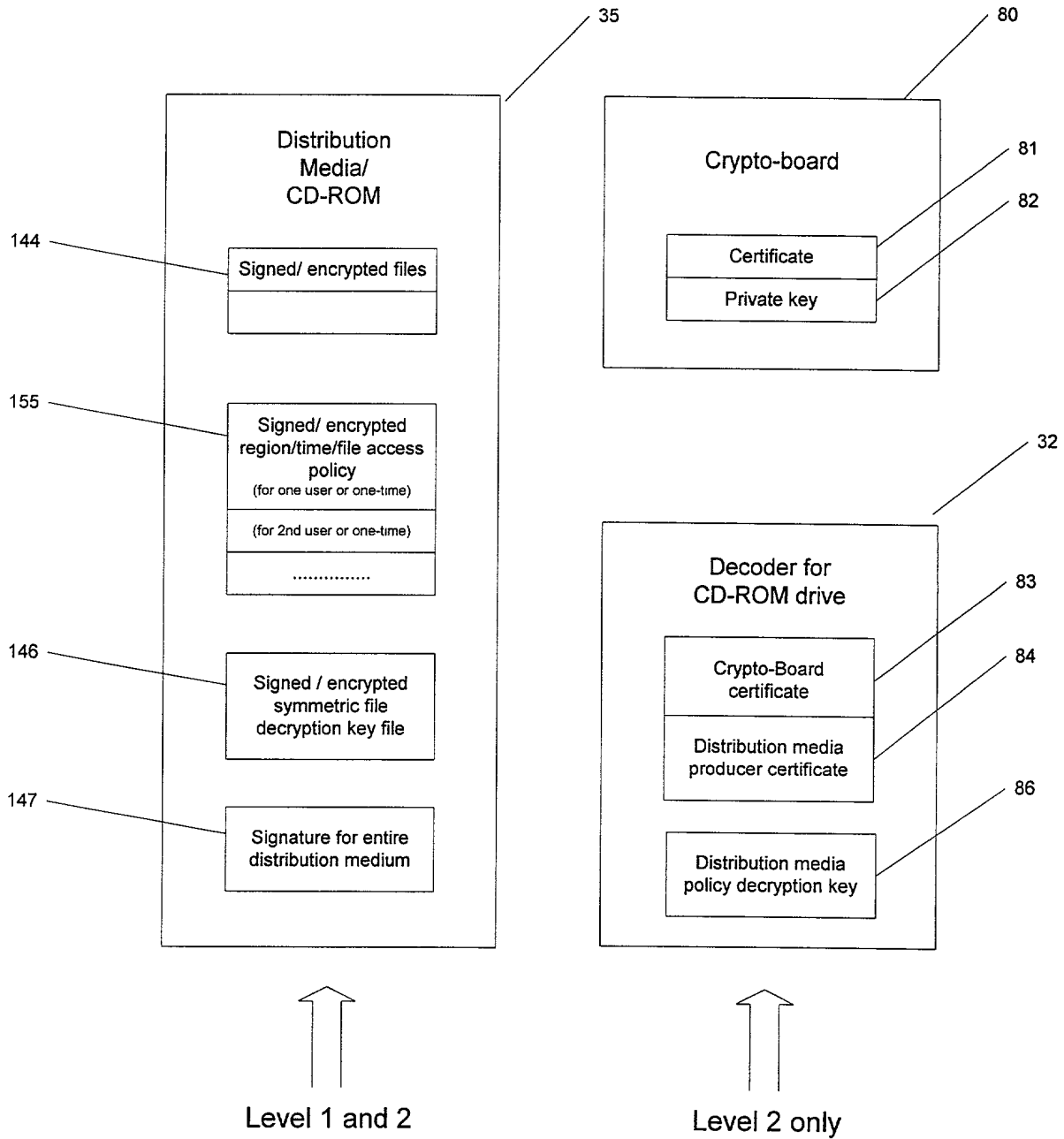


FIG. 6

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled CONTROLLING ACCESS TO STORED INFORMATION, the specification of which

- is attached hereto.
- was filed on _____ as Application Serial No. _____ and was amended on _____.
- was described and claimed in PCT International Application No. _____ filed on _____ and as amended under PCT Article 19 on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information I know to be material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

David L. Feigenbaum, Reg. No. 30,378; Robert E. Hillman, Reg. No. 22,837; and Wolfgang E. Stutius, Reg. No. 40,256.

Address all telephone calls to David L. Feigenbaum at telephone number 617/542-5070.

Address all correspondence to David L. Feigenbaum, Fish & Richardson P.C., 225 Franklin Street , Boston, MA 02110-2804.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Full Name of Inventor: Thomas Mark Hastings

Inventor's Signature:  Date: 10/28/1998

Residence Address: Lexington, MA

Citizen of: United States

Post Office Address: 38 Meriam Street, Lexington, MA 02420

06157/006001

COMBINED DECLARATION AND POWER OF ATTORNEY CONTINUED

Full Name of Inventor: Michael E. McNeil

Inventor's Signature: Michael McNeil Date: 10/27/98

Residence Address: Felton, CA

Citizen of: United States

Post Office Address: 1271 Lost Acre Drive, Felton, CA 95018

Full Name of Inventor: Todd S. Glassey

Inventor's Signature: Todd S. Glassey Date: 27-Oct-98

Residence Address: Scotts Valley, CA

Citizen of: United States

Post Office Address: 109A Bluebonnet Lane, Scotts Valley, CA 95066

Full Name of Inventor: Gerald L. Willett

Inventor's Signature: Gerald L. Willett Date: October 28, 1998

Residence Address: Malden, MA

Citizen of: United States

Post Office Address: 189 Harvard Street, #1, Malden, MA 02148

330287.B11

Applicant or Patentee: Thomas Mark Hastings et al.
Serial or Patent No.:
Filed or Issued: HEREWITH
For: CONTROLLING ACCESS TO STORED INFORMATION

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) and 1.27(c)) - SMALL BUSINESS CONCERN

I hereby declare that I am

- the owner of the small business concern identified below:
- an official of the small business concern empowered to act on behalf of the concern identified below:

Name of Small Business Concern: DIGITAL DELIVERY, INC.

Address of Small Business Concern: 54 Middlesex Turnpike, Bedford, MA 01730

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled CONTROLLING ACCESS TO STORED INFORMATION by inventor(s) Thomas Mark Hastings, Michael E. McNeil, Todd S. Glassey and Gerald L. Willett described in

- the specification filed herewith.
- application serial no. , filed .
- patent no. , issued .

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

Full Name: DIGITAL DELIVERY, INC.

Address: 54 Middlesex Turnpike, Bedford, MA 01730

- INDIVIDUAL
- SMALL BUSINESS CONCERN
- NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status when any new rule 53 application is filed or prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent on which this verified statement is directed.

Name: Thomas Mark Hastings

Title: President & CEO

Address: 54 Middlesex Turnpike, Bedford, MA 01730-1417

Signature: *Thomas Mark Hastings* Date: 10/29/1990

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS <i>Patent</i>	Patent Number	6,370,629
	Issue Date	April 9, 2002
	Application Number	09/182,342
	Filing Date	October 29, 1998
	First Named Inventor	Thomas Mark Hastings
	Attorney Docket Number	SYMM/0013

Address to:
Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Please change the Correspondence Address for the above-identified patent to:

The address associated with Customer Number

OR

Firm or Individual Name

Address

City State ZIP

Country

Telephone Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124)

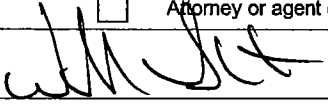
This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the :

Patentee.

Assignee of record of the entire interest. See 37 CFR 3.71. Certificate under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

Attorney or agent of record. Registration Number _____

Signature 

Typed or Printed Name

Date Telephone

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Post Issue, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)Applicant/Patent Owner: Hastings, et al.Application No./Patent No.: 09/182,342Filed/Issue Date: April 9, 2002Entitled: CONTROLLING ACCESS TO STORED INFORMATION BASED ON GEOGRAPHICAL LOCATION AND DATE AND TIMESYMMETRICOM, INC., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. the assignee of the entire right, title, and interest; or
2. an assignee of less than the entire right, title, and interest
- The extent (by percentage) of its ownership interest is _____ %

in the patent application/patent identified above by virtue of either:

- A. An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

OR

- B. A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

1. From: Hastings, et al. To: Digital Delivery, Inc.
The document was recorded in the United States Patent and Trademark Office at Reel 009555, Frame 0985, or for which a copy thereof is attached.
2. From: Digital Delivery, Inc. To: Datum, Inc.
The document was recorded in the United States Patent and Trademark Office at Reel 010456, Frame 0059, or for which a copy thereof is attached.
3. From: Datum, Inc. To: Symmetricon, Inc.
The document was recorded in the United States Patent and Trademark Office at Reel 014120, Frame 0637, or for which a copy thereof is attached.

- Additional documents in the chain of title are listed on a supplemental sheet.

- Copies of assignments or other documents in the chain of title are attached.

(NOTE: A separate copy (i.e., a true copy of the original document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.



Signature

William Slater

Printed or Typed Name

Executive VP and CFO

Title

Sept 4, 2002

Date

(408) 433-0910

Telephone Number

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Acknowledgement Receipt

EFS ID:	2194787
Application Number:	09182342
International Application Number:	
Confirmation Number:	1911
Title of Invention:	CONTROLLING ACCESS TO STORED INFORMATION BASED ON GEOGRAPHICAL LOCATION AND DATE AND TIME
First Named Inventor/Applicant Name:	THOMAS MARK HASTINGS
Customer Number:	38396
Filer:	Frederick D. Kim./Jose Cardenas
Filer Authorized By:	Frederick D. Kim.
Attorney Docket Number:	06175/006001
Receipt Date:	13-SEP-2007
Filing Date:	29-OCT-1998
Time Stamp:	19:46:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1		SYMM_0013_ECHGADD373.pdf	98753 <small>53a7e904b6634dcef082bf72ccae8ff238b12d93</small>	yes	2

Multipart Description/PDF files in .zip description			
Document Description		Start	End
Change of Address		1	1
Assignee showing of ownership per 37 CFR 3.73(b).		2	2

Warnings:

Information:

Total Files Size (in bytes):	98753
-------------------------------------	-------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT ASSIGNMENT

Electronic Version v1.1
 Stylesheet Version v1.1

SUBMISSION TYPE:	CORRECTIVE ASSIGNMENT										
NATURE OF CONVEYANCE:	Corrective Assignment to correct the improper assignment w/o the missing Co-Inventor Agreement; makes assignment appear as Sale rather than Fiduciary Retainer previously recorded on Reel 009555 Frame 0985. Assignor(s) hereby confirms the (replace the Co-Inventor Agreement as part of the Assignment).										
CONVEYING PARTY DATA											
<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th style="width:70%;">Name</th> <th>Execution Date</th> </tr> </thead> <tbody> <tr> <td>Todd S Glassey</td> <td>10/27/1998</td> </tr> <tr> <td>Michael E McNeil</td> <td>10/27/1998</td> </tr> </tbody> </table>		Name	Execution Date	Todd S Glassey	10/27/1998	Michael E McNeil	10/27/1998				
Name	Execution Date										
Todd S Glassey	10/27/1998										
Michael E McNeil	10/27/1998										
RECEIVING PARTY DATA											
<table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td style="width:20%;">Name:</td> <td>Digital Delivery Inc</td> </tr> <tr> <td>Street Address:</td> <td>54 MIDDLESEX TURNPIKE</td> </tr> <tr> <td>City:</td> <td>Bedford</td> </tr> <tr> <td>State/Country:</td> <td>MASSACHUSETTS</td> </tr> <tr> <td>Postal Code:</td> <td>01730</td> </tr> </table>		Name:	Digital Delivery Inc	Street Address:	54 MIDDLESEX TURNPIKE	City:	Bedford	State/Country:	MASSACHUSETTS	Postal Code:	01730
Name:	Digital Delivery Inc										
Street Address:	54 MIDDLESEX TURNPIKE										
City:	Bedford										
State/Country:	MASSACHUSETTS										
Postal Code:	01730										
PROPERTY NUMBERS Total: 1											
<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th style="width:30%;">Property Type</th> <th>Number</th> </tr> </thead> <tbody> <tr> <td>Patent Number:</td> <td>6370629</td> </tr> </tbody> </table>		Property Type	Number	Patent Number:	6370629						
Property Type	Number										
Patent Number:	6370629										
CORRESPONDENCE DATA											
<p>Fax Number: <i>Correspondence will be sent via US Mail when the fax attempt is unsuccessful.</i></p> <p>Phone: 408-890-7321 Email: tglassey@earthlink.net Correspondent Name: Todd Glassey Address Line 1: 305 McGaffigan Mill Rd Address Line 4: Boulder Creek, CALIFORNIA 95006</p>											
ATTORNEY DOCKET NUMBER:	CV165643										
NAME OF SUBMITTER:	Todd S. Glassey										
	This document serves as an Oath/Declaration (37 CFR 1.63).										

OP \$40.00 6370629

Total Attachments: 10

source=DDI-Co-Inventor Agreement#page1.tif

source=DDI-Co-Inventor Agreement#page2.tif

source=DDI-Co-Inventor Agreement#page3.tif

source=DDI-Co-Inventor Agreement#page4.tif

source=DDI-Co-Inventor Agreement#page5.tif

source=DDI-Co-Inventor Agreement#page6.tif

source=Assignment#page1.tif

source=Assignment#page2.tif

source=assignment abstract for 6370629#page1.tif

source=assignment abstract for 6370629#page2.tif

CO-INVENTOR AGREEMENT

This is Co-Inventor Agreement ("Agreement"), is made this 26th day of October, 1998 by and between Todd S. Glassey an individual, and Michael E. McNeil an individual, together herein "Glassey-McNeil", whose mailing address is 109A Bluebonnet Lane, Scotts Valley, CA 95066 and Digital Delivery, Inc., a Massachusetts corporation, having a place of business at 54 Middlesex Turnpike, Bedford, Massachusetts 01730-1417 ("Digital"). This Agreement is made with reference to the facts in the following recitals:

RECITALS

A. Digital is the holder of U.S. Patent Number 5,646,992 for certain data and file protection and encryption technology, described further as encryption and decryption technology employing the use of passwords to control access to stored information on various distribution media. The product produced by Digital under this patent is generally referred to as the Confidential Courier, which is described in non-technical terms as a transmittal envelope which can be opened only by specifically designated persons having the encoded passwords. This patent was issued to Digital on July 8, 1997 (the "Courier Patent").

B. Digital employees Thomas Mark Hastings and Gerald L. Willett, along with Glassey-McNeil have further developed the Courier Patent technology to expand its identification and verification enablement policies by adding the new technology of geo-positioning and time/date encryption with respect to data and file storage and access. It is the intent of Digital to file for a patent on this new technology to the Courier Patent by means of a subsequent patent entitled "Controlling Access to Stored Information" which incorporates the Courier Patent, and is referred to herein as the "Controlling Access Patent".

C. During the course of the development of the technology for the Controlling Access Patent by the parties, it was discussed and agreed in principal that Digital would undertake the submission of the Controlling Access Patent application and that Glassey-McNeil would assign certain rights under the patent with respect to the underlying Courier Patent, provided that certain terms and conditions regarding the mutual rights and exclusive rights to the geo-positioning and time/date encryption policies in the Controlling Access Patent were defined and determined, and that adequate compensation from Digital to Glassey-McNeil was agreed.

D. The purpose of this Agreement is to allow the Controlling Access Patent application to be submitted as early as possible and prior to a definitive agreement between the parties with respect to each party's rights to exploit the Controlling Access Patent, the respective mutual and exclusive rights to the underlying or derivative technology, methodology, or other patentable subject matter contained or referenced in

the Controlling Access Patent, and the compensation to be paid by Digital to Glassey-McNeil for assignment of certain rights therein to Digital.

In consideration of the foregoing facts and recitals, the mutual covenants and undertakings contained therein and herein, the parties agree as follows:

1. PATENT APPLICATION TECHNOLOGY

For purposes of this Agreement, the term:

A. "Confidential Courier" means that technology developed by Digital under the Courier Patent which is embodied in the product produced and sold by Digital under the name Confidential Courier, which contains certain encryption and decryption technology to control and limit access to the information and data contained in specific files.

B. Geo-positioning and time/date technology means the enablement policy which allows data or an event to be pinpointed to occur at a certain time and physical place.

C. GPS Phase II means that geo-positioning and time/date enablement technology invented and developed by Glassey-McNeil that specifically includes a cryptographic signing and verification process with the transmittal of time and geographic positioning information that allows a legally indemnifiable degree of trust to be established in the time and geographic positioning information thus conveyed.

2. AGREEMENT IN PRINCIPLE

The parties are entering this Agreement to set forth certain terms and conditions with respect to the mutual and exclusive rights of each party to the Controlling Access Patent. Although Digital developed, produces and sells the Confidential Courier, which embodies the Courier Patent, there is no prototype nor product yet developed utilizing the new technology of geo-positioning and time/date policies to be patented under the Controlling Access Patent. In view of the uncertainties relative to the cost of developing a product under the Controlling Access Patent and the market potential of such a product, the parties have insufficient information to agree on the compensation to be paid by Digital to Glassey-McNeil for their ideas, inventions, proprietary information and contributions to the Controlling Access Patent.

It is intended that, within one year from the date hereof, a definitive agreement between the parties will be made with respect to this compensation and the mutual and exclusive rights to the Controlling Access Patent. Provided that said compensation can be negotiated by the parties or established by binding arbitration as provided herein, the definitive agreement will include the following terms and conditions:

A. Digital acknowledges that the GPS Phase II technology is solely and exclusively the idea and invention of Glassey-McNeil. Notwithstanding, Digital shall have the rights to utilize the GPS Phase II technology but limited to the Confidential Courier product and product derivatives thereof; and Digital grants to Glassey-McNeil

a perpetual non-exclusive worldwide license for the GPS Phase II technology and derivatives thereof, with rights to sublicense.

B. Glassey-McNeil shall have no rights to any part of the Courier Patent, or to the claims regarding the Courier Patent which are incorporated in the Controlling Access Patent or to the Confidential Courier product now produced by Digital.

C. Digital shall not file any opposition in the United States Patent and Trademark Office or patent offices of any other country, or take any action adverse to the filing of a patent application by Glassey-McNeil for any geo-positioning and time/date technology or technology implementing GPS Phase II, including potential patentable subject matter or products e.g., firewalls, email gateways, protocol bridges, database servers, file servers, hardware based appliances, and the like.

D. Digital shall begin and continue the development of products which shall embody the technology of the Controlling Access Patent in order to enhance or compliment the existing Confidential Courier Product as well as new products exploiting the Controlling Access Patent which are to be sold and distributed by Digital.

E. Glassey-McNeil may develop products which utilize the geo-positioning and/or time/date enablement or GPS Phase II technology, provided that any such products do not include the technology infrastructure covered by the Courier Patent.

Provided that a definitive agreement is negotiated and made by the parties which incorporates the foregoing terms, conditions, covenants, licenses, and compensation to Glassey-McNeil, Glassey-McNeil will execute assignments to Digital with respect to the Controlling Access Patent.

3. FAILURE TO MAKE DEFINITIVE AGREEMENT

A. The parties expressly agree that each of them will negotiate in good faith the terms of a definitive agreement, in light of the provisions in Section 2 above, regarding the patent rights to the Controlling Access Patent and the compensation to be paid by Digital to Glassey-McNeil for the assignment of rights therein as named co-inventors on the Controlling Access Patent application. The parties expressly agree that if they are unable or fail to make a definitive agreement before the anniversary date hereof, then each party shall have all rights as a co-inventor to fully exploit the Controlling Access Patent without accounting or control by the other.

B. If after the one year anniversary hereof, the parties are unable to make a definitive agreement as provided herein, then upon the written request of either party to the other the unresolved issues, terms and conditions will be submitted (i) first to mediation conducted by a qualified mediator, mutually selected by the parties, who has expertise in patent matters and practicable expertise in the commercial encryption industry; and (ii) if mediation does not result in a definitive agreement, then upon written request upon one party to the other, the parties shall submit all unresolved issues to mandatory binding arbitration. The issues will be submitted in writing to the arbitrator,

who shall be mutually selected by the parties, or if the parties are unable to select a single arbitrator, then each party, viz., Digital and Glassey-McNeil shall each select an arbitrator who shall then select a third arbitrator to create an arbitration panel consisting of those three arbitrators. If for any reason the first selected arbitrators cannot agree on a third arbitrator, they may apply to the superior court of Santa Cruz County, California for the name of a qualified neutral third arbitrator. The three arbitrators shall hear all the evidence, and a majority vote of the arbitrators shall make all decisions, determinations and awards in the matters before them.

It is contemplated by the parties that the fundamental issue to be decided by this mandatory arbitration is the amount and structure of the compensation to be paid to Glassey-McNeil for their contribution to the Controlling Access Patent in full respect of the terms set forth in the "AGREEMENT IN PRINCIPLE" in Section 2 hereof. In determining such compensation, the arbitrator(s) shall take into consideration the value of the patent rights to Digital by Glassey-McNeil; the cost of Digital's product development incurred by the parties; the contributions of the parties to Digital's product development; the domestic and international market potential of Digital's new products to be produced under the Controlling Access Patent, including the market potential of the Confidential Courier enhanced by the addition of new features and improvements from the geo-positioning and/or time/date technology in the Controlling Access Patent; the established and potential profitability, commercial success and current or potential popularity of such product(s); the rightful apportionment of profit among the inventors; nonpatented aspects or elements of such product(s), including the costs of manufacturing, business risks.

Any mandatory binding arbitration of matters under this section 3, or consensual arbitration of other matters arising out of this Agreement, shall be conducted by and in accordance with then existing arbitration rules of the American Arbitration Association respecting the computer and electronic commerce industry. Judgment on a binding arbitration award rendered by such arbitrator(s) may be entered in any court having jurisdiction. The parties shall each pay one half of all costs and expenses for the services of any mediator and/or arbitrator(s).

4. DEFAULT IN COMPENSATION

If, after the compensation to be paid by Digital to Glassey-McNeil for their contributions to the technological inventions under the Controlling Access Patent is established by an agreement made by the parties or through a determination from binding arbitration, Digital defaults in the payment terms thereof for any reason, then all rights, i.e. patent, trade secret, etc., to the inventions and technology covered under the Controlling Access Patent, which includes the Confidential Courier, shall revert to Glassey-McNeil as Co-inventors along with Digital. In such event, and each party shall have all right to exploit said inventions and technology without any notice, obligation or accounting to the other. Notwithstanding, the parties shall each execute and deliver such further documents and shall take such other actions as may be reasonably necessary to effect this reversion of rights.

5. NONASSIGNABILITY

The parties hereto have entered into this agreement in contemplation of personal performance hereof by each other and intend that the rights granted and obligations imposed hereunder not be extended to other entities without the other party's express written consent, except that Glassey-McNeil may transfer their interests herein to a corporation whose majority of voting shares are owned and controlled by them. This Agreement shall be binding and shall inure to the benefit of the parties and to their heirs, successors, and assigns.

6. NOTICES

Notices under this Agreement shall be in writing and sent to the parties at the addresses first above written, or to such other addresses as the parties may designate to the other in writing.

7. ATTORNEY FEES

In the event that either party must take legal action, including arbitration, but except for arbitration employed to determine the compensation referenced in Section 3 herein, to enforce or interpret this agreement, or any provision hereof, the prevailing party shall be entitled to recover its reasonable attorney fees and costs as determined by the Court or arbitrator.

8. INTEGRATION

This agreement, any exhibits hereto, set forth the entire agreement and understanding between the parties as to the subject matter hereof and merges all prior discussions between them. Neither of the parties shall be bound by any agreements, understandings or representations with respect to such subject matter other than as expressly provided herein or in a subsequent writing signed by the parties hereto.

9. SEVERABILITY

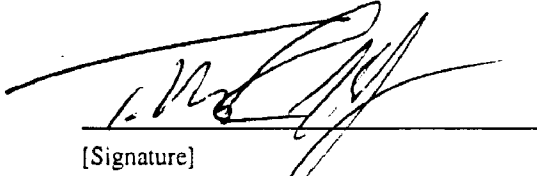
Nothing in this Agreement shall be interpreted or construed as "an agreement to agree" such that this Agreement would be rendered unenforceable. Accordingly, any provision of this Agreement prohibited by, or unlawful or unenforceable, under any applicable law of any jurisdiction, shall be ineffective, without affecting any other provision of this Agreement. To the extent, however, that the provisions of such applicable law may be waived, they are hereby waived to the end that this Agreement may be deemed to be a valid and binding agreement enforceable in accordance with its terms.

10. LAW

This agreement will be governed and interpreted by the laws and courts of the State of California.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement the day and year first above written.

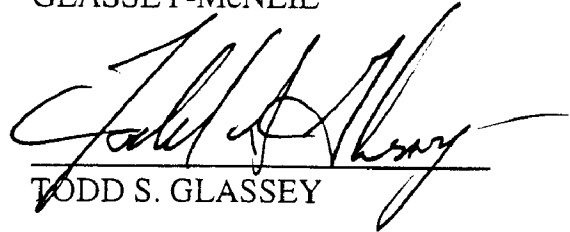
DIGITAL DELIVERY



[Signature]

Tomack Hastings President
[Please Print Name/Title]

GLASSEY-McNEIL



TODD S. GLASSEY

Michael McNeil
MICHAEL E. McNEIL

For valuable consideration, we, Thomas Mark Hastings, of Lexington, Massachusetts; Michael E. McNeil of Felton, California; Todd S. Glassy of Scotts Valley, California; and Gerald L. Willer of Malden, Massachusetts; hereby assign to DIGITAL DELIVERY, INC., a Massachusetts corporation having a place of business at 34 Middlesex Turnpike, Bedford, Massachusetts, and its successors and assigns (collectively hereinafter called "the Assignee"), the entire right, title and interest throughout the world in the inventions and improvements which are subject of an application for United States Patent signed by us, entitled CONTROLLING ACCESS TO STORED INFORMATION, filed _____, and assigned U.S. Serial Number _____, and we authorize and request the attorneys appointed in said application to hereafter complete this assignment by inserting above the filing date and serial number of said application when known; this assignment including said application, any and all United States and foreign patents, utility models, and design registrations granted for any of said inventions or improvements, and the right to claim priority based on the filing date of said application under the International Convention for the Protection of Industrial Property, the Patent Cooperation Treaty, the European Patent Convention, and all other treaties of like purposes; and we authorize the Assignee to apply in all countries in our name or in its own name for patents, utility models, and design registrations and like rights of exclusion and for inventors' certificates for said inventions and improvements; and we agree for ourselves and our respective heirs, legal representatives and assigns, without further compensation to perform such lawful acts and to sign such further applications, assignments, Preliminary Statements and other lawful documents as the Assignee may reasonably request to effectuate fully this assignment.

IN WITNESS WHEREOF, I hereto set my hand and seal at Burlington MASSACHUSETTS, this 28 day of October, 1998
Thomas Mark Hastings L.S.

STATE OF Massachusetts :
COUNTY OF Middlesex :

Before me this 28 day of October, 1998, personally appeared Thomas Mark Hastings known to me to be the person whose name is subscribed to the foregoing Assignment, and acknowledged that he/she executed the same as his/her free act and deed for the purposes therein contained.

Janet Altrill
Notary Public
My Commission Expires: 2/04/2005

[Notary's Seal Here]

this 27th day of October, 1978.

Michael E. McNeil
Michael E. McNeil

L.S.

STATE OF California

COUNTY OF Santa Cruz

Before me this 27 day of October, 1978, personally appeared

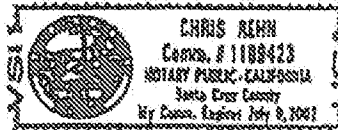
Michael E. McNeil known to me to be the person whose name is subscribed to the foregoing Assignment, and acknowledged that ~~he~~ she executed the same as ~~his~~ her free act and deed for the purposes therein contained.

Chris Rea
Notary Public

My Commission Expires:

July 9, 2002

[Notary's Seal Here]



IN WITNESS WHEREOF, I hereto set my hand and seal at Scotts Valley
this 27 day of October, 1978

Todd S. Glassey
Todd S. Glassey

L.S.

STATE OF Ca

COUNTY OF Santa Cruz

Before me this 27 day of October, 1978, personally appeared

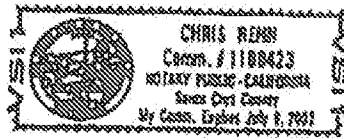
Todd S. Glassey known to me to be the person whose name is subscribed to the foregoing Assignment, and acknowledged that ~~he~~ she executed the same as ~~his~~ her free act and deed for the purposes therein contained.

Chris Rea
Notary Public

My Commission Expires:

July 9, 2002

[Notary's Seal Here]



PATENT
REEL: 9655 FRAME: 0987



United States Patent and Trademark Office

[Home](#) | [Site Index](#) | [Search](#) | [Guides](#) | [Contacts](#) | [eBusiness](#) | [eBiz alerts](#) | [News](#) | [Help](#)**Assignments on the Web > Patent Query****Patent Assignment Abstract of Title**

NOTE: Results display only for issued patents and published applications. For pending or abandoned applications please consult USPTO staff.

Total Assignments: 4**Patent # :** [6370629](#) **Issue Dt:** 04/09/2002 **Application # :** 09182342 **Filing Dt:** 10/29/1998**Inventors:** THOMAS MARK HASTINGS, MICHAEL E. MCNEIL, TODD S. GLASSEY, GERALD L. WILLET**Title:** CONTROLLING ACCESS TO STORED INFORMATION BASED ON GEOGRAPHICAL LOCATION AND DATE AND TIME**Assignment: 1****Reel/ Frame:** [009555/0985](#) **Recorded:** 10/29/1998 **Pages:** 4**Conveyance:** ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).**Assignors:** [HASTINGS, THOMAS MARK](#) **Exec Dt:** 10/28/1998[MCNEIL, MICHAEL E.](#) **Exec Dt:** 10/27/1998[GLASSEY, TODD S.](#) **Exec Dt:** 10/27/1998[WILLETT, GERALD L.](#) **Exec Dt:** 10/28/1998**Assignee:** [DIGITAL DELIVERY, INC.](#)
54 MIDDLESEX TURNPIKE
BEDFORD, MASSACHUSETTS**Correspondent:** FISH & RICHARDSON P.C.
DAVID L. FEIGENBAUM
225 FRANKLIN STREET
BOSTON, MA 02110-2804**Assignment: 2****Reel/ Frame:** [010456/0059](#) **Recorded:** 12/15/1999 **Pages:** 2**Conveyance:** ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).**Assignor:** [DIGITAL DELIVERY, INC.](#) **Exec Dt:** 11/08/1999**Assignee:** [DATUM, INC.](#)
54 MIDDLESEX TURNPIKE
BEDFORD, MASSACHUSETTS 01730**Correspondent:** FISH & RICHARDSON P.C.
DAVID L. FEIGENBAUM
225 FRANKLIN STREET
BOSTON, MA 02110-2804**Assignment: 3****Reel/ Frame:** [012721/0294](#) **Recorded:** 03/26/2002 **Pages:** 9**Conveyance:** SECURITY INTEREST (SEE DOCUMENT FOR DETAILS).**Assignor:** [DIGITAL DELIVERY, INC](#) **Exec Dt:** 07/07/2000**Assignee:** [WELLS FARGO BANK, N.A.](#)
2030 MAIN ST

ORANGE COAST RCBO
IRVINE, CALIFORNIA 92614

Correspondent: WELLS FARGO BANK, N.A.
STEPHEN AMENDT
201 THIRD ST. 8TH FLOOR
ATTN: LOAN DOCUMENTATION AU 2695
SAN FRANCISCO, CA 94103

Assignment: 4

Reel/ Frame: [014120/0637](#)

Recorded: 06/02/2003

Pages: 15

Conveyance: MERGER (SEE DOCUMENT FOR DETAILS).

Assignor: [DATUM, INC.](#)

Exec Dt: 02/03/2003

Assignee: [SYMMETRICOM, INC.](#)

2300 ORCHARD PARKWAY
SAN JOSE, CALIFORNIA 95131-1017

Correspondent: GARY CARY WARE, ET AL.
JOHN J. BRUCKNER
1221 SO. MOPAC EXPRESSWAY, SUITE 400
AUSTIN, TEXAS 78746

Search Results as of: 01/16/2006 09:14 AM

If you have any comments or questions concerning the data displayed, contact OPR / Assignments at 571-272-3350

[| HOME](#) | [INDEX](#) | [SEARCH](#) | [eBUSINESS](#) | [CONTACT US](#) | [PRIVACY STATEMENT](#)