



Notice of Service of Process

Transmittal Number: 12918213
Date Processed: 09/05/2014

Primary Contact: Legal Department
Internet Society
1775 Wiehle Ave
Suite 201
Reston, VA 20190

Entity:	Internet Society Entity ID Number 1867995
Entity Served:	The Internet Society
Title of Action:	Todd S. Glassey vs. MicroSemi Inc
Document(s) Type:	Summons/Complaint
Nature of Action:	Trademark / Copyright / Patent
Court/Agency:	U.S. District Court Northern District, California
Case/Reference No:	CV-14-3629-EDL
Jurisdiction Served:	District Of Columbia
Date Served on TCC:	09/04/2014
Answer or Appearance Due:	21 Days
Originally Served On:	CSC
How Served:	Certified Mail
Sender Information:	Todd S. Glassey 408-890-7321

Information contained on this transmittal form is for record keeping, notification and forwarding the attached document(s). It does not constitute a legal opinion. The recipient is responsible for interpreting the documents and taking appropriate action.

To avoid potential delay, please do not send your response to The Company Corporation

CSC is SAS70 Type II certified for its Litigation Management System.

2711 Centerville Road Wilmington, DE 19808 (888) 690-2882 | sop@cscinfo.com

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

Todd S. Glassey, In Pro Se,
Micheal E. McNeil, In Pro Se

Plaintiff(s)

v.

Civil Action No. CV-14-3629-EDL

Microsemi Inc et Al

Defendant(s)

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

The Internet Society (including but not limited to its IETF operations group), C/O Corporation Service Company,
1090 Vermont Ave NW, Washington DC, 20005

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

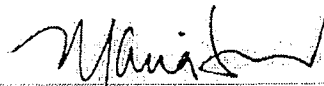
Todd S. Glassey, 305 McGaffigan Mill Road, Boulder Creek CA, 95006 and Michael E. McNeil, PO Box 640, FELTON CA 95018-0640

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date:

8/27/14
8/22/2014


Signature of Clerk or Deputy Clerk

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

(San Francisco Division)

TODD S. GLASSEY, In Pro Se
305 McGaffigan Mill Road
Boulder Creek, California 95006

And

MICHAEL E. MCNEIL, In Pro Se
PO Box 640
Felton CA 95018-0640

Plaintiff,

vs.

MicroSemi Inc; The IETF and ISOC, and
the US Government and Industry
partners (including but not limited to
Apple, Cisco, eBay/Paypal, Google,
Juniper Networks, Microsoft, NetFlix,
and Oracle), USPTO ALJ Peter Chen Esq,
and two individuals (Mark Hastings and
Erik Van Der Kaay) as "NAMED DOES"

Defendants.

) CASE NO. CV-14-3629-EDL
)
) JUDGE E. D. LaPorte, Courtroom E,
) 15th Floor USDC San Francisco
)
)
) **COMPLAINT**
) Sherman Act violation, Fourth, Fifth,
) Seventh and Fourteenth Amendment
) Violations; Foreign Antitrust Act
) violation; RICO Act claims against
) Microsemi and IETF; Copyright Fraud
) (IETF); Patent Infringement (IETF et
) Al.); Tortuous Interference; Assorted
) Patent (Fiduciary) Frauds;
)
) Illegal use of FISA Act provisions in
) those violations by Defendant USG
)
) **Jury Demand Endorsed Hereon**
)
)
)

For this Complaint, Plaintiff Todd S. Glassey and Michael E McNeil state as follows:

Defendants, Does, Patents, and Settlement List

1. Plaintiffs are individuals who were, for all times relevant hereto, residents of Santa Cruz County, California.

2. Defendant Microsemi, Inc. ("**Microsemi**"), is, on information and belief, a Delaware corporation with its principal place of business in Aliso Viejo California. This under Bivens includes the "unknown Officers and those controlling the operations of the Defendant Microsemi" as individuals under the Bivens precedent¹.

3. Defendant Symmetricom, Inc. ("**Symmetricom**"), was, on information and belief, a Delaware corporation with its principal place of business in Irvine California.

4. Defendant Symmetricom did, on information and belief, acquire the assets and liabilities of Datum, Inc. ("**Datum**"), in 2002 through a Merger creating a new Symmetricom Corroboration as the successor to Datum.

5. Defendant Erik Van Der Kaay ("**EVDK**") is by information and belief the CEO and Chairman of the Board of the Datum Corp (the umbrella Corp holding the Business units of Datum and its acquired companies);

6. Defendant Datum did, on information and belief, acquire the assets and liabilities of Digital Delivery, Inc. in or about July 1999.

7. Defendant Digital Delivery Inc ("**DDI**") is a Massachusetts based corporation which Plaintiffs retained for Patent Agency legal representation;

8. Defendant Mark Hastings ("**Hastings**") is by information and belief the President and Founder of DDI and later was made the President of the BanCom (Bandwidth Compression) division of Datum Inc;

9. Both Defendants, Hastings and Van Der Kaay are direct signatories to Glassey and McNeil contract documents with both corporations and both names

¹ (*Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971))

appearing on the DDI settlement and Van Der Kaay's on the TTI Settlement as well herein;

10. Defendant Microsemi ("**Microsemi**") is, on information and belief, the successor in interest for any liabilities of Symmetricom, Datum and DDI to Plaintiffs. As such any use of the predecessor name for Microsemi is only intended to indicate the time frame for the action or claim in this ongoing fraud and Sherman Act Violation.

11. The Defendant Internet Engineering Task Force ("**IETF**") is on information and belief, a Industry-Wide Technology Standards Collective and is operated under the banner and law of the US as a subdivision of the Washington DC Corporation called "The Internet Society".

12. The Internet Society ("**ISOC**") operates the IETF is as the world's Global Standards Organization for the Internet and it is the IETF who has produced the majority of the network standards that applications which infringe on the rights here were written from.

- a. This definition of the IETF includes their management under Bivens and membership in the entire IETF as a whole and in several particular groups including but not limited to the **IETF Intellectual Property Rights Working Group (IPR)**, **IETF GeoSpatial Controls Working Group (GeoPriv)**, the **IETF or Generic Network Working Group (IETF@IETF.ORG)** where everyone talks about everything and time-related ones in both **PKIX WG** (the PKI working group areas) and those pertaining to other protocols like **Secure DNS (DNSSEC)** which uses the Infringing IP extensively as just one of many examples of IETF infringements;

13. The Defendant Internet Society ("**ISOC**" - www.isoc.org) itself includes such other child-organizations as the Internet Corporation for Assigned Names and Numbers ("**ICANN**") and the American Registry for Internet Numbers ("**ARIN**") and its foreign instances.

14. Because of the ISOC and IETF dependence on Computers running "Infringing Networking Drivers and Applications" ("**INDA**") the ISOC as well as the IETF, the ARIN, the ICANN, and all other operating infrastructure itself are named collectively as ***members of the ISOC Family herein;***

15. And that this matter pertains as such to the ISOC all of its many arms and their publications as well as all electronic events performed online by them since the Cease and Desist Order was served on ISOC and its IETF operating unit through their IETF IPR Filing Process in 2004 (their method of service); As such that the IETF and ISOC are named actual defendants to the matter herein;

**The following Parties are NAMED AS DOES in accordance with
provisions of the BIVENS² ruling**

16. The Defendant "United States Government" ("**USG**") from Legislative to Administrative branches, because of its dependence on Computers running "INDA" is named as a Defendant DOE and since the full scope of the names therein are unknown to the Plaintiffs at this time this naming convention meets the strict DOES limitations for the US District Court';

² *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971),

17. Further the following Federal Agencies and Roles are known but the parties filling those roles are unknown at this time and so they are also identified directly as DOES in this matter;

- a. The US Department of Commerce ("**DoC**") and its three key subdivisions (**US PTO** - Patent and Trademark Office, **US NTIA** - National Telecommunications Infrastructure Administration, and **US-NIST** - The US National Institute of Standards and Technology **and in particular its Information Technology Laboratory (NIST-ITL)**) are entities of the United States Government;
- b. **Defendant Peter Chen Esq.**, under Bivens is named as an actual defendant and not a DOE although he now is employed by USPTO, and so is named both under their naming as a DOE and as a real person; Additionally we name Defendant Peter Chen's Lawfirm at the time of the alleged acts herein of Lathem Watkins LLP as a DOE based on Bivens standing for the parties within the firm actually involved (a matter which Discovery will properly disclose);
- c. The **US Department of Energy** as a consumer in operating the US Smart Grid and various other research projects which make it an infringer;
- d. The **US Department of Transportation** and the **US FAA** Flight Tracking and Messaging Systems using infringing technologies nationally herein;
- e. The **US Treasury** as a consumer of the infringed properties and the oversight provider for its agencies the **SEC** as well as the **IRS**;

- f. The US Department of Defense ("DoD");
 - i. Any and all parties (Boeing, Macdonald/Douglas, Lockheed Corp, General Atomics, et Al) building or selling Drones or components thereof to the US Government;
 - ii. Any and all parties building selling or transporting Ballistic Sensor Fused or Controlled Munitions or Munitions Delivery Systems including but not limited to those ballistic devices used to place objects into low and medium orbital tracks;
- g. The **US Intelligence Community** (all agencies and those attached therein).
- h. The Office of the President of the United States of America ("POTUS") and the operations of the Whitehouse Webserver itself;
- i. The Honorable Mr. Jerry Brown, the Governor of the State of California and the State of California itself under 42 U.S.C. § 1983 and its provisions for Civil Litigation against a State under the *Enforcement Act of 1871* and other statutes;

Industry Members of the IETF and ISOC

18. The following are named members of the IETF who all either both use and operate within the IETF itself a formal presence and who both use these controlled Intellectual Properties controlled under the "TTI and DDI Settlement Documents" inside their products and corporate operations both; They include but are not limited to

- a. **Apple Corp**, A Delaware Corporation including all of its external and foreign corporations or assets;
- b. **Cisco Corp**, A Delaware Corporation including all of its external and foreign corporations or assets;
- c. **eBay and Paypal**, each a Delaware Corporation including all of its external and foreign corporations or assets;
- d. **Google**, A Delaware Corporation including all of its external and foreign corporations or assets; and all of its sub-division and free-standing corporations operated outside of the Google brand;
- e. **Juniper Networks**; A Delaware Corporation including all of its external and foreign corporations or assets;
- f. **Microsoft Corporation** a Delaware Corporation and all of its free-standing business units and external corporate assets;
- g. **and Oracle Corp**, A Delaware Corporation including all of its external and foreign corporations or assets;
- h. Additionally there is one other DOE to name as a corporation; That being The **Thales Group ("Thales")** (a Delaware Corporation) the landed US Base of the larger Defense Systems contactor "The Thales Group" of Cedex France, and its **eSecurity Division**, A Delaware Corporation called **"E-Security, Inc"** (nee "nCipher Inc" of Cambridge England).
- i. The eSecurity Division of the Thales Group US operations is located in the State of Florida; and claims against Thales Group and in particular

to the eSecurity Division pertain to its use of TTI Settlement IP and breach of the TTI Settlement through its partner Microsemi;

PATENTS

19. US6370629 ("629") the US patent filed in Plaintiffs behalf by Mark Hastings of DDI, **EP-o-997-808A3**, the Abandoned instance of the US6370629 filed in the EU, **BR9904979** the abandoned instance of '629 filed on Plaintiff's behalf in the Nation of Brazil; **CA2287596** is the abandoned filing of US6370629 in the Nation of Canada, as **2000163379** is the number of the '629 filing in Japan, and finally the South African filing **ZA1999/06799**
20. US6393126 (aka "**3126**" also known as US 20020056042 A1) "a System and methods for generating trusted and authenticatable time stamps for electronic documents" ("3126"), the US patent filed by EVDK showing himself as inventor of IP "he licensed limited derivative uses of from Master Designs for the TTI" belonging to Plaintiff Glassey; Likewise **CA2398415** (CAI2398415 A1) is the unauthorized filing of US6393126 in the Nation of Canada, it exists in the EU (**EP 1279287** A1) and was expanded by re-filing as the **US 20020056042 A1 WO** patent application which did issue;

SETTLEMENT AGREEMENTS

21. **DDI Settlement** - pertains to the Pre-paid legal service agreement with DDI (the Co-Inventor Agreement) and Datum's limited use of the patents' protected IP while its continuing role as Fiduciary persists. The Settlement

Agreement is the other half of the Co-Inventor Agreement Document Pair that is described in detail in the Co-Inventor Agreement.

22. **TTI Settlement** ("TTI") - pertains to the Datum use of the Glassey TrustedTiming Infrastructure and its limited use of the IP in the United States and State of California legal requirements therein.

23. **Co-Inventor Agreement** - The PrePaid Legal Service Agreement and Patent Assignment Documents (self explanatory) - the original Co-Inventor Agreement to was used to create a patent filing, which became the shared use patent US63709629 with DDI and its successors as the permanent fiduciaries in charge and responsible for the costs in those actions.

JURISDICTION AND VENUE

19. This Court has original subject matter jurisdiction over this suit pursuant because of a number of issues the first of which is that this matter pertains to 28 USC § 1338 because the matters in it relate to patents, International filing of patents and copyright infringements; It also relates to Sherman Act and rulings from the US Supreme Court (MGM Studios v Grokster) and other key rulings which State Courts do not have the authority to apply in this matter.

20. This subject matter pertains to the use of the US Foreign Intelligence Service Act to create a set of "Impossible hurdles" for Plaintiffs to cross to bring this into Federal Court which would stop anyone retaining private counsel through the service of a FISA Act Warrant or National Security Letter in the matter herein;

21. This Court has subject matter jurisdiction over the remaining claims at issue in this suit pursuant to is supplemental jurisdiction as codified by 28 USC § 1367 because they form part of the same case and controversy as those claims relating to patents and their infringement through licensing issued via copyright in Global Network Standards for the use of these intellectual properties.

22. This Court has personal jurisdiction over this matter because the Plaintiffs reside in this judicial district and a substantial portion of the events below took place in this district.

23. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims at issue in this dispute occurred in this district.

24. Additionally under the construct of ***Subject Matter Jurisdiction***, because this case uniquely involves both US and a number of both legally and illegally filed International Patents it is both a Sherman Act and the Foreign Antitrust Act with their provisions which now control large parts of the US National Critical Infrastructure this case can only be heard before the US District Court since no State Court has authority to issue Orders against the US Government for patent and international antitrust matters.

25. Finally under Jurisdiction, this matter asks the US District Court a unique and novel question of Federal Law "as to whether Patent Protections in an issued Patent can be set aside by a copyrighted Network Technology Standard under the Defendant IETF's claim that 'Copyright Section 107 Exemptions also allows them to infringe on patent protections on software products they designed the very uses for themselves'".

26. The assertion of this litigation is that this is a statement which on its face directly violates the US Supreme Court ruling in MGM Studios v Grockster while they (the IETF) continue to publish under their own copyright against their use of the technology, a license we allege is "intended to cloud or make impossible to enforce **any Software patent protections globally** against those IP's used without authorization in those standards" and on which they the IETF have since made the world's computers dependent.

27. This question is amplified by the commentary that the IETF in fact uses this same Intellectual Property in the form of programs inside its infrastructure without authorization daily to operate the IETF's computers, and that this was done after codifying it into the global standards for all Local Area Networking today.

28. The question posited on the court by this suit is now that this was formally done to the Plaintiff's IP's and re-licensing enforcement rights by Defendants Microsemi and IETF and their third-party infringers, the question therein before this court is "what are Plaintiffs' recourse herein?".

STATEMENT OF OPERATIVE FACTS

29. This Complaint is being brought in the United States District Court because there are multiple issues in dispute between multiple parties including the US Government and a Global Standards Organization which require the Court to construe the claims of certain US Patents and a set of alleged frauds therein at the Fiduciary level, the relationship of those Patents to US Copyrights when a Global Standards Agency takes that IP and weaves it into the process descriptions of their networking protocols.

30. And finally the effect under MGM Studios v Grokster and other precedents pertaining to Intellectual Property protections what the recourse is against the Standards Agency and their Membership for these actions which force anyone implementing programs that meet that standard to infringe.

31. And additionally for their (the Standards Agency and its parent the ISOC) use of those infringing programs in their own operations.

32. The allegation of the claims is that because the IETF further encoded those protected methods from a US or Foreign Patent into their Standard, this makes anyone using that standard equally culpable for their actions as third-parties to the alleged conversion of private property this suit alleges.

The Complaint

33. This complaint is based on the complaint, supporting evidence exhibits, declarations and memorandums of points and authorities, precedent law, US national IP Policy, *and is fully supported by the US Government mandatory requirements per the TRIPS/PCT treaty agreements.*

34. Additionally aspects of this matter pertain to "a set of alleged frauds which the primary defendant Microsemi committed with in concert with the Global Standards Organization IETF (the Internet Society) to prevent Glassey and McNeil's enforcement demands previously that the IETF and everything it produced since 2004 is based on an active infringement in its operations" and they cease and desist any use of the IP. As such a subsidiary claim against all of the online networking standards produced is included as well.

Defendant IETF and their use

35. The Defendant IETF (The Internet Engineering Task Force) is a global standards organization who operates their infrastructure across the Internet as part of their charter so they use all of the standards they create in the form of programs and infrastructure inside their frameworks. The IETF is an operating unit of the Internet Society and they bear full financial responsibility for its operations and these alleged frauds herein we assert.

36. The IETF has no authorization to use the IP for its own uses and because of that it "likewise cannot publish across its framework anything which infringes because it cannot use that IP inside its own framework".

37. This then is the Catch-22 the IETF has created. They can no-longer operate without infringing the Phase-II Technology Licensing Rights the Plaintiffs are the sole owners of because it is inside the machines they created the standards for.

38. To summarize the claims against IETF and ISOC: The unauthorized use of the Patent-Protected Intellectual Properties is then alleged in both 1) the IETF operating infrastructure and then 2) as direct additions to their documents themselves as the "methods and processes of the protocols they are standardizing"; We further state that this has already been done for a number of the World's Internet Standards such that it created three billion daily infringers; the net-effect is this single Patent now controls (or there are claims for) most all online commerce globally and the loss amounts respective of that include but are not limited to the direct infringements "for any and all Local area and Internet Application Systems" in use globally today.

39. The functional result is that everyone using the Local Area Networking Protocols outside the Internet is also an infringer of those same IP rights;

40. That because of the alleged fraud inside the very standards process itself, an action which could have been stopped by defendant Microsemi as far back as 2004 when the first "Acknowledgement of Glassey and McNeil rights requests were submitted to then 'Symmetricom Corp' as the predecessor to Microsemi", both the IETF (and its membership) and Microsemi equally bear responsibility under the precedents set in MGM Studios v Grokster and others, and are liable herein for any and all damages resulting from their collective and individual actions.

Microsemi blocked verification of all of Plaintiffs verification requests

41. Rather than perform its role under the contract Symmetricom Staff refused to confirm or even respond to the parties we requested they confirm the settlement and our rights to.

2013/2014 Breaches

42. Finally that to Transfer the Settlement Agreement and the Role of Fiduciary codified in it that (see CONTRACTS/DDI-Settlement) Microsemi must formally and publicly assert its liability or no such transfer occurs. Microsemi has refused all communication and demands it agree to the terms of the Contract as the Settlement Agreement requires and that has created a new cause of action in this matter in 2014 which tolls the statutes on all other acts in this matter as well.

43. As such it is in breach of the Settlement Agreement as well currently supporting these claims.

HISTORY: Previous Litigation

44. Prior to the filing of this Complaint in this Court, the Plaintiffs and Symmetricom were parties to a California Superior Court suit captioned *Michael E. McNeil, et al. v Book (Symmetricom) et al.*, which was dismissed without prejudice to any of the claims therein and proceeded as that Court's Case No. CV 165643 (the "State Court Lawsuit").

45. This filing is the transfer of that lawsuit to the Federal Jurisdiction in full because the State Court Lawsuit could not continue to be prosecuted in California Superior Court because, as that case developed, it became apparent that the California itself as the State was conflicted as a major infringer and further the Superior Court would be required to construe "US Patent and simultaneous copyright claims" which no Federal Court has ruled in yet, and perform this ruling against parties in a number of jurisdictions (*the IETF and its international members) to render any judgment on the claims for relief Plaintiffs brought, and that the California State Court lacked the subject matter jurisdiction to do so.

46. Further since the Federal Government is the signatory to the TRIPS agreement the international nature of the abandoned instances of US6370629 patents filed in Japan, Brazil, Canada, South Africa and the EU are only actionable under the TRIPS treaty in the US and only the US District Court has standing in an international treaty.

HISTORY: Plaintiffs' Relationship with Datum

47. In or about October 1997, Plaintiff Glassey approached Datum through Davey Briggs VP of Marketing for the Beverley Massachusetts division of Datum. The purpose of the conversation was to retain Datum to "manufacture a component of the time controls" for an email and document control gateway of Glassey's design. The design was called the Trusted Timing Infrastructure and creates a set of evidence-to-transaction models and the technology to implement them.

48. Initially Datum said "no to building the high-end components of the system" but was very interested in the component level Trusted Local Clock Module as a potential mass-market addition to Datum's existing Board Level Timing Products so they referred GLASSEY to the San Jose California division called BANCOM.

49. At Bancom/Datum Glassey interfaced initially with Mitch Stone ("**STONE**") the VP of Marketing; Glassey's request to Datum if he was right would open new end-user and OEM markets to Datum in the board level timing products area and to further to that Stone opened detailed market analysis discussion between Plaintiff Glassey and Datum, concerning whether Datum and Glassey might undertake broader business efforts together; To allow free and open discussion about Glassey's IP Datum and Glassey entered into a mutual nondisclosure agreement in November 1997 (the "**Datum NDA**"). Mitch Stone processed that NDA.

50. In the months following the execution of the Datum NDA, Glassey and Datum (through Mitch Stone as the principal point of contact) had a variety of conversations and did a variety of industry analysis efforts to determine the total potential of the market sector for this time-stamping evidence system; this effort

included two road trips on which Glassey and Datum VP of Marketing Mitch Stone ran the customer survey with exciting results.

51. The next step was a meeting "with the division presidents of all of Datum and a Board Meeting" which was to happen at a local trade show in Atlanta; to Attend the meeting Glassey was flown out to present the total of the potential to the Board and officers of the corporation for the Trusted Timing Infrastructure components he asked them to build for him. The meeting produced full approval for the joint-development effort.

52. At this point Datum initiated aggressive discussions with Glassey about product design of their systems and how his infrastructure could be used to advance their existing BC635 GPS based timing card as a stand alone and clustered time service module.

53. This excited Datum CEO Erik Van Der Kaay (EVDK); EVDK called Glassey and told him the deal was on. He asked Glassey to both incorporate and bring in at least one more engineering member for his team and promised both guaranteed financing through a monthly payment process to let GMT just focus on the engineering as well as longer term reseller status.

54. To meet that demand, in early 1998 Plaintiff Glassey was joined in his commercial efforts by Plaintiff McNeil in Glassey's new company known as Glassey-McNeil Technologies or "GMT".

55. To support Datum running Payroll for GMT on or about May 4, 1998, Plaintiffs each executed a consulting agreement with Datum for the purpose of securing certain technical consulting services (the "Datum Consulting Agreements"), true

and correct copies of which are attached as Exhibits CONTRACTS:Glassey and Exhibits CONTRACTS:McNeil hereto.

56. The Datum Consulting Agreements were effective from May 4, 1998, to July 4, 1998, and during that period Plaintiffs provided services to Datum exclusively relating to market analysis to support Datum's developing e-commerce division.

57. Upon the expiration of the Datum Consulting Agreements, Plaintiffs and Datum agreed to continue to work together without further written agreements with the understanding, based on the existing Datum NDA, that Plaintiffs would own any and all intellectual property developed by them or shared by them during the term of the continuing relationship and that Plaintiffs would be independent contractors for Datum.

58. Among the tasks Plaintiffs agreed to take on as independent contractors for Datum after July 4, 1998, were the identification of potential acquisition targets for Datum as it sought to expand its e-commerce business.

HISTORY: Plaintiffs' Relationship With DDI

59. From approximately December 1997 onward, Plaintiffs worked to develop other relationships in the industry for the purpose of commercializing their time control technologies.

60. One of the companies that Plaintiffs developed a relationship with was Digital Delivery Inc ("DDI"). Glassey and DDI President Mark Hastings were talking about adding some timing controls to DDI's product suites and so then entered into a Non-Disclosure Agreement (Jun 1997) to further those discussions.

61. Later but under the NDA Glassey disclosed the scope and design of his GeoLocation Controls and Location Based Policy Services to Hastings as his new patent

application; This conversation took place in the employee second floor lounge at Westlaw Main with Westlaw Employee Ruven Schwartz Esq and Datum VP Mitch Stone present. Hastings had accompanied Glassey and Stone to Westlaw to discuss time services and Glassey's Trusted Timing Infrastructure with them as a product potential.

62. Hastings was excited about the idea of using secure time and location information (physical, logical or virtual) as a control aspect of a policy switch. This can be used for many other key applications as well so he became very aggressive with Glassey about getting these 'new features' patent protected and added to Confidential Courier at all costs.

63. One weekend in later August of 1997 Glassey was approached by DDI president Mark Hastings about his (Hastings) acting as Glassey's Patent Agent for the filing of the location based service patent. Glassey initially didnt trust the situation and because Hastings was formally represented by Richards and Fish and they would be representing Glassey before the PTO through Hastings it seemed believable.

64. There were numerous discussions between Glassey and Hastings about this including one key one where it was finally agreed that "with Richards and Fish as counsel of record that Hastings could represent Glassey before the PTO".

65. Under the NDA between Glassey and Hastings, the Plaintiffs turned over the initial Intellectual Properties to the Agent (Hastings and DDI) for the creation of the filing documents for the USPTO;

66. At this Time DDI president Mark Hastings and his counsel from Richards and Fish approached Glassey with a new plan. The "new plan" was that rather than Hastings filing a new patent for Glassey which he would sublicense from Glassey he

would file an amendment to the one he already had and Glassey would share the enforcement rights against its IP through a subsidiary agreement;

67. This was a 100% reversal of the roles under which the original agreement was consummated. Because of this Glassey again was very uncomfortable about and said no initially; it was only after a number of further conversations and Glassey's being assured by Richards and Fish ***the patent would issue quickly*** Glassey agreed.

68. Thus the amended instance of the Hastings "Confidential Courier" patent ("992") was filed in 1998; Everything was fine initially although Glassey and McNeil were concerned about how little of the original ((2 technology one could identify in the filing but it was early in the process and the initial Examination was a year away or so Glassey was told so we just waited.

69. As part of his work with Datum Glassey had introduced Hastings to Datum formally; In early 1999 things changed.

70. Hastings immediately stopped answering questions about the patent's filing and in July in violation of the Co-Inventor "E Assignability Section Hastings reassigned the patent to Datum and sold them Digital Delivery Inc taking a job replacing the then incumbent president of the BANCORM Division of Datum where Glassey's work was done.

71. As to how he did that when Richards and Fish filed the patent originally they omitted the agreement which said the assignment was only valid for one year (in the Co-Inventor Agreement) from the filing and improperly filed it as ASSIGNED instead of CONDITIONALLY ASSIGNED. This allowed Hastings to sign on the reassignment without Plaintiffs Signature. This was corrected with the attached EXHIBITS: PTO-Correction-to-629 (USPTO correction to original filing status).

72. Thus the Federal Record for the original filing was finally corrected on August 6th 2013 to reflect the original assignment as conditional; Glassey's sole purpose for retaining DDI was to get a low cost guaranteed filing in half a dozen jurisdictions and to get the patents issued as soon as possible. The new amended instance of the original DDI patent was to be filed with U.S. Office and the foreign instances agreed upon later (Brazil, EU, Japan, Canada, and South African) as the **Controlling Access Patent** and DDI and Plaintiffs sought to formalize an agreement which would allow for the most prompt filing of the application for the Controlling Access Patent.

HISTORY: The 1998 Pre-paid Legal Services Contract ("The Co-Inventor Agreement")

73. To enable this global patent filing activity effective on or about October 26, 1998, Plaintiffs and DDI entered into a "pre-paid legal services" agreement known as the **Co-Inventor Agreement**, a copy of which is attached hereto as Exhibit:Co-Inventor-Agreement.

74. The Co-Inventor Agreement retains Hastings and his company Digital Delivery Inc of Massachusetts ("DDI") to act as Plaintiffs' Patent Agent with full legal control and power of attorney relative to the limited area of patent filings.

75. According to Recital D of the Co-Inventor Agreement, its purpose was:

[T]o 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.

76. Recital A of the Co-Inventor Agreement commemorated DDI's ownership of the Confidential Courier product and its underlying patent ('992 patent). This is very important when considering how much of the underlying intellectual property from the original patent went into the filing or amendments to US6370629, a number which approaches zero in retrospect, meaning all of US6370629 is in fact PHASE-II technology;

77. Paragraph 1.C. of the Co-Inventor Agreement commemorated that Plaintiffs developed and provided to the Controlling Access Patent application geolocation Controls and Location Based Services known as "**Phase II**" a Term of Art meaning a system providing both physical location information but also very accurate time with phase matching data for aligning cryptographic heartbeats across a network or distributed framework. One very powerful source (though only a single example) of providing such time and location data is obviously the US Governments GPS sources.

78. Thus "Phase-II" technologies provides for a new level of authentication over the basic services Hastings had built into his existing patent. From the data model perspective Phase-II technology represents an authentication schema concurrent with industry standards in cryptography³

79. Paragraph 2.A. of the Co-Inventor Agreement provided further that, "[DDI] acknowledges that the Phase II technology is solely and exclusively the idea and invention of [Plaintiffs]."

³ as an example we list one Phase II authentication schema description - "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." but there are a number of others as well.

80. The Co-Inventor Agreement was designed to be a work-in-progress agreement and was to be replaced in form by a larger agreement. One which codified Plaintiffs' rights to the IP and their third party enforcement rights (any and all uses) for the IP that they purchased the pre-paid legal services for.

81. The Co-Inventor Agreement explicitly contemplated that a future "definitive" agreement would be entered among the parties concerning the compensation to be paid to Plaintiffs as well as the parties' mutual and exclusive rights to the Controlling Access Patent within 365 days of the signing. At that time the Provisional Access and use Rights to both the original filing and Hastings' 992 patent became open.

82. Finally the last possibility documented in the Co-Inventor Agreement was a total failing on Hastings' part where both patents revert to shared by Plaintiffs as the superior rights holder in third-party enforcement of the patent-protected IP.

83. Two days after the Co-Inventor Agreement was executed, on October 29, 1998, the Controlling Access Patent Application (the "**1998 Patent Application**") was filed with the US Patent and Trademark Office ("USPTO"), a copy of which is attached as Exhibits:629-as-authorized hereto and in it McNeil and Hastings and his partner were added to the patent filing so the final title includes all four parties, Glassey as the principal inventor, McNeil as Glassey's senior Engineering Specialist, and Hastings and Willets for their work in the previous patent. As it happens though Willets was never on the original patent and as such shouldn't have been on the final filing as well. This then is allegedly yet another misrepresentation from Hastings in the filing of US6370629.

○

HISTORY: DATUM purchase of DDI violated the DDI/Glassey Contract "no transfer" terms

84. In violation of the IP transfer provision of the Co-Inventor Agreement Datum and DDI consummated a merger on or about July 29, 1999, whereby DDI became a wholly owned subsidiary of Datum upon which merger Datum became the successor-in-interest to all of the rights and responsibilities contemplated by the Co-Inventor Agreement. As such Datum became the Fiduciary although Glassey and McNeil were both very dissatisfied with the situation.

85. Section Five (5) of the Co-Inventor Agreement protects the Role of Fiduciary in what was called the Non-Assignability Clause; which was violated by Defendants and documented in their July 8K (Exhibits: CONTRACTS:CO-Inventor Agreement) report to the Securities and Exchange Commission of the Department of the Treasury, US Government. The section is excerpted here for reference. The reference is split across both Page 4 and Page five (5) continues with the text of section 5.

What it clearly says is ***that the Patent Ownership and the Role of the Patent Agent & Fiduciary here 'may not be assigned to any third party for any reason without a release from Plaintiffs'.***

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.

No such release was ever asked for, contemplated by Plaintiffs or executed, and Datum's solution was simply to immediately attack its new "client" and sue GMT/Glassey and McNeil as individuals and withhold operating funds it as GMT's sole customer at the time owed the company to force an extorted settlement as reported in this complaint.

HISTORY: Robinson Letter

86. Immediately after the prohibited purchase of Digital Delivery Inc., Datum Corp fired Bancom Division President David Robinson (see Notice Letter Exhibits:ROBINSON LETTER were Robinson declares formally "Datum doesn't want your IP" letter from Robinson) and replaced him with Defendant "Hastings" (Mark Hastings).

HISTORY: The 1999 Settlements which Plaintiffs allege "were extorted from Plaintiffs"

87. In addition to Hastings coming on board as an officer of Datum two weeks later in August 1999 Datum without warning filed a lawsuit against Glassey and McNeil ("the dispute");

88. Datum, we allege "also as part of this 'covert plan to bankrupt and steal GMT's assets'" did fabricate claims and filed a California Superior Court Lawsuit against GMT and Glassey and McNeil as individuals; and we assert in doing so violated its role as the Fiduciary which it had to accept to move the patent to it as the "acquiring of any fiduciary responsibility contract" in the US requires;

89. this set of actions were a part of an Overall Plan we assert was created inside Datum by CEO Erik Van Der Kaay and furthered directly by officers of Datum and the Successors Symmetricom and Microsemi both.

90. As part of its manipulating GMT into being forced to accept its terms for settlement Datum froze all payments outstanding to Glassey and McNeil after they had just had Glassey expend significant amounts of personal money developing "designed market analysis and other marketing materials for them". The net effect was they as GMT's sole customer at the time functionally drove GMT into insolvency to extort the two settlement documents; as such they manipulated GMT and both Glassey and McNeil personally to the edge of bankruptcy to extort the two settlement documents, both of which they furthermore allegedly breached;

91. Further because these denial-of-rights actions are still being performed today in the new successor to the Contract, by their refusing to accept the role per the terms of the contract for its transfer to a successor of Symmetricom, they have become as culpable for the Damages as Van Der Kaay and Mark Hastings are for creating them in the first place.

92. Through this set of alleged set of actions by DATUM and Hastings/DDI , and with what turned out to be very bad legal advice from GMT-counsel Jason Book Esq, both Glassey and McNeil were "financially manipulated and coerced into accepting

the settlements that Datum Counsel John Cannon drafted, as such Datum was the sole architect of the forms and their contents in the two settlement documents".

In all instances Book esq. advised Glassey and McNeil that they had no rights and would need to take whatever settlement and scraps Datum was willing to throw to us.

HISTORY: Both Settlement Documents look almost identical

93. John Cannon Esq, Datum's attorney at that time created two settlement documents for this matter. One Settlement for Digital Delivery Inc and a second for the Consulting Work and the IP under it which is the subject of US Patent 6393126 called the TTI Settlement.

94. Both documents used the same template and numbering forms and were drafted by John Cannon Esq of Stadling Locca in Newport Beach California. Hence sections 8.x of the TTI settlement are almost identical to those in the DDI settlement.

HISTORY: 1st Settlement - Controlling Access (DDI Patent Agent services) Settlement

95. The two separate settlement agreements were simultaneously signed in late November 1999, one of which is at issue in this section of the lawsuit and is the so-called **Controlling Access Settlement** also known as the **DDI Patent Rights Settlement/management agreement**, a copy of which is attached as Exhibits:CONTRACTS-DDI-Settlement.

96. The Controlling Access Settlement is the specific document the Co-Inventor Agreement says will replace it in regard to its patent filing efforts.

HISTORY: 2nd Settlement - Trusted Timing Infrastructure (tti) Settlement

The second settlement, the TTI Settlement, is patterned after the first (DDI) settlement as was intended to cover the uses of the limited parts of the Glassey TTI service infrastructure that were the topic of the Settlement itself.

HISTORY: DDI Settlement Breach

97. The Controlling Access Settlement was intended as a cap or umbrella for other documents necessary to complete the deal and properly control the patents and the roles for both parties, but served as the “definitive” agreement between Plaintiffs and Datum concerning the initial compensation to be paid to Plaintiffs; it is very clear about who owns which scope of technology but Plaintiffs would have to wait to see in what form the final patent was issued. It is fully contemplated in 1998 by the Co-Inventor Agreement.

98. Paragraph 2.2 of the Controlling Access Settlement defined the “Controlling Access Patent” for purposes of that agreement to include the 1998 Patent Application as well as foreign patents pending Filing Services under the Fiduciary Role for the Patent Filing Agent herein.

99. Paragraph 2.3 of the Controlling Access Settlement defined “**Phase II Technology**” as:

The method of authentication, encryption and transmission of date/time and/or location data for the purpose of linking together two or more disparate electronic components, such that a trust model is established between them. Such physical elements must individually be capable of computational and cryptographic functionality, but computationally may be isolated from one another. Such electronic components must be physically secure, and communicate with each other over communications channel(s) which may themselves be insecure.

100. Phase II Technology included, and expanded, the technology identified as GPS Phase II technology which had been identified as the property of Plaintiffs in the Co-Inventor Agreement.

101. Pursuant to Paragraph 3.2 of the Controlling Access Settlement, Plaintiffs assigned "all rights, title, and interest" in the 1998 Patent Application and foreign patents based thereon to Datum.

102. However, Datum explicitly agreed in Paragraph 3.3 of the Controlling Access Settlement that Plaintiffs, "own[] all rights, title and interest in the Phase II Technology".

103. Paragraph 3.3 of the Controlling Access Settlement granted Datum a "perpetual, non-exclusive, irrevocable, assignable, sub-licensable, worldwide license for use of the Phase II Technology and derivatives thereof, with rights to sublicense, in connection with the limited scope of the DDI Confidential Courier product and its derivatives".

104. According to the foregoing provisions of the Controlling Access Settlement, Plaintiffs had exclusive rights, title, and interest to Phase II Technology, anywhere in the world, except for the limited rights which Datum had to use that Phase II Technology which was identified in the 1998 Patent Application.

105. Also according to the foregoing provisions of the Controlling Access Settlement which granted all ownership rights in Phase II Technology to Plaintiffs, subject to Datum's license, Datum had an obligation to protect and maintain any and all patents relating to Phase II Technology to which it was assignee.

106. Paragraph 3.6 of the Controlling Access Settlement further clarified the parties' intent that Plaintiffs would continue to have the right to commercialize Phase II Technology.

107. Specifically, Paragraph 3.6 memorialized that Plaintiffs agreed not to, "make, use, or sell any products developed using or derived from the Phase II Technology which also include the technology described in or covered by [Datum's existing Confidential Courier patent]" which under the terms of the original Co-Inventor Agreement was not jointly owned by both DDI and Plaintiffs in the agreement.

108. The above clarifies that Plaintiffs retained all rights to make, use, and sell new "Phase II" Technology which did not also include the technology described in or encompassed by the patent covering the Confidential Courier product; but since that patent (the '992 Patent) had already transited to a shared resource this provision of the settlement was found to be moot and unenforceable.

109. As of the effective date of the Controlling Access Settlement, the 1998 Application had been pending at the US Patent and Trademark Office ("PTO") unchanged from its October 28, 1998, filing date.

HISTORY: The 2001 Controlling Access Patent Application Expansion

110. After the parties executed the Controlling Access Settlement, Datum continued the prosecution of the Controlling Access Patent but ran into disapproval of the original expansion of Hastings' existing patent which was never communicated to Plaintiffs as required under section 8.7 of the Controlling Access Settlement.

111. At no time following the execution of the Controlling Access Settlement were Plaintiffs allowed to be involved in the prosecution of the Controlling Access Patent.

112. At no time following the execution of the Controlling Access Settlement did Datum ever attempt to include Plaintiffs in the prosecution of the Controlling Access Patent or advise them of the status of that prosecution.

113. Following a rejection of the developing application for the Controlling Access Patent once for anticipation and again for obviousness, Hastings under his role as the Bancom Division President at Datum radically expanded the amount of Phase II Technology in the independent claims pursued in the Controlling Access Patent application in its response to office action dated August 20, 2001 (the “**2001 Patent Application Rewrite**”), a copy of which is attached as EXHIBITS:2001-REWRITE hereto.

114. Plaintiffs did not discover the scope and effect of the 2001 Patent Application Rewrite until 2013.

115. As a result of the 2001 Patent Application Rewrite, each of the independent claims Datum pursued in its application for the Controlling Access Patent included vastly more of Plaintiffs’ Phase II Technology than they had ever agreed to license to Datum in the Controlling Access Settlement. This change is detailed in the declaration pertaining to unauthorized changes in the Patent which is attached as EXHIBITS:Patents-2001-rewrite hereto.

116. The consequence of Datum’s radical expansion of the amount of Phase II Technology in the 2001 Patent Application Rewrite was twofold: first, it was sufficient to convince the PTO to grant a notice of allowance of the application and paved the way

for issuance of the patent; and second, it had the effect of subsuming what remained of Plaintiffs' Phase II Technology into the issued Controlling Access Patent and foreclosed them from seeking that patent themselves.

117. The Controlling Access Patent ultimately issued as US Patent No. 6,370,629 (the "**629 Patent**") on April 9, 2002, a copy of which is attached as EXHIBITS:Conformed-Copy hereto.

118. The '629 Patent will be in effect until October 29, 2018.

119. The claims in the 2001 Application Rewrite numbered 12, 18, 21, 25, and 29 were issued verbatim as claims 11, 16, 19, 23, and 27 (respectively) in the '629 Patent.

120. The 629 Patent contained a significant amount of Phase II Technology which Symmetricom had never compensated Plaintiffs for and which Plaintiffs had free reign to license to third parties.

121. Datum, and on information and belief later Symmetricom, prosecuted similar patents to the '629 Patent in other jurisdictions around the world.

HISTORY: Symmetricom's Repudiation Of Plaintiffs' Rights To Phase II Technology

122. In the years following the issuance of the '629 Patent, Plaintiffs attempted to license their Phase II Technology, as embodied in the '629 Patent, to various third parties.

123. Datum (hereafter referred to interchangeably with its parent Symmetricom) interfered with Plaintiffs' attempts to do so by refusing to acknowledge the existence or validity of the Controlling Access Settlement until it produced a countersigned copy for the first time in February 2013.

124. On information and belief, Symmetricom further interfered with Plaintiffs' attempts to license their Phase II Technology by refusing to produce a countersigned copy of the Controlling Access Settlement to Plaintiffs, including refusing to do so in connection with the civil suits relating to the Controlling Access Settlement pending in California Superior Court since 2009 up until the foregoing February 2013 date.

125. These included their actions within the Global Standards Agency called the IETF (Internet Engineering Task Force) who was actively using the infringing IP inside of the systems they were publishing their standards upon as well as including the same infringing IP in the very standards themselves.

126. On information and belief, Symmetricom allowed foreign patents which covered Plaintiffs' Phase II Technology to lapse or become abandoned, despite having the duty to maintain those patents and having knowledge that Plaintiffs relied on them to do so. This constitutes a simple SHERMAN Act event and is clearly an Antitrust action.

COUNT ONE
(Breach of Controlling Access Settlement by
2001 Patent Application Rewrite)

127. Plaintiffs restate the above as if set out in full herein.

128. In 1999, Plaintiffs and Microsemi entered into the Controlling Access Settlement by which they contracted for Microsemi's license to the portion of Plaintiffs' Phase II Technology which was embodied in the 1998 Patent Application and which was incorporated in Microsemi's Confidential Courier .and its derivatives product line.

129. The Controlling Access Settlement is still in force and serves as the basis for Microsemi's continuing claim to be the assignee of the '629 Patent.

130. In 2001 Microsemi breached the Controlling Access Settlement, and its license to Phase-II Technology embodied therein, with its 2001 Application Rewrite to the USPTO, which resulted in the '629 Patent containing claims which read on portions of Plaintiffs' Phase II Technology never contemplated to be so-included by the parties to the Controlling Access Settlement and never licensed by Plaintiffs to Microsemi.

131. As a result of Microsemi's breach of the Controlling Access Settlement, Plaintiffs have been damaged in the amount of licenses they could have received from the Phase II Technology described in the 2001 Application Rewrite, their expectancy therefrom, and/or their lost profits from the 2002 issue date of the '629 through the life of the '629 Patent which will not expire until 2018.

COUNT TWO
**(Breach of Controlling Access Settlement For
Failure to Protect Phase-II IP)**

132. Plaintiffs restate the above as if set out fully herein.

133. The Controlling Access Settlement contemplated that certain portions of Plaintiffs' Phase II Technology would fall within the claims of Controlling Access Patent and that Microsemi would serve as assignee of that patent.

134. The Controlling Access Settlement also commemorated the fact that Plaintiffs were the sole owners of all Phase-II Technology.

135. As assignee to that Phase-II Technology which fell within the Controlling Access Patent, Microsemi had a duty to protect and maintain all such Phase-II Technology, including, without limitation, maintaining all domestic and foreign patent rights thereto.

136. Microsemi (predecessor) had fulfilled that when in writing it asked Plaintiffs for the patent filing release for South Africa; and in fact threatened litigation if it was not produced for both-parties' use in a timely manner (two calendar weeks). No other releases (for the EU, CA, BR, or JP filings) were requested and as such there is a claim under the Sherman Act based therein here for Antitrust as the Fiduciary operating in a Foreign Nation, and under the Foreign Antitrust Act's very stringent "connection to commerce in the US" these filings, as foreign instances of US6370629 and the related unauthorized filings of US6393126, bring this all together under the Sherman Act under its horizontal customer allocation and territorial allocation agreements, something the Defendants acted in preventing the advancement of each of the foreign filings of US6370629 as well as the foreign unauthorized filings of US6393126 entail.

137. Microsemi has breached its duty to maintain the Phase-II intellectual property by allowing certain foreign patents covering Plaintiffs' Phase-II Technology to lapse.

138. As a result of Microsemi's breach of its duty to maintain the patents covering the Phase-II Technology, Plaintiffs have been damaged in an amount to be determined at trial by the global inclusion of this protected IP into Internet and Networking standards. As a result of this the entire world has become an infringer into this IP and its controls.

COUNT THREE
(Unjust Enrichment - Microsemi)

139. Plaintiffs restate the above as if set out fully herein.

140. In 1999, Plaintiffs and Microsemi entered into the Controlling Access Settlement by which they contracted for Microsemi's license to the portion of Plaintiffs' Phase II Technology which was embodied in the 1998 Patent Application.

141. In 2001 Microsemi submitted the 2001 Application Rewrite to the USPTO, which resulted in the '629 Patent issuing containing claims which read on Phase II Technology never contemplated by the parties to the Controlling Access Settlement and never licensed to Microsemi by Plaintiffs.

142. As a result of Microsemi's unilateral and unlawful expansion of the scope of the Controlling Access Patent, and its status as assignee of that patent, Microsemi has been unjustly enriched in the amount that it has benefitted in any way from the Phase-II Technology not included in the 1998 Patent Application.

COUNT FOUR
(Tortuous Interference With Prospective Economic Advantage - Microsemi)

143. Plaintiffs restate the above as if set out fully herein.

144. Plaintiffs are the sole owners of Phase-II Technology with the limited exceptions of Microsemi's license rights as delineated in the Controlling Access Settlement.

145. Microsemi, as the counterparty to the Controlling Access Settlement, had actual knowledge of Plaintiffs' rights to all Phase-II Technology, subject to its limited license rights.

146. After issuance of the '629 Patent, Plaintiffs attempted to license rights to their Phase-II Technology with prospective licensees.

147. On information and belief, Microsemi directly interfered with Plaintiffs' attempts to obtain economic advantage from their Phase II Technology by advising prospective licensees that Plaintiffs had no rights to any of the property embodied in the '629 Patent, including all Phase-II Technology therein.

148. Microsemi likewise repudiated the existence of the Controlling Access Settlement to Plaintiffs and to third parties by, among other things, for thirteen (13) years refusing to produce a fully-executed copy of that agreement (until February of 2013).

149. Microsemi's direct and indirect actions were wrongful and done with the intent to deprive Plaintiffs of their business expectancy with prospective licensees.

150. As a result of Microsemi's tortuous interference with their prospective license arrangements, Plaintiffs have been damaged in an amount to be determined at trial.

COUNT FIVE
(Declaratory Judgment – '629 Patent Contains Phase II Technology Not Within 1998 Patent Application)

151. Plaintiffs restate the above as if set out fully herein.

152. There is an actual controversy as to whether and to what extent the unlicensed 2001 Application Rewrite for the '629 patent filing and the final '629 Patent contain Phase-II Technology which was not contemplated by, or incorporated into, the 1998 Patent Application or the Controlling Access Settlement.

153. This exposure of trade secret and NDA protected information in the US6370629 patent filing constituted first-use inside the Patent Program and prevented Plaintiffs from filing their own patents on the same material.

154. In regard to this claim Plaintiffs request the Court enter a declaratory judgment based upon its construction of the claims of the 2001 Application Rewrite and the '629 Patent and using its comparison of them with those in the 1998 Patent Application to delineate with specificity the components of the claims of the 2001 Application Rewrite and the '629 Patent which read on Phase II Technology and are not contained in the 1998 Patent Application.

155. The purpose of this is to determine whether there is any relevant part of the original patent as a part of '629 or whether it is all content pertaining to the Phase-II IP designs and as such the entire patent is Plaintiff's property based on a allegation of a discovered fraud in the original filing wherein "there isn't any of the IP in the final patent which the Defendants assured Plaintiff's they were contributing to the US6370629 filing", something that would eliminate any of the underlying reasons for the original assignment to Hastings and his company DDI in the beginning of this matter.

156. If it is determined that there is none of the underlying Intellectual Properties from the '992 Patent inside of '629, then the Court is asked to order the immediate 'voiding' of both the Assignment for Management Agreement and the Settlement Agreement therein.

COUNT SIX
(Tortuous Interference With Prospective Economic Advantage - Sherman Act/Antitrust)

157. Plaintiffs restate the above as if set out fully herein.

158. Plaintiffs are the sole owners of Phase-II Technology with the limited exceptions of Microsemi's license rights as delineated in the Controlling Access Settlement.

159. Defendants have a formal responsibility to protect the IP described in the Settlements it controls for all parties. That specifically includes making sure the patents are viable and unauthorized users are not using the IP or authorizing Copyrightable Standards or Code implementing these standardized functions which will infringe on Plaintiffs rights.

160. As such Count Six involves Defendant IETF, the Internet Engineering Task Force and its parent organization the Internet Society (ISOC) for their use of PHASE-II protected IP in many of their standards and now inside of the core drivers which make up the foundation of the World's Internet.

161. Microsemi's through its incarnations over the last decade and their direct and indirect actions in its working with the Defendant IETF are a key part of their tortuous interference.

162. In its interfering with Plaintiffs rights, Microsemi refused to confirm the US 6370629 controlled third-party enforcement rights to Defendant IETF which Plaintiffs enjoyed per the settlement and in doing so (actively participating in the standards process) they defrauded Plaintiffs by placing an IETF controlled copyright onto Plaintiffs Intellectual Property as part of the standards practice by allowing IETF to use Plaintiffs IP in the systems the standards are and were drafted on.

163. As to how these are Sherman Act violations, these actions with the IETF constituted market division or allocation schemes to prevent Plaintiffs from being able to

enforce their rights herein and to enforce a global monopoly against the enforcement of US6370629 in all nations.

164. In addition to its performing this process, the IETF operates its entire existence across a number of computers in a distributed network; In its doing this the IETF has used the infringing IP products themselves inside its very operations in all of its publications; additionally it has included instructions which force a third-party implementing compliance with their design-set to infringe as well meaning anyone implementing the standard as a product would infringe as well as their customers;

165. Historically this was done by IETF with its partner Microsemi and US Government in numerous of its standards despite continuous objection from Glassey over its unauthorized use and the fact the Standards Org as a Consensus based standards organization isn't doing research and cannot claim its doing anything other than IP development for commercial users, and as such has no research exemption.

166. Finally a question arises as to the "the Use of Copyright ss107 exemptions to cover-up patent infringements by 'the party proselytizing the intentional infringement' by forcing its use in their very work product the Internet Protocol 'standards documents'"; and

167. As the second half of this same question, the allegation is that the IETF itself is not a transparent standards process at all and is not comparable or have any real oversight like ANSI or the IEEE and that as such it has become more of the Wild West Show the JEDEC standards committee was found in the US Courts to be in the RAMBUS Matters.

IETF Copyright ss107 Status and MGM v Grokster Standings

168. Additionally as part of Count Six the Court is asked to rule formally on whether the IETF itself is a Research Organization under the Copyright 107 exemption. The purpose of this is to make a determination as to whether the IETF's actions constitute something farther than copyright frauds under *MGM v Grokster*. The Supreme Court ruling in *MGM Studios Inc v Grokster Ltd* set a standard for any party (in this case the IETF a global standards agency operated as a ***benevolent fraternal org*** under the Tax Exempt Umbrella of the Internet Society Corporate Standing we assert "to cover up its real purpose, to allow Silicon Valley companies and others to manipulate global IP standards in their desire to end all patent support in any technology venue".

169. As such they (the IETF) are identical to GROKSTER as an agency distributing IP controlled products under an external agreement and their actions fully controlled by the Supreme Court ruling therein. (see *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005)⁴).

170. The argument being that the IETF is identical to a P2P sharing service and so is the Grokster-Role party in this matter and as such cannot even if they are a research institution (which is highly doubtful since they maintain the Internet Research Task Force (www.irtf.org), a separate org controlled under a separate set of rules and practices) still qualify as a 107-enabled entity as a University could.

171. As such the IETF publication of our their standards which contain our Patent-protected Technologies constitutes a both a direct infringement in the publication as well as an additional Copyright Infringement on the natural copyright

⁴ 545 U.S. 913 (*more*) see also 125 S. Ct. 2764; 162 L. Ed. 2d 781; 2005 U.S. LEXIS 5212; 75 U.S.P.Q.2D (BNA) 1001; 33 Media L. Rep. 1865; 18 Fla. L. Weekly Fed. S 547

issued when the US Government issued the US patent controlling this material. That second claim is tied to the actual copyright and the IETF's failure to enforce any of its Intellectual Property process ruled contained in BCP79, its IP Standards Document;

172. The principal claim is the IETF in refusing to enforce its own rules and practices and in not being a research institute or academic practice, and finally under its blanket use of the infringing technology in its own infrastructure creates a natural-trifecta of claims which exist under a number of standards from the Sherman Act to theft of Trade Secrets and in the intentional damage to the IP in the abandonment's of the patents filed in the EU, South Africa, Japan, Brazil, and Canada all support this fully, that under Patent and US IP and Trade Secret Law, no extension of the ***research exemption under the copyright provision*** exists for the IETF, and further Copyright Exemptions cannot authorized the setting aside of US Patent Law under Title 35 so the IETF creating a written work about a technology cannot "in and of itself carry any right to implement, use or do anything else with that Patent Protected IP, only Patent Licensing satisfies that.

COUNT SEVEN

(Declaratory Judgment – Patent Fraud, Unauthorized Filing of US6393126)

173. Plaintiffs restate the above as if set out fully herein.

174. Plaintiffs are the sole owners of Trusted Timing Infrastructure (TTI) System Technology with the limited provisions of the three derivatives licensed to Microsemi against three of the thirty-two components of the TTI itself.

175. Further that these are licensed for US use only in the Settlement Agreement since sections 8.1 and 8.3 restrict any and all disputes with the products or

their use by any and all third parties including end users to the Courts and Laws of the State of California.

176. Microsemi as predecessor Datum filed a patent against "the entire Trusted Timing Infrastructure IP library" listing Erik Van Der Kaay (US6393126) as the inventor with several of his engineers including those directly involved in the alleged "standards agency frauds" outlined previously in COUNT SIX.

177. The Patent (US6393126) was issued in the US and in a number of other countries and contains a number of controls and claims which overlap those which the US6370629 patent was filed to protect, so the foreign instances of 6393126 control many aspects that the Plaintiffs' rights under US6370629 which were filed in those same nations were intended to. As such the promulgation of 6393126 into foreign filings is an alleged fraud done to control key aspects of what the US6370629 is supposed to.

178. Nothing in the Trusted Timing Infrastructure settlement contemplated Microsemi filing a patent listing itself as the creator of the technology, something blatantly false based on the settlement agreement alone. This claim is further fully supported by the Toby Gellman appellate ruling.

179. The amount of the TTI which the patent was issued against like the 2001 changes to '629 included large amounts of Glassey owned IP from the CertifiedTime Inc Bankruptcy (01-54207-MM - San Jose). Additionally aspects and IP controlled by '629 was added to the '3126 patent without authorization to get it issued as well.

180. We therefore seek an order to the USPTO to remove Erik Van Der Kaay's name from this patent as well as the others and to replace them with Plaintiff Glassey exclusively. Likewise there is no assignment of this patent to Microsemi corporation

planned for or authorized in the settlement so we ask the Court to order the Patent Office to reassign this patent with full rights therein to Plaintiffs;

COUNT EIGHT

(Declaratory Judgment –International transfer of TTI Intellectual Properties to set aside the Settlement Agreement, Unauthorized removal of TTI from US Courts' Jurisdiction)

181. Plaintiffs restate the above as if set out fully herein.

182. Plaintiffs are the sole owners of Trusted Timing System Technology with the limited provisions of the three components licensed for US use only in the Settlement Agreement.

183. Settlement Terms are permanent per section 3.15 and 8.4 of the DDI Settlement contract and require continuous reporting on licensing, and further per sections 8.1 that "any and all disputes for any and all users of the IP sublicensed in the settlement do so in the courts and under the laws of the State of California" and that per section 8.3 these terms are binding on all successors in any form (including but not limited to end-users of the product and any intermediary distribution framework set up to support them).

184. Microsemi corp. at some point entered into a Joint Venture with a Cambridge England company called nCipher based on an introduction Plaintiff Glassey had made several years previous.

Microsemi transferred the protected IP of the TTI settlement to nCipher who took it to England and then brought the product back into the US as an English Copyright and Patent based Product under their name. This violated the terms of the settlement agreement.

COUNT NINE
(Declaratory Judgment –Mandatory Acceptance Requirements for transfer of US6370629 to Microsemi)

185. Plaintiffs restate the above as if set out fully herein.

186. Per section 8.4 each party assuming a control role for the licensing must notify the Plaintiffs of this within the 14 day period agreed to between Microsemi Attorney John Cannon and Plaintiffs as documented in the Cannon South African Patent Instance filing release letter.

187. Plaintiffs request the court issue a declaratory judgment that Microsemi breached this key term and strip Microsemi of the US6370629 patent awarding it in full to Plaintiffs and damages therein as the court sees fit including fraud losses therein.

COUNT TEN
(Declaratory Judgment –Defendant US Government's use of FISA and National Security Letters to cover up other actions and alleged frauds)

Governments Alleged Use of a National Security Letter in this matter

188. Plaintiffs assert that this matter clearly has National Security implications because this single set of IP rights controls all systems inside the Government as well all commerce in the US today; and based on various refusals from the US DoJ and the giving of a Judges position to Defendant PETER CHEN the specific attorney inside the Latham Watkins law firm we believe created the delaying tactic and withholding-the-settlement agreement from everyone, the Plaintiffs believe that the President of the United States (POTUS) or some party working for the President issued a National Security Letter (NSL) to the FISA Court and "that a warrant classifying this fraud loss and the actions of both the Government Employees and those of the Industry Players

herein" was issued in this matter to prevent Glassey and McNeil from getting proper legal help in advancing these fraud claims, and as such this becomes a key civil rights matter therein. That said letter may have even been served on California Judiciary including the Judge in California who dismissed the review of the original contracts and alleged frauds therein while continuing to operate the courts infrastructure on infringing technology as well.

189. This claim is substantiated by every attorney hired by Glassey to prosecute this matter "refusing to answer the question 'as to whether they were contacted by anyone in their State Bar, State Government, US Government or in particular the FISA court in this matter'".

190. As such we request the USDC and this Court immediately reach out to the FISA court and request formal verification of this matter and if said order exists issue a further order "vacating any rulings in this matter by any other court".

191. That the USDC also order the termination of that National Security Letter if it does exist;

192. The justification for this is that an Action denying Bill of Rights protections against Court Access and Property Protection violates all of the FISA Court Members Oath of Office as Judges of the US District Court and that an action on the part of the FISA Court itself constituted both interference with a private citizens Seventh ***Amendment access to competent legal services and the courts therein***, and through that ***a manipulation of the that citizens fifth amendment rights codified in the Settlement or Co-inventor Agreements both***.

193. Further this final claim includes Named DOES named as USG (US Government) and its former officers including Leon Panetta as an individual today, the

following US Government agencies: National Security Council and the President of the United State as an individual and in their respective roles in the US Government.

Summary and Additional Prayer for Relief not included in Counts

WHEREFORE, Plaintiffs Michael E. McNeil and Todd S. Glassey request this Court to enter judgment in their favor on all counts, especially count ten (10), and to award the Plaintiffs damages as requested in specific Counts and cumulative damages in an amount to be determined at trial against "the use of the unauthorized and patent-protected IP rights by IETF and all of its third-party Users as was done with MGM Studios v Grokster herein including in all computing and network infrastructure components (including but not limited to switches, routers, servers, and client platforms including cellular and mobile computing (aka wireless/cellular) systems)" in use globally through the entire effective period of all patents cumulatively including those abandoned today.

Additionally as part of this to

1. award Plaintiffs specific declaratory relief to the effect that the 2001 Application Rewrite and the '629 Patent contain Phase-II Technology which was not identified in the 1998 Patent Application,
2. award them relief in regard to their US3693126 damage claims, and
3. award the Plaintiffs damages against the US Government (POTUS, NSA, National Security Council, DoJ, et Al.) for their alleged use of a NSL and FISA warrant issued to GLASSEY Counsel's (from Hopkins Carley and Berliner Cohen to Mahaney/Ertl) for the effect of this 'classifying the fraud complaint under the FISA and National Security Act (as well as other

legislation) *to reduce or eliminate the effectiveness of Plaintiff's Counsel in the matter herein;*

4. award Plaintiffs

- a. against the IETF and its parent the Internet Society uses in operating the computers they publish virtually everything on and through, as well as the key companies profiting from this as a class including but not limited to Cisco, Google, Apple, Ebay, Paypal, Oracle Microsoft, and
- b. additionally under current US Public Policy to issue formal Court Order to the IETF and Internet Society "that all of their standards must come into immediate conformance with US DMCA provisions and best practices of a Global Standards Org with regard to its IP Management Practices" - meaning there must be a DMCA compliant use and take down policy implemented in all existing IETF standards; and
- c. finally that this court order that the IETF Copyright of all preceding documents is void by this alleged fraud and that by order of the court "no matter what contractual agreement exists between the authors and the IETF as to that IP's licensing", and to award Plaintiffs any award to plaintiffs direct losses, treble damages as authorized by the numerous fraud statutes this suit alleges were violated and any other relief to which the Plaintiffs are entitled, including but not limited to legal fees herein.

d. Based also on the Equal Protection Clause of the Fourteenth Amendment and other aspects of the Fifth and Fourteenth Amendments the denial of both the US Government and the State of California has placed both entities in a position where they have not only violated the Fifth Amendment by allowing the conversion of the disputed properties, but in doing so they also under the fourth Amendment functionally seized property⁵ by claiming this Intellectual Property Right against US and Foreign Patents did not exist, in doing so they have blocked access to the courts therein under the Seventh and Fourteenth Amendments to the US Constitution.

⁵ Boyd v. United States, 116 U.S. 616 (1886)

Respectfully submitted,

Todd S. Glassey, In Pro Se

tglassey@earthlink.net

305 McGaffigan Mill Road
Boulder Creek CA 95006
Telephone: (408) 890-7321

Michael E. McNeil, In Pro Se

Michael E. McNeil, In Pro Se
PO Box 640
Felton CA 95018-0640

Jury Demand

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs demand a trial by jury of all issues so triable.

Plaintiffs

Plaintiffs



PATENTS

**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

09182342.102998

"EXPRESS MAIL" Mailing Label Number EM 529182192US

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 Jean
AMBROSE MEMA

PATENT
ATTORNEY DOCKET NO: 06157/006001

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

86620T-24228160
10/10

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
5 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
10 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
15 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
20 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
25 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
30 authorized. The user can access the stored information if
the actual date or time occurs within the authorized date or
time interval.

09182342.102998

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

09182342.102998
866201.24228160

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.

866201-24828160
09182342-102998

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 different 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. Likewise, access to a sensitive corporate 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 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.

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 (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 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 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 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

09182342-102998

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
15 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
20 data authentication and encryption.

25 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.

09182342-102998

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 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.

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 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.

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 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 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
 5 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
 10 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
 15 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
 20 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
 25 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
 30 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 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 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, 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 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 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,

09182342.102998

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:

09182342-102998

1 ^{sub} 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.

866201.24228160

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 ^{sub} 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 ¹² 13. The apparatus of claim ¹¹ 12, wherein said
receiver is a GPS receiver.

186342.102998
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 ~~sub 4~~ 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 ~~sub 4~~ 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.

18
1 ~~20~~. The method of claim ~~19~~¹⁷, wherein said policy is
2 stored with the stored information.

35
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.

20
1 ~~22~~. The method of claim ~~21~~¹⁹, 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.

21
1 ~~23~~. The method of claim ~~21~~¹⁹, 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.

22
1 ~~24~~. The method of claims ~~21~~¹⁹, 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.

866207-24328160

25. A method for controlling access to stored
information comprising:
forming a policy associating said information with
authorized geographic regions and authorized time intervals;
cryptographically signing said policy and said
information;
storing said signed policy together with said signed
information;
providing a password for unlocking said policy; and
determining an actual geographic position where said
stored information is located based on signals received at a
receiver supplying reliable position information;
determining an actual time;
comparing said actual geographic position and said
actual time with said authorized geographic regions and
authorized time interval of said policy; and
permitting access to said stored information if said
actual geographic position and actual time falls within said
authorized geographic regions and authorized time interval
of said policy.

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

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

See
A3
2
3

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

add
c1

09182342.102998

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

866201-24828160

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: [Signature] Date: 10/28/1998

Residence Address: Lexington, MA

Citizen of: United States

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

09182342-102998

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

09182342.102988

330287.B11

ATTORNEY DOCKET NO. 06157/006001

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. McNeill, 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 1.27(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: 

Date: 10/29/13

09182342.102998

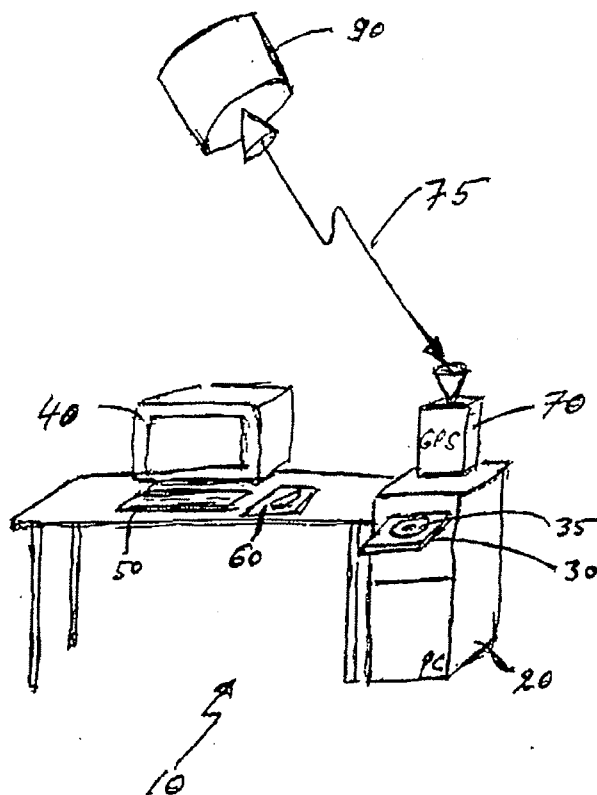
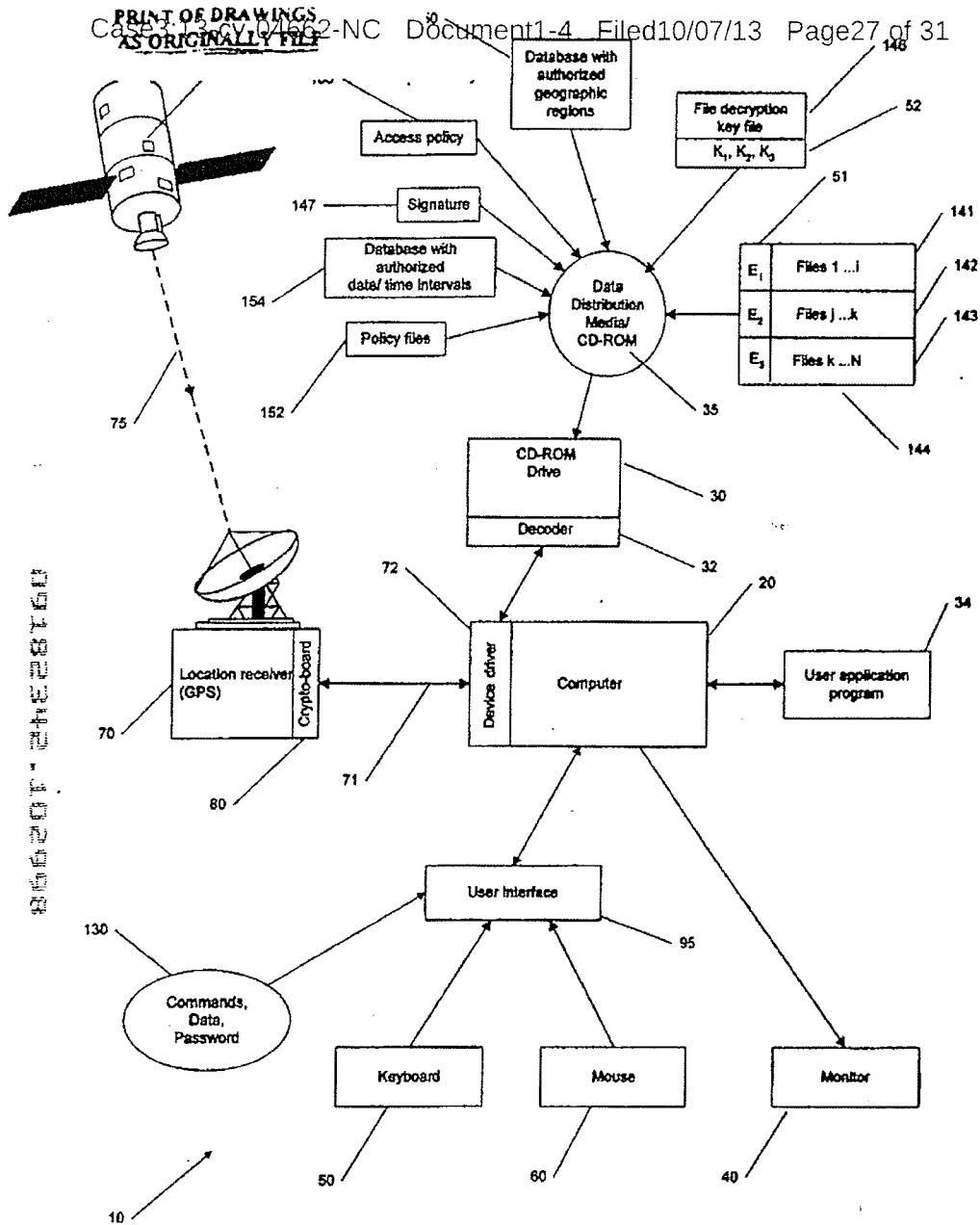


Fig. 1



866201-24E28T60

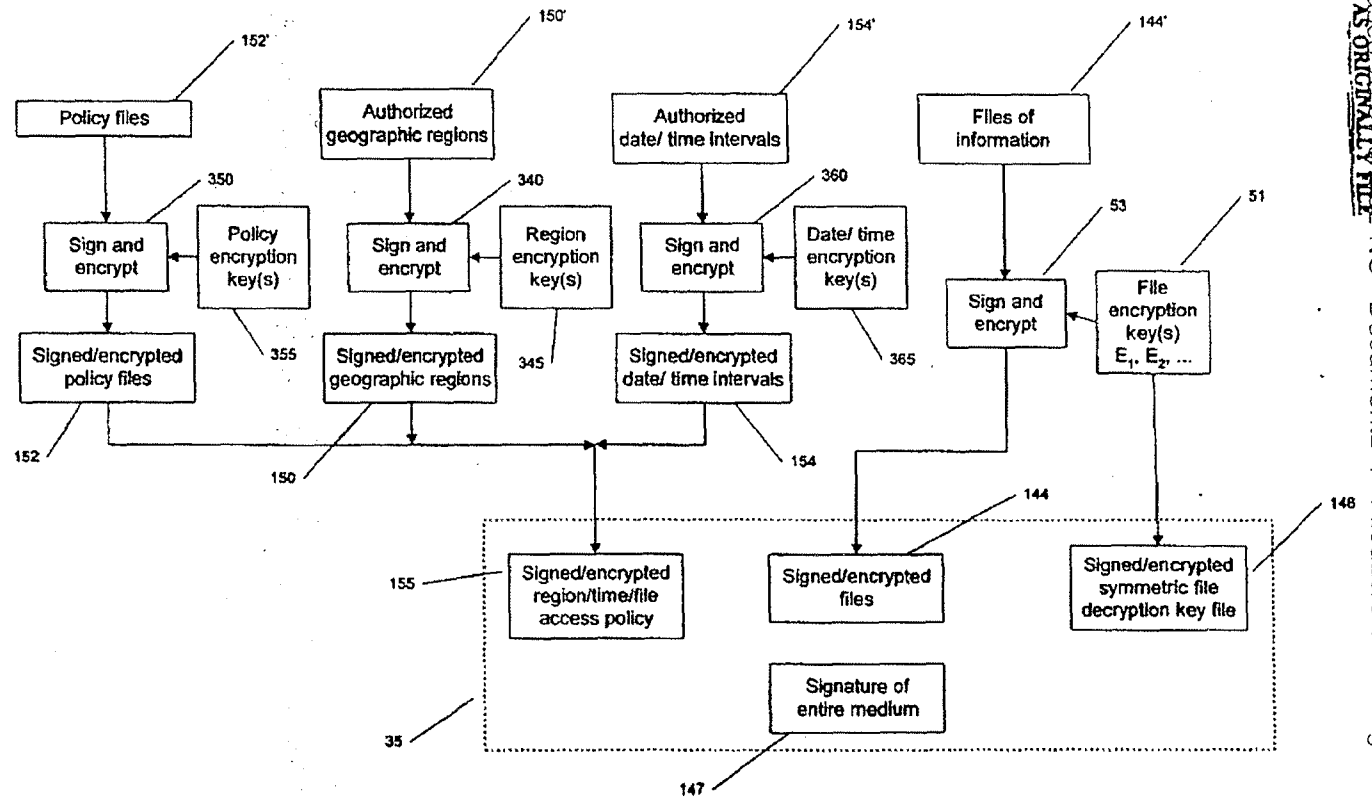


FIG. 3

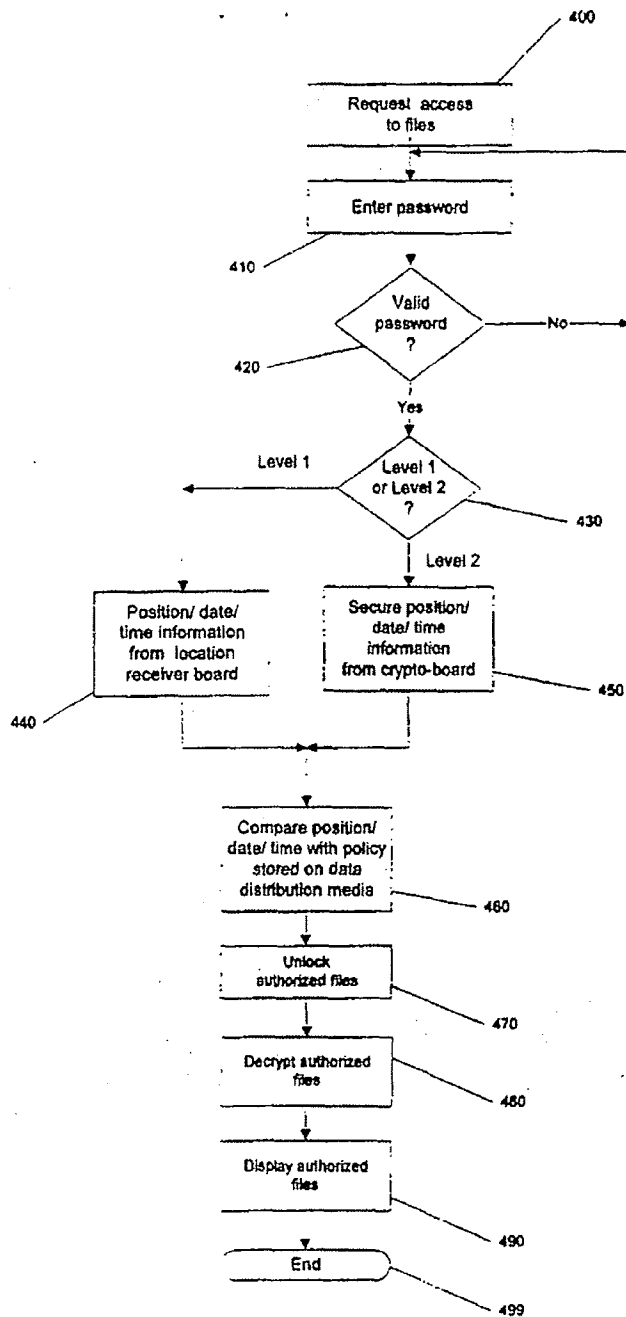


FIG. 4

Level 2

09182312-102999

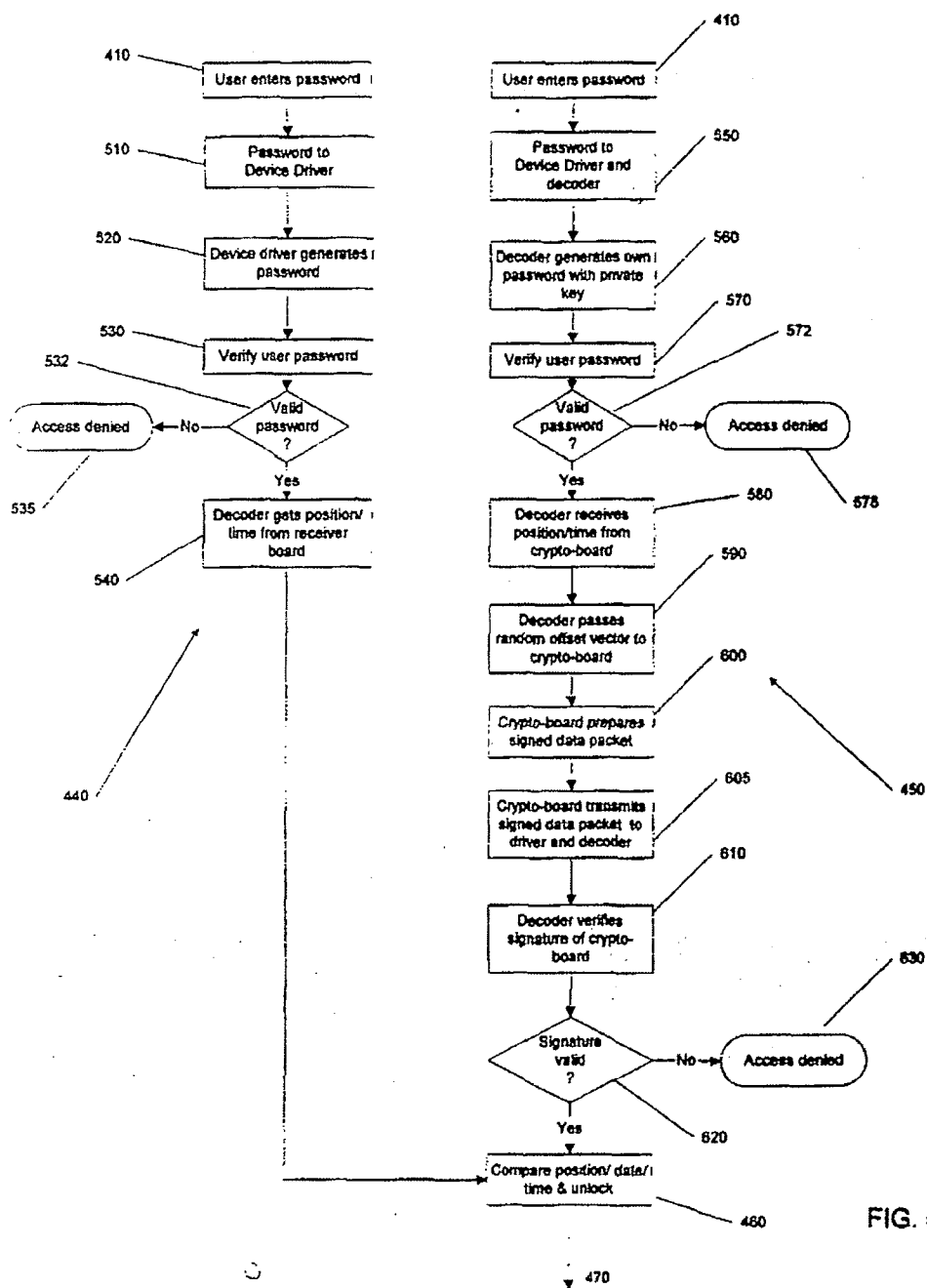


FIG. 5

00001-2122860

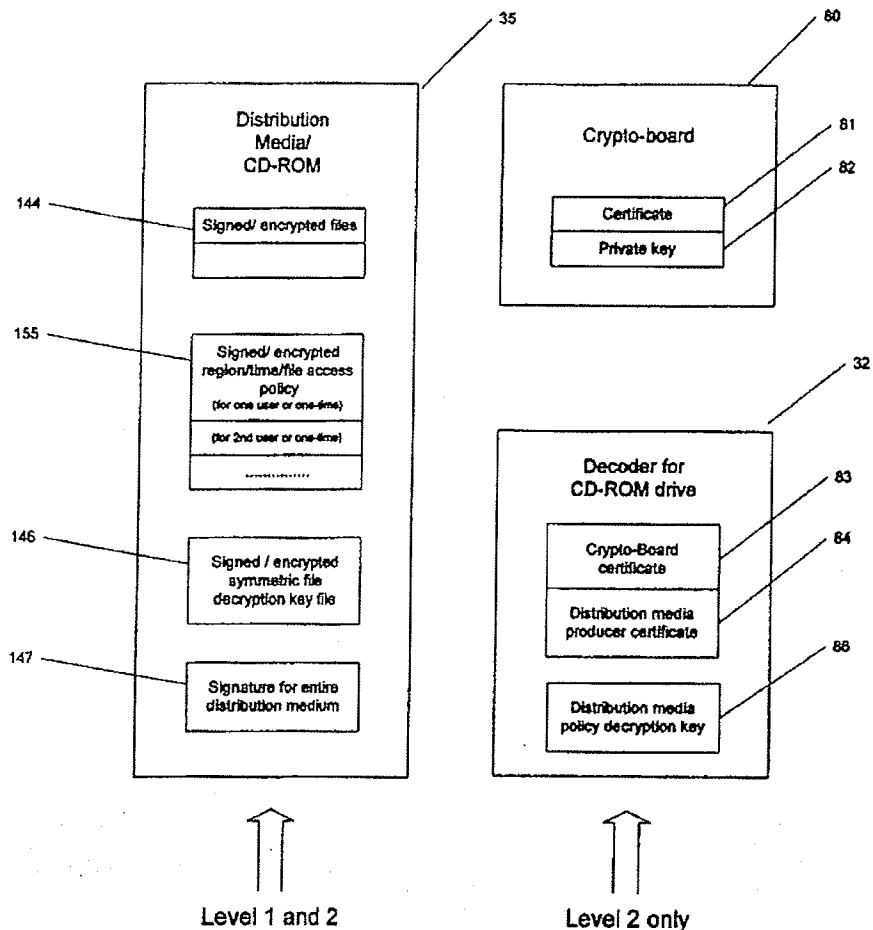


FIG. 6

(12) **United States Patent**
Hastings et al.

(10) **Patent No.: US 6,370,629 B1**
(45) **Date of Patent: Apr. 9, 2002**

(54) **CONTROLLING ACCESS TO STORED INFORMATION BASED ON GEOGRAPHICAL LOCATION AND DATE AND TIME**

(75) Inventors: Thomas Mark Hastings, Lexington, MA (US); Michael E. McNeil, Felton; Todd S. Glassey, Scotts Valley, both of CA (US); Gerald L. Willett, Malden, MA (US)

(73) Assignee: **Datum, Inc.**, Bedford, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/182,342**

(22) Filed: **Oct. 29, 1998**

(51) Int. Cl.⁷ **H04L 9/00**

(52) U.S. Cl. 711/163; 711/153; 711/164; 713/189; 713/193

(58) Field of Search 340/988, 992, 340/993, 991; 380/7, 25; 713/200, 189, 193; 711/163, 164, 147, 152, 153

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,243,652 A 9/1993 Teare et al. 380/21
5,553,143 A 9/1996 Ross et al. 380/25

5,640,452 A 6/1997 Murphy 380/5
5,646,992 A 7/1997 Subler et al. 380/4
5,754,657 A 5/1998 Schipper et al. 380/25
5,757,916 A 5/1998 MacDoran et al. 380/25
5,799,082 A * 8/1998 Murphy et al. 380/7
5,922,073 A * 7/1999 Shimada 713/200
5,987,136 A * 11/1999 Schipper et al. 380/25
6,046,689 A * 4/2000 Newman 340/996
6,057,779 A * 5/2000 Bates 340/825.31
6,057,799 A * 5/2000 Bates 340/825.31

* cited by examiner

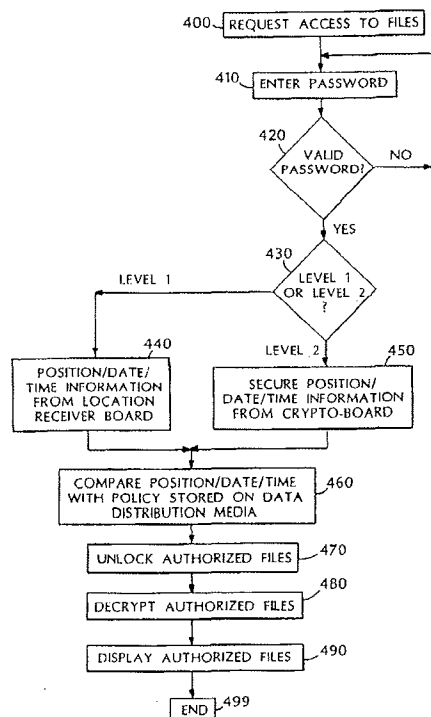
Primary Examiner—Than Nguyen

(74) *Attorney, Agent, or Firm*—Knobbe, Martens, Olson & Bear, LLP

(57) **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.

32 Claims, 6 Drawing Sheets



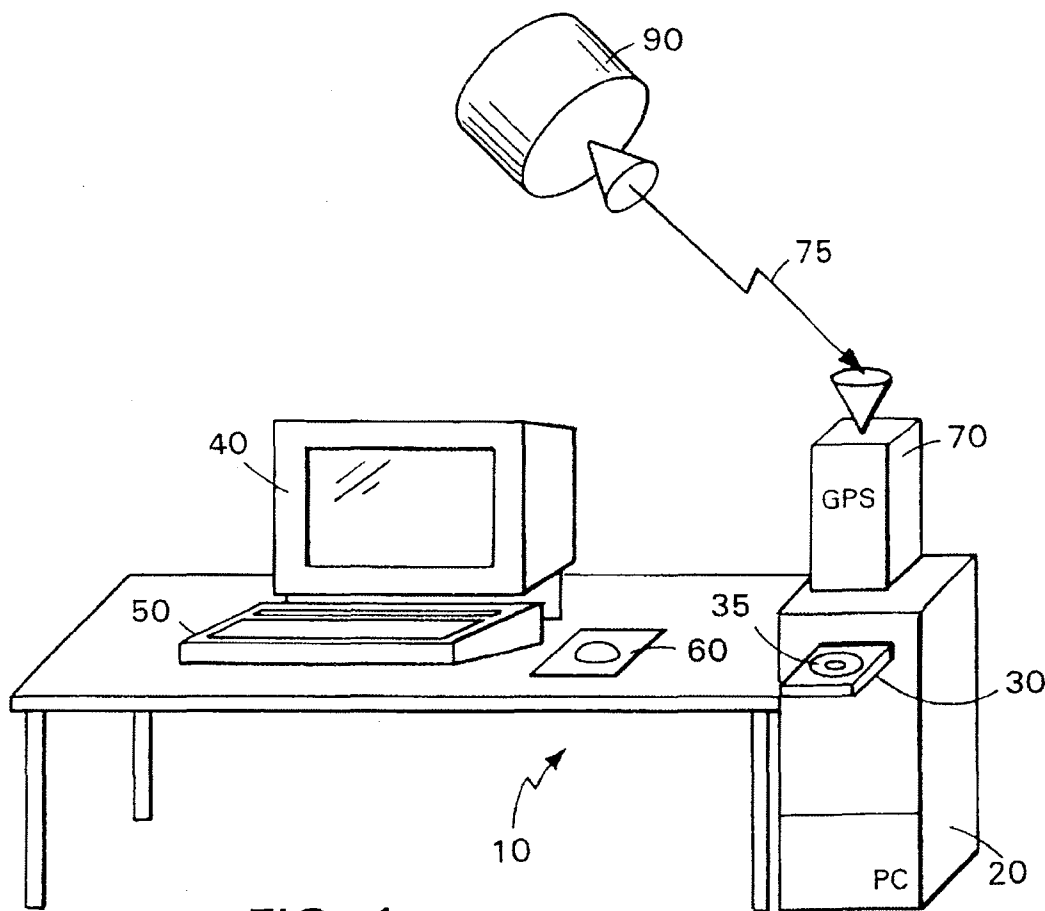
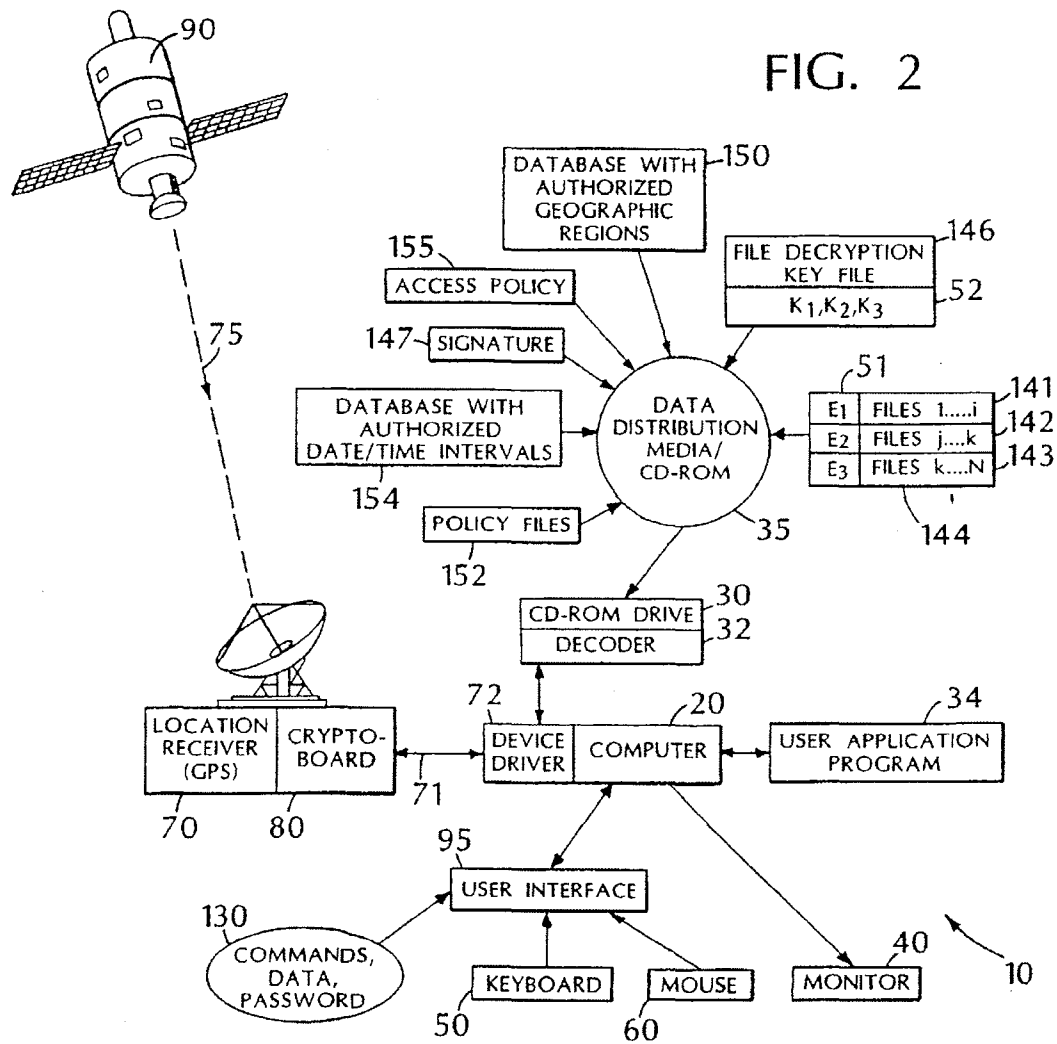


FIG. 1

FIG. 2



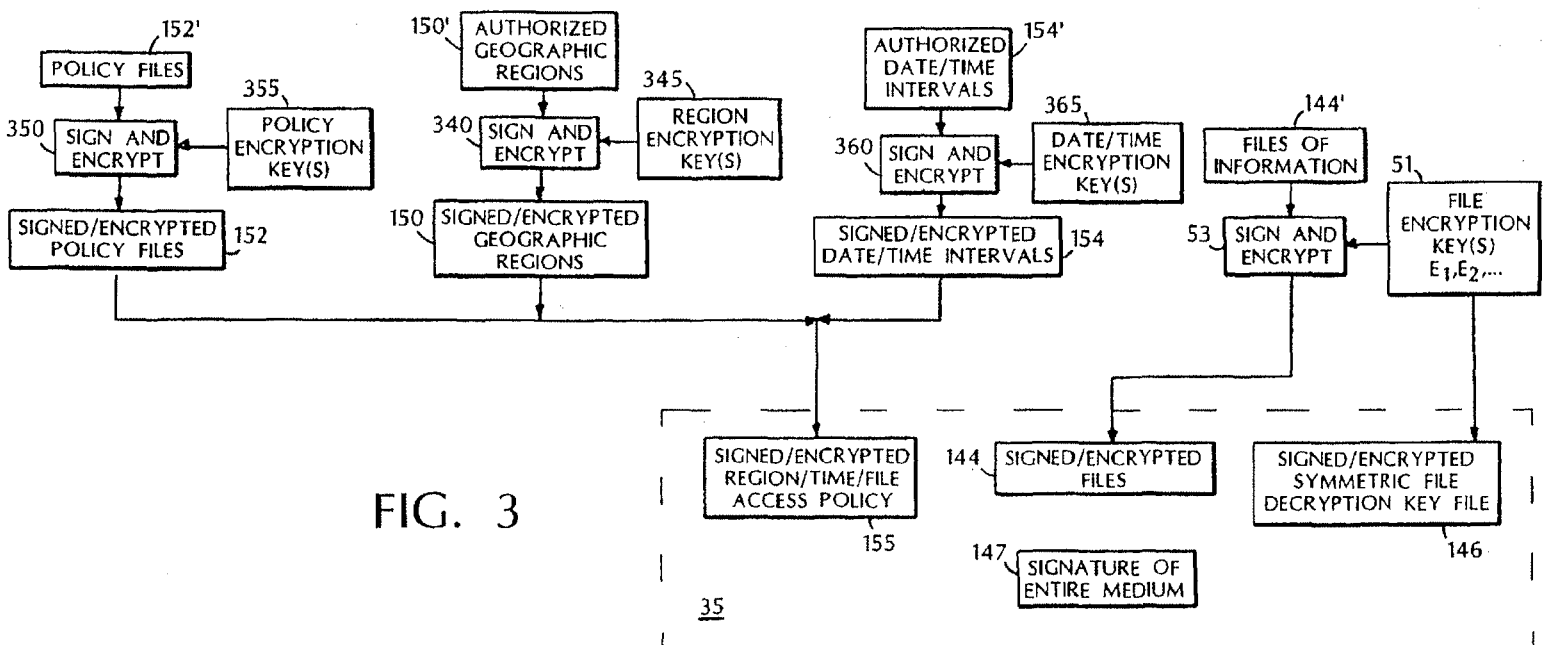
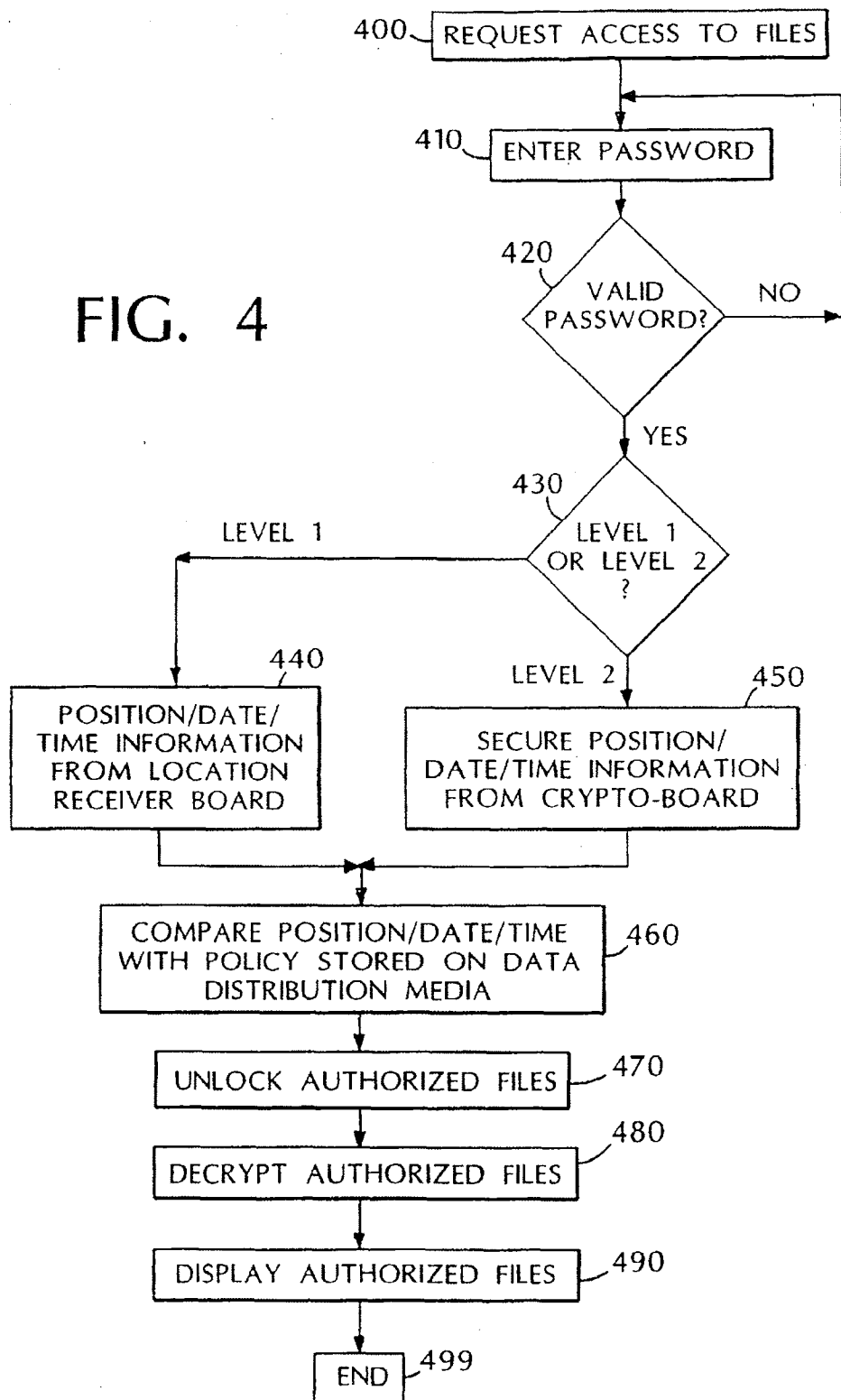
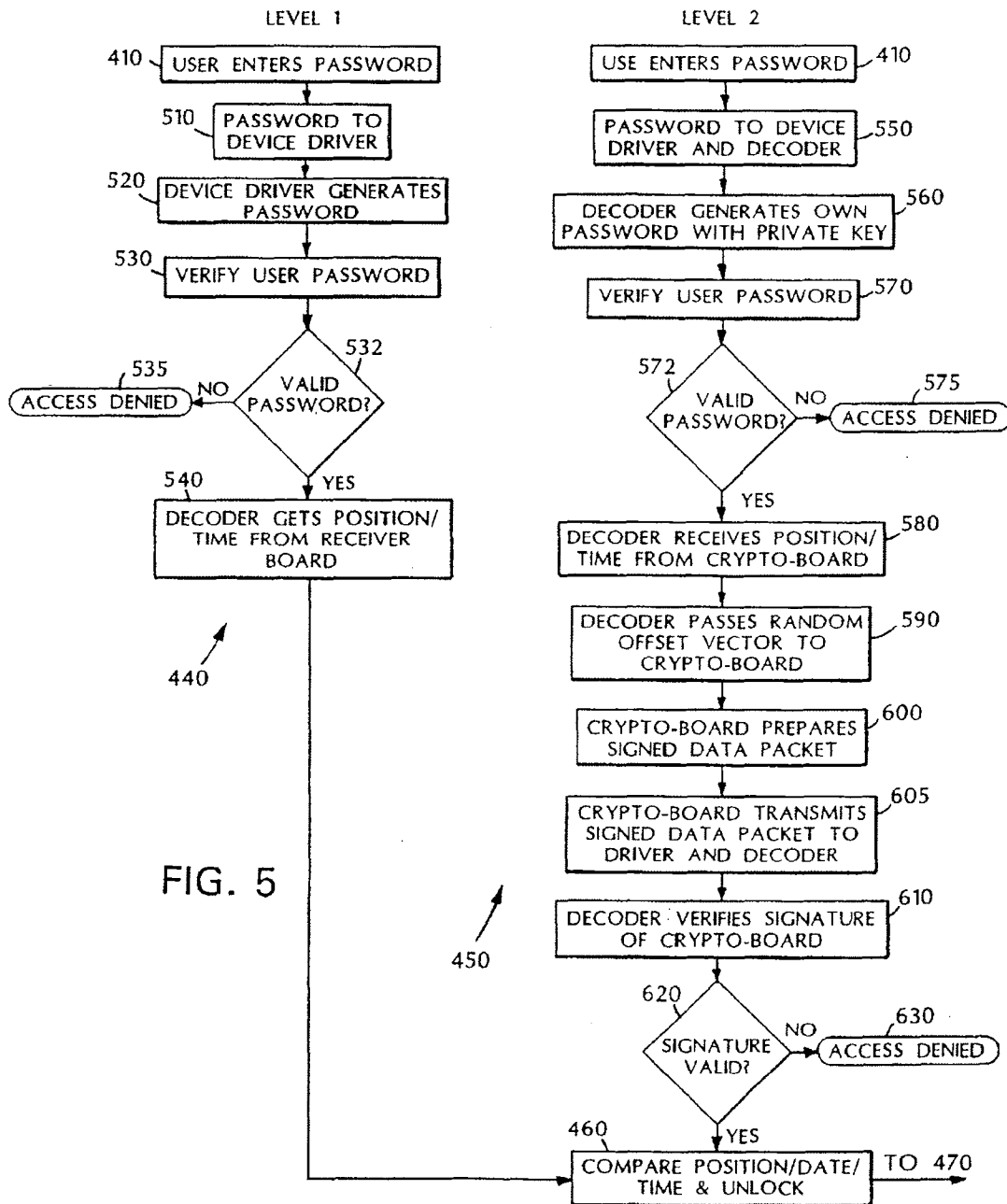


FIG. 4





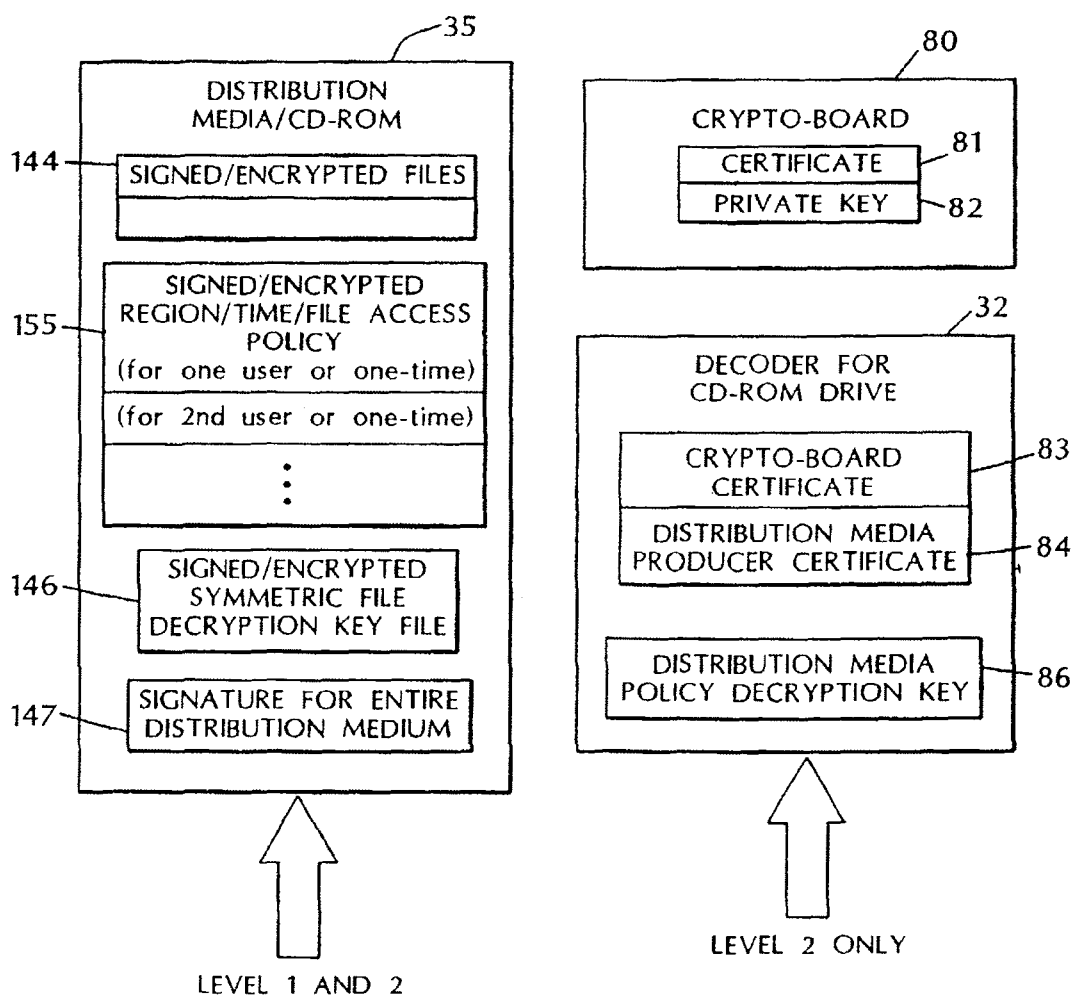


FIG. 6

US 6,370,629 B1

1

CONTROLLING ACCESS TO STORED INFORMATION BASED ON GEOGRAPHICAL LOCATION AND DATE AND TIME

BACKGROUND

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 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 subsets of files. The files may be cryptographically signed and for added protection, may be encrypted. In the scheme discussed in U.S. Pat. No. 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 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.

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 receiver supplying reliable position information. The actual geographic position is then compared with a geographic region within which access to the stored 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 deter-

2

mining 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 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 different 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. Likewise, access to a sensitive corporate 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

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.

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 (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 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 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 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.

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

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.

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.

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 encrypted with a unique file encryption key 51 (E_1 , E_2 , E_3). The correspond-

ing 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. Pat. No. 5,646,992.

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 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.

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 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 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 130, 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 K_1 to K_4 . L_1 and L_2 are two different authorized geographic regions and T_1 , T_2 and T_3 are three different authorized date/time intervals. The user who is in possession of the file decryption key K_1 , e.g., a password, can decrypt Manual A within the geographic regions L_1 and L_3 at time T_1 . The same user can also decrypt Manual D at the same time T_1 in regions L_2 and L_3 , but not within region L_1 . Likewise, the user who has key K_2 can decrypt Image B and Image E within the region L_2 , but not at the same time. Drawing C can be decrypted with key K_3 at any location, but only at time T_3 , while the Business Report F requires key K_4 and can be decrypted at any time, but only within the region L_1 .

TABLE 1

Encrypted File	File Decryption Key	Authorized Geographic Regions	Authorized Date/Time Intervals
Manual A	K_1	L_1 , L_3	T_1
Image B	K_2	L_2	T_1 , T_3
Drawings C	K_3	—	T_3

US 6,370,629 B1

5

TABLE 1-continued

Encrypted File	File Decryption Key	Authorized Geographic Regions	Authorized Date/Time Intervals
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.

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 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 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, 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 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 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.

6

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, 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.

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 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, 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 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 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 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 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.

US 6,370,629 B1

7

What is claimed is:

1. A method for controlling access to stored information comprising:

determining an actual geographic position where said stored information is located based on signals received at a receiver supplying reliable position information; cryptographically signing said actual geographic position with a receiver encryption key; verifying the signature of said actual geographic position; determining that said actual geographic position is within a geographic region within which access to said stored information is authorized; and permitting access to said stored information.

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

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

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

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

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

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

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

9. The method of claim 1, further comprising: encrypting said stored information using an encryption key; and

providing a decryption key which permits decryption of said stored information if said actual geographic position is located within said authorized geographic region.

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

11. Apparatus for controlling access to stored information comprising:

a receiver supplying reliable position information for determining an actual geographic position where said stored information is located, wherein the receiver comprises a receiver encryption mechanism providing a receiver encryption key for cryptographically signing data comprising the actual geographic position; and

a computer for comparing said actual geographic position with a geographic region within which access to said stored information is authorized,

wherein said computer permits access to said stored information if said actual geographic position is located within said authorized geographic region.

12. The apparatus of claim 11, wherein said receiver is a GPS receiver.

13. The apparatus of claim 11, further comprising a reader for reading said stored information wherein said reader

8

comprises a receiver decryption key for verifying the data comprising said cryptographically signed actual position.

14. The apparatus of claim 13, wherein said reader generates an initialization vector which is transmitted to the receiver and included in the signed data.

15. The apparatus of claim 14, wherein said signed initialization vector is verified by the reader before said computer permits access to said stored information.

16. A method for controlling access to a subset of files belonging to a larger set of files of stored information comprising:

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

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

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

cryptographically signing at least the actual geographic position at the receiver;

verifying the signature of the actual geographic position; comparing said actual geographic position with said authorized geographic region; and

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

17. The method of claim 16, wherein said association of the files with the authorized geographic regions is stored as a policy comprising policy files wherein each policy file is accessible with a user password and authorizes, if the user password is valid, access to the files listed in said policy file, if the actual geographic position is located within the authorized geographic region associated with the files.

18. The method of claim 17, wherein said policy is stored with the stored information.

19. A method for controlling access to stored information comprising:

determining an actual date or time at the location of said stored information based on signals received at a receiver supplying reliable time information;

cryptographically signing at least the actual date or time at the receiver;

verifying the signature of the actual date or time;

comparing said actual date or time with a predetermined date or time interval at which access to said stored information is authorized; and

permitting access to said stored information if said actual date or time occurs within said authorized date or time interval.

20. The method of claim 19, further comprising denying access to said stored information if said actual date or time does not occur within said authorized date or time interval.

21. The method of claim 19, wherein said information comprises files and each of said files has an associated authorized date or time interval within which access is permitted, and further permitting access to said file if said actual date or time occurs within said associated authorized date or time interval.

22. The method of claim 19, wherein said stored information is divided into subsets of information and wherein at least one of the subsets has a different authorized date or

US 6,370,629 B1

9

time interval from the other subsets, so that access is authorized to the subset whose authorized date or time interval matches the actual date or time, but not to the subsets whose authorized date or time interval does not match the actual date or time.

23. A method for controlling access to stored information comprising:

forming a policy associating said information with authorized geographic regions and authorized time intervals;

cryptographically signing said policy and said information;

storing said signed policy together with said signed information;

providing a password for unlocking said policy;

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

determining an actual time;

cryptographically signing at least the actual geographic position and the actual time at the receiver;

verifying the signature of the actual geographic position and the actual time;

comparing said actual geographic position and said actual time with said authorized geographic regions and authorized time interval of said policy; and

permitting access to said stored information if said actual geographic position and actual time falls within said authorized geographic regions and authorized time interval of said policy.

24. The method of claim 23, wherein position and time are determined through a Global Orbiting Navigational Satellite System.

25. The method of claim 23, wherein position is determined through an inertial navigation system.

10

26. The method of claim 23, wherein position is determined through a satellite based location determination system.

27. A method for controlling access to stored information, the method comprising:

(a) determining a position;

(b) cryptographically signing data comprising at least a representation of the position;

(c) verifying the signature of the data comprising at least a representation of the position;

(d) determining that access to the stored information is authorized at the position; and

(e) permitting access to the information based at least upon (c) and (d).

28. The method of claim 27, further comprising

(f) providing the cryptographically signed data to an information accessing device, wherein (c) and (e) are performed by the information accessing device.

29. The method of claim 28, further comprising:

(g) identifying a token;

(h) incorporating the token in the data that is cryptographically signed; and

(i) verifying that the cryptographically signed data comprises the token.

30. The method of claim 29, wherein (g) and (i) are performed by the information accessing device.

31. The method of claim 29, wherein (a), (b), and (h) are performed by a position determining device.

32. The method of claim 29, further comprising

(j) providing the token to the position determining device.

* * * * *



DATUMB.006A

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#10/c
605
8-26-01
entered

Applicant	:	Hastings et al.)	Group Art Unit 2187
Appl. No.	:	09/182,342)	
Filed	:	October 29, 1998)	I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on
For	:	CONTROLLING ACCESS TO STORED INFORMATION)	August 16, 2001 (Date) <i>Alexander Franco</i> Alexander Franco, Reg. No. 45,753
Examiner	:	Than Nguyen)	

RESPONSE TO MAY 17, 2001 OFFICE ACTION

Commissioner for Patents
Washington, D.C. 20231

RECEIVED
AUG 24 2001
Technology Center 2100

Dear Sir:

In response to the Office Action mailed on May 17, 2001, please reconsider the above-captioned patent application in view of the following amendments and remarks.

AMENDMENTS

In the Claims

Please Amend Claims 1, 12, 15, 18, 21, and 25;

Please Add New Claims 29-34; and

Please Cancel Claims 9 and 14 as shown in the following clean version of the entire set of pending claims.

1. (Amended) A method for controlling access to stored information comprising:
determining an actual geographic position where said stored information is located based on signals received at a receiver supplying reliable position information;
cryptographically signing said actual geographic position with a receiver encryption key;
verifying the signature of said actual geographic position;

08/22/2001 HUNG61 00000126 09182342

01 FC:202

40-00-00

-1-

23

08/22/2001 HUNG61 00000126 09182342
40-00-00
01 FC:202
02 FC:203

October 29, 1998

determining that said actual geographic position is within a geographic region within which access to said stored information is authorized; and
permitting access to said stored information.

C1
end

2. The method of Claim 1, wherein said receiver comprises a GPS receiver.
3. The method of Claim 1, wherein said information is stored on a computer-readable medium.
4. The method of Claim 3, wherein said computer-readable medium is portable.
5. The method of Claim 3, wherein said computer-readable medium comprises a high-capacity disk.
6. The method of Claim 1, wherein said stored information comprises files and each of said files has an associated geographic region within which access is permitted, and further permitting access to said file if said actual geographic position is located within said authorized geographic region for said file.
7. The method of Claim 6, further comprising denying access to said stored information if said actual geographic position does not match said authorized geographic region.
8. The method of Claim 1, further comprising:
encrypting said stored information using an encryption key; and
providing a decryption key which permits decryption of said stored information if said actual geographic position is located within said authorized geographic region.
9. (Canceled)
10. The method of Claim 1, wherein said stored information is divided into subsets of information and wherein at least one the subsets has a different authorized region from the other subsets, so that access is authorized to the subset whose authorized geographic region is located within the actual geographic position, but not to the subsets whose authorized geographic region is not located within the actual geographic position.
11. The method of Claim 6, wherein said association of the files with the authorized geographic regions is stored as a policy file together with said stored information.

11 12. (Amended) Apparatus for controlling access to stored information comprising:

a receiver supplying reliable position information for determining an actual geographic position where said stored information is located, wherein the receiver

C2

comprises a receiver encryption mechanism providing a receiver encryption key for cryptographically signing data comprising the actual geographic position; and

c3
end a computer for comparing said actual geographic position with a geographic region within which access to said stored information is authorized,

wherein said computer permits access to said stored information if said actual geographic position is located within said authorized geographic region.

13. The apparatus of Claim 12, wherein said receiver is a GPS receiver.

14. (Canceled)

c3
13-15. (Twice Amended) The apparatus of Claim 12, further comprising a reader for reading said stored information wherein said reader comprises a receiver decryption key for verifying the data comprising said cryptographically signed actual position.

16. (Previously Amended) The apparatus of Claim 15, wherein said reader generates an initialization vector which is transmitted to the receiver and included in the signed data.

17. (Previously Amended) The apparatus of Claim 16, wherein said signed initialization vector is verified by the reader before said computer permits access to said stored information.

11-18. (Amended) A method for controlling access to a subset of files belonging to a larger set of files of stored information comprising:

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

c4 associating each of the files from the larger set of files with at least one authorized geographic region within which access to said stored information is authorized;

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

cryptographically signing at least the actual geographic position at the receiver;

verifying the signature of the actual geographic position;

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

providing a file decryption key which authorizes access to and permits decryption of said files belonging to said subset of files, provided that the actual geographic position

October 29, 1998

is located within the authorized geographic region for the files belonging to said subset of files.

19. (Previously Amended) The method of Claim 18, wherein said association of the files with the authorized geographic regions is stored as a policy comprising policy files wherein each policy file is accessible with a user password and authorizes, if the user password is valid, access to the files listed in said policy file, if the actual geographic position is located within the authorized geographic region associated with the files.

20. The method of Claim 19, wherein said policy is stored with the stored information.

19-21. (Amended) A method for controlling access to stored information comprising:
determining an actual date or time at the location of said stored information based on signals received at a receiver supplying reliable time information;
cryptographically signing at least the actual date or time at the receiver;
verifying the signature of the actual date or time;
comparing said actual date or time with a predetermined date or time interval at which access to said stored information is authorized; and
permitting access to said stored information if said actual date or time occurs within said authorized date or time interval.

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

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

24. The method of Claims 21, wherein said stored information is divided into subsets of information and wherein at least one of the subsets has a different authorized date or time interval from the other subsets, so that access is authorized to the subset whose authorized date or time interval matches the actual date or time, but not to the subsets whose authorized date or time interval does not match the actual date or time.

25. (Twice Amended) A method for controlling access to stored information comprising:

October 29, 1998

forming a policy associating said information with authorized geographic regions and authorized time intervals;

cryptographically signing said policy and said information;

storing said signed policy together with said signed information;

providing a password for unlocking said policy;

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

determining an actual time;

cryptographically signing at least the actual geographic position and the actual time at the receiver;

verifying the signature of the actual geographic position and the actual time;

comparing said actual geographic position and said actual time with said authorized geographic regions and authorized time interval of said policy; and

permitting access to said stored information if said actual geographic position and actual time falls within said authorized geographic regions and authorized time interval of said policy.

C6
end

26. (Previously Amended) The method of Claim 25, wherein position and time are determined through a Global Orbiting Navigational Satellite System.

27. (Previously Amended) The method of Claim 25, wherein position is determined through an inertial navigation system.

28. (Previously Amended) The method of Claim 25, wherein position is determined through a satellite based location determination system.

29. (New) A method for controlling access to stored information, the method comprising:

(a) determining a position;

(b) cryptographically signing data comprising at least a representation of the position;

(c) verifying the signature of the data comprising at least a representation of the position;

(d) determining that access to the stored information is authorized at the position;

and

C7

October 29, 1998

(e) permitting access to the information based at least upon (c) and (d).

The method of Claim 27, further comprising

(f) providing the cryptographically signed data to an information accessing device, wherein (c) and (e) are performed by the information accessing device.

(New) The method of Claim 28, further comprising:

(g) identifying a token;

(h) incorporating the token in the data that is cryptographically signed; and

(i) verifying that the cryptographically signed data comprises the token.

(New) The method of Claim 29, wherein (g) and (i) are performed by the information accessing device.

(New) The method of Claim 31, wherein (a), (b), and (h) are performed by a position determining device.

(New) The method of Claim 31, further comprising

(j) providing the token to the position determining device.

REMARKS

In the Office Action, Claims 1-7, 12, 13, and 21-23 were rejected under 35 U.S.C. 103(a) as being unpatentable over Bates (U.S. 6,057,779). Claims 10-11, 18-20, and 24-28 were rejected under 35 U.S.C. 103(a) as being unpatentable over Bates in view of Schipper (U.S. 5,987,136).

Claims 8, 9, and 14-17 were objected to as depending from a rejected claim, but otherwise were allowable.

Claim 1-8, 10-13, and 15-34 are pending in the present application after the above amendments.

Discussion of the Cited Art

Bates discloses a secure cargo transportation system including a cargo container that can be opened only in certain locations. The container is configured with a lock coupled to a global positioning system receiver. The lock can be opened when the container is located within a predetermined distance of a location coordinate. Bates also discloses a corresponding method for controlling access to the cargo container based upon its position. Bates is directed to controlling access to physical objects, such as cargo.

Schipper discloses an apparatus for producing an image together with position information for the image.

Applicants will treat all of the cited references as prior art for purposes of responding to the outstanding Office Action, but reserve the right to swear behind one or more references at a later date.

Responses to Rejections

In order to further the case toward allowance, Applicants have amended the independent claims to incorporate limitations that the Examiner has indicated would make the claims allowable. Applicants, however, disagree with the Examiner's rejections of Claims 1-7, 10-13, and 18-28 and reserves the right to pursue the rejected claims in a continuation application.

By focusing on specific references, claims and limitations, Applicants do not intend to imply an agreement with the Examiner's assertions with respect to other references, claims, and limitations.

As to Claims 1-8 and 10-11

Independent Claim 1 has been amended to incorporate the limitations of Claim 9, which the Examiner indicated was allowable. Accordingly, independent Claim 1 as well as Claims 2-8 and 10-11 which depend therefrom should also be allowable.

As to Claims 12-13 and 15-17

Independent Claim 12 has been amended to incorporate the limitations of Claim 14, which the Examiner indicated was allowable. Accordingly, independent Claim 12 as well as Claims 13 and 15-17 which depend therefrom should also be allowable.

As to Claims 18-20

Independent Claim 18 has been amended to incorporate limitations similar to the limitations added by Claim 9, which the Examiner indicated was allowable. Accordingly, Claim 18 now requires "cryptographically signing at least the actual geographic position at the receiver" and "verifying the signature of the actual geographic position." None of the references cited by the Examiner disclose these limitations and Claim 18 should therefore be allowable. Claims 19-20, which depend from Claim 18, should also be allowable.

As to Claims 21-24

Independent Claim 21 has been amended to incorporate limitations similar to the limitations added by Claim 9, which the Examiner indicated was allowable, but directed to a date

or time. Claim 21 now requires "cryptographically signing at least the actual date or time at the receiver" and "verifying the signature of the actual date or time." None of the references cited by the Examiner disclose these limitations and Claim 21 should therefore be allowable. Claims 22-24, which depend from Claim 21, should also be allowable.

As to Claims 25-28

Independent Claim 25 has been amended to incorporate limitations similar to the limitations added by Claim 9, which the Examiner indicated was allowable, but further including a time. Accordingly, Claim 25 now requires "cryptographically signing at least the actual geographic position and the actual time at the receiver" and "verifying the signature of the actual geographic position and the actual time." None of the references cited by the Examiner disclose these limitations and Claim 25 should therefore be allowable. Claims 26-28, which depend from Claim 25, should also be allowable.

As to New Claims 29-34

Independent Claim 29 requires "(b) cryptographically signing data comprising at least a representation of the position" and "(c) verifying the signature of the data comprising at least a representation of the position." None of the references cited by the Examiner disclose these limitations and Claim 29 should therefore be allowable. Claims 30-34, which depend from Claim 29, should also be allowable.

CONCLUSION

In view of the foregoing remarks, Applicants submit that the application is in condition for allowance. If, however, issues remain which can potentially be resolved by telephone, the Examiner is invited to call the undersigned attorney of record at his direct dial number of (949) 721-6377.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: _____

8/16/01

By: _____

Alexander Franco
Registration No. 45,753
Attorney of Record
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

MARKED-UP VERSIONS OF AMENDMENTS TO THE APPLICATION

In the Claims

1. (Amended) A method for controlling access to stored information comprising:
determining an actual geographic position where said stored information is located based on signals received at a receiver supplying reliable position information;
cryptographically signing said actual geographic position with a receiver encryption key;
verifying the signature of said actual geographic position;
~~comparing determining that~~ said actual geographic position is within a geographic region within which access to said stored information is authorized; and
permitting access to said stored information ~~if said actual geographic position is located within said authorized geographic region.~~
2. The method of Claim 1, wherein said receiver comprises a GPS receiver.
3. The method of Claim 1, wherein said information is stored on a computer-readable medium.
4. The method of Claim 3, wherein said computer-readable medium is portable.
5. The method of Claim 3, wherein said computer-readable medium comprises a high-capacity disk.
6. The method of Claim 1, wherein said stored information comprises files and each of said files has an associated geographic region within which access is permitted, and further permitting access to said file if said actual geographic position is located within said authorized geographic region for said file.
7. The method of Claim 6, further comprising denying access to said stored information if said actual geographic position does not match said authorized geographic region.
8. The method of Claim 1, further comprising:
encrypting said stored information using an encryption key; and
providing a decryption key which permits decryption of said stored information if said actual geographic position is located within said authorized geographic region.
9. (Canceled)

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

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

12. (Amended) Apparatus for controlling access to stored information comprising:

a receiver supplying reliable position information for determining an actual geographic position where said stored information is located, wherein the receiver comprises a receiver encryption mechanism providing a receiver encryption key for cryptographically signing data comprising the actual geographic position; and

a computer for comparing said actual geographic position with a geographic region within which access to said stored information is authorized,

wherein said computer permits access to said stored information if said actual geographic position is located within said authorized geographic region.

13. The apparatus of Claim 12, wherein said receiver is a GPS receiver.

14. (Canceled)

15. (Twice Amended) The apparatus of Claim 14, further comprising a reader for reading said stored information wherein said reader comprises a receiver decryption key for verifying the data comprising said cryptographically signed actual position.

16. (Previously Amended) The apparatus of Claim 15, wherein said reader generates an initialization vector which is transmitted to the receiver and included in the signed data.

17. (Previously Amended) The apparatus of Claim 16, wherein said signed initialization vector is verified by the reader before said computer permits access to said stored information.

18. (Amended) A method for controlling access to a subset of files belonging to a larger set of files of stored information comprising:

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

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

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

cryptographically signing at least the actual geographic position at the receiver;

verifying the signature of the actual geographic position;

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

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

19. (Previously Amended) The method of Claim 18, wherein said association of the files with the authorized geographic regions is stored as a policy comprising policy files wherein each policy file is accessible with a user password and authorizes, if the user password is valid, access to the files listed in said policy file, if the actual geographic position is located within the authorized geographic region associated with the files.

20. The method of Claim 19, wherein said policy is stored with the stored information.

21. (Amended) A method for controlling access to stored information comprising:

determining an actual date or time at the location of said stored information based on signals received at a receiver supplying reliable time information;

cryptographically signing at least the actual date or time at the receiver;

verifying the signature of the actual date or time;

comparing said actual date or time with a predetermined date or time interval at which access to said stored information is authorized; and

permitting access to said stored information if said actual date or time occurs within said authorized date or time interval.

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

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

24. The method of Claims 21, wherein said stored information is divided into subsets of information and wherein at least one of the subsets has a different authorized date or time interval from the other subsets, so that access is authorized to the subset whose authorized date or time interval matches the actual date or time, but not to the subsets whose authorized date or time interval does not match the actual date or time.

25. (Twice Amended) A method for controlling access to stored information comprising:

forming a policy associating said information with authorized geographic regions and authorized time intervals;

cryptographically signing said policy and said information;

storing said signed policy together with said signed information;

providing a password for unlocking said policy;

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

determining an actual time;

cryptographically signing at least the actual geographic position and the actual time at the receiver;

verifying the signature of the actual geographic position and the actual time;

comparing said actual geographic position and said actual time with said authorized geographic regions and authorized time interval of said policy; and

permitting access to said stored information if said actual geographic position and actual time falls within said authorized geographic regions and authorized time interval of said policy.

26. (Previously Amended) The method of Claim 25, wherein position and time are determined through a Global Orbiting Navigational Satellite System.

27. (Previously Amended) The method of Claim 25, wherein position is determined through an inertial navigation system.

28. (Previously Amended) The method of Claim 25, wherein position is determined through a satellite based location determination system.

29. (New) A method for controlling access to stored information, the method comprising:

(a) determining a position;

(b) cryptographically signing data comprising at least a representation of the position;

(c) verifying the signature of the data comprising at least a representation of the position;

(d) determining that access to the stored information is authorized at the position; and

(e) permitting access to the information based at least upon (c) and (d).

30. The method of Claim 29, further comprising

(f) providing the cryptographically signed data to an information accessing device, wherein (c) and (e) are performed by the information accessing device.

31. (New) The method of Claim 30, further comprising:

(g) identifying a token;

(h) incorporating the token in the data that is cryptographically signed; and

(i) verifying that the cryptographically signed data comprises the token.

32. (New) The method of Claim 31, wherein (g) and (i) are performed by the information accessing device.

33. (New) The method of Claim 31, wherein (a), (b), and (h) are performed by a position determining device.

34. (New) The method of Claim 31, further comprising

(j) providing the token to the position determining device.



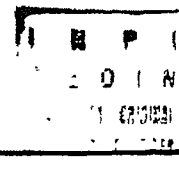
República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI 9904979-1 A**



(22) Data de Depósito 29/10/1999
(43) Data de Publicação 19/12/2000
(RPI 1563)

(51) Int. Cl.⁷:
G11B 23/28



(54) Título **CONTROLE DE ACESSO A UMA
INFORMAÇÃO ARMAZENADA**

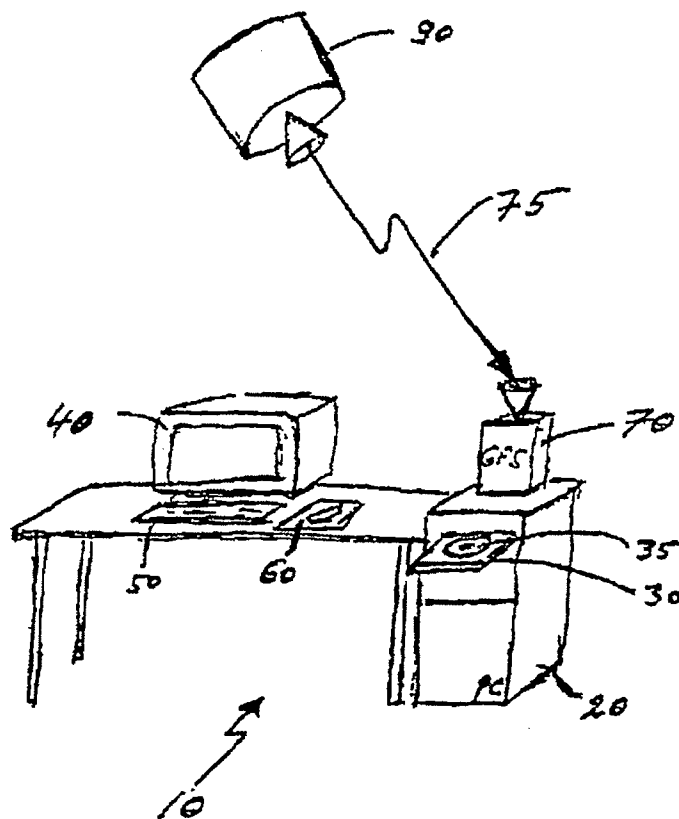
(30) Prioridade Unionista 29/10/1998 US 09/182,342

(71) Depositante(s) Datum Inc (US)

(72) Inventor(es) Thomas Mark Hastings, Michael E. Mcnell, Todd
S. Glassey, Gerald L. Willett

(74) Procurador Dannemann, Siemsen, Bigler & Ipanema Moreira

(57) Resumo Patente de Invenção "CONTROLE DE ACESSO A UMA
INFORMAÇÃO ARMAZENADA" O acesso a uma informação armazenada
por um usuário é controlado comparando-se uma posição geográfica real e/ou
uma data / um tempo real com uma região geográfica e/ou um intervalo de
data / tempo no qual o acesso à informação armazenada está autorizado. A
posição geográfica real onde a informação armazenada está localizada e a
data / o tempo real podem ser determinados, por exemplo, baseado em sinais
recebidos em um receptor que supre informação de posição e de tempo
confiável, tal como um receptor de GPS. O acesso à informação armazenada
é autorizado se a posição geográfica real e/ou a data / o tempo caírem na
região geográfica e/ou no intervalo de data / tempo autorizado. A informação
de posição e de data / tempo suprida pelo receptor pode ser assinada de
forma criptográfica e criptografada.



Relatório Descritivo da Patente de Invenção para "**CONTROLE DE ACESSO A UMA INFORMAÇÃO ARMAZENADA**".

Antecedentes

Esta invenção refere-se ao controle de acesso a uma informação armazenada

Meios de distribuição de dados, tais como CD-ROM, podem armazenar um grande número de arquivos. O produtor do CD-ROM pode desejar controlar o acesso pelos usuários a arquivos em particular, seja porque eles são confidenciais ou porque o acesso está sujeito a um pagamento pelo usuário

O acesso pode ser controlado requerendo-se que o usuário entre com uma senha obtida a partir do produtor do CD-ROM. Senhas diferentes podem desbloquear arquivos diferentes ou subconjuntos diferentes de arquivos. Os arquivos podem ser assinados de forma criptográfica e para proteção adicional podem ser criptografados. No esquema discutido na Patente U S No 5 646 992, incorporada aqui como referência, cada arquivo é criptografado pelo produtor com uma chave única conhecida apenas pelo produtor. O usuário recebe os itens criptografados e, após sua requisição para acesso ser processada pelo produtor, também recebe chaves de descriptografia, isto é, senhas, as quais são usadas para descriptar os respectivos arquivos criptografados. As senhas desbloqueiam apenas aqueles arquivos para os quais o acesso foi requisitado

Sumário

Em geral, em um aspecto da invenção, a invenção caracteriza um controle de acesso a uma informação armazenada determinando uma posição geográfica real onde a informação armazenada está localizada, baseado em sinais recebidos em um receptor que supre uma informação de posição confiável. A posição geográfica real é então comparada com uma região geográfica na qual o acesso à informação armazenada está autorizado. É permitido acesso do usuário à informação armazenada se a posição geográfica real estiver localizada na região geográfica autorizada

As modalidades da invenção incluem os aspectos a seguir. O

receptor que supre a informação de posição pode receber a informação de posição a partir de um sistema de determinação de localização baseado em satélite ou de um sistema de navegação inerte. A informação pode ser armazenada em um meio que pode ser lido em computador, tal como um disco de alta capacidade. A informação armazenada inclui arquivos, e cada um desses arquivos tem uma região geográfica associada na qual o acesso é permitido. O usuário tem acesso a um arquivo específico ou a arquivos se a posição geográfica real estiver localizada na região geográfica autorizada para este arquivo. A informação armazenada pode estar criptografada, e o usuário tem acesso à chave de descryptografia apenas se a posição geográfica real estiver localizada na região geográfica autorizada. A informação armazenada também pode estar dividida em subconjuntos de informação e onde pelo menos um dos subconjuntos tem uma região autorizada diferente dos outros subconjuntos. A associação dos arquivos às regiões geográficas autorizadas pode ser armazenada como um arquivo de política juntamente com a informação armazenada.

Em geral, em um outro aspecto, a invenção caracteriza a determinação de uma data ou tempo real no local da informação armazenada baseado em sinais recebidos em um receptor suprindo uma informação de tempo confiável. A data ou o tempo real é comparado com um intervalo de data ou tempo predeterminado no qual o acesso à informação armazenada está autorizado. O usuário pode ter acesso à informação armazenada se a data ou o tempo real ocorrer no intervalo de data ou tempo autorizado.

Em geral, em um outro aspecto, a invenção inclui um receptor que supre informação de posição confiável para determinação de uma posição geográfica real onde a informação armazenada está localizada. Um computador recebe a informação de posição com uma região geográfica na qual o acesso à informação armazenada está autorizado, e permite acesso à informação armazenada se a posição geográfica real estiver localizada na região geográfica autorizada. As modalidades da invenção incluem os aspectos a seguir. O receptor inclui um mecanismo de criptografia de receptor para assinar de forma criptográfica a posição geográfica real com uma cha-

ve de criptografia de receptor e verificando a assinatura do receptor com uma chave de descryptografia de receptor, antes da posição geográfica real ser comparada com a posição geográfica autorizada

Em geral, ainda em um outro aspecto, a invenção inclui um leitor
5 com uma chave de descryptografia de receptor para verificação da posição real assinada de forma criptográfica.

As modalidades da invenção incluem os aspectos a seguir A leitora gera um vetor de inicialização provendo um deslocamento de posição, o qual é transmitido para o receptor e adicionado à posição geográfica
10 autorizada. O leitor assina de forma criptográfica o deslocamento de posição com uma chave de criptografia de leitora O receptor verifica a assinatura de deslocamento de posição com uma chave de descryptografia de leitora correspondente, antes do deslocamento de posição ser adicionado à posição geográfica real

Em geral, em um outro aspecto, a invenção caracteriza a formação
15 de uma política associando a informação às regiões geográficas autorizadas e a intervalos de tempo autorizado e assina de forma criptográfica a política e a informação A política assinada é armazenada juntamente com a informação assinada O usuário obtém do produtor uma senha para desbloquear a política e obtém acesso à informação armazenada se a posição geográfica real e o tempo real caírem nas regiões geográficas autorizadas e
20 no intervalo de tempo autorizado da política

Dentre as vantagens da invenção estão uma ou mais das que se seguem

Um produtor de informação armazenada pode restringir o uso
25 daquela informação a regiões geográficas designadas ou pode excluir regiões designadas onde o uso não é permitido Por exemplo, um manual de serviços para um automóvel armazenado em um CD-ROM pode conter seções diferentes de informação, as quais são aplicáveis a países e/ou regiões específicas correspondentes Pode ser permitido que um usuário veja
30 apenas a porção da informação a qual é aplicável a sua localização geográfica atual Da mesma forma, o acesso a um relatório de corporação delicado

pode ser limitado a um local específico na instalação. O acesso a uma informação delicada quanto ao tempo pode ser negado antes ou depois de uma certa data ou limitado a um período permitido. Pela associação da informação sobre as regiões geográficas e os intervalos de tempo autorizados aos arquivos de política armazenados no CD-ROM e acessados por uma
 5 senha de usuário, o produtor do CD-ROM pode emitir uma nova senha, para permitir que o usuário acesse um conjunto em particular de arquivos de política e, portanto, a informação armazenada, para uma região e data / tempo correspondentes

10 Outras vantagens e aspectos tornar-se-ão aparentes a partir da descrição a seguir e das reivindicações

Descrição

A FIG 1 é uma vista em perspectiva de um sistema computacional,

15 A FIG 2 é um diagrama de blocos de um sistema baseado em computador para controle do acesso à informação armazenada,

As FIG 3 a 5 são fluxogramas,

A FIG 6 é um diagrama de blocos de elementos criptográficos

Como visto nas FIG 1 a 3, o acesso à informação a qual está
 20 armazenada em um CD-ROM que pode ser lido em computador portátil, o qual serve como um meio de distribuição de dados 35, pode ser controlado baseado em uma posição geográfica real de um sistema computacional 10 no qual a informação deve ser acessada e o tempo em que ela deve ser acessada

25 No sistema computacional 10, um computador 20 é conectado a um teclado 50, um mouse 60, um monitor 40, e um drive de CD-ROM 30. Um receptor de GPS 70 serve como uma fonte de informação de posição e de tempo confiável. O receptor 70 está localizado na posição geográfica real do sistema computacional 10 e recebe sinais 75 de um satélite de GPS
 30 em órbita 90 (sendo mostrado apenas um). O receptor 70 converte os sinais 75 recebidos em dados de posição geográfica 71 até uma precisão de vários metros de longitude, latitude e altura e em dados de data / tempo 71 até

uma precisão de microssegundos. Os dados 71 são transmitidos para o computador 20 via um controlador de dispositivo 72.

Uma cripto-placa de receptor 80 pode conter um certificado de chave pública 81 assinado pelo produtor e uma chave privada correspondente 82, como mostrado na FIG. 6. Os dados de posição geográfica e de data / tempo 71 podem então ser assinados com uma chave privada 82 para autenticar os dados.

A unidade de CD-ROM 30 também pode incluir capacidades de criptografia e de assinatura (decodificador 32), as quais podem ser implementadas em hardware ou em software. O decodificador 32 inclui um certificado de chave pública de cripto-placa 83, o qual é idêntico ao certificado 81, um certificado de produtor 84, para verificação da identidade do produtor, e uma chave de descryptografia de política de meio de distribuição 86 assinada pelo produtor, como mostrado na FIG. 6. O certificado de cripto-placa 83 verifica a assinatura da cripto-placa 80 assinada com a chave privada 82. A chave de descryptografia de política 86 descripta a política de acesso 155 armazenada no CD-ROM 35.

O sistema computacional 10 pode ter vários níveis de segurança, tais como Nível 1 e Nível 2, descritos nos exemplos a seguir.

Em um sistema com segurança de Nível 1, o receptor 70 comunica-se com o computador 20 via um controlador de dispositivo convencional 72 e o drive de CD-ROM 30 é um CD-ROM convencional. Nem o receptor 70 nem o drive de CD-ROM 30 têm capacidades de criptografia / descryptografia adicionais. Para uma segurança aumentada, o computador 20 em um sistema de Nível 1 pode ser um computador "seguro", o qual pode autenticar e/ou encriptar dados. Em um sistema de Nível 2 mais seguro, o receptor 70 pode incluir uma cripto-placa 80 e o drive de CD-ROM 30 pode incluir um decodificador 32. O sistema de Nível 2 é projetado para prover autenticação de dados e transmissão de dados criptografados entre o receptor 70 e o decodificador 32. O computador 20 pode então ser qualquer computador convencional sem autenticação e criptografia de dados.

O dados introduzidos via o teclado 50 e o mouse 60 podem in-

cluír uma entrada de comando e dados típica 130 introduzida via uma interface com usuário 95 (provida por um programa aplicativo 34) e uma ou mais senhas 130 que permitem que um usuário tenha acesso a uma informação armazenada no meio de distribuição de dados 35

5 O CD-ROM 35 armazena tipos diferentes de informação, tal como arquivos com informação 144, uma lista 150 de regiões geográficas autorizadas, uma lista 154 de intervalos de data / tempo autorizados, um ou mais arquivos de chave de descryptografia de arquivo 146, um ou mais arquivos de política 152 e uma assinatura 147 para todo o CD-ROM 35. Como visto na FIG. 3, os arquivos 144, 146, 150, 152, 154 e 155 podem ser assinados e criptografados

Os arquivos 144 podem ser agrupados em subconjuntos 141, 142 e 143. Os arquivos podem pertencer a mais de um subconjunto. (Na discussão a seguir, o termo arquivo refere-se a ambos arquivos e subconjuntos.) Cada arquivo 141, 142 e 143 pode ser criptografado com uma única chave de criptografia 51 (E_1 , E_2 , E_3). As chaves de descryptografia de arquivo correspondentes 52 (K_1 , K_2 , K_3) são armazenados no CD-ROM 35 no arquivo de chave de descryptografia de arquivo 146. A informação adicional sobre as chaves de descryptografia e o arquivo de chave de descryptografia são encontrados na Patente U.S. No. 5.646.992.

Cada arquivo 141, 142 e 143 no CD-ROM 35 está associado a zero, uma ou mais regiões geográficas autorizadas armazenadas na lista 150 de regiões geográficas autorizadas. Por exemplo, uma região pode ser limitada por latitudes e longitudes correspondentes à extensão do Empire State Building na Cidade de Nova York e a uma altitude entre 50 e 60 metros, de modo que o arquivo associado àquela região só possa ser aberto se o receptor 70 estiver localizado em uma certa área de escritório no interior do Empire State Building.

Da mesma forma, cada arquivo 141, 142 e 143 está associado a zero, um ou mais dos intervalos de data / tempo autorizados armazenados na lista 154 de intervalos de data / tempo autorizados.

Cada satélite de GPS 90 mantém um clock extremamente preci-

so O receptor 70 recebe os sinais de clock de GPS como parte dos sinais 75, ou um clock atômico local pode prover sinais de clock similares. Os sinais de clock permitem um controle do acesso à informação baseado no tempo real em que o acesso à informação é tentado. Por exemplo, o produtor 5 pode especificar que o acesso seja garantido apenas (1) antes de uma data / um tempo predeterminado, (2) após uma data / um tempo predeterminado, ou (3) apenas durante um período de data / tempo predeterminado.

O produtor pode associar os arquivos 141, 142 e 143 a itens específicos nas listas 150 e 154 via uma senha 130, a qual o usuário introduz via o teclado 50. A senha 130 pode ser uma senha de usuário válida 10 por mais de um acesso, ou pode ser uma senha para uma única vez. Alternativamente, o produtor pode associar informação específica de região geográfica / data / tempo de listas 150 e 154 com os arquivos 141, 142 e 143 via os arquivos de política 152. Uma senha de usuário válida 130 pode des- 15 bloquear um ou mais arquivos de política 152. Se a posição geográfica real do usuário e a data e o tempo atual estiverem na região geográfica autorizada e na data / no tempo autorizado correspondente à senha de usuário 150, então, o usuário pode ter acesso aos arquivos selecionados via a interface de usuário 95. A informação selecionada é então exibida no dispositivo de saída 40. 20

A Tabela 1 mostra, como um exemplo, como cinco arquivos criptografados, A a F, armazenados no CD-ROM 35 e associados a regiões geográficas autorizadas e datas / tempos correspondentes, podem ser acessados. Cada arquivo está associado a uma de quatro chaves de des- 25 criptografia de arquivo diferentes K1 a K4. L1 e L2 são as duas regiões geográficas autorizadas diferentes e T1, T2, e T3 são três intervalos de data / tempo autorizados. O usuário que está de posse da chave de descryptografia de arquivo K1, por exemplo, uma senha, pode descriptar o Manual A nas regiões geográficas L1 e L3 no tempo T1. O mesmo usuário também 30 pode descriptar o Manual D no mesmo tempo T1 nas regiões L2 e L3, mas não na região L1. Da mesma forma, o usuário que tem a chave K2 pode descriptar a Imagem B e a Imagem E na região L2, mas não ao

mesmo tempo. O Desenho C pode ser descriptografado com a chave K3 em qualquer lugar, mas apenas no tempo T3, enquanto o Relatório Comercial F requer a chave K4 e pode ser descriptografado em qualquer tempo, mas apenas na região L1.

5

Tabela 1

Arquivo Cripto- grafado	Chave de Des- criptografia de Arquivo	Regiões Geográficas Autorizadas	Intervalos de Data / Tempo Autorizados
Manual A	K1	L1, L3	T1
Imagem B	K2	L2	T1, T3
Figuras C	K3	--	T3
Manual D	K1	L2, L3	T1
Imagem E	K2	L2	T2
Relatório F	K4	L1	--

Como mostrado na FIG 3, para fins de assinatura criptográfica com criptografia opcional, o produtor seleciona arquivos fontes 144' a serem escritos no CD-ROM 35 e especifica uma lista de regiões geográficas autorizadas 150' e uma lista de intervalos de data e tempo autorizados 154'. O produtor associa (como mostrado na Tabela 1) cada arquivo ou subconjunto de arquivos com zero, uma ou mais regiões geográficas 150' e zero, um ou mais intervalos de data / tempo 154' e armazena esta associação em um arquivo de política 152'. Cada um dos arquivos 144', 150', 152', 154' pode ser assinado e criptografado nas etapas 53, 340, 350 e 360 com as chaves de criptografia correspondentes 51, 345, 355 e 365, respectivamente. Os arquivos criptografados correspondentes 150, 152 e 154 são então armazenados juntos no CD-ROM 35 como uma política de acesso a região / tempo / arquivo criptografado assinado 155. Também são armazenados no CD-ROM 35, como mencionado acima, os arquivos assinados / criptografados 144, o arquivo de chave de arquivo simétrico assinado / criptografado 146 e a assinatura 147 usada pelo produtor para assinar todo o CD-ROM 35.

Como visto nas FIG 4 e 5, para se ter acesso aos arquivos as-

sinados / criptografados 144, o usuário obtém uma senha 130 (FIG 2) a partir do produtor (etapa 400), e introduz a senha 130 via o teclado 50 (etapa 410). É assumido que a senha 130 seja uma senha para uma única vez, embora as senhas de usuário válidas por mais de uma sessão também possam ser usadas

Como visto na FIG 4, as porções iniciais do fluxo de processo para o Nível 1 e o Nível 3 são quase idênticas

A etapa 420 verifica a senha 130 e o processo então executa a etapa 440 (para o Nível 1, sem nenhuma segurança adicional) ou a 450 (para o Nível 2, com segurança de receptor / drive de CD-ROM), dependendo da configuração do sistema. Os detalhes das etapas 440 e 450 são mostradas na FIG 5 e serão discutidos agora

Como visto na FIG 5, no processo 440, a senha de usuário 130 é enviada para o controlador de dispositivo 72 (etapa 510). Em resposta à senha de uso único 130, o controlador de dispositivo 72 gera a partir da senha de usuário 130 sua própria senha de uso único (etapa 520) e verifica (etapa 530) que o usuário de fato introduziu uma senha de uso único correto 130, desse modo autenticando o usuário para a sessão interativa (etapa 532). Caso contrário, o acesso é negado (etapa 535)

Uma vez que a senha 130 tenha autenticado o usuário, o controlador de dispositivo 72 interroga o receptor 70 quanto à posição e à data / tempo atuais (etapa 540). O controlador de dispositivo 72 então compara os dados de tempo e posição retornados pelo receptor 70 com a política 155, a qual se aplica aos arquivos 144 ou a um subconjunto 141, 142 e 143 dos arquivos (etapa 460). Se o usuário estiver autorizado a acessar os arquivos 144, então, o dado é desbloqueado, descriptografado (etapa 470, FIG 3) com as chaves de descriptografia 52 (etapa 480) e suprido para o programa aplicativo de usuário 34 (etapa 490) e exibido

Em um sistema de Nível 2, o receptor 70 inclui a placa de receptor criptográfico 80, a partir deste ponto referida como a "cripto-placa". Como mencionado antes, a cripto-placa 80 pode assinar e encriptar / descriptar mensagens. O drive de CD-ROM 30 inclui o decodificador 32

para decodificar os dados de posição assinados e recebidos a partir da cripto-placa 80

Como visto na FIG 5, no processo 450, a senha de usuário 130 é enviada para o controlador de dispositivo 72, o qual aceita a senha 130 e a passa inalterada para o decodificador 32 (etapa 550). O controlador 32 então gera internamente com a chave privada 86 sua própria senha de uso único correspondente à senha de usuário (etapa 560) e verifica (etapa 570) se a senha correta 130 foi comunicada pelo controlador de dispositivo 72, desse modo autenticando o usuário para a sessão interativa (etapa 572).
10 Caso contrário, o acesso é negado (etapa 575)

Uma vez que o circuito de criptografia 32 tenha autenticado o usuário, o controlador 32 interroga a cripto-placa 80 via o controlador de dispositivo 72 quanto ao tempo atual e à informação de posição do receptor 70 (etapa 580). A unidade de decodificador 30 provê a cripto-placa 80 com um padrão randômico ou de outro bit assinado para formar um "vetor de inicialização" (etapa 590), isto é, um deslocamento de posição, o qual o controlador de dispositivo 72 passa através da cripto-placa 80 juntamente com a requisição pelo tempo e pela posição (etapa 590).
15

A cripto-placa 80 responde preparando um pacote de acordo com um formato de dados preestabelecido, o qual inclui o tempo atual e a posição geográfica real na latitude e longitude e altitude (etapa 600). Também pode ser incluída uma informação identificando os satélites transmitindo os dados de posição, bem como outros dados necessários para computações. A cripto-placa 80 também armazena o vetor de inicialização provido a um deslocamento conhecido no pacote, e aplica uma assinatura criptográfica ao conteúdo do pacote. A assinatura criptográfica pode ser, por exemplo, uma mensagem de compilação / reedição do pacote de dados, mais uma criptografia da compilação de mensagem, de acordo com alguma chave predeterminada, e pode ser simétrica ou assimétrica, dependendo da chave ou do certificado armazenado na cripto-placa 80.
20
25
30

A cripto-placa 80 então transmite (etapa 605) o pacote de tempo/local assinado para o controlador de dispositivo 72, o qual envia o pa-

cote para o decodificador 32 / o drive de CD-ROM 30. O decodificador 32 compara a assinatura do pacote recebido da cripto-placa 80 com uma assinatura armazenada no decodificador 32 (etapa 610). Se a assinatura for verificada apropriadamente (etapa 620), o vetor de inicialização no pacote é

5 examinado para se determinar se o vetor de inicialização é de fato o mesmo vetor de inicialização o qual o decodificador 32 proveu para a cripto-placa 80 na etapa 590. Se este for o caso, então o pacote recebido pelo decodificador 32 é recente e genuíno, e os dados de tempo e posição são aceitos como válidos.

10 Uma vez que o pacote da cripto-placa 80 esteja autorizado, baseado na assinatura e no vetor de inicialização, o decodificador 32 compara os dados de tempo e posição recebidos da cripto-placa 80 com a política 155, a qual se aplica aos arquivos 144 ou a um subconjunto de arquivos 144 (etapa 460). Se o usuário estiver autorizado a acessar os arquivos 144, então o dado é desbloqueado (etapa 470), descriptografado com as chaves de

15 descriptografia 52 (etapa 480) e suprido para o programa aplicativo do usuário 34 e exibido (etapa 490).

Outras modalidades estão no escopo das reivindicações a seguir. Por exemplo, o receptor de GPS não precisa estar localizado na posição exata do leitor de meios de distribuição de dados, mas poderia estar em

20 um local conhecido (tal como uma sala contendo um servidor de controle provendo serviços computacionais para uma rede de área local em um prédio) em relação ao leitor.

Os arquivos de política 152' também podem designar regiões geográficas onde o acesso a certos arquivos 144 é negado.

25

O controle sobre acesso a arquivos não precisa estar limitado ao uso de senhas providas pelo produtor e introduzidas via um teclado. Por exemplo, certos atributos biométricos, tais como aspectos faciais, impressões digitais e/ou impressões vocais podem ser substituídos ou usados

30 além das senhas.

REIVINDICAÇÕES

- 1 Método para controle de acesso a informação armazenada, que compreende:
 - determinação de uma posição geográfica real onde a referida
 - 5 informação armazenada está localizada, baseado em sinais recebidos em um receptor suprindo uma informação de posição confiável,
 - comparação da referida posição geográfica real com uma região geográfica na qual o acesso à referida informação armazenada está autorizado, e
 - 10 permissão de acesso à referida informação armazenada se a referida posição geográfica real estiver localizada na referida região geográfica autorizada
- 2 Método, de acordo com a reivindicação 1, onde o referido receptor compreende um receptor de GPS
- 15 3. Método, de acordo com a reivindicação 1, onde a referida informação é armazenada em um meio que pode ser lido em computador
- 4 Método, de acordo com a reivindicação 3, onde o referido meio que pode ser lido em computador é portátil
- 5 Método, de acordo com a reivindicação 3, onde o referido
- 20 meio que pode ser lido em computador compreende um disco de alta capacidade
- 6 Método, de acordo com a reivindicação 1, onde a referida informação armazenada compreende arquivos e cada um dos referidos arquivos tem uma região geográfica associada na qual o acesso é permitido, e
- 25 ainda permitindo acesso ao referido arquivo se a referida posição geográfica real estiver localizada na referida região geográfica autorizada para o referido arquivo
- 7 Método, de acordo com a reivindicação 6, que ainda compreende negar o acesso à referida informação armazenada se a referida posição geográfica real não se combinar à referida região geográfica autorizada
- 30 8 Método, de acordo com a reivindicação 1, que ainda compreende

criptografia da referida informação armazenada usando-se uma chave de criptografia, e

provisão de uma chave de descriptografia a qual permite a descriptografia da referida informação armazenada se a referida posição geográfica real estiver localizada na referida região geográfica autorizada

9 Método, de acordo com a reivindicação 1, que ainda compreende

assinatura de forma criptográfica da referida posição geográfica real com uma chave de criptografia de receptor, e

10 verificação da assinatura de receptor com uma chave de descriptografia de receptor antes da posição geográfica real ser comparada com a referida posição geográfica real

10 Método, de acordo com a reivindicação 1, onde a referida informação armazenada é dividida em subconjuntos de informação e onde pelo menos um dos subconjuntos tem uma região autorizada diferente dos outros subconjuntos, de modo que o acesso seja autorizado ao subconjunto cuja região geográfica autorizada esteja localizada na posição geográfica real, mas não aos subconjuntos cuja região geográfica autorizada não esteja localizada na posição geográfica real

20 11 Método, de acordo com a reivindicação 6, onde a referida associação de arquivos às regiões geográficas autorizadas é armazenada como um arquivo de política juntamente com a referida informação armazenada

25 12 Aparelho para o controle de acesso à informação armazenada, que compreende

um receptor que supre uma informação de posição confiável para determinação de uma posição geográfica real onde a referida informação armazenada está localizada, e

um computador para comparar a referida posição geográfica real com uma região geográfica na qual o acesso à referida informação armazenada está autorizado,

onde o referido computador permite acesso à referida informa-

ção armazenada se a referida posição geográfica real estiver localizada na referida região geográfica autorizada

13 Aparelho, de acordo com a reivindicação 12, onde o referido receptor é um receptor de GPS

5 14 Aparelho, de acordo com a reivindicação 12, onde o receptor ainda compreende um mecanismo de criptografia de receptor provendo uma chave de criptografia de receptor para assinar de forma criptográfica a referida posição geográfica real

10 15 Aparelho, de acordo com a reivindicação 14, que ainda compreende um leitor para leitura da referida informação armazenada, onde o referido leitor compreende uma chave de descryptografia de receptor, para verificação da referida posição real assinada de forma criptográfica

15 16 Aparelho, de acordo com a reivindicação 15, onde o referido leitor gera um vetor de inicialização provendo um deslocamento de posição o qual é transmitido para o receptor e adicionado à posição geográfica real

20 17 Aparelho, de acordo com a reivindicação 16, que ainda compreende um mecanismo de criptografia de leitor provendo uma chave de criptografia de leitor para assinar de forma criptográfica o deslocamento de posição, onde a referida assinatura de deslocamento de posição é verificada pelo receptor com uma chave de descryptografia de leitor correspondente, antes do deslocamento de posição ser adicionado à posição geográfica real

25 18 Método para o controle de acesso a um subconjunto de arquivos pertencentes a um conjunto de arquivos maiores de informação armazenada, que compreende

associação de uma única chave de criptografia de arquivo a cada arquivo do conjunto de arquivos maior e a criptografia dos arquivos usando-se as chaves de criptografia associadas,

30 associação de cada um dos arquivos de um conjunto de arquivos maior a pelo menos uma região geográfica autorizada na qual o acesso à referida informação armazenada está autorizado,

determinação de uma posição geográfica real onde a referida

informação armazenada está localizada baseado nos sinais recebidos em um receptor que supre uma informação de posição confiável,

comparação da referida posição geográfica real com a referida região geográfica autorizada, e

5 provisão de uma chave de descryptografia de arquivo, a qual autoriza o acesso e permite a descryptografia dos referidos arquivos pertencentes ao referido subconjunto de arquivos, desde que a posição geográfica real esteja localizada na região geográfica autorizada para os arquivos pertencentes ao referido subconjunto de arquivos

10 19 Método, de acordo com a reivindicação 18, onde a referida associação dos arquivos às regiões geográficas autorizadas é armazenada como uma política compreendendo arquivos de política, onde cada arquivo de política é acessível com uma senha de usuário e autoriza, se a senha de usuário for válida, o acesso aos arquivos listados no referido arquivo de política, se a posição geográfica real estiver localizada na região geográfica
15 autorizada associada aos arquivos

20 20 Método, de acordo com a reivindicação 19, onde a referida política está armazenada com a informação armazenada

20 21 Método para o controle de acesso a uma informação armazenada, que compreende

determinação de uma data ou um tempo real no local da referida informação armazenada baseado em sinais recebidos em um receptor que supre uma informação de tempo confiável,

25 comparação da referida data ou tempo real com um intervalo de data ou tempo real predeterminado no qual o acesso à referida informação armazenada está autorizado, e

permissão de acesso à referida informação armazenada se a referida data ou o tempo real ocorrer no referido intervalo de data ou tempo autorizado

30 22 Método, de acordo com a reivindicação 21, que ainda compreende negar o acesso à referida informação armazenada se a referida data ou tempo real não ocorrer no referido intervalo de data ou tempo auto-

rizado

23 Método, de acordo com a reivindicação 21, onde a referida
informação compreende arquivos, e cada um dos referidos arquivos tem um
intervalo de data ou tempo autorizado associado no qual o acesso é permi-
5 tido, e ainda permitindo acesso ao referido arquivo se a referida data ou
tempo real ocorrer no referido intervalo de data ou tempo autorizado associ-
ado

24 Método, de acordo com a reivindicação 21, a onde a referida
informação armazenada é dividida em subconjuntos de informação e onde
10 pelo menos um dos subconjuntos tem um intervalo de data ou tempo autori-
zado diferente dos outros subconjuntos, de modo que o acesso seja autori-
zado ao subconjunto cujo intervalo de data ou tempo autorizado combinar-
se à data ou ao tempo real, mas não aos subconjuntos cujo intervalo de
data ou tempo autorizado não se combinar à data ou ao tempo real

15 25 Método para controle de acesso a uma informação armaze-
nada, que compreende

formação de uma política associando a referida informação nas
regiões geográficas autorizadas e os intervalos de tempo autorizados;

assinatura de forma criptográfica da referida política e da referi-
20 da informação,

armazenamento da referida política assinada juntamente com a
referida informação assinada,

provisão de uma senha para desbloquear a referida política, e
determinação de uma posição geográfica real onde a referida
25 informação armazenada está localizada, baseado em sinais recebidos em
um receptor que supre uma informação de posição confiável,

determinação de um tempo real,
comparação da referida posição geográfica real e do referido
tempo real com as referidas regiões geográficas autorizadas e o intervalo de
30 tempo autorizado da referida política, e

permissão de acesso à referida informação armazenada se a
referida posição geográfica real e o tempo real caírem nas referidas regiões

geográficas autorizadas e no intervalo de tempo autorizado da referida política

26 Método, de acordo com a reivindicação 1, onde a fonte de posição e tempo confiáveis é um Sistema de Satélite de Navegação de Ór-
5 bita Global

27 Método, de acordo com a reivindicação 1, onde a referida fonte de posição e tempo confiáveis é um sistema de navegação inerte

28 Método, de acordo com a reivindicação 1, onde a referida fonte de posição e tempo confiáveis é um sistema de determinação de loca-
10 lização baseado em satélite

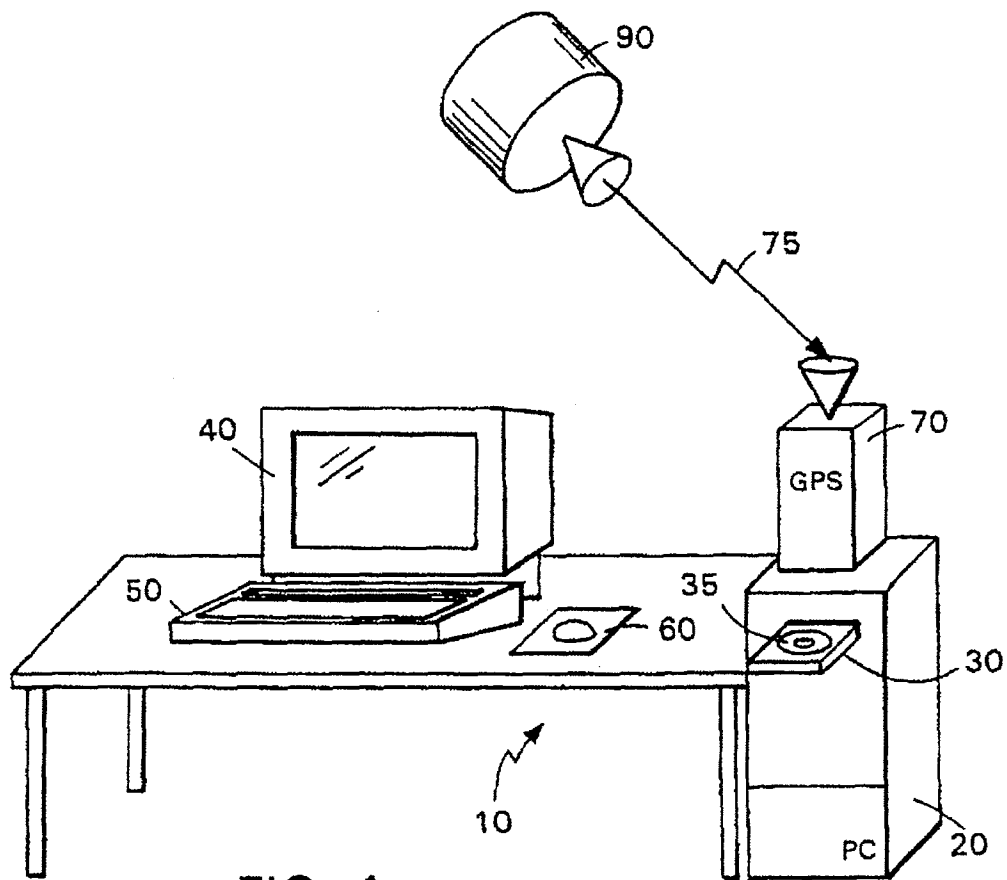
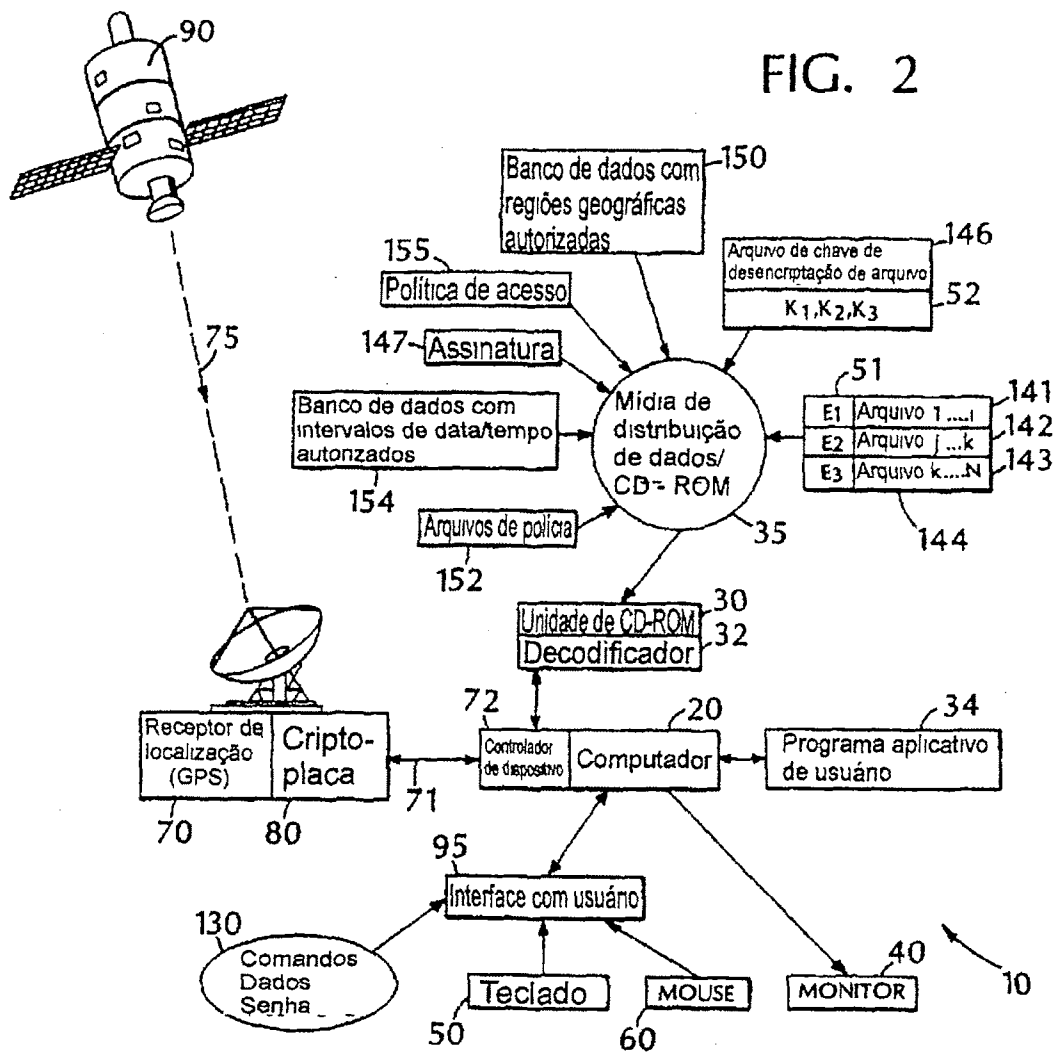


FIG. 1

FIG. 2



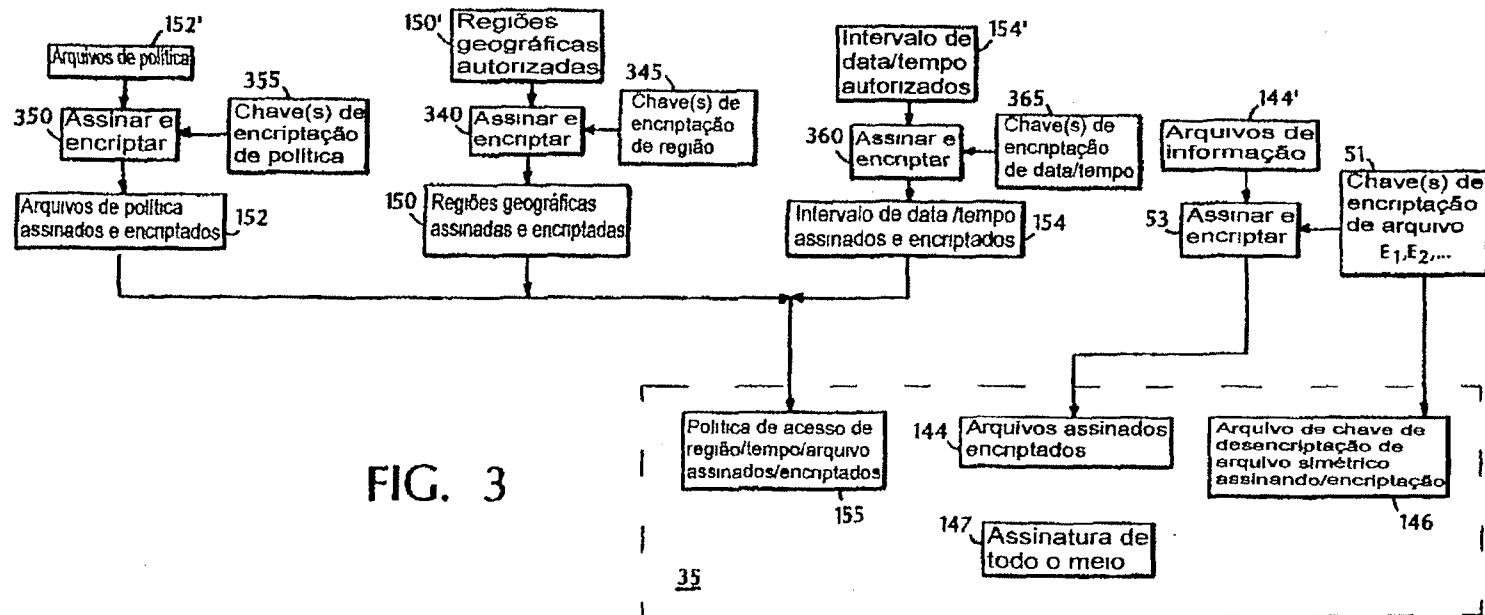
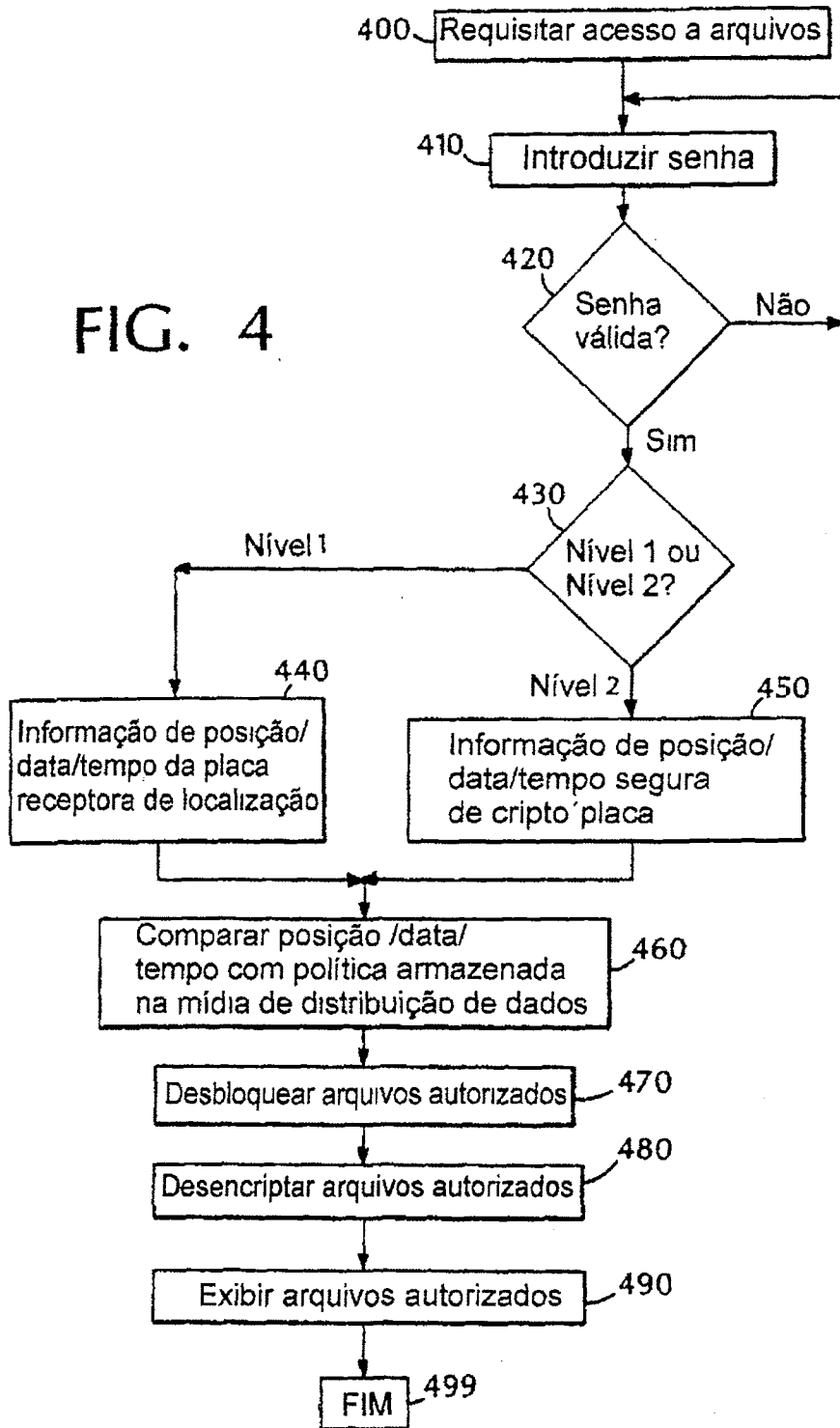
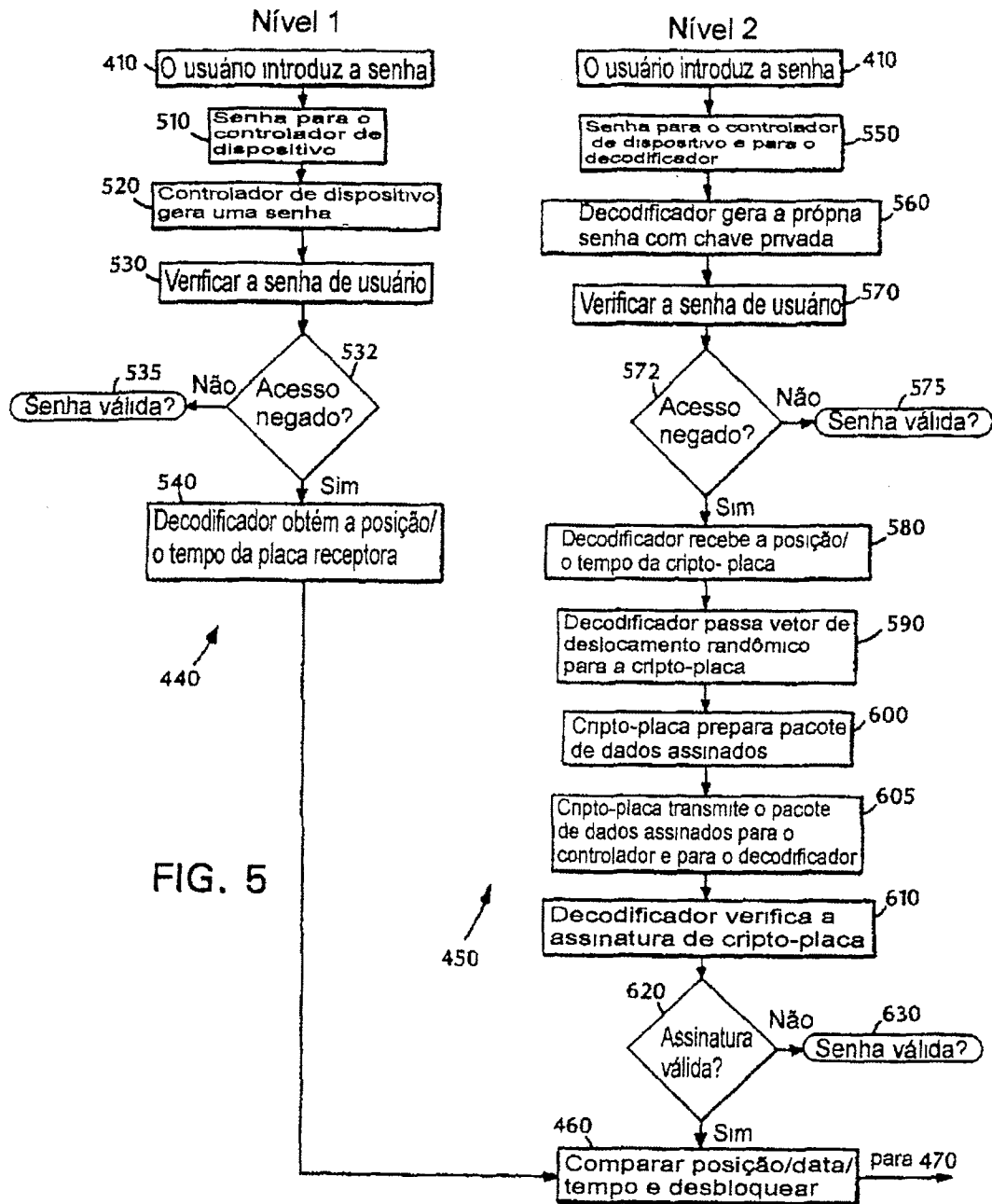


FIG. 3

FIG. 4





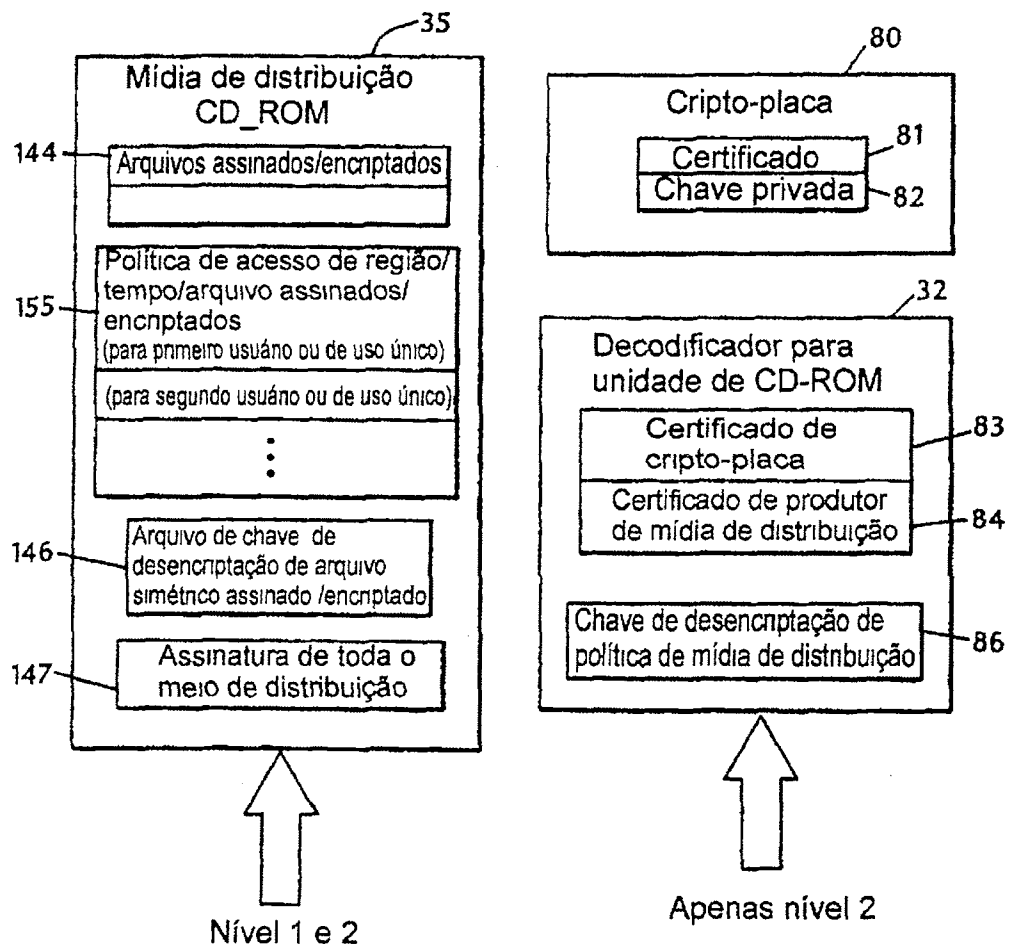


FIG. 6

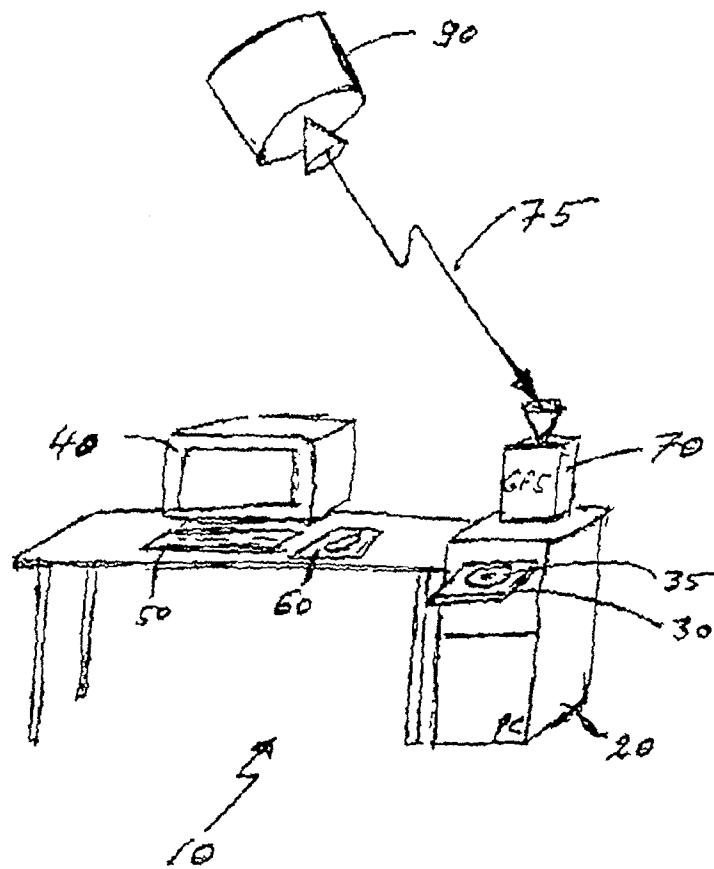


Fig. 1

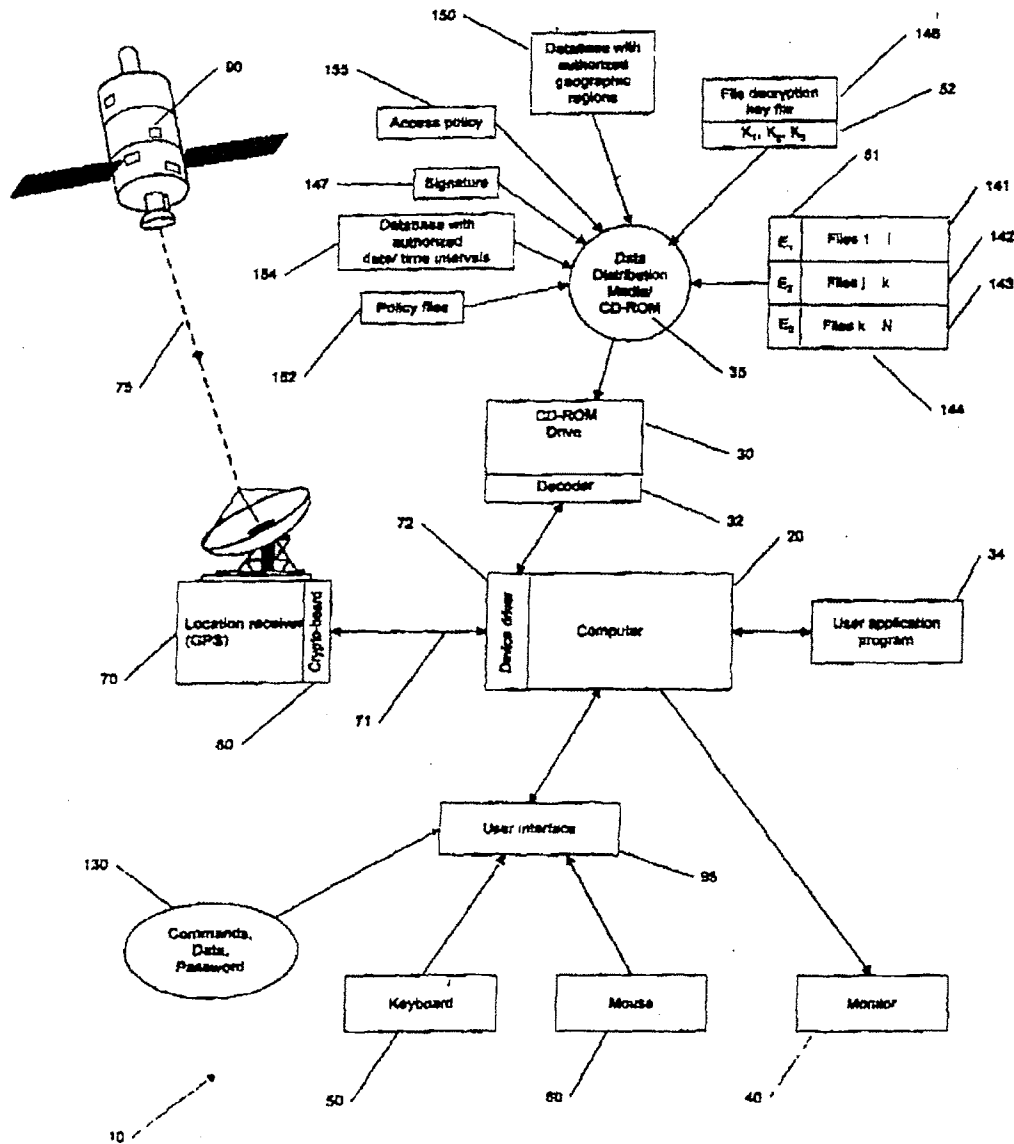


FIG 2

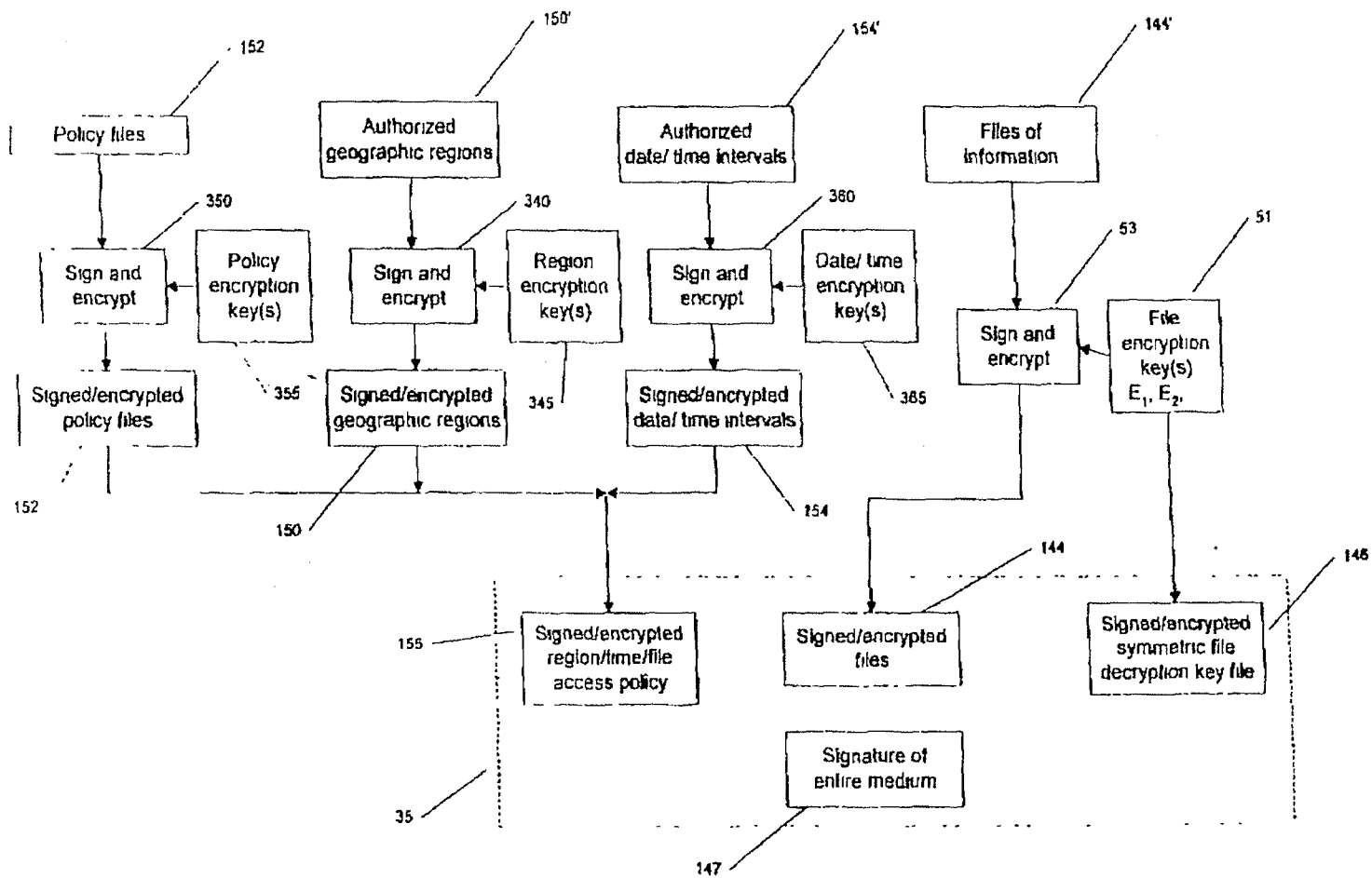


FIG. 3

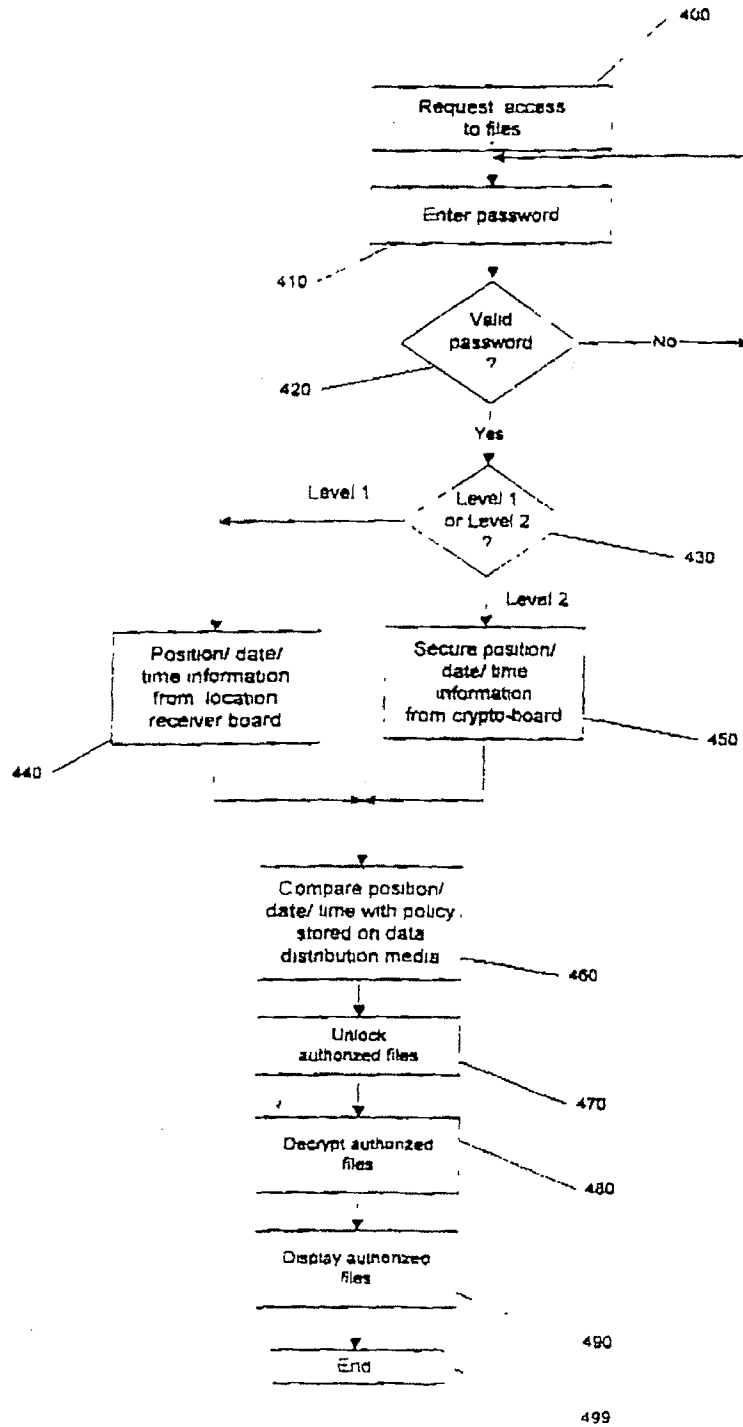


FIG. 4

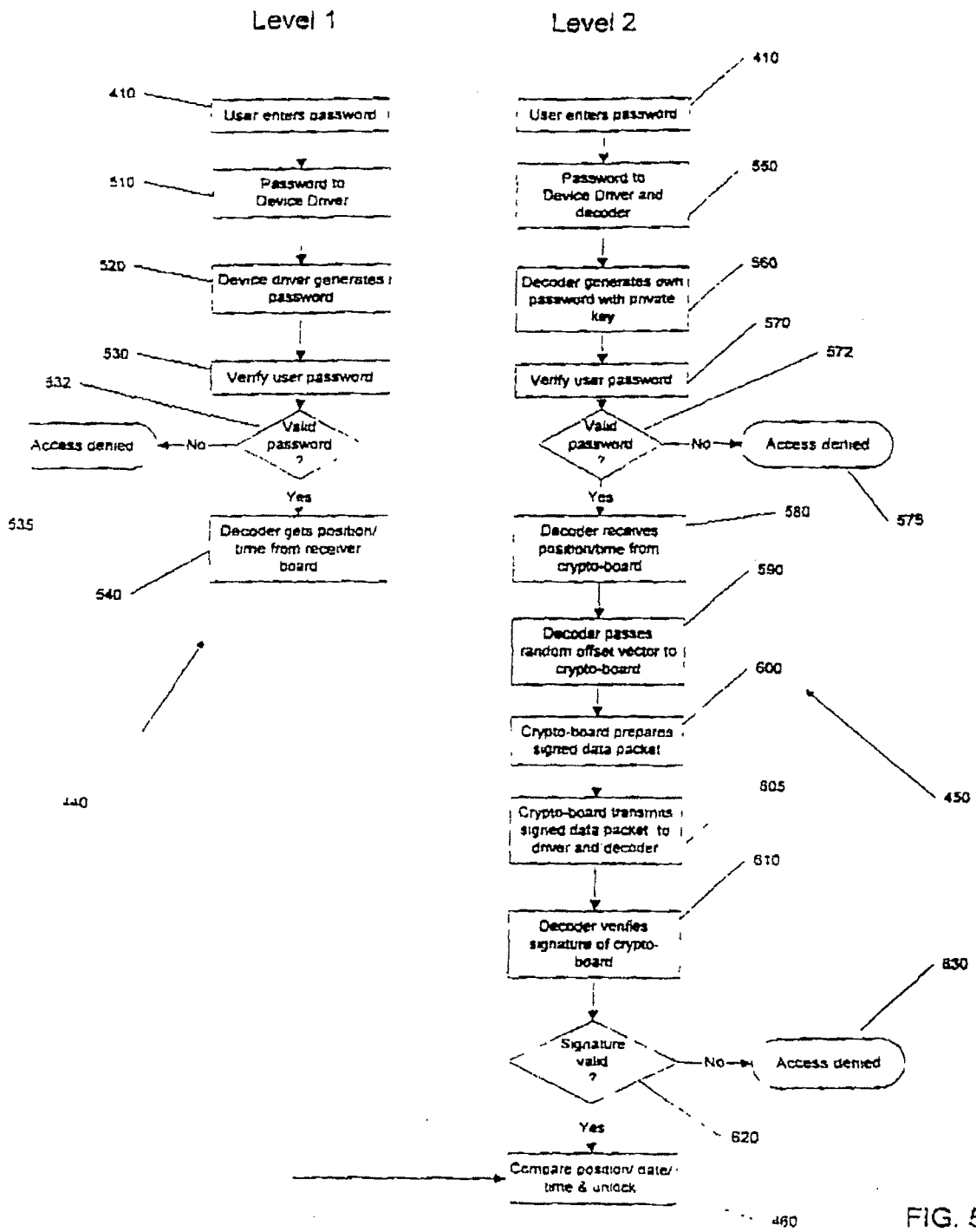


FIG. 5

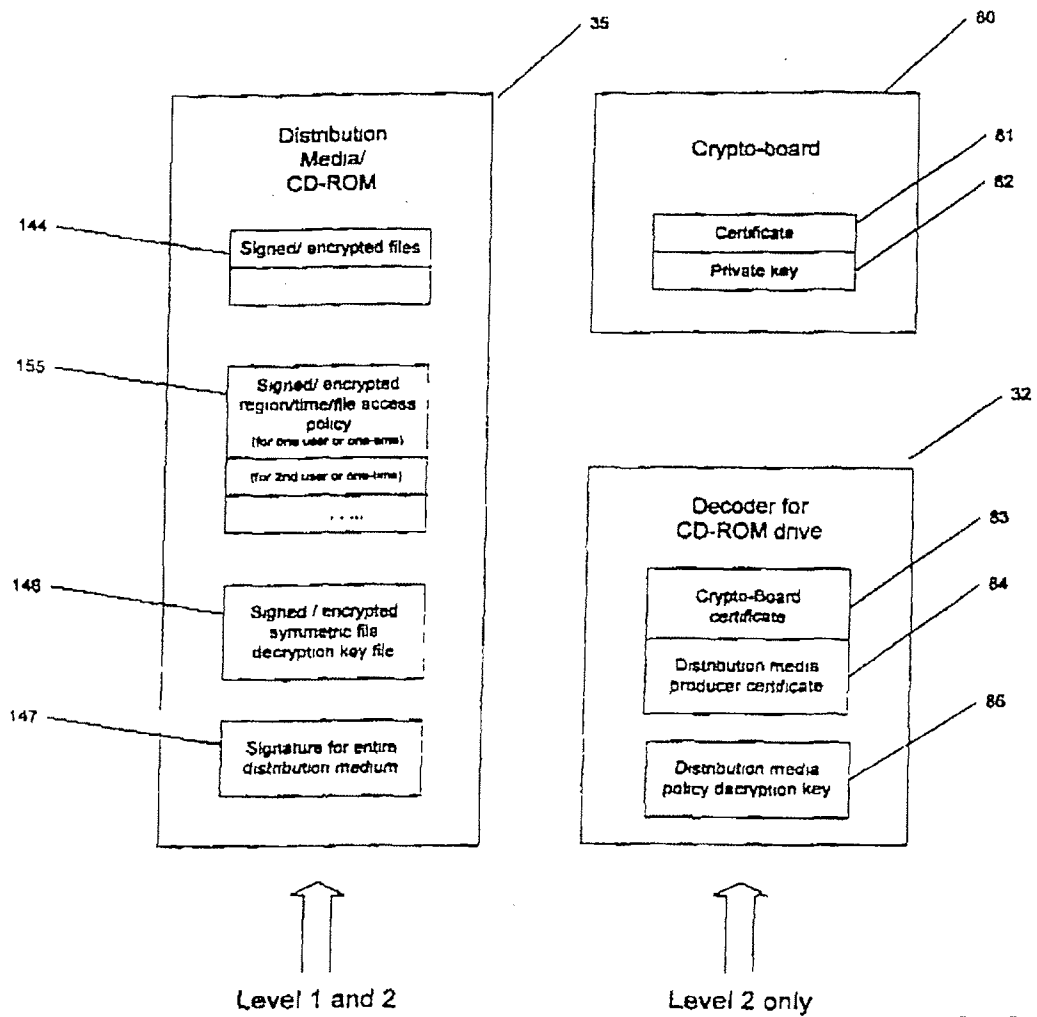


FIG. 6

RESUMO

Patente de Invenção **"CONTROLE DE ACESSO A UMA INFORMAÇÃO ARMAZENADA"**.

O acesso a uma informação armazenada por um usuário é controlado comparando-se uma posição geográfica real e/ou uma data / um tempo real com uma região geográfica e/ou um intervalo de data / tempo no qual o acesso à informação armazenada está autorizado. A posição geográfica real onde a informação armazenada está localizada e a data / o tempo real podem ser determinados, por exemplo, baseado em sinais recebidos em um receptor que supre informação de posição e de tempo confiável, tal como um receptor de GPS. O acesso à informação armazenada é autorizado se a posição geográfica real e/ou a data / o tempo caírem na região geográfica e/ou no intervalo de data / tempo autorizado. A informação de posição e de data / tempo suprida pelo receptor pode ser assinada de forma criptográfica e criptografada.



Canadian Intellectual
Property Office
An Agency of
Industry Canada

Office de la propriété
intellectuelle du Canada
Un organisme
d'Industrie Canada

Canada

[Home](#) > [CPD](#) > [Advanced Search](#) > [Search Results](#) > Patent Summary

Canadian Patents Database

[Link to this page](#)

Patent Summary

(12) Patent Application:	(11) CA 2287596
(54) English Title:	CONTROLLING ACCESS TO STORED INFORMATION
(54) French Title:	CONTROLE D'ACCES A DE L'INFORMATION STOCKEE

[Abstract](#)

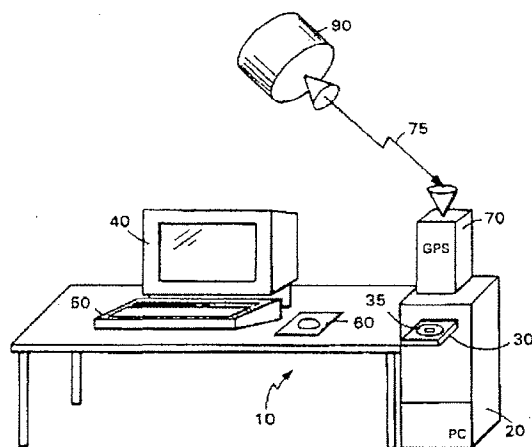
[Patent Details](#)

[View or Download Images](#)

[View Administrative Status](#)

[Show all claims](#)

Representative Drawing



Abstracts

[Third-party disclaimer](#)

English 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.

French Abstract

Patent Details

(51) International Patent Classification (IPC):

G06F 12/14 (2006.01)
G06F 1/00 (2006.01)
G06F 21/00 (2006.01)
H04L 9/32 (2006.01)

(72) Inventors (Country):

HASTINGS, THOMAS MARK (United States of America)
GLASSEY, TODD S. (United States of America)
MCNEIL, MICHAEL E. (United States of America)
WILLETT, GERALD L. (United States of America)

(73) Owners (Country):

SYMMETRICOM, INC. (United States of America)

(71) Applicants (Country):

DATUM, INC. (United States of America)

(74) Agent:

SMART & BIGGAR

(45) Issued:**(22) Filed Date:** 1999-10-26**(41) Open to Public Inspection:** 2000-04-29**Examination requested:** 2003-05-16**(30) Availability of licence:** N/A**(30) Language of filing:** English**Patent Cooperation Treaty (PCT):** No**(30) Application Priority Data:**

Application No.	Country	Date
09/182,342	United States of America	1998-10-29

View or Download Images

Click on a link under View Patent Image to view a section of the image or click on a link under Download Patent Image in PDF format to download a section of the image in PDF format.

If you have any difficulty accessing content, you can call the Client Service Centre at 1-866-997-1936 or send them an e-mail at [CIPO Client Service Centre](#).

Third-party disclaimer

<u>View Patent Image</u>	<u>Download Patent Image in PDF Format</u>	<u>Size of Image (KB)</u>	<u>Number of Pages</u>
Cover Page	Cover Page	35	1
Abstract	Abstract	25	1
Claims	Claims	234	6
Description	Description	573	13
Drawings	Drawings	130	6
Representative Drawing	Representative Drawing	6	1

PDF Readers.

Last Updated: 2012-12-27



Canadian Intellectual
Property Office
An Agency of
Industry Canada

Office de la propriété
intellectuelle du Canada
Un organisme
d'Industrie Canada

Canada

[Home](#) > [CPD](#) > Patent Summary

Canadian Patents Database

Patent Summary

(12) Patent Application: (11) CA 2398415

(54) English Title:

SYSTEM AND METHODS FOR GENERATING TRUSTED
AND AUTHENTICATABLE TIME STAMPS FOR
ELECTRONIC DOCUMENTS

(54) French Title:

SYSTEME ET METHODES DE GENERATION DE
MARQUES D'HORODATAGE FIABLES ET
AUTHENTIFIABLES POUR DOCUMENTS ELECTRONIQUES

[Abstract](#)

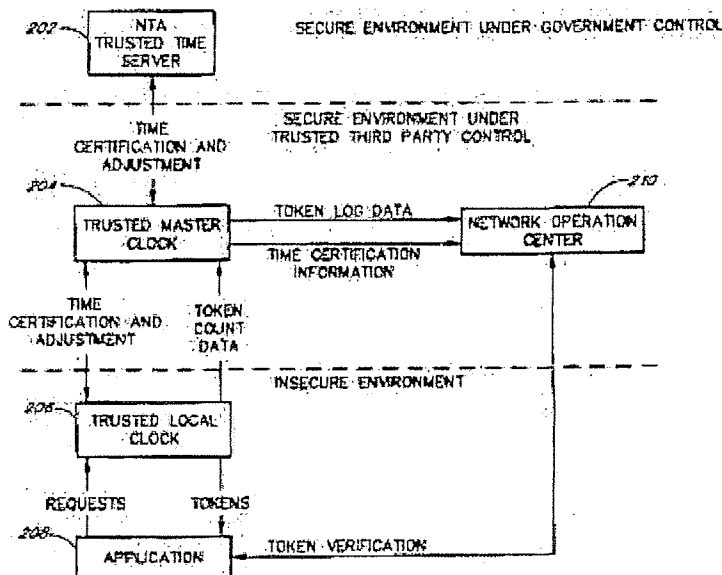
[Patent Details](#)

[View or Download Images](#)

[View Administrative Status](#)

[Show all claims](#)

Representative Drawing



Abstracts

Third-party disclaimer

English Abstract

A trusted time infrastructure system provides time stamps for electronic documents from a local source. The system comprises a trusted master clock (204), a trusted local clock (206), and a network operations center (210). The trusted master clock and network operations center are located within secure environments controlled by a trusted third party. The trusted local clock may be located in an insecure environment. The trusted master clock is certified to be synchronized with an accepted time standard, such as a national time server (202). The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. Time stamps and certifications are signed by the issuing device using public key cryptography to enable subsequent authentication. The network operations center logs clock certifications and responds to requests for authentication of time stamps.

Patent Details

(51) International Patent Classification (IPC):

H04L 7/00 (2006.01)
G04C 11/00 (2006.01)
G06F 1/04 (2006.01)
G06F 21/00 (2006.01)
H04L 9/30 (2006.01)
H04L 29/06 (2006.01)

(72) Inventors (Country):

ROBINSON, DAVID (United States of America)
DOWD, GREGORY L. (United States of America)
TYO, DAVID (United States of America)
VAN DER KAAY, ERIK H. (United States of America)

(73) Owners (Country):

ROBINSON, DAVID (Not Available)
DOWD, GREGORY L. (Not Available)
TYO, DAVID (Not Available)
VAN DER KAAY, ERIK H. (Not Available)

**(71) Applicants
(Country):**

DATUM, INC. (United States of America)

(74) Agent:

FETHERSTONHAUGH & CO.

(45) Issued:

(22) Filed Date:

2002-08-20

**(41) Open to Public
Inspection:**

2004-02-20

**(30) Availability of
licence:**

N/A

(30) Language of filing:

English

**Patent Cooperation Treaty
(PCT):**

No

**(30) Application Priority
Data:**

None

View or Download Images

Click on a link under View Patent Image to view a section of the image or click on a link under Download Patent Image in PDF format to download a section of the image in PDF format.

If you have any difficulty accessing content, you can call the Client Service Centre at 1-866-997-1936 or send them an e-mail at [CIPO Client Service Centre](#).

Third-party disclaimer

<u>View Patent Image</u>	<u>Download Patent Image in PDF Format</u>	<u>Size of Image (KB)</u>	<u>Number of Pages</u>
Cover Page	Cover Page	49	2
Abstract	Abstract	25	1

<u>View Patent Image</u>	<u>Download Patent Image in PDF Format</u>	Size of Image (KB)	Number of Pages
Claims	Claims	158	5
Description	Description	1,065	15
Drawings	Drawings	176	8
Representative Drawing	Representative Drawing	11	1

[PDF Readers.](#)

Last Updated: 2012-06-18

Declaration pertaining to Modification of the Patent
(AKA the 2001 patent rewrite)

I, Todd S Glassey, declare the following under the US Perjury Statue and swear that this information is true and correct and to those things I rely on information and belief, they also are true and correct.

1. The 2001 Patent Application Rewrite modified Claim 1 to insert Phase II Technology as indicated below in bold and italics:

A method for controlling access to stored information comprising:

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

Cryptographically signing said actual geographic position with a receiver encryption key;

Verifying the signature of said actual geographic position;

Determining that said actual geographic position is within a geographic region within which access to said stored information is authorized; and

Permitting access to said stored information.

2. The 2001 Patent Application Rewrite modified Claim 12 to insert Phase II Technology as indicated below in bold and italics:

Apparatus for controlling access to stored information comprising:

A receiver supplying reliable position information for determining an actual geographic position where said stored information is located, ***wherein the receiver comprises a receiver encryption mechanism providing a receiver encryption key for cryptographically***

signing data comprising the actual geographic position; and

A computer for comparing said actual geographic position with a geographic region within which access to said stored information is authorized,

Wherein said computer permits access to said stored information if said actual geographic position is located within said authorized geographic region.

3. The 2001 Patent Application Rewrite modified Claim 18 to insert

Phase II Technology as indicated below in bold and italics:

A method for controlling access to a subset of files belonging to a larger set of files of stored information comprising:

Associating a unique file encryption key with each file from the larger set of files and encrypting the files using the associated encryption keys;

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

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

Cryptographically signing at least the actual geographic position at the receiver;

Verifying the signature of the actual geographic position;

Comparing said actual geographic position with said authorized geographic region; and

Providing a file decryption key which authorizes access to said subset of files, provided that the actual geographic position is located within the authorized geographic region for the files belonging to said subset of files.

4. The 2001 Patent Application Rewrite modified Claim 21 to insert Phase II Technology as indicated below in bold and italics:

A method for controlling access to stored information comprising:

Determining an actual date or time at the location of said stored information based on signals received at a receiver supplying reliable time information;

Cryptographically signing at least the actual date or time at the receiver;

Verifying the signature of the actual date or time;

Comparing said actual date or time with a predetermined date or time interval at which access to said stored information is authorized; and

Permitting access to said stored information if said actual date or time occurs within said authorized date or time interval.

5. The 2001 Patent Application Rewrite modified Claim 25 to insert Phase II Technology as indicated below in bold and italics:

A method for controlling access to stored information comprising:

Forming a policy associating said information with authorized geographic regions and authorized time intervals;

Cryptographically signing said policy and said information;

Storing said signed policy together with said signed information;

Providing a password for unlocking said policy;

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

Determining an actual time;

Cryptographically signing at least the actual geographic position and the actual time at the receiver;

Verifying the signature of the actual geographic position and the actual time;

Comparing said actual geographic position and said actual time with said authorized geographic regions and authorized time interval of said policy; and

Permitting access to said stored information if said actual geographic position and actual time falls within said authorized geographic regions and authorized time interval of said policy.

6. The 2001 Patent Application Rewrite included a new independent Claim 29 which was entirely comprised of Phase II Technology:

A method for controlling access to stored information, the method comprising:

- (a) Determining a position;
- (b) Cryptographically signing data comprising at least a representation of the position;
- (c) Verifying the signature of the data comprising at least a representation of the position;
- (d) Determining that access to the stored information is authorized at the position;
- (e) Permitting access to the information based at least upon (c) and (d).

None of the OFFICE ACTIONS were disclosed to GLASSEY or MCNEIL as required under Section 8.7 of the Settlement Agreement nor was any license to re-write any of the claims or the addition of the final claim Authorized in any

form by Glassey or McNeil under any aspect of the original or settlement agreements;

This declaration is made under the US Perjury Statute as described in the opening preamble.

// Todd S. Glassey - 8/20/2014

CONTROL OVER ACCESS TO STORED INFORMATION

Patent number: JP2000163379
Publication date: 2000-06-16
Inventor: HASTINGS THOMAS MARK; MCNEIL MICHAEL E;
 GLASSEY TODD S; WILLETT GERALD L
Applicant: DATUM INC
Classification:
 - international: G06F15/00; G01S5/14; G06F12/00; G06F12/14;
 G09C1/00; H04L9/14
 - european: G06F1/00N7R2; G06F21/00N9A2
Application number: JP19990308358 19991029
Priority number(s): US19980182342 19981029

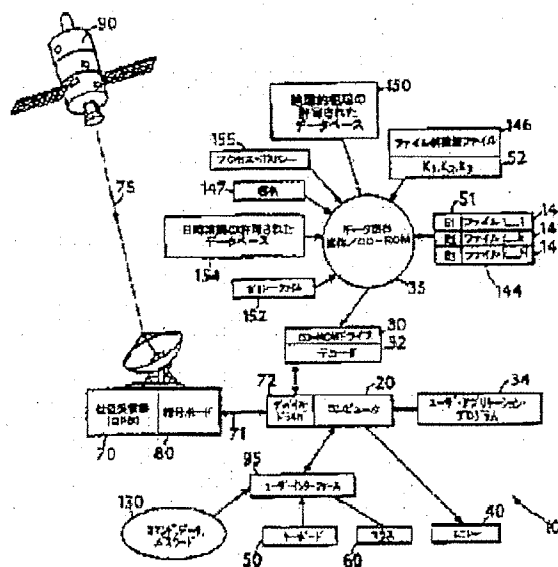
Also published as:

EP0997808 (A2)
 US6370629 (B1)
 EP0997808 (A3)
 CA2287596 (A1)
 BR9904979 (A)

Report a data error here

Abstract of JP2000163379

PROBLEM TO BE SOLVED: To limit the use of information to a specified geographic area by determining the geographic position of stored information to be arranged according to a signal received by a receiver supplying position information and controlling access to the stored information. **SOLUTION:** A GPS receiver 70 is arranged at the actual geographic position of a computer system 10 and receives a signal 75 from a circulating GPS satellite 90. According to the received data, the actual geometric position of information stored in a portable computer-readable CD-ROM used as a data distribution medium 35 is determined and the receiver 70 converts the received signal 75 geometric position data of precision of several meters as to the latitude and altitude and day/hour data 71 of precision of microseconds. Then the data 71 are passed through a device driver 72 to control access to stored information on the data distribution medium 35 through a CD-ROM drive 30.



Data supplied from the esp@cenet database - Worldwide

MENU **SEARCH** **INDEX** **DETAIL** **JAPANESE** **LEGAL STATUS**

Please click here for details of Stored Data Information of [DETAIL], [JAPANESE], and [LEGAL STATUS].

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-163379

(43)Date of publication of application : 16.06.2000

(51)Int.Cl. G06F 15/00
G01S 5/14
G06F 12/00
G06F 12/14
G09C 1/00
H04L 9/14

(21)Application number : 11-308358

(71)Applicant : DATUM INC

(22)Date of filing : 29.10.1999

(72)Inventor : HASTINGS THOMAS MARK
MCNEIL MICHAEL E
GLASSEY TODD S
WILLETT GERALD L

(30)Priority

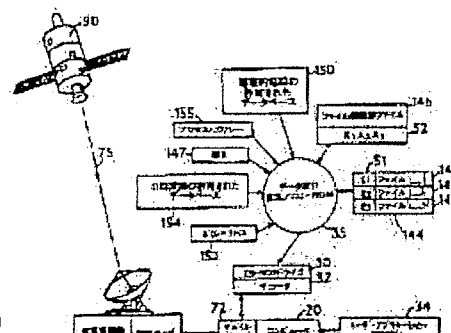
Priority number : 98 182342 Priority date : 29.10.1998 Priority country : US

(54) CONTROL OVER ACCESS TO STORED INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To limit the use of information to a specified geographic area by determining the geographic position of stored information to be arranged according to a signal received by a receiver supplying position information and controlling access to the stored information.

SOLUTION: A GPS receiver 70 is arranged at the actual geographic position of a computer system 10 and receives a signal 75 from a circulating GPS satellite 90. According to the received data, the actual geometric position of information stored in a portable computer-readable CD-ROM used as a data distribution medium 35 is determined and the receiver 70



Filing info	Patent H11-308358 (29.10.1999)
Publication info	2000-163379 (16.6.2000)
Detailed info of application	Kind of final decision(Deemed to be withdrawn) Date of final decision in examination stage(23.1.2007)
Renewal date of legal status	(22.6.2007)

Legal status information includes 8 items below. If any one of them has any data, a number or a date would be indicated at the relevant part.

1. Filing info(Application number, Filing date)
2. Publication info(Publication number, Publication date)
3. Detailed info of application
 - * Kind of examiner's decision
 - * Kind of final decision
 - * Date of final decision in examination stage
4. Date of request for examination
5. Date of sending the examiner's decision of rejection(Date of sending the examiner's
6. Appeal/trial info
 - * Appeal/trial number, Date of demand for appeal/trial
 - * Result of final decision in appeal/trial stage, Date of final decision in appeal/tri
7. Registration info
 - * Patent number, Registration Date
 - * Date of extinction of right
8. Renewal date of legal status

For further details on Legal-Status, visit the following link. [PAJ help\(1-5\)](#)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-163379

(P2000-163379A)

(43) 公開日 平成12年6月16日 (2000.6.16)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D
G 0 1 S 5/14		G 0 1 S 5/14	
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 A
12/14	3 1 0	12/14	3 1 0 K
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D

審査請求 未請求 請求項の数28 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願平11-308358

(22) 出願日 平成11年10月29日 (1999. 10. 29)

(31) 優先権主張番号 0 9 / 1 8 2 3 4 2

(32) 優先日 平成10年10月29日 (1998. 10. 29)

(33) 優先権主張国 米国 (U S)

(71) 出願人 599153541

デイトム インコーポレイテッド
アメリカ合衆国 マサチューセッツ州 ベ
ッドフォード ミドルセックスターンパイ
ク 54

(72) 発明者 トーマス マーク ヘイスティングス
アメリカ合衆国 マサチューセッツ州
02420 レキシントン メリアムストリー
ト 38

(74) 代理人 100079119

弁理士 藤村 元彦 (外1名)

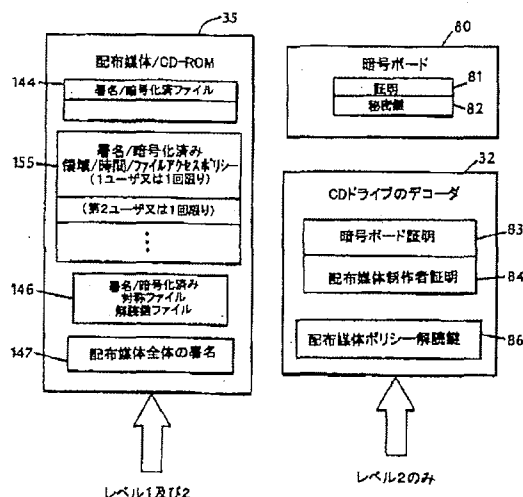
最終頁に続く

(54) 【発明の名称】 格納情報へのアクセス制御

(57) 【要約】 (修正有)

【課題】 情報の使用を指定された地理的領域に制限で
きる格納された情報へのアクセス制御方法。

【解決手段】 ユーザによる格納情報へのアクセスは、
実際の地理的位置又は実際の日/時を格納情報へのアク
セスが許可された地理的領域又は期間と比較することに
よって制御される。格納情報が位置する実際の地理的位
置及び実際の日/時は、例えば、GPS受信機などの信
頼できる位置及び時間情報を供給する受信機で受信され
た信号に基づいて確定される。実際の地理的位置又は日
/時が許可された地理的領域又は期間内である場合に格
納情報へのアクセスが許可される。受信機から供給され
る位置及び日/時の情報は、暗号法により署名及び暗号
化されてもよい。



【特許請求の範囲】

【請求項1】 格納情報へのアクセスを制御する方法であって、
信頼できる位置情報を供給する受信機で受信した信号に基づいて前記格納情報が位置する実際の地理的位置を確定するステップと、
前記実際の地理的位置を前記格納情報へのアクセスが許可された地理的領域と比較するステップと、
前記実際の地理的位置が前記許可された地理的領域内に位置する場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。

【請求項2】 請求項1に記載の方法であって、前記受信機はGPS受信機からなることを特徴とする方法。

【請求項3】 請求項1に記載の方法であって、前記格納情報はコンピュータ可読の媒体に格納されることを特徴とする方法。

【請求項4】 請求項3に記載の方法であって、前記コンピュータ可読の媒体は可搬型であることを特徴とする方法。

【請求項5】 請求項3に記載の方法であって、前記コンピュータ可読の媒体は大容量ディスクからなることを特徴とする方法。

【請求項6】 請求項1に記載の方法であって、前記格納情報は、各々がアクセスが許可される関連した地理的領域を含むファイルからなり、前記実際の地理的位置が前記ファイルの該許可された地理的領域内に位置する場合に前記ファイルへのアクセスを許すステップを更に有することを特徴とする方法。

【請求項7】 請求項6に記載の方法であって、前記実際の地理的位置が前記許可された地理的領域に一致しない場合に、前記格納情報へのアクセスを拒否するステップを更に有することを特徴とする方法。

【請求項8】 請求項1に記載の方法であって、暗号鍵を用いて前記格納情報を暗号化するステップと、前記実際の地理的位置が前記許可された地理的領域内に位置する場合に、前記格納情報の解読を許す解読キーを提供するステップと、を更に有することを特徴とする方法。

【請求項9】 請求項1に記載の方法であって、暗号法により前記実際の地理的位置に受信機の暗号鍵で署名するステップと、
実際の地理的位置が前記許可された地理的領域と比較される前に受信機の解読キーで前記受信機の署名を検証するステップと、を更に有することを特徴とする方法。

【請求項10】 請求項1に記載の方法であって、前記格納情報は情報のサブセットに分割され、前記サブセットの少なくとも1つは他のサブセットと異なる許可された地理的領域を有し、該許可された地理的領域が実際の地理的位置内に位置するサブセットへのアクセスは許可され、前記許可された地理的領域が実際の地理的位置内

に位置しないサブセットへのアクセスは許可されないことを特徴とする方法。

【請求項11】 請求項6に記載の方法であって、前記許可された地理的領域との該関連はポリシーファイルとして前記格納情報と共に格納されることを特徴とする方法。

【請求項12】 格納情報へのアクセスを制御するための装置であって、

信頼できる位置情報を供給して前記格納情報が位置する実際の地理的位置を確定する受信機と、

前記実際の地理的位置を前記格納情報へのアクセスが許可される地理的領域と比較するコンピュータと、を有し、

前記コンピュータは、前記実際の地理的位置が前記許可された地理的領域内に位置する場合に前記格納情報へのアクセスを許すことを特徴とする装置。

【請求項13】 請求項12に記載の装置であって、前記受信機はGPS受信機であることを特徴とする装置。

【請求項14】 請求項12に記載の装置であって、前記受信機は、前記実際の地理的位置に暗号法により署名するための受信機暗号鍵を提供する受信機暗号メカニズムを更に有することを特徴とする装置。

【請求項15】 請求項14に記載の装置であって、前記格納情報を読み取る読取装置を更に有し、前記読取装置は、該暗号法により署名された実際の位置を検証する受信機解読キーを含むことを特徴とする装置。

【請求項16】 請求項15に記載の装置であって、前記読取装置は、前記受信機に送信されて前記実際の地理的位置に加えられる位置オフセットを提供する初期化ベクトルを生成することを特徴とする装置。

【請求項17】 請求項16に記載の装置であって、前記位置オフセットに暗号法により署名するための読取装置暗号鍵を提供する読取装置暗号メカニズムを更に有し、前記位置オフセットが前記実際の地理的位置に加えられる前に、該位置オフセット署名は前記受信機によって対応する読取装置解読キーにより検証されることを特徴とする装置。

【請求項18】 格納情報のより大規模なファイルセットに属するファイルサブセットへのアクセスを制御する方法であって、

該大規模ファイルセットのファイルの各々に一意のファイル暗号鍵を関連付けて、該関連暗号鍵を用いて前記ファイルを暗号化するステップと、

前記格納情報へのアクセスが許可される少なくとも1つの許可された地理的領域を前記大規模ファイルセットのファイルの各々に関連付けるステップと、

信頼できる位置情報を供給する受信機で受信された信号に基づいて、前記格納情報が位置する実際の地理的位置を確定するステップと、

前記実際の地理的位置を前記許可された地理的領域と比

較するステップと、
実際の地理的位置が前記ファイルサブセットに属するファイルの前記許可された地理的領域内に位置する場合には、前記ファイルサブセットに属する前記ファイルへのアクセスを許可し解読を許すファイル解読キーを供給するステップと、を有することを特徴とする方法。

【請求項19】 請求項18に記載の方法であって、前記ファイルと前記許可された地理的領域との前記関連はポリシーファイルを含むポリシーとして格納され、前記ポリシーファイルの各々は、ユーザ・パスワードにより10 アクセスでき、実際の地理的位置が前記ファイルに関連した前記許可された地理的領域内に位置しユーザ・パスワードが有効な場合に前記ポリシーファイルにリストされたファイルへのアクセスを許可することを特徴とする方法。

【請求項20】 請求項19に記載の方法であって、前記ポリシーは前記格納情報と共に格納されることを特徴とする方法。

【請求項21】 格納情報へのアクセスを制御する方法であって、

信頼できる時間情報を供給する受信機で受信された信号に基づいて前記格納情報の位置における実際の日付又は時間を確定するステップと、
前記実際の日付又は時間を前記格納情報へのアクセスが許可される所定の日付又は時間の期間と比較するステップと、
前記実際の日付又は時間が該許可された日付又は時間の期間内に発生した場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。

【請求項22】 請求項21に記載の方法であって、前記実際の日付又は時間が前記許可された日付又は時間の期間内に発生しなかった場合に前記格納情報へのアクセスを拒否するステップ、を更に有することを特徴とする方法。

【請求項23】 請求項21に記載の方法であって、前記情報は、各々がアクセスが許される関連した許可された日付又は時間の期間を有するファイルを有し、前記実際の日付又は時間が該関連した許可された日付又は時間の期間内に発生した場合に前記ファイルへのアクセスを許すステップを更に有することを特徴とする方法。

【請求項24】 請求項21に記載の方法であって、前記格納情報は情報のサブセットに分割され、前記サブセットの少なくとも1つは他のサブセットと異なる許可された日付又は時間の期間を有し、前記実際の日付又は時間に一致する許可された日付又は時間の期間を有するサブセットへのアクセスは許可され、前記実際の日付又は時間に一致しないサブセットへのアクセスは許可されないことを特徴とする方法。

【請求項25】 格納された情報へのアクセスを制御する方法であって、

前記情報を許可された地理的領域及び許可された期間と関連付けたポリシーを形成するステップと、

暗号法により前記ポリシー及び前記情報に署名を行うステップと、

該署名されたポリシーを該署名された情報と共に格納するステップと、

前記ポリシーのロックを解除するパスワードを供給するステップと、

信頼できる位置情報を供給する受信機で受信された信号に基づいて、該格納された情報が位置する実際の地理的位置を確定するステップと、

実際の時間を確定するステップと、

前記実際の地理的位置及び前記実際の時間を前記ポリシーの前記許可された地理的領域及び前記許可された期間と比較するステップと、

前記実際の地理的位置及び前記実際の時間が前記ポリシーの前記許可された地理的領域及び前記許可された期間内である場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。

20 【請求項26】 請求項1に記載の方法であって、前記信頼できる位置及び時間の供給源は全地球周回ナビゲーション衛星システムであることを特徴とする方法。

【請求項27】 請求項1に記載の方法であって、前記信頼できる位置及び時間の供給源は慣性航法システムであることを特徴とする方法。

【請求項28】 請求項1に記載の方法であって、前記信頼できる位置及び時間の供給源は衛星ベースの位置確定システムであることを特徴とする方法。

【発明の詳細な説明】

30 【0001】

【発明の属する技術分野】本発明は、格納された情報へのアクセス制御に関する。

【0002】

【従来の技術】例えばCD-ROM等のデータ配布媒体には多数のファイルを格納することができる。CD-ROMの製作者は、秘密扱いである、又はユーザによる支払いを要するという理由から特定のファイルへのユーザのアクセスを制御することを望む場合がある。

40 【0003】ユーザに対しCD-ROM製作者から得られるパスワードの入力を要求することによってアクセスを制御してもよい。異なるパスワードによって、異なるファイル又は異なるファイルのサブセットのロックが解除（アンロック）されてもよい。ファイルは、暗号によって署名され、更に保護のために暗号化されてもよい。製作者がその製作者だけが知っている一意の鍵（キー）によって各ファイルを暗号化する方法について記載された米国特許第5,646,992号を参考文献としてここに挙げる。ユーザが暗号化されたアイテムを受け取り、製作者がそのユーザのアクセス要求を処理した後、ユーザは暗号化された各ファイルの解読に用いられる解読鍵（すな

わち、パスワード)を受け取る。パスワードは、アクセスが要求されたファイルのみロックを解除する。

【0004】

【発明の概要】本発明は、信頼できる位置情報を供給する受信機により受信した信号に基づいて配置される格納情報の実際の地理的位置を確定することによって格納情報へのアクセスを制御することを一つの特徴としている。次に、実際の地理的位置は、格納情報に対するアクセスが許可される地理的な領域と比較される。実際の地理的位置が許可された地理的領域内に位置する場合、ユーザは格納情報へのアクセスを許される。

【0005】本発明の実施例は、以下の特徴を含んでいる。位置情報を供給する受信機は、衛星ベースの位置確定システム又は慣性航法装置から位置情報を受信することができる。その情報は、コンピュータ可読の媒体(例えば、大容量ディスク)に格納される。格納情報はファイルを含み、これらのファイルの各々はアクセスが許可される関連した地理的領域を含む。実際の地理的位置がファイルに許可された地理的領域内に位置する場合、ユーザはその特定のファイルにアクセスできる。格納情報は暗号化することができ、実際の地理的位置が許可された地理的領域内に位置する場合だけ、ユーザは解読鍵にアクセスできる。また、格納情報は情報のサブセットに分割することができ、少なくとも1つのサブセットは他のサブセットとは異なる許可領域を有する。許可された地理的領域とファイルとの対応は、ポリシーファイル(policy file)として格納情報と共に格納される。

【0006】本発明は他の特徴として、信頼できる時間情報を供給する受信機により受信された信号に基づいて格納情報の位置における実際の日付又は時間を確定する。実際の日付又は時間は、格納情報に対するアクセスが許可された所定の日付又は時間の期間と比較される。実際の日付又は時間が許可された期間内にある場合、ユーザは格納情報にアクセスすることができる。

【0007】本発明は他の特徴として、格納情報が位置する実際の地理的位置を確定するために信頼できる位置情報を供給する受信機を含む。コンピュータは、格納情報へのアクセスが許可される地理的領域と位置情報を受信し、実際の地理的位置が許可された地理的領域内に位置する場合にアクセスを許可する。本発明の実施例は以下の特徴を有している。受信機は、暗号法により実際の地理的位置に受信機暗号鍵で署名して、実際の地理的位置が許可された地理的領域と比較される前に、その受信機署名を受信機解読鍵で検証する受信機暗号メカニズムを含む。

【0008】更に他の特徴として、本発明は、暗号によって署名された実際の位置を検証するための対応する受信機解読鍵を有する読取装置を含む。本発明の実施例は、以下の特徴を含む。読取装置は、受信機に送信されて実際の地理的位置に加えられる位置オフセットを提供

する初期化ベクトルを生成する。読取装置は、読取装置暗号鍵によって位置オフセットに暗号署名する。受信機は、位置オフセットが実際の地理的位置に加えられる前に、対応する読取装置解読鍵により位置オフセットの署名を検証する。

【0009】本発明の他の特徴として、情報と許可された地理的領域及び許可された期間とを関連させるポリシーを形成し、暗号によってその情報及びポリシーに署名する。署名されたポリシーは、署名された情報と共に格納される。ユーザは、実際の地理的位置及び実際の時間がそれぞれ許可された地理的領域及び許可された期間内にある場合に、製作者からポリシーのロックを解くためのパスワードを得て、格納情報にアクセスすることができる。

【0010】本発明の利点について以下に述べる。格納情報の製作者は、その情報の使用を指定された地理的領域に制限するか、又は使用が許されない指定領域を除外することができる。例えば、CD-ROMに格納される自動車のサービス・マニュアルは、対応する特定の国及び/又は領域に適用できる異なるセクションの情報を含んでいてもよい。ユーザは、現在の地理的位置に適用できる一部の情報のみを見ることが許されてもよい。同様に、機密に関わる会社のレポートへのアクセスは、特定の施設位置に限られていてもよい。時間に敏感な情報に対するアクセスは、一定の日の前又は後に拒否されるか、又は許された期間に限られてもよい。許可された地理的領域及び期間についての情報を、CD-ROMに格納されユーザ・パスワードによってアクセスされるポリシー・ファイルと関連させることによって、CD-ROMの製作者は、ユーザが特定のポリシー・ファイルの一式、従って、対応する領域及び日/時間で許可された情報にアクセスすることを許可する新たなパスワードを発行することができる。

【0011】本発明の他の利点及び特徴は、下記の記載及び特許請求の範囲から明らかになる。

【0012】

【発明の実施の形態】図1ないし図3に示すように、データ配布媒体35として用いられる携帯用のコンピュータ可読のCD-ROMに格納された情報へのアクセスは、情報へのアクセスがなされるコンピュータ・システム10の実際の地理的位置及びアクセスされる時間に基づいて制御されてもよい。

【0013】コンピュータ・システム10において、コンピュータ20はキーボード50、マウス60、モニター40及びCD-ROMドライブ30に接続されている。GPS受信機70は、信頼できる位置情報及び時間情報の供給源として機能する。受信機70は、コンピュータ・システム10の実際の地理的位置に位置し、周囲するGPS衛星90(1つのみを示す)から信号75を受信する。受信機70は、受信信号75を経度、緯度及

び高度について数メートルの精度の地理的位置データ71、及びマイクロ秒の精度の日/時データ71に変換する。データ71は、デバイス・ドライバ72を経てコンピュータ20に送信される。

【0014】図6に示すように、受信機暗号ボード80は、製作者によって署名された公開鍵証明書81及び対応する秘密鍵82を含んでもよい。また、地理的位置及び日/時データ71は、データを認証するために秘密鍵82によって署名されてもよい。また、図6に示すように、CD-ROMドライブ30は、ハードウェア又はソフトウェアとして組み込まれた暗号及び署名機能(デコーダ32)を含んでもよい。デコーダ32は、証明書81と同一の暗号ボード公開鍵証明書83、製作者の身元確認のための製作者証明84、及びその製作者によって署名された配布媒体ポリシー解読鍵86を含む。暗号ボード証明83は、秘密鍵82によって署名された暗号ボード80の署名を検証する。ポリシー解読鍵86は、CD-ROM35に格納されたアクセス・ポリシー155を解読する。

【0015】下記の実施例に記載するように、コンピュータ・システム10は、レベル1及びレベル2等の数レベルのセキュリティを有することができる。レベル1のセキュリティを有するシステムにおいて、受信機70は従来のデバイス・ドライバ72を介してコンピュータ20と通信する。また、CD-ROMドライブ30は従来のCD-ROMである。受信機70及びCD-ROMドライブ30は、付属の暗号/解読機能を有していない。セキュリティを高めるため、レベル1のシステムのコンピュータ20は、データを認証及び/又は暗号化することができる「信頼できる」コンピュータである。さらに安全のため、レベル2のシステムにおいては、受信機70は暗号ボード80を含み、CD-ROMドライブ30はデコーダ32を含んでもよい。レベル2のシステムは、データ認証、及び受信機70とデコーダ32との間のデータ伝送の暗号化を行うように設計される。また、コンピュータ20は、データ認証及び暗号化を行わない市販のコンピュータであってもよい。

【0016】キーボード50及びマウス60からの入力データは、ユーザ・インタフェース95を介して入力された通常のコマンド及びデータ入力130(アプリケーション・プログラム34によって提供される)、及びユーザがデータ配布媒体35に格納された情報にアクセスするための一つ以上のパスワード130を含んでもよい。

【0017】CD-ROM35は、情報ファイル144、許可された地理的領域のリスト150、許可された日/時の期間のリスト154、一つ以上のファイル解読鍵ファイル146、一つ以上のポリシー・ファイル152及びCD-ROM35全体の署名147等の種々の情報を格納する。図3に示すように、ファイル144、1

46、150、152、154及び155は署名及び暗号化されてもよい。

【0018】ファイル144は、サブセット141、142及び143にグループ化されてもよい。また、ファイルは複数のサブセットに属していてもよい。(以下の説明において、ファイルの語は、ファイル及びファイル・サブセットの両者を意味する)。ファイル141、142及び143のそれぞれは、一意的なファイル暗号鍵51(E1、E2、E3)によって暗号化されてもよい。対応するファイル解読鍵52(K1、K2、K3)は、CD-ROM35のファイル解読鍵ファイル146に格納される。解読鍵及び解読鍵ファイルに関する更なる情報は、米国特許第5,646,992号に記載されている。

【0019】CD-ROM35上のファイル141、142及び143の各々は、許可された地理的領域のリスト150に格納された許可された地理的領域のうちゼロ又は1つ以上と関連付けられている。例えば、ニューヨーク市のエンパイアステートビルに対応する緯度及び経度、及び50ないし60メートルの高度で領域が区切られ、その領域に関連するファイルは、受信機70がエンパイアステートビルの一定のオフィス領域内に位置する場合にのみ開くことができる。

【0020】同様に、ファイル141、142及び143の各々は、許可された日/時の期間のリスト154に格納された許可された期間のうちゼロ又は1つ以上と関連付けらる。GPS衛星90のそれぞれは、極めて高精度のクロックを維持する。受信機70は信号75の一部としてGPSクロック信号を受信するか、又は、ローカルな原子時計が同様のクロック信号を提供する。情報へのアクセスが試みられているときに、クロック信号によって実際の時間に基づいた情報へのアクセスが制御可能になる。例えば、製作者は、(1)所定の日/時の前、(2)所定の日/時の後、又は、(3)所定の日/時の期間の間だけアクセスが許されるように指定することができる。

【0021】ユーザがキーボード50から入力するパスワード130によって、製作者はファイル141、142及び143とリスト150及び154の特定のアイテムとを関連付けることができる。パスワード130は、複数のアクセスに有効なユーザ・パスワード、又は1回限りのパスワードであってもよい。または、製作者は、ポリシー・ファイル152によってリスト150及び154の特定の地理的領域/日/時の情報とファイル141、142及び143とを関連付けることができる。有効なユーザ・パスワード130は、一つ以上のポリシー・ファイル152のロックを解除するものであってもよい。ユーザの実際の地理的位置及び現在の日付及び時間がユーザ・パスワード150に対応する許可された地理的領域及び許可された日/時内である場合、ユーザはユーザ・インタフェース95を介して選択したファイルに

アクセスすることができる。次に、選択された情報は出力装置40上に表示される。

【0022】表1は、1例として、CD-ROM35に格納され、対応する許可された地理的領域及び日/時と関連付けられた5つの暗号化済みファイルAないしFにどのようにアクセスすることができるかを示している。各ファイルは、4つの異なるファイル解読鍵K1ないしK4のうちの1つと関連付けられている。L1及びL2は2つの異なる許可された地理的領域であり、T1、T2及びT3は3つの異なる許可された日/時の期間である。ファイル解読鍵K1（例えば、パスワード）を所有するユーザは、時刻T1において地理的領域L1及びL*

*3内のマニュアルAを解読することができる。同じユーザは、また、領域L2及びL3内で同一の時刻T1においてマニュアルDを解読することができるが、領域L1内では解読できない。同様に、鍵K2を有するユーザは、領域L2内で画像B及び画像Eを解読できるが、同じ時刻では解読できない。図面Cは、時刻T3ではいかなる位置においても解読することができるが、業務報告書Fは鍵K4を必要とし、領域L1内であればいつでも解読することができる。

【0023】

【表1】

暗号化されたファイル	ファイル解読鍵	許可された地理的領域	許可された日/時の期間
マニュアルA	K1	L1, L3	T1
画像B	K2	L2	T1, T3
図面C	K3	--	T3
マニュアルD	K1	L2, L3	T1
画像E	K2	L2	T2
報告書F	K4	L1	--

図3に示すように、任意の暗号による暗号署名のために、製作者はCD-ROM35に書くべきソース・ファイル144'を選択し、許可された地理的領域150'のリスト及び許可された日時/期間154'のリストを指定する。製作者は、各ファイル又はファイル・サブセットをゼロ又は1つ以上の地理的領域150'、及びゼロ又は1つ以上の日時/期間154'と関連付けて（表1参照）、この関連付けをポリシーファイル152'に格納する。ファイル144'、150'、152'、154'の各々は、ステップ53、340、350及び360において対応する暗号鍵51、345、355及び365によって署名、暗号化される。対応する暗号化されたファイル150、152及び154は、署名、暗号化された領域/時間/ファイルアクセス・ポリシー155として格納される。上述した如く、署名/暗号化されたファイル144、署名/暗号化された対称ファイル解読キーファイル146、及び製作者がCD-ROM35全体に署名するために用いられる署名147もまたCD-ROM35に格納される。

【0024】図4及び図5に示すように、署名/暗号化ファイル144にアクセスするために、ユーザは製作者からパスワード130（図2）を得て（ステップ400）、キーボード50からパスワード130を入力する（ステップ410）。パスワード130は1回限りの（ワンタイム）パスワードであると仮定される。但し、複数のセッションに有効なユーザ・パスワードを用いる

こともできる。

【0025】図4に示すように、レベル1及びレベル2に関するプロセス・フローの初期の部分はほとんど同一である。ステップ420においてパスワード130をチェックし、システム構成に従い、ステップ440（レベル1の場合、追加のセキュリティなし）又はステップ450（レベル2の場合、受信機/CD-ROMドライブのセキュリティ有り）を実行する。図5に示されるステップ440及びステップ450の詳細について以下に説明する。

【0026】図5に示すように、プロセス440において、ユーザのパスワード130はデバイス・ドライバ72に送られる（ステップ510）。デバイス・ドライバ72は、ワンタイム・パスワード130に応答して、それ自身のワンタイム・パスワードをユーザ・パスワード130から生成し（ステップ520）、ユーザが実際に正しいワンタイム・パスワード130を入力したことを検証し（ステップ530）、ユーザにインタラクティブ・セッションを認証する（ステップ532）。さもないければ、アクセスは拒否される（ステップ535）。

【0027】一度、パスワード130によってユーザが認証されると、デバイス・ドライバ72は現在の位置及び日/時を受信機70に問い合わせる（ステップ540）。次に、デバイス・ドライバ72は、受信機70から戻された時間及び位置データと、ファイル144又はファイル・サブセット141、142及び143に適用

するポリシー155を比較する(ステップ460)。ユーザがファイル144へのアクセスを許可されると、次に、データは解読鍵52によってロックが解かれて(ステップ470、図3)解読され(ステップ480)、ユーザのアプリケーション・プログラム34に供給され表示される(ステップ490)。

【0028】レベル2のシステムにおいて、受信機70は、以下において「暗号ボード」と称される暗号の受信機ボード80を含む。前述のように、暗号ボード80はメッセージの署名及び暗号化/解読を行うことができる。CD-ROMドライブ30は、暗号ボード80により署名され暗号ボード80から受信される位置データを復号するためのデコーダ32を含む。

【0029】図5に示すように、プロセス450において、ユーザ・パスワード130は、パスワード130を受付けそれを変更せずにデコーダ32に渡すデバイス・ドライバ72に送られる(ステップ550)。次に、ドライバ32は、ユーザ・パスワードに対応するそれ自身のワンタイム・パスワードを秘密鍵86によって内部で生成し(ステップ560)、正しいパスワード130がデバイス・ドライバ72に送信されたことを検証し(ステップ570)、ユーザにインタラクティブ・セッションを認証する(ステップ572)。さもなければ、アクセスは拒否される(ステップ575)。

【0030】一度、暗号回路32がユーザを認証すると、ドライバ32はデバイス・ドライバ72を介して暗号ボード80に受信機70からの現在の時刻及び位置情報について問い合わせる(ステップ580)。デコーダ装置30は、暗号ボード80に「初期化ベクトル」、すなわち、デバイス・ドライバ72が時間及び位置についての要求とともに暗号ボード80に渡す位置オフセットを形成する(ステップ590)ための署名されたランダム又は他のビット・パターンを供給する(ステップ590)。

【0031】暗号ボード80は、現在の時刻及び緯度、経度、高度による実際の地理的位置を含む予め確立されたデータ・フォーマットに応じたパケットを準備することによって応答する(ステップ600)。また、計算に必要な他のデータと同様に位置データを送信する衛星の識別情報が含まれていてもよい。暗号ボード80は、また、供給された初期化ベクトルをパケット内に既知のオフセットで格納し、パケット内容に暗号署名を適用する。暗号の署名は、例えば、メッセージ・ダイジェスト/パケット・データの寄せ集め(ハッシュ)、さらにある所定鍵によるメッセージ・ダイジェストの暗号であってもよく、あるいは暗号ボード80に格納された証明又は鍵に応じて対称又は非対称であってもよい。

【0032】次に、暗号ボード80は、パケットをデコーダ32/CD-ROMドライブ30に中継するデバイス・ドライバ72に署名された時間/位置パケットを送

信する(ステップ605)。デコーダ32は、暗号ボード80から受信したパケットの署名をデコーダ32に格納された署名と比較する(ステップ610)。その署名が適切に検証されると(ステップ620)、パケット内の初期化ベクトルが調べられ、ステップ590においてデコーダ32が暗号ボード80に実際に供給した初期化ベクトルと同一の初期化ベクトルであるかを確定する。これが本当ならば、デコーダ32が受信したパケットは最近のもので真性なものであり、時間及び位置データは有効であるとして受け付けられる。

【0033】一度、暗号ボード80からのパケットが署名及び初期化ベクトルに基づいて許可されると、デコーダ32は、暗号ボード80から受信した時間及び位置データをファイル144又はファイル・サブセット144に適用されるポリシー155と比較する(ステップ460)。ユーザがファイル144へアクセスすることが許可されると、データのロックは解かれ(ステップ470)、解読鍵52により解読されて(ステップ480)、ユーザ・アプリケーション・プログラム34に供給され表示される(ステップ490)。

【0034】他の実施例は、特許請求の範囲内である。例えば、GPS受信機は正確にデータ配布媒体読取装置の位置に配置されている必要はなく、読取装置に対して既知の位置(例えば、建物のローカルエリア・ネットワークにコンピュータ・サービスを提供するコントロール・サーバを含む部屋など)に配置されていればよい。また、ポリシー・ファイル152'は、一定のファイル144に対するアクセスが拒否される地理的領域を指定してもよい。

【0035】ファイルに対するアクセスの制限は、製作者によりキーボードから入力されるパスワードに限定されない。例えば、顔の特徴、指紋及び/又は声紋などの一定の生物測定学的属性をパスワードに加えて、又はパスワードの代りに用いてもよい。

【図面の簡単な説明】

【図1】コンピュータ・システムの斜視図である。

【図2】格納情報へのアクセスを制御するコンピュータベースのシステムのブロック図である。

【図3】フローチャートである。

【図4】フローチャートである。

【図5】フローチャートである。

【図6】暗号の構成要素を示すブロック図である。

【主要部分の符号の説明】

10 コンピュータ・システム

20 コンピュータ

32 デコーダ

35 データ配布媒体

70 GPS受信機

80 暗号ボード

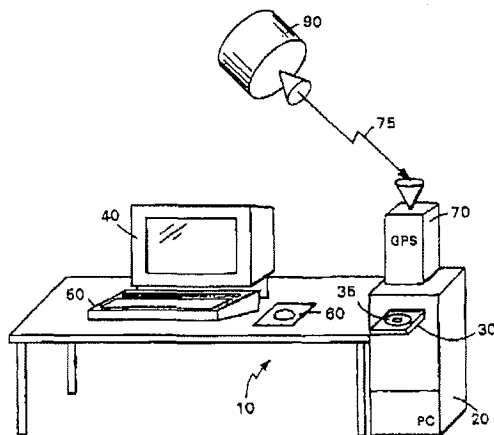
81 証明書

8 2 秘密鍵
8 3 暗号ボード公開鍵証明
8 4 製作者証明
8 6 配布媒体ポリシー解読鍵
9 0 GPS衛星

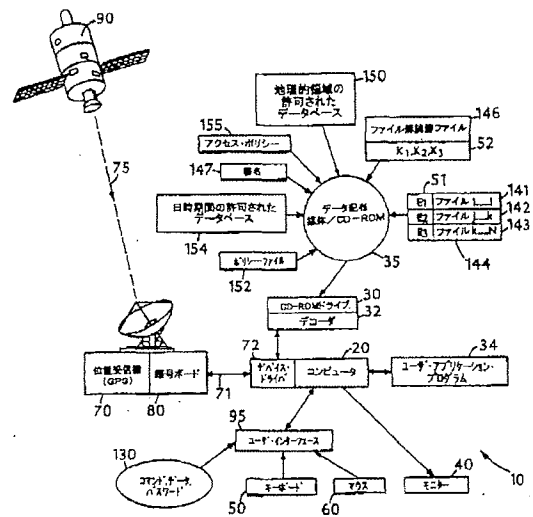
* 1 4 4 情報ファイル
1 4 6 ファイル解読鍵ファイル
1 4 7 配布媒体の署名
1 5 5 アクセス・ポリシー

*

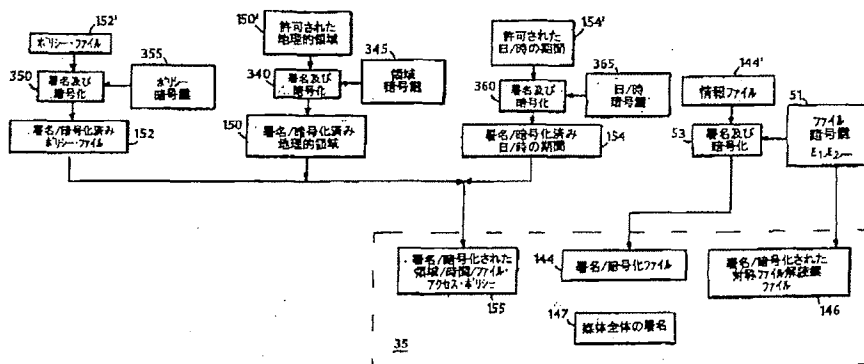
【図1】



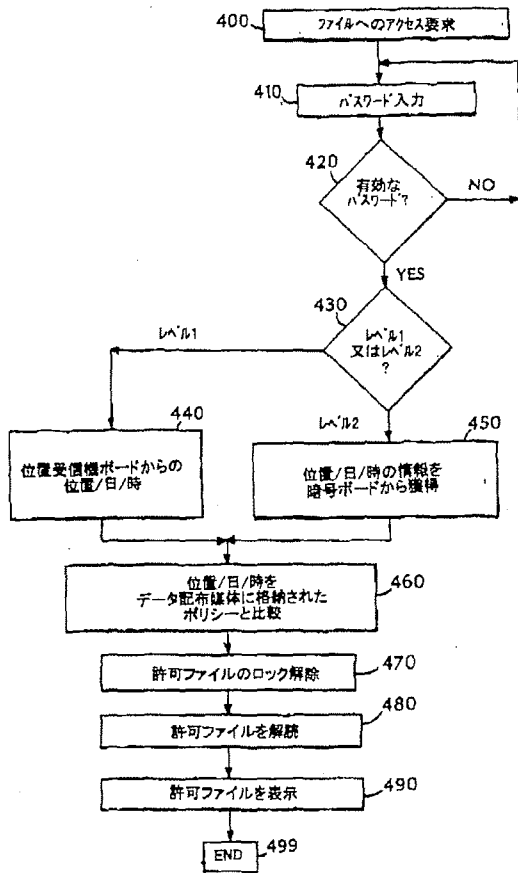
【図2】



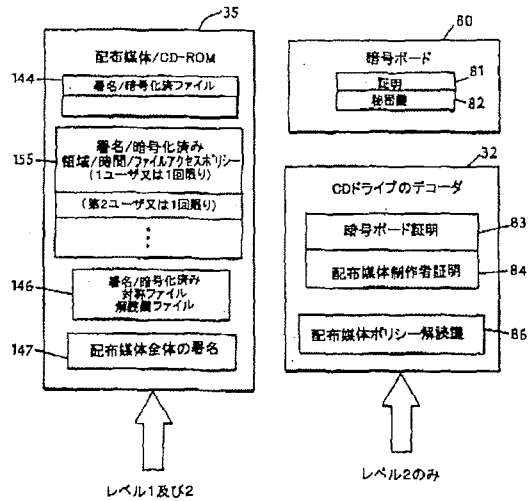
【図3】



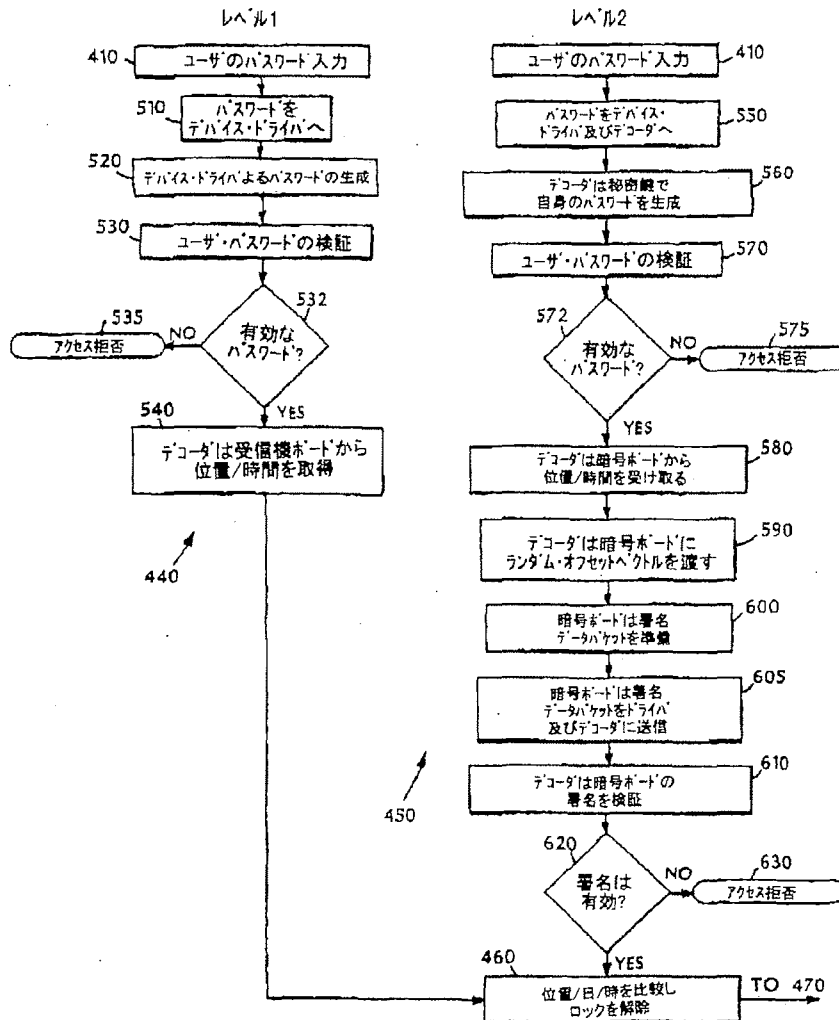
【図4】



【図6】



【図5】



フロントページの続き

(51) Int. Cl.⁷
H04L 9/14

識別記号

FI

デマコード (参考)

H04L 9/00

641

(72) 発明者 マイケル イー マックニール
アメリカ合衆国 カリフォルニア州
95018 フェルトン ロストエイカードラ
イブ 1271

(72) 発明者 トッド エス. グラッシ
アメリカ合衆国 カリフォルニア州
95066 スコッツバリー ブルーボネット
レーン 109エイ

(72)発明者 ジェラルド エル、 ウィレット
アメリカ合衆国 マサチューセッツ州
02148 マルデン#1 ハーバードストリ
ート 189



Companies and Intellectual
Property Commission
a member of the dti group

CIPRO IP ONLINE SERVICES

close | print

Details Abstract Description Claims Drawings Sequence Listing

REPUBLIC OF SOUTH AFRICA

PATENTS

REGISTER OF PATENTS

Official application No.			Lodging date: provisional		Acceptance date	
21	01	1999/06799	22		21-Jun-2000	

International classification No.			Lodging date: complete		Granted date	
51	G06F		23	28-Oct-1999	47	30-Aug-2000

International application No.			International filing date		priority date	

Full name(s) of patentee(s)	
71	161879. DATUM INC

Applicants substituted			Date registered	
71				

Assignee(s)			Date registered	
71				

Full name(s) of Inventor(s)	
72	161875. HASTINGS THOMAS MARK
	161877. GLASSEY TODD S
	161876. MCNEIL MICHAEL E

Priority claimed			
Country	Number	Date	
33	161878. WILLETT GERALD L	31	09/182.342
		32	29-Oct-1998

Title of invention	
54	CONTROLLING ACCESS TO STORED INFORMATION

Address for service	

74	162879. SPOOR & FISHER ROCHESTER PLACE 173 RIVINIA ROAD MORNINGSIDE , SANDTON	
<hr/>		
Patent of addition No.		Date of any change
61		
<hr/>		
Fresh application based on		Date of any change
<hr/>		
©2009 CIPRO PUBLIC PATENT SEARCH		(close)

USPTO PATENT FULL-TEXT AND IMAGE DATABASE[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Help](#)[Bottom](#)[View Cart](#)[Add to Cart](#)[Images](#)

(1 of 1)

United States Patent**5,646,992****Subler , et al.****July 8, 1997**

Assembly, distribution, and use of digital information

Abstract

Hierarchically organized graphical representations of items and groups of the items of digital information which are available to be ordered by a user are displayed. The user interactively explores the representations and selects items or groups to be ordered, using a pointer. While the graphical representations are being displayed, a list of items or groups which have been selected for inclusion in an order is also displayed. Software is executed which automatically determines the configuration of the computer, and matches the configuration with the stored configuration information prior to the user placing an order. A user may automatically be given access to items in a later revision of the medium if the user had access to the items in an earlier revision.

Inventors: Subler; Ronald J. (Charlestown, MA), Hastings; Thomas Mark (Lexington, MA)**Assignee:** Digital Delivery, Inc. (Bedford, MA)**Family ID:** 22423643**Appl. No.:** 08/126,217**Filed:** September 23, 1993**Current U.S. Class:****705/53 ; 380/281; 705/27.2; 705/56****Current CPC Class:**

G06F 21/10 (20130101); G06Q 30/0643 (20130101); G06Q 10/087 (20130101); G06F 2221/2107 (20130101); G11B 20/00086 (20130101)

Current International Class:

G06Q 10/00 (20060101); G06F 21/00 (20060101); G06F 1/00 (20060101); G11B 20/00 (20060101); H04L 009/00 ()

Field of Search:

;380/3,4,5,9,10,21,23,24,25,30,49,50,63

References Cited [Referenced By]**U.S. Patent Documents**

<u>4528643</u>	July 1985	Freeny
<u>4905163</u>	February 1990	Garber et al.
<u>5276901</u>	January 1994	Howell et al.
<u>5319705</u>	June 1994	Halter et al.
<u>5412717</u>	May 1995	Fischer

Primary Examiner: Gregory; Bernarr E.

Attorney, Agent or Firm: Fish & Richardson P.C.

Claims

What is claimed is:

1. A method for controlling access to a subset of items arbitrarily selected from among a larger set of items of digital information, comprising

encrypting said items belonging to said set using encryption keys, each of said items belonging to said set being encrypted using a corresponding one of said encryption keys, said corresponding one of said encryption keys being unique among said encryption keys used for encrypting said items belonging to said set, and

providing a decryption key which permits decryption of said items belonging to said arbitrarily selected subset of items.

2. The method of claim 1 wherein said encryption keys are associated with corresponding decryption keys, and said method further comprises

encrypting said decryption keys using a single global encryption key,

said global decryption key being said decryption key which is independent of the composition of said arbitrarily selected subset.

3. The method of claim 1 further comprising

generating a request for access to said items belonging to said subset,

incorporating in said request a request encryption key based on information unique to said request, said request encryption key being associated with a corresponding request decryption key,

encrypting said global decryption key in accordance with said request encryption key, and

decrypting said global decryption key in accordance with said request decryption key.

4. The method of claim 3 wherein said request for access to said items comprises an order placed by a computer.

5. The method of claim 3 wherein said information unique to said request comprises information associated with said computer.

6. The method of claim 3 wherein said information unique to said request is based on randomized data.

7. The method of claim 3 wherein said information unique to said request is based on a serial number of a medium on which said digital information is stored.

8. The method of claim 1 wherein said encryption keys are associated with corresponding decryption keys, and said method further comprising

recording said larger set of items on a high-capacity random access storage medium, and

recording said decryption keys on said medium.

9. The method of claim 8 further comprising encrypting said decryption keys prior to recording on said medium.

10. A method for controlling access to a subset of items arbitrarily selected from among a larger set of items of digital information, comprising

recording said larger set of items on a high-capacity storage medium, and

encrypting said items belonging to said set using encryption keys, each of said items belonging to said set being encrypted using an encryption key which is unique among said items belonging to said set, said encryption keys being associated with corresponding decryption keys, and

encrypting said decryption keys using a single global encryption key, said global encryption key being associated with a corresponding global decryption key, said global decryption key permitting decryption of said items belonging to said arbitrarily selected subset of items,

recording said decryption keys on said medium,

generating a request for access to said items belonging to said subset,

incorporating in said request a request encryption key based on information unique to said request, said request encryption key being associated with a corresponding request decryption key,

encrypting said global decryption key in accordance with said request encryption key, and

decrypting said global decryption key in accordance with said request decryption key.

11. Apparatus for controlling access to a subset of items arbitrarily selected from among a larger set of items of digital information, comprising

an encryption mechanism for encrypting said items belonging to said set using encryption keys, each of said items belonging to said set being encrypted using an encryption key which is unique among said items belonging to said set, and

a decryption key provider for providing a decryption key permitting decryption of said items belonging to said arbitrarily selected subset of items.

12. A method for restricting use of decryption keys which are provided to a user for the purpose of allowing decryption of information stored on a high-capacity storage medium, comprising,

encrypting the respective decryption keys using respectively different encryption keys,

providing the decryption keys to the user, and

enabling the user to decrypt the respective decryption keys using the respective encryption keys.

13. The method of claim 12 wherein said encryption keys are generated based on information unique to a computer on which said information is to be used.

14. The method of claim 12 wherein said encryption keys are generated based on randomized information.

15. The method of claim 12 wherein said information unique to said computer comprises a network address.

16. The method of claim 12 wherein said information unique to said computer comprises a computer serial number.

17. The method of claim 12 wherein said information unique to said computer comprises a disk serial number.

18. The method of claim 12 wherein said information which is unique to a single computer is delivered, from said computer to a location where said encrypting is done, as part of a request for access to said encrypted information.

19. A method for enabling a publisher to control access to digital information items distributed to users in the form of successive revisions of a high-capacity random access storage medium, comprising

encrypting said digital information items as distributed on said high-capacity random access storage medium,

giving a user access to selected ones of said items by providing decryption information for decrypting said selected items,

storing information indicative of items to which users had been given access in earlier revisions of said medium, and

enabling a user automatically to have access to items in a later revision of said medium if said user had access to said items in an earlier revision.

20. A method for controlling access to items of digital information stored on a high capacity storage medium, comprising

encrypting one group of said items by a mechanism which enables decryption based on a single decryption

key not recorded on said medium, and

encrypting another group of said items by a mechanism which requires different decryption keys, not recorded on said medium, for each of said other items.

21. The method of claim 20 further comprising

storing information on said medium which indicates which of said items belong to which of said groups.

Description

BACKGROUND OF THE INVENTION

This invention relates to assembly, distribution, and use of digital information.

Assembly, distribution, and use of information in digital form is fast becoming the norm rather than the exception to using "hard" copy. Virtually every kind of information may be treated in this way: sounds and music, executable programs, databases, pictures, animations, and fonts. The devices for embodying the digital information also vary widely. Examples include high-capacity storage media, like CD-ROMs, and switched telephone network communication.

In the case of CD-ROMs, publishers often already have available bundles of digital information which are being distributed in other modes (for example, on low-density diskettes). Because of the large capacity of CD-ROMs many bundles of digital information may be stored on a single disk. The bundles may be related, as in a set of different type fonts, or they may be unrelated. The publisher assembles the different bundles and creates a master data file which is then used to produce multiple identical disks for distribution.

A bundle stored on the CD-ROM may include not only the content which interests the end user (e.g., the text of an encyclopedia), but also executable programs which enable the user to find and make use of the content.

SUMMARY OF THE INVENTION

In general, in one aspect, the invention features a graphical user interface for aiding use of a group of items of digital information. Hierarchically organized graphical representations of the items and groups of the items which are available to be ordered by the user are displayed to the user. The user interactively explores the representations and selects items or groups to be ordered, using a pointer. While the graphical representations are being displayed, a list of items or groups which have been selected for inclusion in an order is also displayed.

Embodiments of the invention include the following features. The graphical user interface enables a user to preview additional detailed information concerning an item when a representation of an item is displayed, using a pointer. Also displayed are representations of actions which may be invoked, using a pointer, to cause an order to be effected and to enable a user to have access to an item that has been ordered.

In general, in another aspect, the invention features aiding a user in placing an order for access at a computer to an item of digital information offered by a distributor. Stored configuration information which identifies

configurations of computers sufficient to enable use of the item is distributed to the user. Software is executed which automatically determines the configuration of the user's computer, and matches the computer configuration with the stored configuration information. A signal is issued to the user, prior to the user placing the order, if the configuration and the stored configuration information do not match.

Embodiments of the invention include the following features. The item of digital information is distributed on a high-capacity random access storage medium. The configuration information is also stored on the medium, as is the software which automatically determines the configuration and matches the computer configuration with the stored configuration information.

In general, in another aspect, the invention features enabling a publisher to control ordering of items of digital information by a user from among a larger set of items of digital information made available by the publisher. The publisher is enabled to store packaging information identifying packages of items which are available for ordering. The user is enabled to select packages for ordering and is prevented from ordering items in bundles other than packages included in the packaging information.

Embodiments of the invention include the following features. The bundles which the user is prevented from ordering include individual items and supersets of the packages. The items in the larger set are made available to the user as recorded information on a high-capacity random access storage medium. The packaging information is recorded on the same storage medium. At least one of the items may belong to more than one of the packages. The packaging information also defines packages of packages which are available for ordering.

In general, in another aspect, the invention features controlling access to a subset of items arbitrarily selected from among a larger set of items of digital information. Each of the items belonging to the set are encrypted using an encryption key which is unique among the items belonging to the set. A decryption key is provided which is sufficient to permit decryption of the items belonging to the arbitrarily selected subset of items.

Embodiments of the invention include the following features. The encryption keys are associated with corresponding decryption keys, which are themselves encrypted using a single global encryption key (the decryption key mentioned above) that is independent of the composition of the arbitrarily selected subset. A request by the user (e.g., an order) for access to the items belonging to the subset incorporates a request encryption key based on information unique to the request. The request encryption key has an associated request decryption key. The global decryption key is encrypted in accordance with the request encryption key and decrypted in accordance with the request decryption key. The information unique to the request comprises information associated with the computer. The larger set of items is recorded on a high-capacity random access storage medium and the decryption keys are also recorded on the medium. The decryption keys are encrypted prior to recording on the medium.

In general, in another aspect, the invention features restricting use of a decryption key for the purpose of decrypting an encrypted item stored on a high-capacity storage medium usable with more than one computer. The decryption key is encrypted using information which is unique to a single computer and later decrypted for use in the single computer to decrypt the encrypted item.

Embodiments of the invention include the following features. The information unique to the computer may include a network address or a computer serial number, or may be based on random information derived from the state of the computer system, or may incorporate a serial number of the storage medium. The information which is unique to a single computer may be delivered, from the computer to a location where the encrypting

is done, as part of a request for access to the encrypted item.

In general, in another aspect, the invention features aiding a publisher in assembling items of digital information for mastering on a high-capacity random access storage medium by automatically verifying the existence and integrity of each of the items prior to assembly for mastering.

In general, in another aspect, the invention features enabling a publisher to control access to digital information items distributed to users in the form of successive revisions of a high-capacity random access storage medium. The digital information items are in encrypted form on the high-capacity random storage medium. A user is given access to selected ones of the items by providing decryption information suitable for decrypting the selected items, storing information indicative of items to which users had been given access in earlier revisions of the medium, and enabling a user automatically to have access to items in a later revision of the medium if the user had access to the items in an earlier revision.

Among the advantages of the invention are the following.

A wide range of benefits are provided by the invention both to the user and to the publisher. The publisher is provided with powerful tools both for marketing and for controlling access to items to be distributed. For marketing purposes, the publishers may include, e.g., on a CD-ROM, digital information implementing a wide range of marketing approaches, including previews of items, information describing the items, disabled versions of the items, and icons representing the items.

Publishers may easily maintain information regarding successive revisions of titles being distributed, and may arrange for users to have automatic access in later revisions to items that they paid for in earlier revisions.

The publisher can provide a large number and wide variety of items to a user, permitting the user to browse and preview the items, giving the user the opportunity to pick and pay for only those items of interest. The publisher need not fear that other items made available to the user, but not paid for, can be used.

The packaging of items in the system allows publishers to create item groupings that are sensible from a marketing or other viewpoint, and to present those groupings to the user as products. The product groupings can be revised and updated as needed.

The publisher can include the item grouping information and software for previewing, browsing, and ordering all on a single CD-ROM.

Prechecking the items during pre-mastering assures that the final CD-ROM will include the items intended and that they will be usable.

The user is provided with a powerful, easy-to-use interface to browse through and analyze the features of a wide range of items and product groupings, to pick and choose those which it wishes to order, to place the order, and then to install the items on his computer. This provides an easy and highly effective way to shop, not only for software, and databases, but for virtually any product.

For items which are to be loaded into and used on a local computer, the user can be assured, prior to placing an order, that the item will operate with the configuration represented by the local computer.

Giving access to multiple items via a single decryption key provided to the user when the order is accepted saves time and effort.

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

DESCRIPTION

We first briefly describe the Figures.

FIG. 1 is an overall block diagram of a computer-based system for assembling, distributing, and using digital information on a CD-ROM.

FIG. 2 is a block diagram of a computer-based system for pre-mastering a CD-ROM.

FIG. 3 is a block diagram of a database structure.

FIG. 4 is a flow diagram of an encryption/decryption process.

FIGS. 5 through 25 are views of displays shown to an end user.

FIG. 26 is a view of a display shown to an order taker.

FIGS. 27 through 30 are views of displays shown to a pre-mastering user.

Referring to FIG. 1, in one example of the invention, a system 10 enables a publisher 12 to pre-master and distribute digital information on CD-ROMs 14, and an end user 16 easily to make use of the information.

Generally, the result of the publisher's work is a set of pre-mastered data 22 which is in form to permit mastering of multiple CD-ROMs 14 using a conventional mastering system 24. The pre-mastered data is set up by a pre-mastering system 18 which includes software running on a workstation. The inputs to the pre-mastering system 18 include end user system software 26, bundles of digital information 28, 30 (called valued and non-valued items, respectively), facilities 32 associated with the end user system software, and information entered by the user 12 using a keyboard or mouse (not shown). Valued items may be items which the user may order and pay for, such as clipart images. Non-valued items may be items which need not be paid for, such as free games, or marketing information describing a range of items. Among other things, the pre-mastering system checks and verifies the valued items 28 being included in the pre-mastering data set. The valued items are stored on the CD-ROM in encrypted form and are unusable by the end user until he has paid for their use. The pre-mastering system also maintains a pre-mastering database 34 which maintains information about the different sets of pre-mastered data 22.

The end user gets access to and makes use of digital information stored on the CD-ROM with the aid of end user system software 36. End user system software 36 is a version of the original end user system software 26 which has been configured by the pre-mastering system 18, combined with selected facilities 32, and stored on the CD-ROM. The software 36 is loaded into and runs on the user's workstation. Among other things, the end user system software creates and maintains an end user database 38, e.g., on the workstation hard disk.

The end user system software includes code which allows the user to browse through information representing the items, to preview certain items, to generate and send a purchase order 40 to an order taking

system 42, to receive back an acknowledgment of the order, to "unlock" the order items, and to install them on the workstation.

The purchase order indicates which of the valued items (or groups of valued items) the user wishes to order. The order may also include information which is unique to the particular workstation being used and assures that the acknowledgment returned in response to the order will permit use of the items only on the particular workstation. The order may be delivered to the order taker under program control (e.g., via FAXmodem, modem, network packet, or cable system) or under user control (e.g., via voice telephone call, FAX, or printed matter)

Information stored on the CD-ROM with respect to a valued item includes information about which computers and peripheral equipment are suitable for use with the item. Before an order is sent to the order taker, the end user system checks the actual configuration of the user's workstation against the stored compatibility information to make sure they match.

Once the order has been accepted, an order acceptance 44 is returned to the end user system. The order acceptance includes decryption information which is based on information previously sent from the end user system and aids in decryption of the valued items. The order acceptance also may include other information (for example control data for controlling the collection of information on user activity). The system is configured so that a single item of decryption information sent from the order taking system to the end user system is enough to allow decryption of whichever valued items are chosen by the user even though each valued item has been encrypted with a different encryption key and even though the order may specify an arbitrary selection of valued items.

The order taking system 42 includes software running on a workstation. The software provides an environment in which an order taker 46 can process the order and cause the order acceptance to be returned. The order taking system software maintains an order taking database 50. Information generated by the order taking system may be passed to accounting, order entry, and marketing analysis systems 52.

The end user system includes code which provides an integrated windowed graphical user interface through which users may browse, preview, order, unlock, and install valued items and other information stored on the CD-ROM.

The pre-mastering system enables the publisher to manage successive revisions of a CD-ROMs to permit, among other things, a user to have free access to revised versions of valued items which the user paid for via an earlier revision.

Pre-mastering System

As seen in FIG. 2, the pre-mastering system manages the pre-mastering user interface 102. It provides a windowed graphical user interface which enables the user to guide the processing of the items to be included on the CD-ROM on an item by item basis.

Referring to FIG. 27, an Item Definition window 502 offers the user the ability to define an item for use in pre-mastering an item efficiently. The user may enter a name for the item in box 504, a title for the item in box 506, and a short description in box 508. The software automatically provides a revision number in box 512 to maintain a sequenced record of item changes.

To initiate a new item, the user selects the New button on the item browser, and selects the type of item (e.g., atomic item or group item). The user enters a publisher ID which uniquely identifies the item for that title. The system automatically assigns an internal ID and revision number to the item. Other than type, internal ID, revision, number, and publisher ID, all other fields will initially have the value determined by inheritance as follows. If the field has a value in a title which this title is derived from, that value is used. Otherwise the value is marked as not specified. From the initial set of values, any further modifications to the item's fields may override the inherited values or cause them to be used again (to undo an override).

When an item is initially created, its status is set to incomplete. Once the item is validated, if sufficient information has been entered to allow a pressing the status is changed to complete. Once a pressing is performed using this item, the status is set to locked and no further changes are allowed to this revision of the item. A new revision must be created if edits are required. If a locked item is deleted its status is set to obsolete.

The item type box is a field which allows the user to select from a restricted list of item classifications used by the end user system.

A set of buttons 520 allows the user to call up other windows to provide additional information for an item. The files button 522 invokes a window in which the user may indicate the source files that will make up an item. The keywords button 524 invokes a window 526 (FIG. 28) which contains a box 528 that displays available keywords for use with the item. A box 530 displays the list of keywords that have been selected from box 528 for use with this item. Box 532 provides a place for the user to edit a keyword selected in box 530. In general, the keywords applicable to an item may already exist; if so they may be imported by the pre-mastering system and displayed in box 528 for selection. Alternatively new keywords for the item may be keyed in by hand in box 532 to build a keyword set for the item.

If the user selects Attributes button 534 (FIG. 27), he is presented with an Attributes window 536 (FIG. 29). Window 536 includes a box 540 which displays available attributes for selection by the user. In general, the attributes applicable to an item may already exist; if so they may be imported by the pre-mastering system. Alternatively new attributes for the item may be keyed in by hand to build an attribute set for the item. Box 542 displays the attributes that have been selected. Box 544 provides a place for the user to edit or add new attributes and box 546 enables the value of the attribute to be edited or added.

If the user selects the Facilities button 538 (FIG. 27), he is presented with a Facilities window that includes boxes enabling the user to select facilities that are to be made available for the item being premastered.

If the user selects the Vendors button 550, he is presented with a Vendors window that allows the entry of information about the vendor of the item.

If the user selects the Thumbnails button 552, the user is presented with a Thumbnail window 554 (FIG. 30). A box 556 allows the selection of setup information for displaying the thumbnail associated with the item. The setup information includes a resolution, and a label for the spreadsheet. A box 558 enables the user to specify the source path of the file or files that make up the item. A box 560 enables the user to specify the destination path on the CD-ROM. The user may enter or edit resolution information in box 562, label information in box 564 and label font information in box 566.

In addition to providing a graphical user interface, the pre-mastering system processes end user system software 104 to place it in condition to be recorded on the CD-ROM. The pre-mastering system verifies and

moves to the CD-ROM pre-mastering area all executable, library, and data files required by the end user system to be able to display, preview, order, decompress, decrypt, and install any items on the CD-ROM. The pre-mastering software also produces relations which map specific methods for each of the above facilities to each item on the CD-ROM. The pre-mastering software also generates all key tables required by the end user system as well as the order taker software.

The pre-mastering system maintains a pre-mastering database 106 that contains the following information with respect to each revision and pressing of each title:

date of the revision and pressing

whether publisher has full rights or must pay royalty to manufacturer

the title number

the revision number

In the course of processing items for inclusion on the CD-ROM, the pre-mastering system creates a CD-ROM database 108 in two versions; one is held by the publisher (we shall call it the Publisher's Database); the other (a subset of the publisher's version) is included in the pre-mastered data to be stored on the CD-ROM (the CD-ROM Database).

CD-ROM Database

As seen in FIG. 3, both versions of the CD-ROM database are organized on an item by item basis. An item 130 may be an atomic item 132 or a group item 136 which represents a collection of items.

Each item is identified by an internal ID number, a vendor ID number, a publisher ID number, an original manufacturer ID number, a title for the item (for display at the end user's workstation), a description of the item, and a list of properties of the item. Properties associated with an item include

original manufacturer

licensing rights due to manufacturer

whether the item is orderable or not

whether the item is valued or non-valued

whether the item is visible to the end user or not

comments

list fields, described below

Each item has associated with it file information 140 for the files which make up the item. For each file, this includes where the file came from (its source path), where it is to be stored on the CD-ROM (its release path), where it is suggested that the file be installed on the user's system, the file size, a checksum, and a file type.

Each item also has associated with it information concerning one or more thumbnails 142 which are representative of the content of the item. An example of a thumbnail is a graphic of a single letter from an item which contains the entire font. Multiple thumbnails may be needed for use with different display modes (resolutions). The information concerning each thumbnail is its source path and its release path on the CD-ROM, a short title to appear under the thumbnail when displayed, font information for the short title, and identification of facilities needed to expose the thumbnail to the user.

Each item may also have associated with it one or more previews 144. Examples of previews are demonstrations, animations, copyright information, and bit maps. They are designed to enable a user to learn about an item without actually having access to the item. The information which both versions of the CD-ROM database hold with respect to previews for an item includes the identity of the primary preview and alternate previews, the files where the previews are located, the source path, the CD-ROM path, the title that appears on menus which give the user a choice of previews, and type of preview.

The container link information 148 defines relationships between atomic items and group items. An atomic item may be part of multiple packages, and packages may be linked in groups of items.

Each item may have an associated set of keywords 150 used for searching within the item. Because the same keywords may be used for more than one of the items, rather than tie a separate dedicated set of keywords to each item, keyword links 152 are provided to point to the keywords applicable to a given item.

In the same vein, an item may have attributes 154, but as multiple items may share attributes, attribute links 156 are provided to point to the attributes applicable to a given item.

Comments 158 may be entered with respect to an item, for documentation purposes.

For purposes of keeping track of sets of pre-mastered data, a set of items intended to be recorded on CD-ROMs is called a title. An example of a title would be images of major league baseball players. The properties of a title and of a revision include its name, its date, and comments. Titles may have title previews 162.

Titles are hierarchical in the sense that certain titles may be derived from other titles. In the case of title derivation, the derived title will inherit all the properties and items of the title from which it is derived. Any changes or additions to the derived title will only apply within its own scope. Subsequent changes to the title derived from will propagate to all derived titles dynamically.

Items are also hierarchical. An item within a particular title will inherit any unspecified properties from the corresponding items with the same identity (same internal ID) in any titles from which the particular title is derived. For example, if a title "Pictures of Cars" is derived from a title "Pictures of Machines" and one of the items contained in both titles is a picture of a Porsche then for all properties not specified for the "Pictures of Cars" title, the values specified for the same item in the "Pictures of Machines" title will be used. This mechanism allows specific properties only relevant to an individual title to be specified while not requiring general properties common to a group of titles to be re-entered.

When any change is made in a title, production of additional CD-ROMs represents a new revision. The CD-ROM database includes information which indicates which revision of the title is presented and indicates the upgradeability of each item. For a new revision, a new decryption key is generated for each item.

A given revision of a given title may have multiple pressings 164. A pressing is an instance of a title as it is recorded on multiple CD-ROMs which differs from the CD-ROMs of other pressings of the same title and revision only by the decryption keys associated with the respective valued items. The properties of a pressing include the date of pressing, a description of the pressing, and a seed for the encryption key. The seed is an encryption key used to encrypt the decryption keys generated for the first pressing of the given title and revision. A pressing could be a run of say 1000 CD-ROMs. In each new pressing, the encryption key and corresponding decryption key for the decryption key file is changed, but the underlying decryption keys for the items are not changed. This provides an additional security feature versus a system in which a pressing covers many thousands of CD-ROMs.

Upgrade tables 167 in the CD-ROM database indicate the extent to which an end user is permitted access to items to which he previously had access in an earlier revision. There is an upgrade table with respect to each prior revision or pressing. Each upgrade table includes a list of new item numbers. Each new item number is associated with an old item number and with a key. The key is the actual decryption key for use with the item on the current CD-ROM, encrypted with the original encryption key for that item on the revision or pressing to which the table pertains. Thus the tables, together with information previously obtained by the end user with respect to the earlier pressing or revision, is sufficient to permit decryption of items to which the user previously had access.

The version of the CD-ROM database recorded on the CD-ROM is identical to the publisher's version except that it only includes the one title which relates to the items stored on the CD-ROM and all hierarchical information has been resolved to produce a single independent set of records.

In addition to the general title information and the information concerning each item in the title, the CD-ROM database includes vendor information, keyword information, and attribute information which are referenced by items in the title.

An example of a possible database definition for the CD-ROM database is set forth in Appendix A, incorporated by reference.

Returning to FIG. 2, the pre-mastering system also generates encryption keys and key files for use for a given pressing. The encryption scheme is described in more detail below.

The pre-mastering system also processes 112 the original items to generate processed items. This is done after the CD-ROM database has been set up and the encryption keys and key files have been generated. The title information in the database indicates the items to be included in the pre-mastering data. Items to be included are processed one after another. To process an item, first the files which make up and which are associated with the item are located and fetched.

Each file is verified by the following steps. A check is made to be sure the file exists and is the same version as the one that the user originally specified when populating the database. This check is made on the basis of size, checksum, and modification date. A check is also made that the item includes (and has accessible) all required fields (for example, bitmaps may always require an x-size and a y-size).

After verification, the files making up the item are compressed (if called for) and encrypted (if called for). Compression and encryption may use any appropriate compression and encryption schemes. The files making up the item are compressed and/or encrypted if the database so indicates (which will be typical for large

items, to be compressed, or valued items, to be encrypted).

Referring to FIG. 4, the sequence of steps involved in encryption and decryption of an item in the pre-mastering, order taking, and end user systems begins with the generation of a unique item encryption key for the item 170. Encryption keys may be generated by any of a variety of known schemes. The unique item encryption key 170 is applied to the valued item 172 to generate an encrypted valued item 174. It is that encrypted item that is recorded on the CD-ROM 176. The CD-ROM may carry an encrypted version of an item decryption key file 178. The encrypted item decryption key file is an encrypted file which lists the encrypted items on the disk and associates with each item an item decryption key 180 which corresponds to the item encryption key used to encrypt the file. The actual item decryption key file 182 is encrypted using a unique key file encryption key 184. Thus, the CD-ROM contains all of the decryption keys needed to decrypt all of the items contained on it, but they cannot be used without decrypting the file which holds them. That decryption requires an actual key file decryption key 186 which corresponds to the key file encryption key for decryption key file. The actual key file decryption key is not included on the CD-ROM but rather is obtained by the end user as part of the process of ordering and paying for use of selected valued items, as follows.

The actual key file decryption keys are provided by the publisher to the order taker and maintained in the order taking system. Each order from an end user to the order taker includes a unique request number 188 and a list of IDs of selected valued items 190. The request number identifies the CD-ROM in a way that enables the order taking system to fetch the actual key file decryption key. The order taking system uses the request number to generate an encrypted key file decryption key 192 which is delivered to the end user system. The end user system has access to the request number in that the request number was generated at the end user workstation. The end user system uses the request number to decrypt the encrypted key file decryption key 192, thus recovering the actual key file decryption key 186. This is used to generate (unlock) the actual item decryption key file 182 from the encrypted version 178. Then the IDs for the selected valued items 190 are used to control the retrieval of the selected decryption keys. They are stored on the hard disk of the end user's workstation and used to decrypt the valued items for subsequent use. Alternatively they may be stored on a network file server (for example, when an enterprise license or bulk license and software for counting active copies is used) or on other media such as Flash RAM, EEPROM (EEROM) or even ROM (for example when the key is pre-encoded in a PCMCIA card).

Part of the key file decryption key is a set of check sum/hash totals on the item decryption keys for the items in the order. This provides an additional layer of protection, making it more difficult for the end user to use the key file decryption key to free up item decryption keys for items not ordered.

Referring again to FIG. 2, the finished CD-ROM contains processed items 200 (which include valued items and information other than valued items, e.g., marketing materials), configured end user executables 202, the end user CD-ROM database and the key files 206.

The system may be used to distribute a title which spans multiple volumes (e.g., multiple physical CD-ROMs). The CD-ROM database is then duplicated on each of the volumes and the thumbnails and selected non-valued items may be duplicated on some or all of the CD-ROMs. The database includes volume number as an identifier so that the end user system will not be confused as to which physical volume is currently in place. As a result, the publisher may virtually ignore size constraints and the user may compose an order which spans several volumes.

End User System

When the user starts the end user system, the main menu (FIG. 5) appears. Among the menu choices are Preview and Search 302 (which leads to the main browsing and searching facilities); Order, Unlock, and Install 304, which leads to the processes for generating orders, and unlocking and installing items; Samples and Other Info 306, which provides the same functions as Preview and Search, for free product and general information; and System Setup 308, where users can review and modify information about themselves, their system, and the publisher.

When the user invokes the System Setup item, the submenu of FIG. 6 appears. The Customer Information selection 310 leads to a window of information about the end user which is needed when an order is to be placed. The Vendor Information selection 312 leads to information about the name, address, phone, FAX, customer support technical support and related numbers from the publisher. The Computer Information selection 314 provides system configuration information needed to run the end user system, such as the location of the CD-ROM reader.

The Samples and Other Info selection 306 on the main menu gives the user access (through a sub-menu (FIG. 7) to self-running demos 316, try-out (disabled) products 318 or free products 320.

The Preview and Search selection 302 of the main menu gives the user access (through a sub-menu, FIG. 8) to alternative choices for previewing 322 or searching 324 through items on the disk for the purpose of locating those which the end user wishes to purchase. The search functions are a subset of the preview functions described below.

The Order, Unlock, and Install selection 304 of the main menu leads to a sub-menu (FIG. 9) which enables the user to Place Order 326, Unlock Order 328, or Install Unlocked Order 330.

When the Preview selection 322 is invoked, a multiple window screen 332 (FIG. 10) appears. The screen provides constant simultaneous viewing of three important aspects of the content of the CD-ROM and makes navigation, previewing, and ordering of items easy and simple. The three aspects are displayed in three windows. The Viewer window 334 continually provides graphical illustrations 336 of one or more items stored in the CD-ROM. The user may use the scroll bar 338 to navigate through the items which to finds ones of interest.

The Position window 340 illustrates the hierarchy of the items on the CD-ROM and the position of each item, or category, or package within the hierarchy. The hierarchy does not depend on the physical location of the items on the CD-ROM but rather is governed by a marketing hierarchy imposed by the publisher in the course of pre-mastering and embodied in the CD-ROM database. The scroll bar 342 permits easy navigation through the hierarchy and the Position and Viewer windows are synchronized so that scrolling in one causes corresponding scrolling in the other.

An Order Pad window 344 gives the user access to the ordering facilities and displays information about orders.

The lowest level in the hierarchy of items illustrated in the Viewer and Position windows are the items. Items (e.g., individual clipart images) may be bundled into packages for purposes of sale. Each package typically contains items of a broader category (e.g., sound effects), and there are typically different packages within a given category. Categories typically are not subject to being purchased in a single transaction. Only the packages within a category may be purchased in a single transaction. There may be packages of packages and

so on. Furthermore packages may contain items of different types.

The user may easily switch what is shown in the Viewer window between all of the items stored on the CD-ROM (using the disk contents button 345) and the items which were generated in the most recent search (using the search results button 347).

The type of each thumbnail is indicated in the upper right corner, for example by a "C" 350 for Category, or by a "P" for package, or blank for an individual item. At the lower right corner of each thumbnail is an indication of whether the item or package has been ordered (a "?"), ordered and unlocked (a checkmark), ordered, unlocked, and installed (filled circle) or not yet ordered (blank). The status indicator for a package or group indicates the highest level of status achieved by all items in the package or group.

Each thumbnail is accompanied by an textual title 354 which includes one line of content and a second line repeating in text what is indicated in the hierarchical symbol 350. Initially the Viewer displays thumbnails 346 of the highest level bundles in the hierarchy, in this case categories.

When the user double clicks on a category thumbnail, the category is opened to reveal thumbnails 360 (FIG. 11) corresponding to all of the entries at the next lower level of the item hierarchy. As shown, this next lower level may itself include categories.

Double clicking on one of the thumbnails at this lower level (e.g., the "Type 1 Category") opens that category and displays package thumbnails 362 (FIG. 12). In this case, each thumbnail is a sample of one of the font letters. Clicking on one of the package thumbnails leads to display (in this case) of the thumbnails 364 (FIG. 13) for individual items (here individual fonts).

The hierarchy may be navigated in the reverse direction simply by clicking on the Previous button 366.

By clicking an individual item thumbnail, the user may cause display of additional information about that item (for example more comprehensive displays of the font (FIG. 14)).

Clicking on the Info button 368 (FIG. 13) provides other detailed marketing information (FIG. 15) about items represented by selected thumbnails.

The information for every item includes the item identifying number 370, the version number 372, the size 374, the title 376, a description 378, a file format 380, the status 382, and the installed path 384. Of these items all but the last two are derived from the CD-ROM database. The last two are derived from the end user database.

The middle of the window provides information 386 (derived from the CD-ROM database) specific to the particular type of item. The keywords subwindow 388 shows keywords assigned to the item (either by the publisher via the CD-ROM database, or by the end user).

The end user may click the order item button 390 (FIG. 13) at any time to add a selected item to an order, and may click the install item button 392 at any time to install a selected item that has been ordered and unlocked.

Thus the windowed graphical user interface enables the user to engage in browsing, previewing, ordering, searching, and installation activities easily and quickly while viewing and interacting with a single screen of three windows and control buttons.

SEARCHING/BROWSING

The end user may search the content of the CD-ROM using keyword information and the values of attributes. Keyword information may be stored on the CD-ROM as part of the CD-ROM database, as a result of pre-mastering, or may be added by the end user and stored in the end user database. Attribute information is supplied by the publisher in the course of pre-mastering and stored in the CD-ROM database. Attributes are publisher specified information categories which apply to all items of a given type. The attribute values for an item appear in the window that is displayed when the info button is clicked (reference numeral 386 in FIG. 15).

The end user invokes the search function by clicking on the Search button 390 (FIG. 13). When the search is completed the results are represented by thumbnails displayed in the Viewer window. The Search is replaced with a Search Again button. When the search again button is pressed searching is restricted to the field of results of the prior search.

When the Search button is clicked, a window 400 (FIG. 16) is displayed enabling the user to specify the search criteria and control the progress of the search. At the top of the window are four pull down menus. The first pull down menu 402 permits selection from all of the groups of items recorded on the CD-ROM. The second pull down menu 404 permits selection from a list of all of the attributes defined for the selected group. The third pull down menu 406 permits selection of a logical search operator (e.g., greater than). The fourth pull down menu 408 permits selection of one of the possible values which exist for the selections made in the other three pull down menus.

If the user wishes to apply a combination search, he then clicks on the Apply button 409. Then he selects a combinational operator in the Combination Rule pull down menu 410. And then he enters the next search rule in the menus 402, 404, 406, 408, and finally clicks on the Start button 412. The search criteria are displayed in box 414 for review. The Where is it function (described below) may also be used to locate a desired item.

Being able to locate a desired item is especially useful at the end of the searching process. The search may have led to items which are individually not orderable (so that the user needs to find the package which contains the item and which is orderable) or to items which are orderable in multiple packages (so that the user needs to determine which package is most suitable to order).

Ordering

The end user uses the Order Pad window 344 (FIG. 10) to compose a new order, place an order, review an order that has been composed or an order that has been placed, to unlock the items of an order that has been placed and accepted, and to install the items of an order that has been unlocked.

An order is composed by assembling in the Order Pad window a list of orderable items, packages, and categories. The list is assembled in any one or more of three ways. One way is to drag and drop the entity from the Viewer window. A second way is to select the item in the Viewer window and then click on the Order Item button (390, FIG. 3). A third way is to select the item in the Viewer window and then select Add to Order from the Contents pull down menu 391 (FIG. 10). The Contents pull down menu is shown in FIG. 24. As seen in FIG. 25, when the Where is it entry 421 is selected in the Contents pull down menu, a list is displayed showing the packages and categories in which the selected item is found. This aids the user in deciding which package may be the best to buy to get the desired item.

Returning to FIG. 10, the entities which make up the order are listed 420 in the order pad window in the same order as in the Position Window and may be expanded or contracted in the same way.

If an attempt is made to order a collection of items that was not intended by the publisher to be sold as an entity, an error message like the one shown in FIG. 18 is displayed. A similar error message (FIG. 19) is displayed when the user attempts to order an item which is too low in the hierarchy to be separately ordered.

If the user double clicks on an entry in the list displayed in the Order Pad window, thumbnails of the items which make up the entry are displayed in the Viewer window.

The user deletes an entry from the order list by selecting it and then clicking on the Remove Item button 422 (FIG. 17).

To move on to the process for placing the order, the user clicks on the Place Order button 424 (FIG. 17). The Clear Order button deletes the entire order list from the window.

Clicking on the Place Order button causes a order information window 426 (FIG. 20) to be displayed. Sections at the top of the window show the customer number (received from the order taker and entered after the first order is placed), and the customer name, company name, voice and FAX phone numbers, and disk serial number (all entered by the user during setup and subject to change by clicking on the Set Up button 428). The disk title is automatically provided from the CD-ROM database. The request number is generated by the end user system as described earlier and is unique to the order. This may be achieved either using the serial number or network address of the computer on which the end user system is running or by using randomized information (e.g., information derived from the state of the computer system) that makes it highly unlikely that two requests will be the same. In some implementations the request number can incorporate a disk serial number. Information about payment 430 is user editable by clicking on the Set Up button. Ordering information 432 is also editable through the Set Up procedures.

The Cancel button 436 removes the order from the system and returns the user to the Viewer. A placed order may be saved by clicking on the Save button 438. Clicking on the Unlock Order button 440 advances the user to the unlock and install routines after the order has been placed and the key has been returned. The Help button 442 does what its name implies.

The user may view, unlock, and install orders previously composed using the scroll bar 444 (FIG. 17). When the user clicks on an order shown in the scroll bar list, that order is displayed in the Order Pad window. That order may then be viewed or unlocked.

The ordering may be done by several methods. In a telephone conversation the user may read the information to a clerk and receive back the decryption key. In a FAX order the information and key are passed by in FAX format. In a printed order the order and key are printed on paper and the papers are FAXed. Modem to modem communication is also possible. The purchased item list is not editable (because it is permanently associated with the request number) and is copied from the list in the Order Pad window.

Unlocking

When an order has been placed and the decryption keys have been returned, the user enters the keys in the Unlock Order window 450 (FIG. 21) which is displayed by clicking on the unlock button 440 (FIG. 20).

Alternatively the user may select an entry in the Order pull-down menu. The user enters the keys in the key fields 452. The end user system checks the keys and tells the user if a mistake has been made in entering them. Once valid keys have been entered, the unlocking step has been completed and a corresponding message is displayed to the user.

The user may then click on the Save button 454 if he wishes to wait until later to perform the installation of the unlocked items, or on the Install button 456 if he wishes to proceed immediately to installation.

Installing

When the user indicates his wish to install the items of an unlocked order, the installation window 460 (FIG. 22) is presented. The installation window shows the request number 462 and date 464 of the order and lists 466, allows the user to control whether packages or items are displayed, and whether installed or uninstalled items or both are displayed 468. The user may select items or packages on the display and the system shows the required disk space to install the displayed items 469.

When the display shows the items and packages which the user wishes to install, he clicks on the Install button 470. This leads to display of a control window 472 (FIG. 23). In window 472 the user may choose the location for storing each item in the order. The Next Item button 476 controls the contents of the Item box 474. A Recommended Target box 478 shows the recommended location as indicated in the CD-ROM database. The user indicates the actual directory desired in box 480 in the usual way for Windows applications. The Install All Here box allows the user to handle installation of all items to the same directory at once,

Installation of each item involves decryption using the decryption key for that item found in the decryption key file on the CD-ROM database, and decompression.

Alternatively it is possible to arrange for the unlocked items on the CD-ROM to be used directly with on-the-fly decryption and decompression if appropriate facilities are provided.

Other interfaces, not so heavily dependent on the mouse actions by the user, may also be provided.

End User Database

Appendix B (incorporated by reference) includes an example of a database structure for use in the end user database. The end user database is created and maintained on the user's computer with the aid of routines included in the end user system stored on the CD-ROM.

As seen Appendix B, the end user database includes information such as the customer's number, name, address, telephone numbers, credit card information, disk information, and order and key information.

Order Taking System

In order to generate keys for delivery to the end user in response to an order, the order taker is presented with a screen 490. A box 491 contains the unique request number associated with the order. This number may be obtained electronically over a telephone line or entered manually by the order taker when the request number is spoken to the order taker over the phone by the end user. The disk title and disk description boxes 492, 493, display information that is derived automatically by the order taking system from the request number.

Box 494 contains the list of items being ordered. In one implementation this information would be derived automatically over the telephone line as part of the order. In another, the user would read the list of items to the order taker who would then enter them by keyboard or by selection from a scrolled item list 495.

Once the order is completed, the order taker selects "Generate Keys" and the "keys" are computed and displayed in boxes 496 and 497. The two entries in boxes 496 and 497 together comprise the decryption key for the decryption key file discussed earlier. They are displayed as two "keys" for convenience in delivering them by voice. The keys could either be delivered electronically or by voice to the user.

The order taking database is derived from order taking information sent from the pre-mastering system (see FIG. 1) The order taking database includes tables for each revision. A table for a given revision includes a list of item numbers, the title of each item, the decryption key for each item, and optional information such as accounting information. The database also includes a section for each pressing of each revision. That section contains, for each pressing, the key that was used to encrypt the decryption key of a prior pressing.

Other embodiments are within the scope of the claims.

For example, the nomenclature of the discussion above has centered on a commercial implementation in which a publisher wishes to distribute items in exchange for payments associated with user orders. But the system is also useful for non-commercial applications, such as for internal use within a corporation to distribute information (e.g., marketing information, manuals, product specifications) to employees. Many organizations are beginning to use CD-ROMs for internal distribution of proprietary information such as architectural drawings, financial transaction histories, and CAD/CAM/CAE designs. In those contexts the "order" is not associated with a payment, and encryption may or may not be needed.

The arrangements for decryption may be varied. For example, the decryption keys for selected items may not be included in the item decryption key file 182. This will be indicated in the CD-ROM database. When an end user orders such an item, the order acceptance will include an individual decryption key for each ordered item.

Alternatively, a single encryption key may be used to encrypt all items in a title, and a single corresponding decryption key may be provided to decrypt all items.

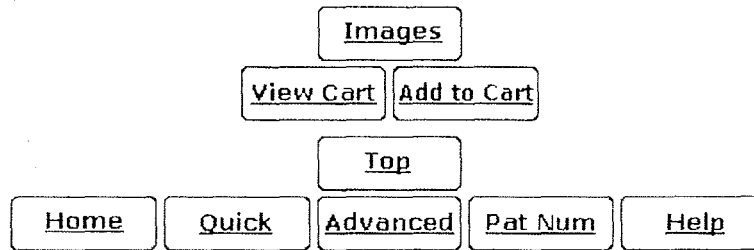
Furthermore, a hybrid scheme could be used in which some items on a title (e.g., less valuable ones) are protected by a single encryption key while others are protected on a one key per item basis.

The medium in which the digital information is conveyed need not be CD-ROM but could be floppy disks, tape, magnetic-optical storage, ROM chips, flash-RAM chips, normal hard disks, and other high-capacity media that may be developed in the future.

Furthermore the digital information may be distributed by a non-storage medium, including computer network media and side-band broadcasting. In the latter case, for example, side-band information sent by TV network, cable networks, and syndicators to their affiliates could be used more extensively if the transmitter knew that only authorized affiliates would be able to decrypt the broadcast signal and extract the original information. Similarly, broadcast frequency or cable channels could be used to distribute secure information. The invention is likely to be applicable to other non-storage media not yet developed.

Appendix C contains source code for an implementation of the invention which may differ in some respects from the implementation described above. The code in Appendix C was built using the following tools: Borland C++ Version 3.1, Raima dbVista version 3.21, Blaise CPalette Library version 1.0, and Symantec Object Graphics Library version 1.01. In Appendix C, DDKEY.EXE is the executable for the order taker system; DD.EXE is the executable for the end user system; the pre-mastering system is embedded in DD.EXE; CRYPTIT.EXE and KEYIT.EXE are part of the pre-mastering process. A portion of the disclosure of this patent application contains material which is subject to copyright protection. The owner has no objection to facsimile reproduction by anyone of the patent application, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

* * * * *



USPTO PATENT FULL-TEXT AND IMAGE DATABASE

Home	Quick	Advanced	Pat Num	Help
Bottom				
View Cart		Add to Cart		
Images				

(1 of 1)

United States Patent
van der Kaay , et al.

6,393,126
May 21, 2002

**Please see images for: (Certificate of Correction) **

System and methods for generating trusted and authenticatable time stamps for electronic documents

Abstract

A trusted time infrastructure system provides time stamps for electronic documents from a local source. The system comprises a trusted master clock, a trusted local clock, and a network operations center. The trusted master clock and network operations center are located within secure environments controlled by a trusted third party. The trusted local clock may be located in an insecure environment. The trusted master clock is certified to be synchronized with an accepted time standard, such as a national time server. The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. Time stamps and certifications are signed by the issuing device using public key cryptography to enable subsequent authentication. The network operations center logs clock certifications and responds to requests for authentication of time stamps.

Inventors: van der Kaay; Erik H. (Corona del Mar, CA), Tyo; David (Yorba Linda, CA), Robinson; David (San Jose, CA), Dowd; Gregory L. (San Jose, CA)

Assignee: Datum, Inc. (Irvine, CA)

Family ID: 32909224

Appl. No.: 09/510,408

Filed: February 22, 2000

Related U.S. Patent Documents

<td< td=""></td><td< td=""></td><

<u>Application Number</u>	<u>Filing Date</u>	<u>Patent Number</u>	<u>Issue Date</u>
338074	Jun 23, 1999		

Current U.S. Class:	380/241 ; 380/239; 380/36; 713/159; 713/172; 713/178; 713/185
Current CPC Class:	G06F 21/725 (20130101); G06Q 30/06 (20130101); H04L 63/12 (20130101); H04L 63/123 (20130101); H04L 63/0823 (20130101); G06F 2221/2115 (20130101); G06F 2221/2151 (20130101); H04L 2463/121 (20130101); H04L 63/126 (20130101); H04L 2463/102 (20130101)
Current International Class:	G06F 21/00 (20060101); G06Q 30/00 (20060101); H04L 29/06 (20060101); H04N 007/167 ()
Field of Search:	;380/239,241,36 ;713/159,172,178,185

References Cited [Referenced By]

U.S. Patent Documents

<u>4709347</u>	November 1987	Kirk
<u>4816989</u>	March 1989	Finn et al.
<u>5001752</u>	March 1991	Fischer
<u>5027297</u>	June 1991	Garitty et al.
<u>5136647</u>	August 1992	Haber et al.
<u>5323315</u>	June 1994	Highbloom
<u>5386542</u>	January 1995	Brann et al.
<u>5422953</u>	June 1995	Fischer
<u>5444780</u>	August 1995	Hartman, Jr.
<u>5500897</u>	March 1996	Hartman, Jr.
<u>5504878</u>	April 1996	Coscarella et al.
<u>5689688</u>	November 1997	Strong et al.
<u>5745574</u>	April 1998	Muftic
<u>5748740</u>	May 1998	Curry et al.
<u>5768382</u>	June 1998	Schneier et al.
<u>5923763</u>	July 1999	Walker et al.
<u>6148082</u>	November 2000	Slattery et al.

Primary Examiner: Decady; Albert

Assistant Examiner: Jack; Todd

Attorney, Agent or Firm: Knobbe Martens Olson & Bear LLP

Parent Case Text

RELATED APPLICATIONS

This is a continuation-in-part application of a copending application entitled "System and Method for Providing a Trusted Third Party Clock and Trusted Local Clock," U.S. application Ser. No. 09/338,074, filed Jun. 23, 1999, which is hereby incorporated by reference.

Claims

What is claimed is:

1. A system for providing a source of time certified to be synchronized with an accepted standard, the system comprising:
 - a trusted master clock certified through a first certificate to be synchronized to the accepted standard, the trusted master clock maintained within a secure environment under control of a trusted third party;
 - a trusted local clock certified by the trusted master clock through a second certificate to be synchronized with the trusted master clock, the trusted local clock being a tamper-resistant device configured to be located in an insecure environment; and
 - a network operations center configured to provide verification information for verifying the certification of the synchronization of clocks within the system, the network operations center maintained within a secure environment under control of a trusted third party.
2. The system of claim 1, wherein the first and second certificates are cryptographically signed and wherein the first certificate and the second certificate can be the same certificate.
3. The system of claim 1, wherein the verification information comprises a public key of a clock.
4. The system of claim 1, wherein the trusted local clock is configured to provide trusted temporal tokens that cryptographically bind data to time.
5. The system of claim 4, wherein the verification information comprises an indication of the validity of a submitted trusted temporal token.

6. The system of claim 1, wherein the network operations center is further configured to receive certification information from the trusted master clock.

7. The system of claim 6, wherein the certification information comprises a time calibration certificate of a certified clock.

8. The system of claim 1, wherein the network operations center is further configured to log time calibration certificates.

9. A system for time stamping digital documents, wherein the time foot which the time stamp is derived is certified to be synchronized to an accepted standard the system comprising:

a trusted master clock certified to be synchronized to the accepted standard through a first cryptographically signed certificate, the trusted master clock maintained within a secure environment under control of a trusted third party;

a trusted local clock certified by the trusted master clock to be synchronized with the trusted master clock through a second cryptographically signed certificate, the trusted local clock configured to provide time stamps, the trusted local clock being a tamperresistant device configured to be located in an insecure environment; and

a network operations center configured to provide time stamp verification information, the network operations center maintained within a secure environment under control of a trusted third party.

10. The system of claim 9, wherein the verification information comprises a time calibration certificate of a certified clock.

11. The system of claim 9, wherein the verification information comprises a public key of a clock.

12. The system of claim 9, wherein the verification information comprises an indication of the validity of a submitted time stamp.

13. The system of claim 9, wherein the network operations center is further configured to log time calibration certificates.

14. A method of providing trusted temporal tokens, the method comprising:

maintaining a red master clock within a secure environment;

causing the trusted master clock to be certified through a first certificate as synchronized with a trusted time server;

certifying a trusted local clock through a second certificate to be synchronized with the

trusted master clock, the trusted local clock being configured to provide trusted temporal tokens, the trusted local clock being a tamper-resistant device configured to be located in an insecure environment; and

providing busted temporal token verification information in response to verification requests.

15. The method of claim 14, further comprising providing trusted temporal tokens through the trusted local clock in response to time stamping requests.

16. The method of claim 14, wherein the first and second certificates are cryptographically signed and wherein the first certificate and the second certificate can be the same certificate.

17. The method of claim 14, wherein the verification information comprises a public key of a clock.

18. The method of claim 14, wherein the verification information comprises an indication of the validity of a trusted temporal token.

19. The method of claim 14, wherein the verification information is provided by a network operations center, the network operations center being maintained within a secure environment.

20. The method of claim 14, further comprising logging the certifications of the clocks.

21. The method of claim 14, further comprising logging the number of trusted temporal tokens issued by the trusted local clock.

22. The method of claim 14, further comprising billing a client based on the number of temporal tokens issued to the client.

23. The method of claim 14, further comprising billing a client in exchange for certifying the synchronization of the trusted local clock.

24. A system for providing time certified to be synchronized with a trusted source, the system comprising:

a trusted clock configured to provide time, the trusted clock certified through a chain of at least two signed certificates to be synchronized to the trusted source, wherein each of the signed certificates certifies that two clocks are synchronized; and

a verification module configured to provide verification information for verifying the synchronization of the trusted clock with the trusted source, wherein the verification module provides the verification information based at least upon the chain of signed certificates.

25. The system of claim 24, wherein the signed certificates are digitally signed.
26. The system of claim 24, wherein the signed certificates are cryptographically signed.
27. The system of claim 24, wherein the verification information comprises at least one of the signed certificates.
28. The system of claim 24, wherein the verification information comprises the signed certificates.
29. The system of claim 24, wherein the verification information comprises an indication that the trusted clock has been certified to be synchronized to the trusted source.

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to methods and systems for providing and verifying a trusted source of certified time, and, more particularly, the invention relates to digitally time stamping electronic documents wherein the time stamp can be validated and verified as synchronized with an accepted standard.

2. Description of the Related Art

Electronic Commerce (e-commerce) is a rapidly expanding aspect of the economic world and demands the use of Electronic Commerce transactions. Such transactions, however, have outgrown the policies and controls that regulate traditional Paper Commerce. For example, a paper document can be typed, signed in ink, and mailed through the post office. The post office can then affix a time stamp and receipt at the destination. There are long standing legal and accounting policies that authenticate this type of transaction. When an electronic document is sent between two computers, however, it does not leave behind the same degree of tangible evidence. Even if the electronic document is stored in a computer's memory, the contents, signature, and time stamp can be manipulated by anyone with access to the computer.

Accounting and legal regulatory bodies are currently developing and mandating Electronic Commerce certification processes to provide reliable authentication for electronic transactions much like those available for paper transactions. Many of the certification processes depend on the creation of a digital signature using public key cryptography that authenticates the "Who," "What," and "When" of a document.

Public key cryptography was developed in the 1970s to solve problems involved with symmetric key cryptography. In public key cryptography systems, two corresponding keys are generated. One key, called a private key, is held privately by the keyholder. A second key, called a public key, is published openly for anyone that wants to secretly communicate with the keyholder or verify the authenticity of messages sent by the keyholder. Because the sender and the receiver use different keys, public key cryptography is also known as asymmetric key cryptography.

To send a secret message with public key cryptography, an entity "A" encrypts a message using the public key of an entity "B." "A" then transmits the encrypted message to "B." "B" decrypts the encrypted message with "B"'s corresponding private key. Since the message encrypted with "B"'s public key can only be decrypted with the corresponding private key, held only by "B," the privacy of the communication is ensured.

To authenticate the content and origin of a message, "A" uses a one-way hash function to create a message digest. A message digest is a fixed length data element that uniquely represents the source message. Since the hash function is one-way, nothing about the content of the source message can be inferred from the message digest. For example, two message digests from two messages that differ by only one character would appear to be a completely random reordering of characters. "A" then signs the message by encrypting the digest using "A"'s private key. The signature is typically appended to the message itself. "A" then transmits the signed message to "B." In order to authenticate the received message, "B" uses the same one-way hash functions used by "A" to create a message digest from the received message. "B" then decrypts the encrypted digest using "A"'s public key. If the decrypted digest matches the digest created from the received message, then the received message must be the identical message from which the decrypted digest was originally derived. Furthermore, that the decrypted digest was decrypted using "A"'s public key ensures that the decrypted digest was originally encrypted with "A"'s private key. The successful matching of digests, therefore, ensures that the message received by "B" is the identical message signed by "A."

Encrypting a message itself establishes secrecy. Signing a message provides for message authentication and establishes the "who" and "what" of a message. Encryption and signatures can also be combined by encrypting a message before creating a message digest and signature. By combining encryption and signatures, secret, authenticatable communications can be accomplished.

A very significant attribute of public key cryptography is that there is no need to share a secret key or to transmit a secret key from the keyholder to a proposed communication partner. It is, however, necessary to establish credibility for who owns public and private keys. For instance, "C" could claim to be "A" and send a message to "B." To prevent being fooled, "B" needs to be sure that "A"'s public key, is in fact paired with the private key owned by a real "A." A Certification Authority (CA) solves this problem. (Note: The use of the word "certification" in certification authority relates to the association of public keys with particular owners and is distinct from the concept of a Time Calibration Certificate (TCCert), as used herein, which relates to the certification of a clock as

synchronized with an accepted standard.) CAs provide digital certificates which contain public keys and are used to transmit the public keys in a secure, authenticated manner to participants in e-commerce transactions.

In addition to the cryptographic techniques and digital certificates provided by CAs, security and authentication of transactions is also supported by an extensive body of protocol standards. It is necessary for "A" to format messages, signatures, message digests, etc., with protocols that can be recognized by "B." Cryptography, digital certificates, protocols, and standards together make up what is termed the Public Key Infrastructure (PKI). With PKI, one can easily guarantee the "who" and "what" of a transaction.

"When" is a measure of the time at which an event occurred and is a concept easily taken for granted. A worldwide system of time standardization is in operation. Each country that is signatory to the Treaty of the Meter maintains a National Timing Laboratory (NTL), which houses the local country's standard time clock. These clocks are kept synchronized to the world standard of time maintained in Paris, France. The world standard for commercial time is Coordinated Universal Time (UTC). In the United States, Congress has mandated that official United States "time" follow the clock maintained by the National Institute of Standards and Technology (NIST), located in Boulder, Colorado. This standard is referred to as UTC-NIST. Any time stamp for a transaction that must survive technical, auditing, or legal scrutiny must be made by a clock that is synchronized to UTC-NIST, and the synchronization process must be "traceable." Throughout this document, reference is made to UTC-NIST but the invention described is applicable to operation in any country and with standard time clocks maintained by any country's respective national timing laboratory.

The use of "traceable" clocks in paper commerce has been sufficient to provide the "when" of ordinary paper transactions. While there have been numerous cases of falsification of dates on paper documents, the risk to commerce has been relatively small. In the case of e-commerce, however, falsification of dates creates a much greater risk because it is possible to invade computer-directed processes and effect fraud on a very large scale. Such computer crimes frequently involve falsification of electronic time stamps; and for this very reason, protection of the electronic clocks that generate those time stamps from tampering is a high priority in Electronic Commerce.

Current network procedures provide for the synchronization of all workstation clocks in a network. NIST and other agencies provide network time servers that have clocks traceable to UTC-NIST. Client workstations can synchronize their time with the network time servers through a common protocol. The Network Time Protocol (NTP) is commonly used in TCP/IP networks such as the Internet, but other protocols are also used.

Unfortunately, once a local workstation clock is synchronized to the network time server, its time may be subject to manipulation regardless of the reliability of the source network time server. Thus far, little work has been done to ensure that the source of the time used

to generate time stamps can be trusted. Today, the majority of applications utilizing time stamps simply use the system clock from their host system. Procedures for setting or offsetting a system clock are commonly known. Thus, there is no inherent trust in a system clock in a conventional system.

Attempts to overcome this problem include time stamp sequencing wherein the time stamp incorporates information regarding the order in which documents are time stamped in relation to other time-stamped documents. (See, for example, U.S. Pat. No. 5,136,647 to Haber et al.) Other attempts to overcome the problem incorporate the use of other time sources such as NTP or Global Positioning System (GPS). While these attempts are significant improvements over using the system clock, the improvements still fall short of fitting into the trust models required for electronic business today.

Still other systems employ the use of certified time that is maintained by a trusted third party's system located outside the local network. The trusted third party system remains synchronized with UTC-NIST through a common protocol. The local network application server then establishes communication with the third party's system whereby a data object (document or message digest) is sent to the third party system where a "time stamp" is affixed to the data object, either in clear text or in cryptographically embedded text. Such a system may be impractical, however, considering the need for external communication for each instance of time stamping, especially when many time stamps are required by the local network.

Another system introduces a local clock into the local network, thus avoiding the problems associated with obtaining time stamps from an outside source. The local clock must be periodically synchronized with a UTC-NIST traceable clock. In order to avoid frequent certification and calibration between the local clock and the UTC-NIST traceable clock, the local clock is advantageously a cesium atomic clock. Cesium atomic clocks are commercially available and their frequency, and hence time, is derived from an atomic phenomena caused by the energy difference of certain cesium atom electron orbits. Thus, as long as the cesium atomic clock is operating, it will be accurate enough to satisfy most practical applications. Such clocks only lose one second in 30,000 years of normal operation. For this reason, cesium atomic clocks are termed "primary reference sources." Unfortunately, when used locally, there is still the possibility that the time value in the clock could, through system malfunction or intentional manipulation, be altered to an incorrect value that would not be apparent to a user.

Trusted time, in the context of the present invention, is time that is certified to be traceable to the legal time source for the application in which it is being used. The legal time source for commercial applications operating in the United States, as legislatively mandated by Congress, is the National Institute of Standards and Technology (NIST). The infrastructure for providing trusted time must provide a strong trust model, including a certification log for auditing and to prevent repudiation at a later date.

The need for trusted time has become recognized over the last two years as marked by the launch of standardization activities in the The Internet Engineering Task Force (IETF). In

addition, most Certification Authority (CA) product and service vendors have announced development activities and new products in this area. The present disclosure describes a Trusted Time Infrastructure (TTI) that meets the requirements for providing trusted time. The present disclosure also shows how the TTI fits in with the trust models and cryptographic standards that have been developed to ensure that secure and legally binding electronic transactions can take place today.

SUMMARY OF THE INVENTION

A Trusted Time Infrastructure (TTI) system provides time stamps, in the form of trusted temporal tokens, for electronic documents from a local source. A preferred embodiment of the system comprises a trusted master clock, a trusted local clock, and a network operations center. The trusted master clock and the network operations center are located within secure environments controlled by a trusted third party. The trusted local clock may be located in an insecure environment. The trusted master clock is certified to be synchronized with an accepted time standard, such as a national time server. The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. Time stamps and certifications are signed by the issuing device using public key cryptography to enable subsequent authentication. The network operations center logs clock certifications and responds to requests for authentication of time stamps.

The delivery of trusted time by the trusted local clock is ensured by: (1) the physical security of the devices in the system; (2) authentication of communications between the devices in the system; (3) the link of certifications through which time can be traced to an accepted standard; and (4) the specified accuracy of clocks within the system.

In an alternative embodiment, each issued time calibration certificate incorporates the time calibration certificate of the issuing clock. The time calibration certificate of the trusted local clock is then incorporated into the issued trusted temporal tokens. Accordingly, the chain of certifications from which trusted time is derived from an accepted source is incorporated into each trusted temporal token.

In another embodiment, the system provides a local source of trusted time through a trusted local clock. In still another embodiment, methods of billing clients are based upon the number of trusted temporal tokens issued or, alternatively, based upon the number of clock certifications performed. Billing features of the system support the billing methods. These and other aspects of the present invention will be further described in the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiments of the present invention are described below in connection with the drawings in which like reference numbers represent corresponding components throughout, and in which:

FIG. 1 illustrates the four principal levels of the global timing hierarchy;

FIG. 2 illustrates a schematic of the key components of a preferred embodiment of the TTI and the key transactions between these components;

FIG. 3 illustrates a functional block diagram of the Network Operations Center;

FIG. 4 illustrates one embodiment of a TTI system including a network of clocks and applications;

FIG. 5 illustrates an overview of the process by which a preferred embodiment of the TTI system generates trusted temporal tokens;

FIG. 6 illustrates a preferred embodiment of the process by which an upper clock certifies the time of a lower clock;

FIG. 7 illustrates a preferred embodiment of the process by which trusted temporal tokens are generated by a Trusted Local Clock; and

FIG. 8 illustrates a process by which an application can verify the authenticity of a trusted temporal token.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following description, reference is made to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention. Where possible, the same reference numbers will be used throughout the drawings to refer to the same or like components. Numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be understood by one skilled in the art that the present invention may be practiced without the specific details or with certain alternative equivalent devices and methods to those described herein. In other instances, wellknown methods, procedures, components, and devices have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

1. Global Timing Hierarchy

As illustrated in FIG. 1, the global timing hierarchy has four principal levels:

1. International Timing Authority (BIPM) Layer
2. National Timing Authority (NTA) Layer
3. Timing Distribution Layer

4. Application Layer

The Trusted Time Infrastructure (TTI) provides a system for commercial or private timing distribution services to deliver to the application layer a "trusted temporal token" or "trusted time stamp" that cryptographically binds the current time of day derived from the NTA to a unique data request submitted by an application. Such a request may be made in response to events, transactions, or document submittals. public key digital signatures are preferably used as the binding mechanism to ensure the identity of the time distribution service and to protect the temporal token from undetected manipulation.

The time delivered by the TTI is preferably Universal Coordinated Time (UTC). The means by which the NTAs synchronize their UTC clocks (e.g., UTC(NIST)) with the International Bureau of Weights and Measures (BIPM) in France is outside of the scope of this disclosure. However, the UTC delivered by most of the major NTAs can be expected to be within nanoseconds of UTC (BIPM), while any of the other NTAs are still within microseconds of UTC (BIPM). Thus, for trusted time applications, where time is typically certified to be accurate to within 100 milliseconds at the application layer, the choice of which NTA to use is a legal issue for a particular country and not one of accuracy.

2. Trusted Time Infrastructure (TTI)

FIG. 2 illustrates a schematic of the key components of a preferred embodiment of the TTI and also illustrates the key transactions between these components. The embodiment of FIG. 2 comprises an NTA Trusted Time Server (NTTS) 202, a Trusted Master Clock or Trusted Third Party Clock (TMC) 204, a Network Operations Center (NOC) 210, a Trusted Local Clock (TLC) 206, and an application 208. Although only one instance of each component is depicted in FIG. 2 for instructive purposes, numerous instances of each element may be present in an actual TTI system.

2.1 Secure Communication Through Public Key Infrastructure (PKI)

The various elements in the TTI system communicate securely using PKI. Although PKI is often used to encrypt confidential communications, PKI can also be used to verify the origin of a communication through digital signatures. In the TTI system, the privacy of the communication between elements is generally not an issue. Instead, it is the authenticity of the communication that is generally of concern.

PKI authentication supports two aspects of the TTI system. First, PKI authentication supports authentication of communications between elements in the TTI system in order to maintain the integrity of the system as a whole. For example, if a Trusted Master Clock (TMC) 204 communicates with a Trusted Local Clock (TLC) 206 in order to certify its time calibration, the TMC 204 must know for sure the identity of the TLC 206 that it is certifying. In another example, if a TMC 204 notifies the Network Operations Center (NOC) 210 of a time calibration certification of a TLC 206, the NOC 210 must be able to

authenticate the identity of the certifying TMC 204. In an additional example, if a TMC 204 is capable of adjusting the time of a TLC 206, the TLC 206 must be able to verify that it is indeed a valid TMC 204 that is adjusting its time. In accordance with this first aspect, trusted temporal tokens preferably include the signed time calibration certification of the certifying clock. The NOC 210, through its PKI authentication capabilities, provides a system through which trusted time can be traced to the NTA Trusted Time Server (NTTS) 202 from any TLC 206 through authenticated time calibration certifications. In other words, the source of time from which a trusted temporal token has been derived can be traced back through signed time certifications to the NTTS 202.

A second aspect in which PKI authentication supports the TTI system is in authentication of temporal tokens themselves. The trusted temporal token includes a signed concatenation of a digest of the message to be time stamped as well as the time calibration certification of the issuing TLC 206. This signed concatenation allows the authenticity of the temporal token itself to be verified as being unaltered and issued by a particular TLC 206.

2.2 Key System Elements

2.2.1 Trusted Time Server

The NTA Trusted Time Server (NTTS) 202 is the highest level clock in the TTI and is preferably located in a secure environment under government control. The NTTS 202 is the source of legal time from which the TTI derives its trusted time. The secure environment should be accessible only to trusted agents of the government timing authority (e.g. NIST), in order to ensure the integrity of the NTTS 202. The NTA is responsible for monitoring the accuracy of the NTTS-produced time and the operation of the NTTS 202 itself.

The NTTS 202 is responsible for measuring the clock offsets of the TMC 204 units. The NTTS 202 preferably performs this measurement over the Public Switched Telephone Network (PSTN). To measure the clock offsets of the TMCs, the NTTS 202 preferably supports a variant of Network Time Protocol (NTP) called Secure NTP (SNTP). NTP has been in use as a standard Internet Protocol since the early 1980s. SNTP is currently before the IETF as a draft protocol. It differs from NTP primarily in the establishment of a more robust authentication scheme based on more modern PKI techniques. For redundancy, two NTTS units are preferably located at the NTA, preferably at geographically separate locations.

2.2.2 Trusted Master Clock

The Trusted Master Clock (TMC) 204 is an intermediary clock that serves to pass a trusted source of time from the NTA Trusted Time Server (NTTS) 202 to the Trusted Local Clock (TLC) 206 where the trusted time is actually used. The TMC 204 is preferably a stand-alone server located in a secure environment under the control of a trusted third party. This trusted third party can be the entity or organization implementing

the whole TTI system or part of the TTI system. Again, the secure environment is preferably accessible only to trusted agents of the trusted third party to prevent tampering with the TMC 204.

Only one TMC is illustrated in FIG. 2 for teaching purposes. Typically, however, the TTI network will contain a minimum of two TMCs. In some configurations, two or more TMCs may be linked in series between the NTTS 202 and the TLC 206. These and other configurations will be shown below.

The TMC 204 preferably comprises a Rubidium oscillator; a GPS receiver for monitoring the oscillator; cryptographic hardware; and a timing engine that generates trusted time. Each TMC 204 has a set of TLCs that it is responsible for time certifying. These sets of TLCs will be assigned by the Network Operations Center (NOC) 210. Preferably, the NOC 210 will ensure that at least two TMCs will be assigned to each TLC. This structure ensures sufficient redundancy so that the failure of a single TMC will not affect the operation and trust of the TLCs. It should be understood that a non-redundant configuration can be advantageously used when redundancy is not a concern.

The TMC 204 preferably uses the NT operating system configured for enhanced security. The TMC housing is designed to meet NIST Federal Information Processing Standard (FIPS) 140-1 Level 3 physical protection and tamper detection requirements (FIPS 140-1 is titled "Security Requirements for Cryptographic Modules"). Cryptographic calculations, including key generation, are performed by dedicated hardware. In the preferred embodiment, the private signing key of the TMC 204 is never exported from the cryptographic card. The cryptographic device also contains a high quality random number generator that can be used to generate new PKI key pairs. Sensitive cryptographic information is preferably contained in battery-backed memory, which will be erased in the event of a tamper alarm. The TMC 204 is preferably designed to receive a NIST validation rating of FIPS 140-1 Level 1 overall and Level 3 for physical security.

Audit trails are created for all TMC events, including all operator actions (logs include operator IDs), alarms, time certifications, and all remote NOC communications. These logs are digitally signed to prevent (by detection) subsequent forgery or alteration. The TMC 204 will typically include a GPS receiver that can be used to initialize the TMC 204 and to monitor the health of the TMC 204. If any abnormalities are detected in the TMC time source, the TMC 204 goes off line, attempts to isolate the problem, and shuts down.

The TMC 204 uses Secure NTP (SNTP) and User Datagram Protocol (UDP) to access each of its assigned TLCs periodically to measure its time offset. If the time of TLC 206 is within a certain offset (typically 100 ms) from the NTTS 202, the TMC 204 certifies the TLC 206 to be within that offset. The TMC 204 may also send small time corrections to the TLC 206 that can be used to make adjustments to the TLC 206 clock to keep it within specification. If a TMC 204 finds that a TLC 206 has a valid, recent Time Calibration Certificate (TCCert) then it takes no action.

2.2.3 Network Operations Center

The Network Operations Center (NOC) 210 serves as the central control facility for the TTI system. The NOC 210 is preferably located in a secure environment under the control of a trusted third party.

FIG. 3 illustrates a functional block diagram of the NOC 210. The NOC 210 communicates with the various elements of the TTI through a communications network 302. The communications network 302 may comprise the Public Switched Telephone Network (PSTN), the Internet, and/or other computer networks. A firewall 304 protects the internal systems of the NOC 210 from external attack through the communications network 302. The NOC 210 comprises an element manager 306, which is a configuration and maintenance system that has the ability to remotely configure and monitor the NTTS 202, TMCs 204, and TLCs 206 using a secure management protocol. In addition, the NOC 210 comprises a central database 308 that is used to store all TMC and TLC time certification logs.

The NOC 210 also comprises a web server 310 that handles temporal token verification requests sent via the World Wide Web. The web server 310 interfaces with the element manager 306 to initiate a verification action and to return the response to the requester. The web server 310 preferably uses Secure Sockets Layer (SSL) with server authentication in order to encrypt and authenticate the server data exchanged between the client and the server. The NOC 210 further comprises a billing system 312 for trusted time service subscribers. The billing system 312 logs data regarding the number of tokens issued by a TLC 206.

The NOC 210 comprises three additional functional components that implement the PKI authentication capability of the TTI system. The Registration Authority (RA) 312 associates each device in the TTI system with a name. In this manner, TTI devices can be identified, monitored, and controlled. The Certification Authority (CA) 314 associates a public key with each device using the name of the device provided by the RA 312. The Online Certificate Status Protocol (OCSP) responder 316 responds to requests for digital certificates for devices in the TTI system. The OCSP responder 316 serves as a trusted source of digital certificates. Digital certificates provide a data structure associating a public key with a signing device and allow verification/authentication of the signed communications of TTI devices. Since the NOC 210 knows all elements comprising the TTI, the NOC 210 acts as an RA 312 to the CA 314 for the issuance of digital certificates to the TTI elements. The TTI preferably uses ITU-T X.509v3 digital certificates. Each element within the TTI preferably has a distinguished name so that it may be uniquely identified. The name structure is preferably aligned with the International Telecommunications Union--Telecommunication Standardization Sector (ITU-T) X.501/X.520 standards for distinguished names. The use of an RA, a CA, and an OCSP responder is known in the art and information regarding this topic is available from entities such as the IETF (Internet Engineering Task Force).

The NOC 210 preferably also comprises a billing system 318 that interacts with the element manager 306 and the database 308 in order to assemble client billing

information. A number of different billing schemes will be discussed in the section on billing below.

2.2.4 Trusted Local Clock

The Trusted Local Clock (TLC) 206 provides trusted time, preferably in the form of a trusted temporal token, to the application 208 on request. The TLC 206 is hosted in a customer-owned server and is preferably a PCIV2.1 compliant card that is tamper-resistant and is assumed to be operating in an insecure host in an insecure environment.

The TLC 206 comprises an oscillator and a timing engine, which generates trusted time. A Time Calibration Certificate (TCCert) typically has a period during which it is valid. The range of accuracy specified by the TCCert during the valid period accounts for the accuracy of the TLC's oscillator and timing engine. The TCCert therefore, serves as assurance of the accuracy, during the valid period, of the certified clock.

The TLC 206 preferably uses a real time operating system to control the on-card functions. The TLC 206 preferably has its own Ethernet TCP/IP connection for communications with the TMC 204 and NOC 210.

Cryptographic calculations in the TLC 206 are preferably performed using a dedicated hardware PCMCIA (Personal Computer Memory Card International Association) cryptography engine. This cryptographic device preferably also contains a high quality pseudorandom number generator. Key generation is performed on the PCMCIA device. The private key for the TLC 206 will preferably never be exported from the PCMCIA cryptography engine. Sensitive cryptographic information is contained in battery-backed memory that is preferably erased in the event of a tamper alarm. The TLC 206 preferably has a NIST validation rating of FIPS 140-1 Level 1 overall and Level 3 for physical security. Audit trails are preferably created for all TLC events, including all operator actions (logs include operator IDs), alarms, time certifications performed, temporal tokens issued, and all remote NOC 210 communications. These logs are digitally signed to prevent (by detection) subsequent forgery or alteration.

Like the TMC 204, the TLC 206 can include a GPS receiver to initialize the TLC 206 and to monitor the health of the TLC 206. If any abnormalities are detected in the TLC time source, the TLC 206 goes off line, attempts to isolate the problem, and shuts down.

2.2.5 Application

The application 208 is any process or device that requests trusted temporal tokens from the TLC 206. The application 208 can run on the same server that hosts the TLC 206 or the application 208 can run on any other machine in communication with the host server. The application 208 can request verification of a time stamp through the NOC 210. Alternatively, a time stamp obtained by an application 208 can be passed to another application. The other application can then perform the verification of the time stamp through the NOC 210.

Client applications 208 access the TLC 206 using a Trusted Time Application Program Interface (TTAPI). The TTAPI will communicate with its associated TLC 206 using the Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol. Server applications co-located with a TLC 206 access the TLC 206 using a Trusted Local Clock Application Program Interface.

2.3 TTI System FIG. 4 illustrates one embodiment of a TTI system 400 including a network of clocks and applications. The system 400 comprises two NTTs 202A-B for redundancy, preferably located in separate locations. Two TMCs 204A-B are directly certified by the NTTs. The TMC 204A directly certifies a TLC 206A, while the TMC 204B directly certifies a TLC 206D. The TMC 204A also certifies another TMC 204C, which in turn certifies a TLC 206B, and similarly TMC 204B certifies TMC 204D, which in turn certifies TLC 206C. As illustrated, time certification logs are passed from the TLCs 206 up to the highest level TMCs 204 and then on to the NOC 210.

In the case that any clock fails, the device below that clock in the TTI can request service from an alternate clock. If the NTTS 202A fails, for example, the TMC 204A can request certification from the NTTS 202B. Similarly, if the TMC 204A fails, the TLC 206A and the TMC 204C can request certification from the TMC 204B.

Applications 208A, 208B, and 208C request trusted time tokens from their respective TLCs. Upon receiving trusted time tokens, the applications then can route verification requests to the NOC 210.

2.4 Application Bounded Time Service

Another embodiment of the TTI system or a portion thereof may be configured as an application bounded time service. In application bounded time service, trusted time is provided to a specific application offered by a single third party. For example, if Company X wants to sell certified e-mail gateway servers, each equipped with a TLC, the TLCs will be synchronized by TMCs operated by Company X. Company X's TMCs in turn are certified by TMCs of a trusted third party. Depending on the particular application, application bounded time service may require a separate NOC.

3. Calibration and Certification

This section describes how clock calibration and certification is performed in the TTI. Individual timing elements in the TTI are enabled for operation when they possess a Time Calibration Certificate (TCCert). In the preferred embodiment, TLCs cannot issue trusted temporal tokens unless they have been issued a valid TCCert. Also in the preferred embodiment, a TMC cannot certify a lower clock unless the TMC has been issued a valid TCCert.

After measuring the calibration of a lower clock, an upper clock issues a TCCert to the lower clock to certify that the time of the lower clock is within a certain tolerance with

respect to the upper clock. The upper clock signs the TCCerts to assure authenticity.

3.1 Procedural Overview

FIG. 5 illustrates an overview of the process by which a preferred embodiment of the TTI system generates trusted temporal tokens. The steps illustrated in FIG. 5 are also depicted by the arrows between elements in FIG. 3.

At a first step 502, the NTTS 202 certifies a TMC 204, sends a TCCert to the TMC 204, and records the certification locally. The TMC 204 then sends the TCCert to the NOC 210 for logging at a step 504. At this point, the TMC 204 possesses a valid TCCert and is capable of time certifying other lower clocks. At a step 506, the TMC 204 time certifies a TLC 206, sends a TCCert to the TLC 206, and records the certification. The TMC 204 also retrieves from the TLC 206 the number of trusted temporal tokens that the TLC 206 has issued since the last certification. This number is preferably used for billing purposes. At a step 508, the TMC 204 sends the TCCert and the token count of the TLC 206 to the NOC 210 for logging.

Once the TLC 206 has been certified, the TLC 206 is ready to issue trusted temporal tokens under its new TCCert. At a step 512, an application requests and the TLC 206 issues a new trusted temporal token. At a step 514, the application verifies the authenticity of the temporal token through the NOC, possibly at a future date.

3.2 TCCERT Generation

FIG. 6 illustrates a preferred embodiment of the process by which an upper clock certifies the time of a lower clock, as in steps 502 and 506 of FIG. 5. In the context of this illustration, an upper clock is intended to represent the NTTS or a TMC, while a lower clock is intended to represent another TMC or a TLC that is further down the chain of trusted time from the NTTS than the upper clock. When a higher level clock measures the offset of a lower clock and finds it within specification, a TCCert is created to record this determination. At a step 602, the lower clock creates a TCCert Request (TCCertReq) which preferably comprises:

Upper Clock ID;

Lower Clock ID;

Lower Clock Accuracy;

Lower Clock Signature Parameters; and

Lower Clock Signature (across above fields).

The lower clock then sends the TCCertReq to the upper clock. At a step 604 the upper clock receives the TCCertReq from the lower clock. The upper clock validates the

signature of the lower clock and verifies that the lower clock ID is correct at a step 606. At a step 608, the upper clock measures the time offset of the lower clock using Secure NTP (SNTP).

The upper clock determines whether the offset of the lower clock is within acceptable limits at a step 610. If the lower clock is within acceptable limits, control passes to a step 614. At the step 614, the upper clock calibrates or adjusts and again measures the offset of the lower clock if necessary. At a step 616, the upper clock creates the TCCert by appending preferably the following fields to the TCCertReq:

TCCert Time;

Class of Service ID;

Lower Clock Offset;

TCCert Accuracy;

TCCert Expire Time;

Delay;

TCCert of Upper Clock (optionally); and

Upper Clock Signature Parameters.

To create the final TCCert, the upper clock appends its digital signature across the TCCertReq and the above-appended fields. By optionally including the TCCert of the upper clock in the TCCert of a lower clock, the complete trace of trusted time from the NTTS down to the lowest level can be encapsulated in each TCCert. At a step 618, the upper clock stores and records the TCCert and sends the TCCert to the lower clock.

If, at step 610, the time of the lower clock is found to be out of acceptable limits, it is possible that the clock has failed or has been tampered with. In this case, control passes to step 612. At step 612, the field TCCert Time is set to an illegal value, and the field Class of Service ID is set to "Out of Calibration." If a lower clock has been found to be out of calibration, any TCCerts or trusted temporal tokens issued by the lower clock since its last TCCert issuance should be considered suspect. Accordingly, the NOC 210 should be notified of the out of calibration measurement so that its database can reflect the invalidity of the previous TCCert and any trusted temporal tokens derived from it. If the NOC 210 has been notified of the out of calibration measurement, control is optionally passed back to step 614 for recalibration and recertification of the lower clock.

3.2.1 NTTS to TMC Calibration

The NTTS measures the clock offsets of the TMCs using PSTN connections and the

SNTP protocol preferably once per day. The TMC clock offsets are expected to be within 10 milliseconds of UTC as provided by the NTTS. For successful clock offset measurements, the NTTS returns a TCCert indicating the TMC is enabled for time calibration of lower clocks. The NTTS TCCert Expiration Date is preferably seven (7) days from the date of TCCert issuance. In order to keep the NTA implementation simple, an NTA-level CA may not be used. Therefore, the NTTS may not explicitly verify the validity of the TMC certificates that it receives via SNTP with the respective CAs that produced them. Rather, the NTTS simply verifies that the received certificate matches the one that was loaded in its internal database during initialization for that timing service. Should a certificate be received via SNTP that is not in the NTTS database, the NTTS will log an error message with the received certificate and will refuse the connection.

The NTTS preferably logs all clock offset measurement information to paper. The printed records preferably contain the following information:

UTC Time of Calibration;

Trusted Master Clock Name;

Measured Offset;

NTTS Certificate Serial Number; and

Trusted Master Clock Certificate Serial Number.

3.2.2 TMC to TLC Calibration

Each TMC has a set of TLCs that it is responsible for certifying. Using SNTP, each TMC contacts each of the TLCs in its set once per day and requests its TCCert. If the received TCCert is less than 24 hours old, the TMC skips certification of that unit, closes the SNTP session and moves on to query the next TLC on its list. If the received TCCert is equal to or greater than 24 hours old, the TMC measures the TLC's time offset, computes the time correction, and sends this correction to the TLC clock to keep it within specification. The offset is again measured, and if the TLC clock is within specification, the TMC issues a TCCert to the TLC stating that it is within a certain offset from UTC. It is expected that the TMC will certify the TLC to be within 100 ms of UTC.

3.3 Trusted Time Guarantee

The preferred embodiment of the TTI system combines a number of aspects to guarantee that the time stamp on a trusted temporal token has been derived from a source of time that is synchronized with an accepted standard, or that the TTI system provides "trusted time." The first aspect is that the physical devices of which the TTI system is comprised are either located in physically secure, trusted, facilities, or are designed to be physically tamper proof. The second aspect is that communications between elements in the TTI system are authenticated, and, if necessary, encrypted using the PKI system. The third

aspect is that the time maintained by a TLC can be linked, through certifications using SNTP calibrations of a chain of trusted clocks, all the way to the NTTS or to another commonly accepted source of time. The fourth aspect is that each clock to be certified is specified to maintain at least a certain accuracy over the duration of a valid TCCert. Accordingly, each TCCert can guarantee that the certified clock's time will be within its specified accuracy during the valid period of its TCCert plus the possible temporal variations introduced by the variations due to the accuracy of the foregoing certifying clocks during the valid periods of their respective TCCerts.

4. Trusted Temporal Token Generation and Verification

Once a TLC 206 has a valid TCCert, the TLC 206 is capable of issuing valid trusted temporal tokens. The tokens preferably include a concatenation of the data to be time-stamped and a time stamp supplied by a trusted source of time, in this case, the internal clock of the TLC 206. The signing of the complete message by the TLC 206 functions to bind the data to the time stamp such that the time stamp cannot be altered without detection.

Once a token is generated, it is retained to the requesting application. The requesting application can then verify the authenticity of the token. In addition or in the alternative, the application may pass the token on to another application that may choose to verify the token again in the future.

An application can confirm the authenticity of the token by (1) checking with the NOC 210 that the issuing TLC 206 was in possession of a valid TCCert at the time of token issue, and (2) verifying the signature of the token by obtaining, preferably from the NOC 210, a digital certificate containing the corresponding public key of the TLC 206.

4.1 Token Generation

FIG. 7 illustrates a preferred embodiment of the process by which trusted temporal tokens are generated by a TLC 206. At a first step 702, an application 208 sends a request, including the data to be time stamped, to the issuing TLC 206. The data, in most cases, will comprise a digest, created by a one-way hash function, of the electronic document to be time stamped. At a step 704, the TLC 206 receives the data and concatenates the data with the current time with a TCCert Log Pointer (typically an upper clock ID, a lower clock ID, and the time of the TCCert). The TLC 206 then signs the concatenation to form the trusted temporal token. In an alternative embodiment, the TCCert itself is included rather than the TCCert Log Pointer. At a step 706, the TLC 206 returns the trusted temporal token to the application 208. Thereafter, the TLC 206 increments its internal log of the number of tokens issued for billing purposes. The number is subsequently transmitted, either directly or through a TMC 204, to the NOC 201 for processing and billing.

4.2 Token Verification

FIG. 8 illustrates a preferred embodiment of the process by which an application can verify the authenticity of a trusted temporal token. At a first step 802, the application connects to and authenticates the identity of the NOC 210. Next, the application sends a verification request, including the token to be verified, to the NOC 210 at a step 804. The NOC 210 maintains a database of all of the TCCerts of all of the clocks in the TTI system. In addition, the NOC 210 either includes or has access to the CA for all of the TTI elements. The CA is the source of digital certificates through which the signatures of the TTI elements can be verified.

From step 804, the preferred embodiment of the present process proceeds to a step 806. At the step 806 the NOC 210 determines the authenticity of the submitted token using the TCCerts in its database and the digital certificate associated with the issuing TLC 206. At a subsequent step 808, the NOC 210 supplies a signed verification notification, indicating the status of the submitted token, to the requesting application.

In an alternative embodiment, the process proceeds to a step 810 from the step 804. At the step 810, the NOC 210 determines whether the issuing TLC 206 was in possession of a valid TCCert. If so, the NOC 210 supplies a digital certificate of the issuing TLC 206 to the requesting application at a step 812. At a step 814, the application confirms the authenticity of the token using the digital certificate to verify the token's signature. If, at step 810, the NOC determines, by checking its databases, that the issuing TLC 206 did not possess a valid TCCert or that the TCCert is suspect, the process proceeds to step 816. At step 816, the NOC 210 sends notification to the requesting application that the token cannot be authenticated.

5. Security Schemes

A number of different schemes can be used in conjunction with the disclosed TTI to ensure that the time stamp contained in a trusted temporal token is indeed derived from a source of trusted time. The schemes have varying advantages and disadvantages and balance increased security with increased verification, processing, and storage costs. The objective of these schemes is to ensure that a trusted temporal token has been issued by a TLC with a valid TCCert.

5.1 Basic Scheme A

A first security scheme relies upon the fact that a TLC has been issued a TCCert within a fixed period previous to the token issue in order to guarantee the validity of an issued time stamp. A TCCert is given a valid duration, such as, for example, seven days, during which the certified TLC can issue time stamps. If a TCCert expires or the TLC is issued a new TCCert, the old TCCert is destroyed by the TLC. In order to check the validity of a token, an application or the NOC 210 checks that the time of a time stamp corresponds to a valid period of the TCCert included in or referenced by the trusted temporal token. The NOC 210 must also check that the TCCert itself is valid by tracing the source of trusted time through additional TCCerts of higher clocks up to the NTTS 202.

5.2 Basic Scheme B

A variation of the previous scheme relies upon the alternative fact that a TLC was issued a valid TCCert within a certain time after issuing a trusted temporal token. In this case, TCCerts are considered valid for a fixed duration, such as seven days, before they are issued. Here, it is assumed if a TLC keeps time to within acceptable limits of NTTS time, the TLC has maintained this time for a reasonable period previous to the certification. In order to implement such a system, the TLCs would have to incorporate a reference to a TCCert that has not yet been issued in each trusted temporal token. The NOC 210 could then associate the references with the later issued TCCerts upon their issuance. The checking of trusted temporal tokens under this scheme could be achieved in a manner similar to the previous scheme.

5.3 High Trust Scheme

A high trust scheme combines the aspects of Basic Schemes A and B above. In this scheme, the NOC checks that a TCCert has been issued to the issuing TLC within a fixed period before and within a fixed period after the issuance of the trusted temporal token. In this case, the trusted temporal token need only contain a reference to the TCCert issued the TLC before the token issue. The NOC can then determine whether a subsequent TCCert has been issued within the requisite time period following the token issuance.

5.4 Alternative Scheme

An alternative scheme provides a similar trust guarantee to scheme A, particularly, that a TLC has been issued a TCCert within a fixed period prior to issuing a trusted temporal token. This scheme, however, eliminates the necessity of archiving all of the individual TCCerts for all of the TLCs in the TTI system. Instead, each TCCert contains the complete TCCert of the issuing clock. In this manner, each TCCert will contain a complete, authenticatable chain of certifications from the NTTS all the way down to the issuing TLC. Instead of cataloguing the TCCerts of all of the individual clocks, each trusted temporal token will contain the complete chain of TCCerts linking the trusted time, from which the token was derived, to the NTTS. The public keys of each of the certifying or issuing clocks would then be made available through the CA 314 of the NOC 210, possibly using an Online Certificate Status Protocol (OCSP) responder 316, so that individual applications can independently verify the validity of trusted temporal tokens and the chain of trusted time leading to its creation.

6. Business Model

A billing scheme can also be integrated into the disclosed invention in order to facilitate the operation of the TTI as part of an on-going business concern. A number of different billing schemes providing various benefits can be used in conjunction with the TTI system.

6.1 Per Stamp Billing

The disclosed system provides mechanisms for TLCs to transmit to the NOC the number of time stamps issued. The NOC can be adapted to log this information and create billing reports for individual clients automatically. In this case clients could be billed for each time stamp issued.

6.2 Flat Rate Certification

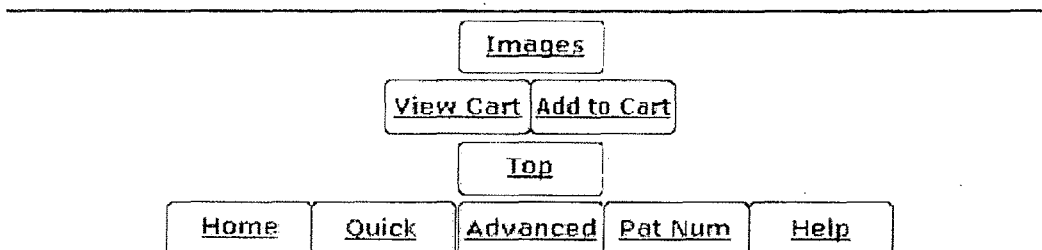
An alternative scheme is based upon billing clients for time certification of each TLC located on the clients' premises. In this case, a client pays for each issued TCCert and receives a flat rate on all of the time stamps issued during the valid TCCert period. In this case, the NOC coordinates and automates billing procedures.

6.3 Charges for Verification

In one business model, verification services for issued time stamps are provided free of charge to any entity wanting to check the validity of a time stamp. Alternatively, verification services could be provided for a fee through the NOC.

While certain exemplary preferred embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention. Further, it is to be understood that this invention is not limited to the specific construction and arrangements shown and described since various modifications or changes may occur to those of ordinary skill in the art without departing from the spirit and scope of the invention as claimed. It is intended that the scope of the invention be limited not by this detailed description but by the claims appended hereto.

* * * * *



USPTO PATENT FULL-TEXT AND IMAGE DATABASE[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Help](#)[Bottom](#)[View Cart](#)[Add to Cart](#)[Images](#)

(1 of 1)

United States Patent**6,370,629****Hastings , et al.****April 9, 2002**

Controlling access to stored information based on geographical location and date and time

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.

Inventors: Hastings; Thomas Mark (Lexington, MA), McNeil; Michael E. (Felton, CA), Glassey; Todd S. (Scotts Valley, CA), Willett; Gerald L. (Malden, MA)

Assignee: Datum, Inc. (Bedford, MA)

Family ID: 22668040

Appl. No.: 09/182,342

Filed: October 29, 1998

Current U.S. Class: 711/163 ; 711/153; 711/164; 713/189; 713/193

Current CPC Class: G06F 21/6218 (20130101); G06F 2221/2111 (20130101); G06F 2211/007 (20130101)

Current International Class: G06F 1/00 (20060101); G06F 21/00 (20060101); H04L 009/00 ()

Field of Search: ;340/988,992,993,991 ;380/7,25 ;713/200,189,193
;711/163,164,147,152,153

References Cited [Referenced By]**U.S. Patent Documents**

<u>5243652</u>	September 1993	Teare et al.
<u>5553143</u>	September 1996	Ross et al.
<u>5640452</u>	June 1997	Murphy
<u>5646992</u>	July 1997	Subler et al.
<u>5754657</u>	May 1998	Schipper et al.
<u>5757916</u>	May 1998	MacDoran et al.
<u>5799082</u>	August 1998	Murphy et al.
<u>5922073</u>	July 1999	Shimada
<u>5987136</u>	November 1999	Schipper et al.
<u>6046689</u>	April 2000	Newman
<u>6057779</u>	May 2000	Bates
<u>6057799</u>	May 2000	Bates

Primary Examiner: Nguyen; Than

Attorney, Agent or Firm: Knobbe, Martens, Olson & Bear, LLP

Claims

What is claimed is:

1. A method for controlling access to stored information comprising:

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

cryptographically signing said actual geographic position with a receiver encryption key;

verifying the signature of said actual geographic position;

determining that said actual geographic position is within a geographic region within which access to said stored information is authorized; and

permitting access to said stored information.

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

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

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

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

6. The method of claim 1, wherein said stored information comprises files and each of said files has an associated geographic region within which access is permitted, and further permitting access to said file if

said actual geographic position is located within said authorized geographic region for said file.

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

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

9. The method of claim 1, further comprising:

encrypting said stored information using an encryption key; and

providing a decryption key which permits decryption of said stored information if said actual geographic position is located within said authorized geographic region.

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

11. Apparatus for controlling access to stored information comprising:

a receiver supplying reliable position information for determining an actual geographic position where said stored information is located, wherein the receiver comprises a receiver encryption mechanism providing a receiver encryption key for cryptographically signing data comprising the actual geographic position; and

a computer for comparing said actual geographic position with a geographic region within which access to said stored information is authorized,

wherein said computer permits access to said stored information if said actual geographic position is located within said authorized geographic region.

12. The apparatus of claim 11, wherein said receiver is a GPS receiver.

13. The apparatus of claim 11, further comprising a reader for reading said stored information wherein said reader comprises a receiver decryption key for verifying the data comprising said cryptographically signed actual position.

14. The apparatus of claim 13, wherein said reader generates an initialization vector which is transmitted to the receiver and included in the signed data.

15. The apparatus of claim 14, wherein said signed initialization vector is verified by the reader before said computer permits access to said stored information.

16. A method for controlling access to a subset of files belonging to a larger set of files of stored information comprising:

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

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

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

cryptographically signing at least the actual geographic position at the receiver;

verifying the signature of the actual geographic position;

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

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

17. The method of claim 16, wherein said association of the files with the authorized geographic regions is stored as a policy comprising policy files wherein each policy file is accessible with a user password and authorizes, if the user password is valid, access to the files listed in said policy file, if the actual geographic position is located within the authorized geographic region associated with the files.

18. The method of claim 17, wherein said policy is stored with the stored information.

19. A method for controlling access to stored information comprising:

determining an actual date or time at the location of said stored information based on signals received at a receiver supplying reliable time information;

cryptographically signing at least the actual date or time at the receiver;

verifying the signature of the actual date or time;

comparing said actual date or time with a predetermined date or time interval at which access to said stored information is authorized; and

permitting access to said stored information if said actual date or time occurs within said authorized date or time interval.

20. The method of claim 19, further comprising denying access to said stored information if said actual date or time does not occur within said authorized date or time interval.

21. The method of claim 19, wherein said information comprises files and each of said files has an associated authorized date or time interval within which access is permitted, and further permitting access to said file if said actual date or time occurs within said associated authorized date or time interval.

22. The method of claim 19, wherein said stored information is divided into subsets of information and wherein at least one of the subsets has a different authorized date or time interval from the other subsets, so that access is authorized to the subset whose authorized date or time interval matches the actual date or time, but not to the subsets whose authorized date or time interval does not match the actual date or time.

23. A method for controlling access to stored information comprising:

forming a policy associating said information with authorized geographic regions and authorized time intervals;

cryptographically signing said policy and said information;

storing said signed policy together with said signed information;

providing a password for unlocking said policy;

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

determining an actual time;

cryptographically signing at least the actual geographic position and the actual time at the receiver;

verifying the signature of the actual geographic position and the actual time;

comparing said actual geographic position and said actual time with said authorized geographic regions and authorized time interval of said policy; and

permitting access to said stored information if said actual geographic position and actual time falls within said authorized geographic regions and authorized time interval of said policy.

24. The method of claim 23, wherein position and time are determined through a Global Orbiting Navigational Satellite System.

25. The method of claim 23, wherein position is determined through an inertial navigation system.

26. The method of claim 23, wherein position is determined through a satellite based location determination system.

27. A method for controlling access to stored information, the method comprising:

(a) determining a position;

(b) cryptographically signing data comprising at least a representation of the position;

(c) verifying the signature of the data comprising at least a representation of the position;

(d) determining that access to the stored information is authorized at the position; and

(e) permitting access to the information based at least upon (c) and (d).

28. The method of claim 27, further comprising

(f) providing the cryptographically signed data to an information accessing device, wherein (c) and (e) are performed by the information accessing device.

29. The method of claim 28, further comprising:

(g) identifying a token;

(h) incorporating the token in the data that is cryptographically signed; and

(i) verifying that the cryptographically signed data comprises the token.

30. The method of claim 29, wherein (g) and (i) are performed by the information accessing device.

31. The method of claim 29, wherein (a), (b), and (h) are performed by a position determining device.

32. The method of claim 29, further comprising

(j) providing the token to the position determining device.

Description

BACKGROUND

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 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 subsets of files. The files may be cryptographically signed and for added protection, may be encrypted. In the scheme discussed in U.S. Pat. No. 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 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.

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 receiver supplying reliable position information. The actual geographic position is then compared with a geographic region within which access to the stored 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 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 different 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. Likewise, access to a sensitive corporate 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 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.

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 (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 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 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 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.

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

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.

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.

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 encrypted with a unique file encryption key 51 (E.sub.1, E.sub.2, E.sub.3). The corresponding file decryption keys 52 (K.sub.1, K.sub.2, K.sub.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. Pat. No. 5,646,992.

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 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.

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 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 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 Authorized Encrypted File Geographic Date/Time File Decryption Key Regions
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 33, 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.

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 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 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, 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 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 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, 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.

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 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, then the packet received by the decoder 32 is recent and genuine, and the time and position data are accepted as valid.

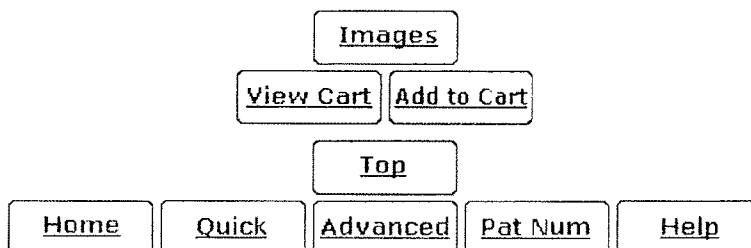
Once the packet from the crypto-board 80 is authorized based on the signature and the initialization vector, the decoder 32 compares the time and position data received from the crypto-board 80 with the policy 155 which applies to the files 144 or to a subset of files 144 (step 460). If the user is authorized to access the files 144, then the data is unlocked (step 470), decrypted with 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 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 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.

* * * * *



PATENTS II



001-57-006001

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

FEBRUARY 23, 1999

PTAS

FISH & RICHARDSON P.C.
DAVID L. FEIGENBAUM
225 FRANKLIN STREET
BOSTON, MA 02110-2804



UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 10/29/1998

REEL/FRAME: 9555/0985
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

HASTINGS, THOMAS MARK

DOC DATE: 10/28/1998

ASSIGNOR:

MCNEIL, MICHAEL E.

DOC DATE: 10/27/1998

ASSIGNOR:

GLASSEY, TODD S.

DOC DATE: 10/27/1998

ASSIGNOR:

WILLETT, GERALD L.

DOC DATE: 10/28/1998

ASSIGNEE:

DIGITAL DELIVERY, INC.
54 MIDDLESEX TURNPIKE
BEDFORD, MASSACHUSETTS

SERIAL NUMBER: 09182342

FILING DATE: 10/29/1998

PATENT NUMBER:

ISSUE DATE:

+ No Doctation Required +
Reviewed By Transition Systems
Initials: <i>AK</i>
Reviewed By Billing Department
Initials: _____

RECEIVED

MAR 10 1999

FISH & RICHARDSON P.C.
BOSTON, MA

LUCASH GESMER&UPDEGROV Fax:617-350-6878

Jun 10 '99 14:16

P.34

05/05/99 WED 18:44 FAX 617542888

F&R PC BOSTON

9555/0985 PAGE 2

SHARMALLA SIMPSON, EXAMINER
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS

05/05/99 WED 16:44 FAX 617547 76

F&R PC BOSTON

0000

Substitute Form PTO-1595

11-06-1998

Attorney Docket No.: 06157/006001

SHORT

Assistant Commissioner for Patent

100873007

Document.

1. Name of conveying party(ies):
Thomas Mark Hastings, Michael E. McNeil, Todd
S. Glassey and Gerald L. Willett

2. Name and address of receiving party(ies):
Digital Delivery, Inc.
54 Middlesex Turnpike
Bedford, Massachusetts

Additional name(s) attached? ☐ Yes ☒ NoAdditional names/addresses attached? ☐ Yes ☒ No

3. Nature of conveyance:
☒ Assignment
☐ Merger
☐ Security Agreement
☐ Change of Name
☐ Other:

Execution Date: October 27, 1998, Michael E. McNeil and Todd S. Glassey and October 28, 1998, Thomas Mark Hastings and Gerald L. Willett

4. Application number(s) or patent number(s):
If this document is being filed with a new application, the execution date of the application is: October 27, 1998, Michael E. McNeil and Todd S. Glassey, and October 28, 1998, Thomas Mark Hastings and Gerald L. Willett
A. Patent Application No.(s):
B. Patent No.(s):

Additional numbers attached? ☐ Yes ☒ No

5. Name/address of party to whom correspondence concerning document should be mailed:

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

6. Total number of applications/patents involved: 1

7. Total fee (37 CFR 3.41): \$40
☒ Enclosed
☐ Authorized to charge deposit account

8. Deposit account number: 06-1050
If the fee above is being charged to deposit account, a duplicate copy of this cover sheet is attached. Please apply any additional charges, or any credits, to our Deposit Account No. 06-1050.

DO NOT USE THIS SPACE

9. Statement and signature: To the best of my knowledge and belief, the foregoing information is true and correct and the attached is the original document.

David L. Feigenbaum

Name of Person Signing

Signature

Date

10/29/98

Total number of pages including cover sheet, attachments, and document: 4

11/05/1998 BOSTON 0000094 09102362

01 FC:501

40.00 DP

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 McNeil
AMBROSE McNeil

10549 U.S. PTO
09/10/98
10/29/98

ASSIGNMENT

For valuable consideration, we, Thomas Mark Hastings, of Lexington, Massachusetts; Michael E. McNeil of Felton, California; Todd S. Glassey of Scotts Valley, California; and Gerald L. Willert of Malden, Massachusetts; hereby assign to DIGITAL DELIVERY, INC., a Massachusetts corporation having a place of business at 54 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 23 day of October, 1998

Thomas Mark Hastings L.S.

STATE OF Massachusetts:

COUNTY OF Middlesex : ss.

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.

Janeth Altwell
Notary Public

My Commission Expires: 2/04/2005

[Notary's Seal Here]

IN WITNESS WHEREOF, I hereto set my hand and seal at Scotts Valley, Calif.
this 27th day of October, 1998.

Michael E. McNeil
Michael E. McNeil

L.S.

STATE OF California:COUNTY OF Santa Cruz :ss.

Before me this 27 day of October, 1998, personally appeared

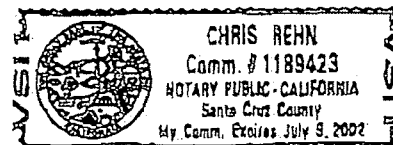
Michael E. McNeil known to me to be the person whose name is subscribed to the foregoing Assignment, and acknowledged that he she executed the same as his her free act and deed for the purposes therein contained.

Chris Rehn
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, 1998.

Todd S. Glassey
Todd S. Glassey

L.S.

STATE OF Ca:COUNTY OF Santa Cruz :ss.

Before me this 27 day of October, 1998, personally appeared

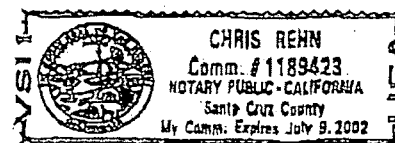
Todd S. Glassey known to me to be the person whose name is subscribed to the foregoing Assignment, and acknowledged that he she executed the same as his her free act and deed for the purposes therein contained.

Chris Rehn
Notary Public

My Commission Expires:

July 9, 2002

[Notary's Seal Here]



IN WITNESS WHEREOF, I hereto set my hand and seal at Burlington, Massachusetts
this 28 day of October, 1998

Gerald L. Willett Jr.
Gerald L. Willett

L.S.

STATE OF Massachusetts:COUNTY OF Middlesex: ss.

Before me this 28 day of October, 1998, personally appeared

Gerald L. Willett Jr. 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.

Jean Alshill
Notary Public

My Commission Expires: 2/04/2005

[Notary's Seal Here]

May it please the Court, the following is an extract from the SEARCH function inside the IETF.ORG Intellectual Property Rights Webpage (<http://www.ietf.org/ipr>) listing statements from search term "GLASSEY"; As you can see from the listing Glassey and McNeil filed numerous documents pertaining to Glassey's and McNeil's rights for the Standards Agency's unauthorized use of the protected Phase-II Intellectual Properties in its publications.

Patent Owner/Applicant Search Result

Total number of IPR disclosures found: 20

IPR that was submitted by *glassey*, and is related to *RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"*

2013-10-27 • ID # 2224 "Todd S. Glassey's Statement about IPR related to RFC 3161"

IPR that was submitted by *glassey*, and is related to *draft-ietf-geopriv-local-civic-03, "Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)"*

2012-07-18 • ID # 1829 "Glassey's Statement about IPR related to draft-ietf-geopriv-local-civic-03"

IPR that was submitted by *glassey*, and is related to *draft-ietf-geopriv-deref-protocol-07, "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)"*

2012-07-15 • ID # 1825 "Todd S. Glassey's Statement about IPR related to draft-ietf-geopriv-deref-protocol-07"

IPR that was submitted by *glassey*, and is related to *draft-ietf-geopriv-deref-protocol-06, "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)"*

2012-07-12 • ID # 1818 "Patent Recovery Corp (Glassey/McNeil)'s Statement about IPR related to draft-ietf-geopriv-deref-protocol-06 and (most all GeoPriv, DNSSec, and timestamping protocols will also infringe)"

IPR that was submitted by *glassey*, and is not related to a specific IETF contribution.

2012-01-24 • ID # 1669 "Todd Glassey's Statement about IPR related to Informational Publication"

IPR that was submitted by *glassey*, and is related to *RFC 4776, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information"*

2008-06-24 • ID # 963 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4776 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"

2008-06-19 • ID # 954 IPR disclosure ID# 963 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4776 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey

GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 3694, "Threat Analysis of the Geopriv Protocol"**

- 2008-06-24 • ID # 962 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3694 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 962 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3694 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 5139, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)"**

- 2008-06-24 • ID # 961 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 5139 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 961 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 5139 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 3693, "Geopriv Requirements"**

- 2008-06-24 • ID # 960 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3693 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 960 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3693 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 4589, "Location Types Registry"**

- 2008-06-24 • ID # 957 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4589 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 957 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4589 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital

Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to ***RFC 3825, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information"***

- 2008-06-24 • ID # 956 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3825 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 956 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3825 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to ***RFC 4745, "Common Policy: A Document Format for Expressing Privacy Preferences"***

- 2008-06-24 • ID # 955 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4745 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 955 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4745 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to ***RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"***

- 2004-07-15 • ID # 461 "Glassey's Statement about possible IPR claimed in RFC 3161"

Additionally since the computers it operates to provide these publication services execute code which implements this 'description of the infringement' as real-world code, it directly infringes itself in its operations.

There is no copyright section 107 exemption for patent protected technologies whether enforced directly against the US patent or a license providing for those same controls to another party, as is the case in this shared-patent case.

will page 7

Delivered by: per

FISH & RICHARDSON P.C.

225 Franklin Street
Boston, Massachusetts
02110-2804Telephone
617 542-5070Facsimile
617 542-8906Web Site
www.fr.com

Date May 5, 1999

To Ms. Jennifer Eilers

Facsimile number 06157 00600001 350-6878

From Lesley J. Arcidy
Secretary to David L. FeigenbaumRe 06157/006001
GPSNumber of pages
including this page

7

Message Jennifer: Here is a copy of the recorded assignment. Lesley

NOTE: This facsimile is intended for the addressee only and may contain privileged or confidential information. If you have received this facsimile in error, please call us collect at 617 542-5070 immediately to arrange for its return. Thank you.



06157-00600
UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

FEBRUARY 23, 1999

PTAS

FISH & RICHARDSON P.C.
DAVID L. FEIGENBAUM
225 FRANKLIN STREET
BOSTON, MA 02110-2804



UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 10/29/1998

REEL/FRAME: 9555/0985
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

HASTINGS, THOMAS MARK

DOC DATE: 10/28/1998

ASSIGNOR:

MCNEIL, MICHAEL E.

DOC DATE: 10/27/1998

ASSIGNOR:

GLASSEY, TODD S.

DOC DATE: 10/27/1998

ASSIGNOR:

WILLETT, GERALD L.

DOC DATE: 10/28/1998

ASSIGNEE:

DIGITAL DELIVERY, INC.
54 MIDDLESEX TURNPIKE
BEDFORD, MASSACHUSETTS

SERIAL NUMBER: 09182342
PATENT NUMBER:

FILING DATE: 10/29/1998
ISSUE DATE:

* No Locking Required *
Reviewed By: <u> </u>
Initials: <u> </u>
Reviewed By: <u> </u>
Initials: <u> </u>

RECEIVED

MAR 10 1999

FISH & RICHARDSON P.C.
BOSTON

9555/0985 PAGE 2

SHARMALLA SIMPSON, EXAMINER
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS

Substitute Form PTO-1595

11-06-1998

Attorney Docket No.: 06157/006001

SH-T

Assistant Commissioner for Patent

100873007

Document.

1. Name of conveying party(ies):
Thomas Mark Hastings, Michael E. McNeil, Todd
S. Glassey and Gerald L. Willett

2. Name and address of receiving party(ies):
Digital Delivery, Inc.
54 Middlesex Turnpike
Bedford, Massachusetts

Additional name(s) attached? ☐ Yes ☒ NoAdditional names/addresses attached? ☐ Yes ☒ No

3. Nature of conveyance:
☒ Assignment
☐ Merger
☐ Security Agreement
☐ Change of Name
☐ Other:

Execution Date: October 27, 1998, Michael E.
McNeil and Todd S. Glassey and October 28,
1998, Thomas Mark Hastings and Gerald L.
Willett

4. Application number(s) or patent number(s):
If this document is being filed with a new application, the execution date of the application is: October 27, 1998,
Michael E. McNeil and Todd S. Glassey, and October 28, 1998, Thomas Mark Hastings and Gerald L. Willett
A. Patent Application No.(s):
B. Patent No.(s):

Additional numbers attached? ☐ Yes ☒ No

5. Name/address of party to whom correspondence
concerning document should be mailed:

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

6. Total number of applications/patents involved: 1

7. Total fee (37 CFR 3.41): \$40

☒ Enclosed
☐ Authorized to charge deposit account

8. Deposit account number: 06-1050

If the fee above is being charged to deposit
account, a duplicate copy of this cover sheet is
attached. Please apply any additional charges, or
any credits, to our Deposit Account No. 06-1050.

DO NOT USE THIS SPACE

9. Statement and signature: To the best of my knowledge and belief, the foregoing information is true and correct
and the attached is the original document.

David L. Feigenbaum
Name of Person Signing

Signature

Date

Total number of pages including cover sheet, attachments, and document: 4

11/05/1998 0000094 09102342

01 FC:501

40.00 DP

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 Jean
AMBROSE Jean

10/29/98
09/182342
U.S. PRO

ASSIGNMENT

For valuable consideration, we, Thomas Mark Hastings, of Lexington, Massachusetts; Michael E. McNeil of Felton, California; Todd S. Glassey of Scotts Valley, California; and Gerald L. Willett of Malden, Massachusetts; hereby assign to DIGITAL DELIVERY, INC., a Massachusetts corporation having a place of business at 54 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 23 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 Alwell
Notary Public

My Commission Expires: 2/04/2005

[Notary's Seal Here]

IN WITNESS WHEREOF, I hereto set my hand and seal at Scotts Valley, Calif.this 27th day of October, 1998.Michael E. McNeil
Michael E. McNeil

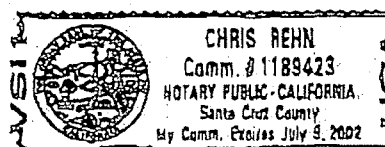
L.S.

STATE OF California:COUNTY OF Santa Cruz :ss.Before me this 27 day of October, 1998, personally appearedMichael 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 Rehn
Notary Public

My Commission Expires:

July 9, 2002

[Notary's Seal Here]

IN WITNESS WHEREOF, I hereto set my hand and seal at Scotts Valleythis 27 day of October, 1998.Todd S. Glassey
Todd S. Glassey

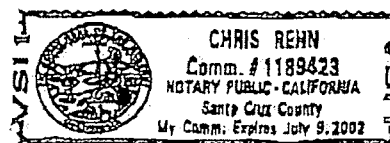
L.S.

STATE OF Ca:COUNTY OF Santa Cruz :ss.Before me this 27 day of October, 1998, personally appearedTodd 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 Rehn
Notary Public

My Commission Expires:

July 9, 2002

[Notary's Seal Here]



IN WITNESS WHEREOF, I hereto set my hand and seal at Burlington, Massachusetts,
this 28 day of October, 1998

Gerald L. Willett Jr. L.S.
Gerald L. Willett

STATE OF Massachusetts:

COUNTY OF Middlesex: ss.

Before me this 28 day of October, 1998, personally appeared

Gerald L. Willett Jr. 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.

Jason A. Hill
Notary Public

My Commission Expires: 2/04/2005

[Notary's Seal Here]

Admin

From: Todd S. Glassey <Todd.Glassey@www.GMTsw.com>
To: jbook@SCLAWFIRM.COM
Subject: Re: The proposed GM/DD deal...
Date: Wednesday, April 28, 1999 6:05 PM

Mark,
sounds like you want to rattle your saber too, OK I'll draw too but this is silly and wasteful. Just for the fun of it I am carboning our counsel on this matter so you know I am ready to rock and roll if you want to.

So - you read my responses, and then when you done fuming up, have a cup of coffee, take a day or so and we can talk.

I really do want to work this out with you without any legal entanglements, and am willing to come to a lump sum or structured settlement on these issues and potentially to lump them all into the same deal, but, Mark - you wanna draw any more blade - go ahead and my response will be total 100% commitment to the battle and I will prevail, because winning for me doesn't necessarily mean winning \$\$\$.

It means being proved legally right, and as such - I have a substantially different agenda than you do. Lets not escalate this any farther than we have to.

Todd

----- Original Message -----

From: Mark Hastings <mark@digitaldelivery.com>
To: 'Todd S. Glassey' <Todd.Glassey@GMTsw.com>
Sent: Wednesday, April 28, 1999 9:20 AM
Subject: RE: The proposed GM/DD deal....

> I am in receipt of your documents. Interestingly, they both state that they
> are to be sent by U.S. Mail and Fax. Clearly, you did not do either.

That was my fault there, sorry.

>

> I have only read them quickly, and my first comment is that on numerous
> occasions in discussions with you and your attorneys, Mary Lee Crooks and
> Jason Book, GMT is to share half of the expense of actually creating the
> patent application.

No No No - there is no agreement that GMT is going to pay you squat unless we see substantially more than the three percent we are talking about now, and that's what the discovery proves. I have the email.

>The total was just under \$15,000.00. Consequently, GMT
> should be prepared to send a check to cover GMT share of the expense of
> filing the patent. This is and has always been a condition of the royalty
> arrangement between GMT and DDI as discussed in the presence of your
> attorneys and subject to discovery.

BS Mark - You personally made the decision to take your side of the process and turn it over to your lawyers that spent a considerable amount of "your" money having them draft the same document we were in the process of working on because we were not moving fast enough for you - and you chose to do so without a clear contract in place with us as to what you would actually own of our core technologies, or to our financial culpability on your expenses.

for filing a patent against our core IP. No, the responsibility for that decision and its expense rests solely on you.

However, not to stop you since you demanded that we work with your lawyers on reviewing and editing the draft. Further, since the specific use of the technology that McNeil and I were authorizing you to use as part of our broader GeoPositional datapoint systems, was part of a larger system, we had to also in the process fully review your original patent to validate that the things we were claiming were true and provable. All this work was of course reviewed by our counsel as well and the costs of that has been borne totally by us at this point.

So, the actuality of it is that we paid our attorneys and staff substantially more than your \$15K to date and you should be compensating us for half the costing on our side as well. Want to trade checks? (or maybe we should we draw blades a little more)

>
> I also am concerned about some of the claims in this agreement. But I will
> elaborate on those when I have had time to more closely review the documents
> and consult with counsel.

Please do, they represent the terms of the original agreement to agree, which now based on Datum's acquiring your company is worth a whole lot more than you originally thought it would be. But that's not the point. We signed over the patent to you for considerations already agreed upon in the Coinventors agreement, or we can take it up with both the Court and the Patent Office.

Also realize that you are forcing the merging of the Datum and DD matters into one homogenous mass; that you may as such force a number of issues that you as the president of the new division won't like the answers to.

I am not the naive little boy that came into this process, and I have a number of issues that *will* be addressed between us privately or in open court.

These issues include:

1) The royalty and compensation agreement between myself and Datum on the sale of materials in to the EC product domain and that's all EC products. Also all the boiler plate on what Datum has to do to prove best efforts for the development of the business line, base level compensation, etc, etc.

and in the interest of creating a harmonious universe, I'll make of point of using Datum gear in my toys and inventions as long as it is the right decision for the product effort. Same with the standards efforts, I'll also surrender as part of the settlement, a number of the relationships I have introduced you to in the form of

However, one of the key terms will have to not be bound to purchase only datum equipment, if datum cannot supply what I need to address my specific requirements.

Also both parties will have a mutual gag order as part of the settlement, unless we decide that we need to work on a common standards approach (which I BTW, strongly suggest we do). Glassey and McNeil in this process will continue to work with any of the standards teams they are

2) Any further royalties that Datum will wind up owing to GMT

3) The completion of the Digital Delivery contracts and compensation for our licensing you the geoPositional policy use for Confidential Courier ONLY. Also the memorialization of the Coinventors agreement.

4) The commissions on the presentation of Coastek and Digital Delivery for acquisition by Datum at industry standard rates (Lehman Rates)

If not, then lets just leave it to the lawyers and the Federal Government (did you know that a provable conspiracy doesn't take direct knowledge, just the commission of an act in the collective furtherance of a Feleony - check with counsel on that one if you like) and if you force the issue I could prove that is what "you folks" did, you conspired to "do me".

Surely you must know that the totality of the email between Robinson and I is so damning, especially Robinson's letter to us saying that we could only be Marketing People since we were not competent as engineers in late November of 1998. Its funny he never bothered to say that to me when I introduced you to Judah Levine or put the federally funded timeserver into your computer room....

Or when I introduced you to Verisign under the terms of our pre-existing Intellectual Property agreements (The NDA and the PPT presentation that Mitch has on what GMT was claiming ownership of at the outset of the relationship. You will see the timestamp is covered there as well) , or Entrust or Digital Signature Trust.

It clearly says we are there for one purpose and that's market development, but then how could we have developed any of the core Datum IP then?

And when you really look at it, it's really funny how the TTI looks like the concept I came into Datum with when I left Coastek. Funny, also how the Robinson Report to Erik van der Kaay of last December is a mere two pages long. Showing 4 servers and 4 communications protocols. But that was the extent of it. Two lousy pages. What it meant is that there was no Datum product yet, what there was, was a two page outline in Dave's head.

So when we proposed the TTI2, a 2 server, 1 protocol model, as our response to Dave with several approaches, Both SW and HW based service models, Dave immediately stands up and say's "Hey that's mine.", but the truth of the matter is that it just isn't his work. There is no "Dave" and certainly not any Datum in it anywhere.

It is a generic board level product with a standard industry clock chip. There doesn't need to be any fancy logic in the TLC at all to make the trust process models work and that was something that they just never got. Anyone could build it, that was the point. It, our TTI2, uses the Secure ACTS protocol we are working on with NIST now so there is no Trusted Third party timing provider in this model, just the Timing providers at the Governmental levels. This flattens the timing model and is totally different than the Datum DRobinson architecture description as of Dec 22, 1998.

The bottom line is that there was at the time we split in mid October, 1998, no specific Datum IP's had been developed, except that of porting the BC635 architecture to new secure timebase model.

The relationships, including the one with Digital Delivery are protected under the terms of the Datum NDA I executed since they predated the Datum/Glassey relationship there will be no problem proving this.

This is further demonstrated by my telling Mitch Stone about you, Digital Delivery, under the terms that I was comp'd. I did the same with Coastek.

Mitch's response was to pass the information along to the powers that be, Eric and Dave Robinson, who decided that they would not honor the terms under which the introduction was given to Mitch, because Mitch was not an officer of Datum Corporation, just the vp of the division of the company I was assigned to work with, they seem to feel this will fly. However, there are two problems with this.

The first is that I was told by everyone at Datum including Erik van der Kaay that Mitch was my go between, that is between the company and myself. He approved my invoices and everything I did, was at his direction. So, if that is the case and under the NDA terms, Mitch, Datum Corporation's Representative to Glassey, et al., was contaminated and bound by the company's agreement to honor my intellectual properties, so by violating the terms of the NDA by revealing the name of Digital Delivery before finding out whether they, they, the Datum executive management team would comply with the terms under which it was submitted, and since of course Mitch Stone, the vice president of sales for Bancom Division at the time, I think that the courts will have this wrapped up without too much bloodshed. It also is a key concept to bring out that the original proposal to Datum was made to Davey Briggs of the FTS division, because that is where I see the bulk of the profit being derived. Yes the board business is good, but the board level system is infrastructure and selling core infrastructure without a end to end product plan is a loser and so we approached Datum with particular interest in the cesium devices. With that in mind, we need to make sure that the compensation plan adequately addresses moneys earned from extra Cesium and Rubidium product sales as well:

Here's how it worked. Mitch was legally obligated to not reveal the name of Digital Delivery or the interests in the company until the terms of the agreement were ratified or consummated regarding a purchase position in Digital Delivery and Coastek. But this didn't happen and since he was the legally binding representative of the corporation for me, it was appropriate to present the opportunity through him and so by that token - I am owed compensation for the acquisition.

I am not being unreasonable here and have asked for what everyone in the industry gets as a baseline. That is "Standard Lehman numbers", which are calculated at 5% first million or fraction thereof, 4% on the second million, and 3% thereafter for each whole or fractional million, which for example if the stock trade was at a 5M valuation, the commission would come to somewhere in the \$180K range.

Now that we have had our tirades, Mark, don't try and play me for a fool. I know exactly what cards I am holding and so do you. So before we make this a pissing match and each spend considerable moneys on our "Fighting Cocks" lets look at the situation. Clearly I can prove that there was "some deal" done verbally between me and Datum. I presented Datum at the beginning of the relationship with a specific list of the things that we (GMT) and I (Todd Glassey) owned and that were not part of the agreement between us.

This included every relationship I had that was pre-existing the signing of the GMT Datum contractors contract. The reason Mitch demanded this is because he didn't have the power to rewrite the contractors contract and Robinson wanted paper between me and Datum before I went anywhere else to shop my technology ideas and market development ideas around.

That I presented you to Datum for acquisition is easily provable and that I did it under the guise that I wanted separate compensation for it is a no brainer since it, my relationship with you, was specifically excluded from Datum's ownership as part of any IP's that are or were to be developed under the contracting agreement.

As to the mad rush to get us to sign something, He, Robinson, was real clear that he had nothing without me, he commented on how much he wanted to cut his monthlong vacation short, so he could get back to the farm and start work on what Datum was going to do about this new possibility I had presented to them.

SO NOW THAT YOUR PROBABLY PRETTY PISSED LETS LOOK AT THE CONSEQUENCES

So what is the short side of a lawsuit between us? at the very least the PR damage to you and Datum in the industry will be "catastrophic", BUT if I am at all successful in the Conspiracy matter, some of "you" people may be doing time in the CampFed. Let alone the potential damage to Datum Stock prices and the like. Oh and the patent, that will be tied up for years.

My mistake in the Datum matter is clearly that I trusted Dave Robinson at his word and this is not panning out at this point, but based on a number of easily demonstrable events, and Dave's clearly provable intent to "not honor his agreements", this matter might just as well go to court.

My damage is that I have to spend a bunch of my inheritance money on a lawsuit and

>
> I have also explicitly told you that this and any other agreements between
> GMT and Datum will have to be executed simultaneously.

>
> I will speak with you soon regarding a resolution to this agreement.

>
> Sincerely,

>
> Mark Hastings
> President

>
>
>
>

> > -----Original Message-----

> > From: Todd S. Glassey [mailto:Todd.Glassey@www.GMTsw.com]

> > Sent: Tuesday, April 27, 1999 2:34 PM

> > To: T. Mark Hastings

> > Subject: Fw: The proposed GM/DD deal...

> >
> >
> >
> >

> > ----- Original Message -----

> > From: Todd S. Glassey <Todd.Glassey@GMTsw.com>

> > To: Jason Book <JBook@SCLAWFIRM.COM>; Mark

> > Hastings<Mark@DigitalDelivery.COM

> > >; Michael E Mcneil <MEMcNeil@GMTsw.COM>

> > Sent: Saturday, April 17, 1999 6:55 PM

> > Subject: The proposed GM/DD deal...

> >
> >
> >
> >

> > > Mark, here are those two files I thought I had sent to you
> > in January...

> > > These are the rough copies and my feeling is that as to the
> > content of the

> > > agreement itself, we just need to back end the content of

> > > the reciprocity

> > > sections into the main agreement.

> > >

> > > Let me know if you have any problem with the content of the
> > main body of

> > the

> > > agreement and we can talk about it.

> > >

> > >

> > > Regards,

> > >

> > > Todd S. Glassey, President and CTO

> > > GMTIabs, Inc.

> > > (831) 438-7811

> > >

> > >

> > >

Admin

From: Todd S. Glassey <Todd.Glassey@www.GMTsw.com>
To: Jason Book <JBook@SCLAWFIRM.COM>; Michael E McNeil <MEMcNeil@www.GMTsw.com>
Subject: The proposed GM/DD deal...
Date: Saturday, April 17, 1999 6:55 PM

Mark, here are those two files I thought I had sent to you in January...
These are the rough copies and my feeling is that as to the content of the
agreement itself, we just need to back end the content of the reciprocity
sections into the main agreement.

Let me know if you have any problem with the content of the main body of the
agreement and we can talk about it.

Regards,

Todd S. Glassey, President and CTO
GMTlabs, Inc.
(831) 438-7811

May 1, 1999

T. Mark Hastings
President & C.E.O.
Digital Delivery, Inc.
54 Middlesex Turnpike
Bedford, MA 01730-1417

Via Facsimile
and U.S. Mail

Re: Draft Agreement between Todd S. Glassey, Michael E. McNeil,
and Digital Delivery, Inc.

Dear Mr. Hastings:

Enclosed please find the above-referenced Agreement (the "Agreement") for your review and comment. The Agreement incorporates the terms set forth in the Co-Inventor Agreement between the parties dated October 26, 1999.

As I know you are aware, the last term to be finalized in the Agreement is the compensation to be paid to Glassey-McNeil. Please review the following alternative compensation structures and provide us with your comments regarding same. In the event that one of the alternatives set forth below is acceptable to you, please let us know and we will insert the appropriate text into Paragraph 6 of the Agreement. Other alternatives are possible and should be suggested in the event that the alternatives set forth herein are not acceptable.

Alternative 1

In consideration for the Assignment under which Glassey-McNeil assigned to Digital all rights, title and interest in and to certain intellectual property essential to the Controlling Access to Stored Information patent, Glassey-McNeil shall receive from Digital the total sum of Three Hundred Thousand Dollars (\$300,000.00), payable in cash or certified funds of the US shall be paid to Glassey-McNeil within 2 calendar years from the

T. Mark Hastings
May 1, 1999
Page 2

execution of this agreement That this payment is made in lieu of a formal licensing agreement and shall be the totality of financial reciprocity for the conveyance of the intellectual properties as specified in the body of this agreement.

In the event that Digital fails to perform according to the foregoing payment terms 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, each party shall have all right to exploit said inventions and technology without any notice, obligation or accounting to the other. The parties shall, nevertheless, each execute and deliver such further documents and shall take such other actions as may be reasonably necessary to effect this reversion of rights.

Alternative 2

In consideration for the Assignment under which Glassey-McNeil assigned to Digital all rights, title and interest in and to certain intellectual property essential to the Controlling Access to Stored Information patent, Glassey-McNeil shall receive from Digital a royalty equal to Three Percent (3%) of gross sales of all products sold by Digital which incorporate the technology contained in the Controlling Access Patent or otherwise relate to such technology. Such royalty shall be payable by Digital to Glassey-McNeil over the entire useful life of the Controlling Access Patent (the "Royalty Period"). Within thirty (30) days following any month that ends during the Royalty Period, Digital shall submit a written report to Glassey-McNeil, setting forth all gross sales of the products described in this Paragraph 6 during any part of said month within the Royalty Period. All such reports shall accurately set forth the basis for all royalties due under this Agreement. Payment of all royalties due in respect of each monthly reporting period shall be submitted to Glassey-McNeil with the report for such period.

We look forward to your prompt response and cooperation in finalizing the Agreement as soon as possible. Thank you.

T. Mark Hastings
May 1, 1999
Page 3

Very truly yours,

Todd Glassey, president

TSG:tsg
Enclosure

AGREEMENT

This Agreement ("Agreement") is made effective as of October 26, 1998, by and between, on the one hand, TODD S. GLASSEY and MICHAEL E. McNEIL, each an individual (collectively "Glassey-McNeil"), and on the other hand, DIGITAL DELIVERY, INC., a Massachusetts corporation ("Digital"). The Agreement is made with reference to 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. Willet, 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. The intent of Digital and Glassey-McNeil has been that Digital would file for a patent on such new technology, as applied to and integrated with the Courier Patent, such new patent to be titled "Controlling Access to Stored Information". In accord with this intent, Glassey-McNeil, along with Thomas Mark Hastings and Gerald L. Willet, have executed that certain Assignment dated _____, 1998 (the "Assignment"), under which Glassey-McNeil assigned to Digital all rights, title and interest in and to certain intellectual property essential to the Controlling Access to Stored Information patent, for the consideration set forth in this Agreement.

C. Digital then filed, on _____, 1998, the Controlling Access to Stored Information patent, said patent having been assigned U.S. Serial Number _____. At this time, the Controlling Access to Stored Information patent is being prosecuted through the United States Patent and Trademark Office.

D. Glassey-McNeil and Digital also entered into that certain Co-Inventor Agreement, dated October 26, 1998 (the "Co-Inventor Agreement").

E. By this Agreement, Glassey-McNeil and Digital desire to reduce to writing the

compensation to be paid by Digital to Glassey-McNeil in consideration for the Assignment, to supercede the Co-Inventor Agreement in its entirety, and to memorialize their rights with respect to other intellectual property as described in this Agreement.

NOW, THEREFORE, in consideration of the foregoing Recitals, and for other good and valuable consideration receipt of which is hereby acknowledged, Glassey-McNeil and Digital hereby agree as follows:

AGREEMENT

1. Definitions. The following terms shall have the following meanings for purposes of this Agreement:
 - 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. Rights to GPS Phase II. 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, royalty-free, non-exclusive worldwide license for the GPS Phase II technology and derivatives thereof, with rights to sublicense.
3. Rights to Courier Patent. 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 not produced by Digital.
4. No Opposition to Patents. Digital shall not file any opposition in the United

States Patent and Trademark Office or similar 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, e-mail gateways, protocol bridges, database servers, file servers, hardware based appliances, and the like.

5. **Product Development.** 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. 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.
6. **Compensation to Glassey-McNeil.** TO BE INSERTED AS PER COVER LETTER.
7. **Amendment.** This Agreement may be supplemented, amended, or modified only by the mutual agreement of Glassey-McNeil and Digital. No supplement, amendment, or modification of this Agreement will be binding unless it is in writing and signed by Glassey-McNeil and Digital.
8. **No Waiver.** No waiver of a breach, failure of any condition, or any right or remedy contained in or granted by this Agreement will be effective unless it is in writing and signed by the party waiving the breach, failure, right, or remedy. No waiver of any breach, failure, right, or remedy, will be deemed a waiver any other breach, failure, right, or remedy, whether or not similar, nor will any waiver constitute a continuing waiver unless the writing so specifies.
9. **Attorney's Fees.** If either party to this Agreement undertakes litigation or arbitration against the other party arising out of or in connection with this Agreement, the successful or prevailing party or parties will be entitled to recover from the other party, as an element of his costs of suit, and not as damages, reasonable attorney's fees, arbitration costs, and court costs incurred. The "prevailing party" shall be determined under California Civil Code § 1717(b)(1) or any successor statute.
10. **Governing Law.** This Agreement shall be governed by and interpreted in accord with the laws of the State of California.
11. **Venue.** Any dispute, including litigation or arbitration, that arises under or relates to this Agreement (whether contract, tort, or both) shall be resolved in the Santa

Cruz County Superior Court, Santa Cruz, California, or by way of an arbitration in the County of Santa Cruz, State of California.

12. **Severability.** If any provision in this Agreement is invalid or unenforceable, that provision shall be construed, limited, modified, or if necessary severed to the extent necessary to eliminate its invalidity or unenforceability, without invalidating the remaining provisions of this Agreement.
13. **Binding Effect.** This Agreement shall be binding upon and inure to the benefit of the parties hereto, and any permitted heirs, executors, administrators, successors, and assigns thereof.
14. **Entire Agreement.** This Agreement constitutes the final, complete, and exclusive statement of the terms of the agreement between the parties pertaining to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings of the parties. No party has been induced to enter into this Agreement by, nor is any party relying on, any representation or warranty outside those expressly set forth in this Agreement.

IN WITNESS WHEREOF AND WITH INTENT TO BE BOUND, Glassey-McNeil and Digital have executed this Agreement on the dates set forth opposite their signatures below:

Glassey-McNeil:

TODD S. GLASSEY

March ____, 1999.

MICHAEL E. McNEIL

March ____, 1999.

Digital:

DIGITAL DELIVERY, INC., a Massachusetts corporation

By: _____
THOMAS MARK HASTINGS, President

March ____, 1999.

Admin

From: Mark Hastings <mark@digitaldelivery.com>
To: 'Todd S. Glassey' <Todd.Glassey@www.GMTsw.com>
Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com
Subject: Royalty agreement between DDI and GMT
Date: Friday, April 16, 1999 5:32 AM

doc. was empty

Admin

From: Mark Hastings <mark@digitaldelivery.com>
To: 'Todd S. Glassey' <Todd.Glassey@www.GMTsw.com>
Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com
Subject: Royalty agreement between DDI and GMT
Date: Friday, April 16, 1999 5:32 AM

couldn't attach doc -

Admin

From: Todd S. Glassey <Todd.Glassey@www.GMTsw.com>
To: Mark Hastings <mark@digitaldelivery.com>
Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com
Subject: Re: Need to get some closure on the DD/GMT deal...
Date: Thursday, April 15, 1999 10:47 PM

Hi Mark how is the family, well I hope...

As to meeting here, yes absolutely - lets do that. Re: I sent you the edited proposal for your review about a month ago. If you need another copy I can resend it or Jason can... u

What I had proposed was that we structure the deal in two segments. The first is the conveyance of the derivative and core GeoPositional IP and the extend policy interface it creates. The second is how we do the licensing/royalties agreement.

BTW, I have been looking at the structure and form of software license deals and they, in my mind, to be effective need some kind of audit and proofing plan, as well as a lot of language to protect us from lying to each other.

While I have no reason to believe that this would happen, we both deal straight up, the lawyers will not let me "not have this language" in the contract.

So I would propose, since I really don't want to be auditing your books every year and we still can't really put a demonstrative value on the addition of the GeoPositional Policy Interface to the abilities of Digital Delivery, that maybe some structured settlement would be easier for all concerned...

What do you think?

Todd.

----- Original Message -----

From: Mark Hastings <mark@digitaldelivery.com>
To: 'Todd S. Glassey' <Todd.Glassey@GMTsw.com>; Mark Hastings <mark@digitaldelivery.com>
Cc: <jbook@SCLAWFIRM.COM>; <memcNeil@GMTsw.com>
Sent: Tuesday, April 13, 1999 4:56 PM
Subject: RE: Need to get some closure on the DD/GMT deal...

> Hi Todd:
>
> Long time no hear. Hope all is going well for you at GMT.
>
> I too would like to complete our agreement. However, I am not sure about
> having received a deal from you. When was it sent?
>
> I would also like to forward copies of the email and fax messages that
were
> exchanged prior to your input into the application to your attorneys
office
> so that they have a complete record.
>
> I will be in the S.F. Bay Area the week of April 26 and possibly we could
> meet at that time to work out some of the details.
>
> Later,
>
> Mark Hastings,

> President
> Digital Delivery, Inc.
>
> > -----Original Message-----
> > From: Todd S. Glassey [mailto:Todd.Glassey@www.GMTsw.com]
> > Sent: Monday, April 12, 1999 7:30 PM
> > To: T. Mark Hastings
> > Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com
> > Subject: Need to get some closure on the DD/GMT deal...
> >
> >
> > Mark, we are about to file the core technology patent for the
> > geopositional.
> > timestamping tools and need to get our deal finished, or at least the
> > non-financial portions thereof concluded.
> >
> > Let me know what your comments on the deal I forwarded to you
> > were. The
> > terms and conditions of the components exclusive of the financial
> > compensation were just as we had agreed so in the very least
> > I want to get
> > that completed at the earliest convince.
> >
> > Todd Glassey, President
> > GMTsw, Inc.
> >
> >
> >

Admin

From: Mark Hastings <mark@digitaldelivery.com>
To: 'Todd S. Glassey' <Todd.Glassey@www.GMTsw.com>; Mark Hastings <mark@digitaldelivery.com>
Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com
Subject: RE: Need to get some closure on the DD/GMT deal...
Date: Tuesday, April 13, 1999 4:56 PM

Hi Todd:

Long time no hear. Hope all is going well for you at GMT.

I too would like to complete our agreement. However, I am not sure about having received a deal from you. When was it sent?

I would also like to forward copies of the email and fax messages that were exchanged prior to your input into the application to your attorneys office so that they have a complete record.

I will be in the S.F. Bay Area the week of April 26 and possibly we could meet at that time to work out some of the details.

Later,

Mark Hastings;
President
Digital Delivery, Inc.

> -----Original Message-----

> From: Todd S. Glassey [mailto:Todd.Glassey@www.GMTsw.com]

> Sent: Monday, April 12, 1999 7:30 PM

> To: T. Mark Hastings

> Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com

> Subject: Need to get some closure on the DD/GMT deal....

>

>

> Mark, we are about to file the core technology patent for the
> geopositional

> timestamping tools and need to get our deal finished, or at least the
> non-financial portions thereof concluded.

>

> Let me know what your comments on the deal I forwarded to you
> were. The

> terms and conditions of the components exclusive of the financial
> compensation were just as we had agreed so in the very least

> I want to get

> that completed at the earliest convince.

>

> Todd Glassey, President.

> GMTsw, Inc.

>

>

Admin

From: Todd S. Glassey <Todd.Glassey@www.GMTsw.com>
To: T. Mark Hastings <mark@digitaldelivery.com>
Cc: jbook@SCLAWFIRM.COM; memcNeil@www.GMTsw.com
Subject: Need to get some closure on the DD/GMT deal...
Date: Monday, April 12, 1999 4:29 PM

Mark, we are about to file the core technology patent for the geopositional timestamping tools and need to get our deal finished, or at least the non-financial portions thereof concluded.

Let me know what your comments on the deal I forwarded to you were. The terms and conditions of the components exclusive of the financial compensation were just as we had agreed so in the very least I want to get that completed at the earliest convince.

Todd Glassey, President
GMTsw, Inc.

Admin

From: Admin <admin@sclawfirm.com>
To: Michael E. McNeil <memcneil@got.net>; Todd S. Glassey <todd.glassey@gmtsw.com>
Subject: Second Draft of Agreement between Glassey-McNeil and Digital Delivery, Inc.
Date: Wednesday, March 03, 1999 4:13 PM

Dear Todd and Michael,

Attached in rtf format please find the above-referenced Agreement, as well as a draft of a "cover letter" to Mark Hastings for Michael's signature. These documents are revised and drafted in accord with our brief conference of Thursday, February 25, 1999. Please review the attached documents and let me know your comments.

Best Regards,

Jason R. Book, Esq.
BOSSO, WILLIAMS, SACHS, BOOK, ATACK & GALLAGHER, P.C.
133 Mission Street, Suite 280
P.O. Box 1822, Santa Cruz, CA
95061-1822
(v.) (831) 426-8484
(f.) (831) 423-2839
(f.) (831) 458-9172

Admin

Todd. Glassey
@gntsw.com

From: Admin <admin@sclawfirm.com>
To: Michael E. McNeil <memcneil@got.net>; Todd S. Glassey <tgsman@earthlink.net>
Subject: Second Draft of Agreement between Glassey-McNeil and Digital Delivery, Inc.
Date: Wednesday, March 03, 1999 3:44 PM

Dear Todd and Michael,

Attached in rtf format please find the above-referenced document, as well as a draft of a "cover letter" to Mark Hastings for Michael's signature. Please review the attached documents and let me know your comments.

Best Regards,

Jason R. Book, Esq.
BOSSO, WILLIAMS, SACHS, BOOK, ATACK & GALLAGHER, P.C.
133 Mission Street, Suite 280
P.O. Box 1822, Santa Cruz, CA
95061-1822
(v.) (831) 426-8484
(f.) (831) 423-2839
(f.) (831) 458-9172

CONDITIONAL ASSIGNMENT OF PATENT
(for Filing and Management)

Conditional Assignment per terms of attached Co-Inventor Agreement

Whereas, we (Todd S Glassey)(and Michael E. McNeil) establish this conditional assignment per the terms of the Co-Inventor Agreement for Patent Filing and Management Services from Mr. Mark Hastings and Mr. Gerald Willets as individuals and through their Corporation, Digital Delivery Inc.

Period for Conditional Assignment

Said assignment is for the period of one calendar year as described in the Original Contract for Patent Filing Services called the Co-Inventor Agreement. Said assignment is for the filing of the US Patent and its foreign instances per the Co-Inventor Agreement and the Agreed-Upon group of foreign nations.

Hastings and Willets *(individually as named INVENTORS and as Digital Delivery inc)

As part of this assignment per the terms of the executed Co-Inventor Agreement Mark Hastings and Gerald Willets agree to act as our Agent(s) through their company Digital Delivery Inc (as individuals and professionally as Digital Delivery Inc).

Assignment by Agents

As a conditional assignment any reassignment of these rights must be properly documented per USPTO filing requirements. Further any and all re-assignment of these rights is per the terms of the Assignment Section of the Co-Inventor Agreement's Assign per the Terms and Conditions of the attached Co-Inventor Agreement. Without this release for Assignment from Glassey and McNeil no such reassignment may take place.

Payment for Assignment creates Pre-Paid legal Services Contract for Patent Agent Services

It is further stated in this assignment that as the sole compensation for "limited rights to use" as described in the Co-Inventor Contract between Hastings/Willets and Glassey/McNeil that the document constitutes a formal Pre-Paid Legal Service Agreement in the form of the Patent Filing and Management Services contemplated in the International Filings per the Co-Inventor Agreement

Executed this 10th day of July, 2013 Boulder Creek California, witness our signatures

Todd S Glassey	Michael E McNeil
<i>Todd S Glassey</i> 10-July-2013	<i>Michael E. McNeil</i> 2013-07-10

NOTARY

Before me personally appeared said Todd S. Glassey and Michael E. McNeil and acknowledge the foregoing instrument to be their free act and deed this 10th day of July, 2013

Seal :

*PLEASE SEE ATTACHED
CALIFORNIA ALL-PURPOSE Acknowledgment*

(Notary Public) _____

Date: _____ Location: _____

CO-INVENTOR AGREEMENT

This is Co-Inventor Agreement ("Agreement"), is made this 26th day of October, 1999 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.

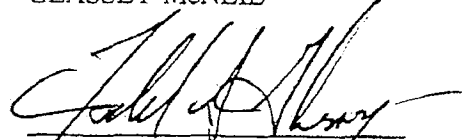
IN WITNESS WHEREOF, the parties hereto have executed this Agreement the day and year first above written.

DIGITAL DELIVERY


[Signature]

Todd S. Glassey President
[Please Print Name/Title]

GLASSEY-McNEIL


TODD S. GLASSEY

Michael E. McNeil
MICHAEL E. McNEIL

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California

County of Santa Cruz

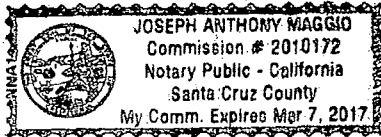
On 10 July 2013 before me, JOSEPH MAGGIO

personally appeared TODD STEVEN GLASSEY AND
MICHAEL E McVEIL

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.



Place Notary Seal Above

Signature Joseph Maggio
Signature of Notary Public

OPTIONAL

Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another document.

Description of Attached Document

Title or Type of Document: Conditional Assignment of Patent

Document Date: 10 July 2013 Number of Pages: 6

Signer(s) Other Than Named Above:

Capacity(ies) Claimed by Signer(s)

Signer's Name: Todd Glassey

☒ Individual

☐ Corporate Officer — Title(s):

☐ Partner — ☐ Limited ☐ General

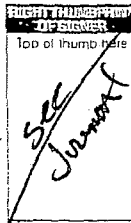
☐ Attorney in Fact

☐ Trustee

☐ Guardian or Conservator

☐ Other:

Signer Is Representing: Self



Signer's Name: Michael E McVeil

☒ Individual

☐ Corporate Officer — Title(s):

☐ Partner — ☐ Limited ☐ General

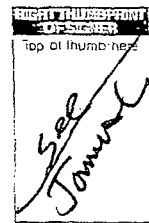
☐ Attorney in Fact

☐ Trustee

☐ Guardian or Conservator

☐ Other:

Signer Is Representing: Self



OTHER

-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Proc-Type: 2001,MIC-CLEAR

Originator-Name: webmaster@www.sec.gov

Originator-Key-Asymmetric:

MFgwCgYEVQg8AQICaf8DSgAwRwJAW2sNKK9AVtBzYZmr6aGjlWyK3XmZv3dTINen
TWSM7vrzLADbmYQaionwg5sDW3P6oaM5D3tdezXm7z1T+B+twIDAQAB

MIC-Info: RSA-MD5,RSA,

BHnZPXTGQtC5RSGZ1NRfbVVIPGNjXocmtTn4Hsc1Xv9rJpKv05dkapPM4LuAj4cY

+6G2gw6gskCQ0je4mYyFJg==

<SEC-DOCUMENT>0000892569-99-002093.txt : 19990809

<SEC-HEADER>0000892569-99-002093.hdr.sgml : 19990809

ACCESSION NUMBER: 0000892569-99-002093

CONFORMED SUBMISSION TYPE: 8-K

PUBLIC DOCUMENT COUNT: 2

CONFORMED PERIOD OF REPORT: 19990729

ITEM INFORMATION:

ITEM INFORMATION:

FILED AS OF DATE: 19990806

FILER:

COMPANY DATA:

COMPANY CONFORMED NAME:

DATUM INC

CENTRAL INDEX KEY:

0000027119

STANDARD INDUSTRIAL CLASSIFICATION:

INSTRUMENTS FOR MEAS & TESTING OF ELECTRICITY & ELEC SIGNALS [3825]

IRS NUMBER:

952512237

STATE OF INCORPORATION:

DE

FISCAL YEAR END:

1231

FILING VALUES:

FORM TYPE: 8-K

SEC ACT:

SEC FILE NUMBER: 000-06272

FILM NUMBER: 99679642

BUSINESS ADDRESS:

STREET 1: 9975 TOLEDO WAY

CITY: IRVINE

STATE: CA

ZIP: 92618

BUSINESS PHONE: 714-598-7500

MAIL ADDRESS:

STREET 1: 9975 TOLEDO WAY

CITY: IRVINE

STATE: CA

ZIP: 92618

</SEC-HEADER>

<DOCUMENT>

<TYPE>8-K

<SEQUENCE>1

<DESCRIPTION>FORM 8-K DATED JULY 29, 1999

<TEXT>

<PAGE> 1

SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT

Pursuant to Section 13 or 15(d) of the
Securities Exchange Act of 1934

Date of Report (Date of earliest event reported)

July 29, 1999

DATUM INC.

(Exact name of Registrant as specified in charter)

Delaware	0-6272	95-2512237
(State or other jurisdiction of incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

9975 Toledo Way, Irvine, California	92618-1819
(Address of principal executive offices)	(Zip Code)

Registrant's telephone number, including area code (949) 598-7500

Not Applicable (Former

name or former address, if changed, since last report.)

Page 1 of 5 Pages
Exhibit Index Begins on Page 5

<PAGE> 2

ITEM 2. ACQUISITIONS OR DISPOSITION OF ASSETS.

Acquisition of Digital Delivery, Inc.

On July 29, 1999, Datum Inc., a Delaware corporation ("Registrant"), acquired Digital Delivery, Inc., a Massachusetts corporation ("DDI"), pursuant to an Agreement and Plan of Merger, dated as of July 29, 1999 (the "Merger Agreement"), by and among Registrant, Datum Acquisition Sub., Inc., a wholly owned subsidiary of Registrant (the "Merger Subsidiary") and DDI. The acquisition was effected by the merger (the "Merger") of the Merger Subsidiary with and into DDI, with DDI surviving the Merger. The Merger was approved by the unanimous written consent of DDI's stockholders ("DDI Stockholders") on July 29, 1999. No vote by the Registrant's stockholders was required.

DDI is a leading provider of secure information and management software. DDI's patented encryption models and leading-edge compression technologies enable organizations to distribute data and conduct electronic commerce securely via the Internet, intranet, Extranet, CD-ROM and digital versatile disk.

Pursuant to the Merger Agreement, the Registrant agreed to issue 214,286 shares of its Common Stock, par value \$0.25 per share, in return for all the issued and outstanding shares of DDI Common Stock held by the stockholders of DDI Stockholders, and paid an aggregate total of \$1,500,000 out of cash on hand (the "Merger Consideration"). The DDI Stockholders will also receive additional consideration based on certain performance criteria of the Registrant through March 31, 2002.

The Merger Agreement is more fully described in Exhibit 2.1 to this Current Report and is incorporated herein by reference.

ITEM 7. FINANCIAL STATEMENTS, PRO FORMA FINANCIAL INFORMATION AND EXHIBITS.

(a) FINANCIAL STATEMENT OF BUSINESS ACQUIRED

The historical Financial Statements of DDI required to be filed under this Item are not available at this time and, accordingly, are not included herein. By an amendment to this Report to be filed as soon as practicable, the Registrant plans to submit such financial

statements.

(b) PRO FORMA FINANCIAL INFORMATION

The Pro Forma Financial Information to filed under this Item is not available and, accordingly is not included herein. By an amendment to this Report to be filed as soon as practicable, the Registrant plans to submit such pro forma information.

2

<PAGE> 3

(c) Exhibits

Exhibit Number

2.1 Agreement and Plan of Merger Agreement, dated July 29, 1999, among the Registrant, DDI and the Merger Subsidiary. Exhibit A (Form of Escrow Agreement), Exhibit B (Form of Investment Letter), Exhibit C (DDI Disclosure Schedule), Exhibit D (Datum Disclosure Schedule), Exhibit E (Form of Employment Agreement), Exhibit F (Form of Opinion of Counsel of DDI), Exhibit G (Form of Opinion of Counsel to Datum), Schedule I (Surviving Corporation Board of Directors and Officers), and Schedule II (DDI Stockholders) have been omitted pursuant to Rule 601(b)(2) of Regulation S-K. A copy of any Exhibit or Schedule will be submitted to the Commission supplementally upon request.

3

<PAGE> 4

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the Registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Date: July 29, 1999

DATUM INC.

/s/ DAVID A. YOUNG

David A. Young
Chief Financial Officer

4

<PAGE> 5

INDEX TO EXHIBITS

<TABLE>
<CAPTION>

Exhibit	Description	Page
2.1	Agreement and Plan of Merger Agreement, dated July 29, 1999, among the Registrant, DDI and the Merger Subsidiary. Exhibit A	6

(Form of Escrow Agreement), Exhibit B (Form of Investment Letter), Exhibit C (DDI Disclosure Schedule), Exhibit D (Datum Disclosure Schedule), Exhibit E (Form of Employment Agreement), Exhibit F (Form of Opinion of Counsel of DDI), Exhibit G (Form of Opinion of Counsel to Datum), Schedule I (Surviving Corporation Board of Directors and Officers), and Schedule II (DDI Stockholders) have been omitted pursuant to Rule 601(b)(2) of Regulation S-K. A copy of any Exhibit or Schedule will be submitted to the Commission supplementally upon request.

</TABLE>

</TEXT>

</DOCUMENT>

<DOCUMENT>

<TYPE>EX-2.1

<SEQUENCE>2

<DESCRIPTION>AGREEMENT & PLAN OF MERGER AGREEMENT

<TEXT>

<PAGE> 1

EXHIBIT 2.1

AGREEMENT AND PLAN OF MERGER

DATED AS OF JULY 29, 1999

BY AND AMONG

DATUM INC.,

DATUM ACQUISITION SUB, INC.,

AND

DIGITAL DELIVERY, INC.,

AND

THE DDI INDEMNITORS

(AS DEFINED HEREIN)

<PAGE> 2

AGREEMENT AND PLAN OF MERGER

This AGREEMENT AND PLAN OF MERGER, dated as of July 29, 1999 (this "Agreement"), is made and entered into by and among Datum Inc., a Delaware corporation ("Datum"), Datum Acquisition Sub, Inc., a Massachusetts corporation and wholly-owned subsidiary of Datum ("Sub"), Digital Delivery, Inc., a Massachusetts corporation ("DDI"), and, with respect to certain indemnification provisions hereof, Mssrs. Hastings, Subler, Fishman, Rubbico, Timothy Bowe and Morlock, each as further identified in Schedule II attached hereto, jointly and severally (the "DDI Indemnitors").

WHEREAS, the Board of Directors of each of Datum, Sub and DDI believes it to be desirable and in the best interests of Datum, Sub and DDI and each of their respective stockholders to merge Sub with and into DDI (the "Merger"); and

WHEREAS, Datum, Sub, DDI and the DDI Indemnitors desire to make certain representations, warranties and agreements in connection with the Merger and also to prescribe various conditions to the Merger;

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth in this Agreement, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

ARTICLE 1

THE MERGER

1.1 The Merger. At the Effective Time (as defined in Section 1.2), upon the terms and subject to the conditions set forth in this Agreement, the Sub shall be merged with and into DDI in accordance with the provisions of the Massachusetts Business Corporation Law ("MBCL"). DDI shall be the surviving corporation in the Merger (the "Surviving Corporation"). Sub and DDI are sometimes referred to herein as the "Constituent Corporations". As a result of the Merger, each outstanding share of capital stock of DDI shall be canceled and converted into the right to receive the Merger Consideration, in the manner provided in Article 2 hereof.

1.2 Effective Time. At the Closing (as defined in Section 1.3), articles of merger (the "Articles of Merger") shall be executed by the parties hereto and filed with the Secretary of the Commonwealth of the Commonwealth of Massachusetts (the "Secretary of State"). The Merger shall become effective at the time of filing of the Articles of Merger (the "Effective Time").

1.3 Closing. The closing of the Merger (the "Closing") shall take place at the offices of Stradling Yocca Carlson & Rauth, 660 Newport Center Drive, Suite 1600, Newport Beach, California 92660, at 10:00 a.m. (PST) on the date all of the conditions set forth herein have been satisfied or waived in accordance with this Agreement (the "Closing Date"). At the Closing, Datum, Sub and DDI shall deliver the certificates and other documents and instruments required to be delivered hereunder.

1.4 Articles of Organization, Bylaws and Purpose of the Surviving Corporation. At the Effective Time: (i) the Articles of Organization of DDI as in effect immediately prior to the Effective Time, including, without limitation, provisions related to the number, class and par value

<PAGE> 3

per share of authorized shares, shall be the Articles of Organization of the Surviving Corporation until thereafter amended; and (ii) the Bylaws of DDI as in effect immediately prior to the Effective Time shall be the Bylaws of the Surviving Corporation until thereafter amended, and (iii) the purpose of DDI immediately prior to the Effective Time shall be the purpose of the Surviving Corporation until thereafter amended.

1.5 Directors and Officers of the Surviving Corporation. The directors and officers of the Surviving Corporation from and after the Effective Time shall be as set forth on Schedule I attached hereto, until their successors shall have been duly elected or appointed and qualified or until their earlier death, resignation or removal in accordance with the Surviving Corporation's Article of Organization and Bylaws.

1.6 Effects of the Merger. Subject to the foregoing, the effects of the Merger shall be as provided in the applicable provisions of the MBCL.

1.7 Further Assurances. Each party hereto shall execute such further documents and instruments and take such further actions as may reasonably be requested by one or more of the others to consummate the Merger, to vest the Surviving Corporation with full title to all assets, properties, rights, approvals, immunities and franchises of either of the Constituent Corporations or to effect the other purposes of this Agreement.

ARTICLE 2

EXCHANGE OF SHARES

2.1 Exchange of Shares. At the Effective Time, by virtue of the Merger and without any action on the part of the holders of the capital stock of Sub or DDI:

(a) Cancellation of Treasury Stock. All shares of capital stock owned by DDI as treasury stock shall be canceled and no stock of Datum or other consideration shall be delivered in exchange therefor.

(b) Determination of Merger Consideration. Each issued and outstanding share of DDI common stock, \$1.00 par value ("DDI Stock"), issued and outstanding immediately prior to the Effective Time, except as otherwise provided in Section 2.1(a), shall be converted into the right to receive the "Merger Consideration" determined as set forth in Section 2.2; provided, however, that such Merger Consideration is subject to adjustment and set-off pursuant to Sections 2.3 and 9.3 hereof.

(c) Conversion of Sub Common Stock. Each share of common stock, par value \$0.01 per share, of Sub issued and outstanding immediately prior to the Effective Time shall be converted into and exchangeable for 1,000 shares of common stock, \$1.00 par value per share, of the Surviving Corporation. It is the intention of the parties that, immediately after the Merger, Datum shall own all of the issued and outstanding capital stock of the Surviving Corporation.

2.2 Merger Consideration. The Merger Consideration shall consist of the Primary Consideration and the Additional Consideration, if any, all as defined below.

(a) Primary Consideration. At the Closing, the holders of DDI Stock issued and outstanding immediately prior to the Effective Time (each, a "DDI Stockholder" and listed on

2

<PAGE> 4

Schedule II attached hereto), without any action on the part of the DDI Stockholders, shall be entitled to receive (subject to clause (b) below) in the aggregate in exchange for such DDI Stockholders' DDI Stock: (i) 214,286 shares of Datum common stock, par value \$0.25 per share ("Datum Common Stock", and such amount of shares, the "Primary Stock Consideration"); and (2) \$1,500,000.00 cash (the "Primary Cash Consideration", and collectively with the Primary Stock Consideration, the "Primary Consideration").

(b) Escrow of Primary Stock Consideration. At the Closing, 42,857 shares of Datum Common Stock (the "Escrowed Shares") shall be taken from the Primary Stock Consideration and placed into an escrow account, substantially similar to the form attached hereto as Exhibit A (the "Escrow Agreement"), for the purposes of indemnifying Datum in accordance with Section 9.2(d). The Escrowed Shares shall be held in escrow until the date (the "Release Date") of the earlier to occur of (a) the final, full settlement, whether through negotiated settlement, arbitration or court proceeding, of all claims existing as of the Effective Date among Todd S. Glassey and Michael E. McNeil (together, "Glassey-McNeil") and DDI; and (b) March 31, 2002. Upon the Release Date, the Escrowed Shares shall be distributed directly to the DDI Stockholders at the addresses and in accordance with the Ownership Percentages set forth on Schedule II.

(c) Additional Consideration. "Additional Consideration" shall consist of the First Earn-Out, the Second Earn-Out and the Hardware Sales Earn-Out, all as defined below and payable by Datum to the DDI Stockholders as follows.

(i) Definitions. For the purposes of determining the Additional Consideration:

(A) the term "Business" shall mean the development, distribution, marketing and sale of software, software applications, software development tools, systems solutions (including related hardware) and related services, such as installation, customer training, systems integration and

technical support, for electronic business and information security management applications (including DDI's Confidential Courier, Title Builder and Catalogue Builder software (all such software, the "Software")) (such Software and related services and hardware, the "Software Products"), as conducted by Datum's E-Business Solutions Division; provided, that Datum shall conduct all such development, distribution, marketing and sale of Software Products through the E-Business Solutions Division; and provided, further, however, that companies or businesses acquired by Datum, or the businesses of any acquiror of Datum in the event Datum is acquired, after the Merger shall be deemed excluded from the "Business" unless otherwise agreed by Datum.

(B) the term "Attributable to the Business" shall mean derived from or contributed to the Business, as reasonably determined by Datum's independent certified public accountants in accordance with generally accepted accounting principles ("GAAP") and past Datum accounting practices consistently applied.

(C) the term "Net Operating Income" shall mean, with respect to the Business, pre-tax income as reasonably determined by Datum's independent certified public accountants, in accordance with GAAP and past Datum accounting practices consistently applied, as the difference obtained by subtracting sales marketing expense, product development expense and general and administrative expense from Gross Margin. "Gross Margin" shall mean the difference obtained from subtracting cost of goods sold from sales revenue. In addition, Net Operating Income shall be determined with adherence to the following:

3

<PAGE> 5

(t) repayment of Advances, other than Advances used to make Restricted Payments (both as defined in Section 2.3(b) below), and accrued, unpaid interest thereon will be deducted from Gross Margin in calculating the Net Operating Income for the First Earn-Out Period (as defined below).

(u) there shall not be subtracted any Glassey-McNeil/DDI Damages (as defined in Section 9.2(d) below);

(v) sales of assets of the Business shall be included in sales revenue; provided, however, that, subject to Section 9.8 below, proceeds from the sale of all or substantially all of the assets of the Business shall not be so included;

(w) there shall not be subtracted any amortization or other expenses incurred by Datum, Sub or DDI in effecting the Merger, including without limitation legal and accounting expenses;

(x) the effect of any transactions between Datum (or any of its subsidiaries other than DDI) and the Business on other than an arm's-length basis shall be recalculated as if they had been on an arm's-length basis;

(y) subject to clauses (w) and (x) above, Datum may charge the Business for any costs directly incurred by Datum (or any of its subsidiaries other than DDI) on the Business's behalf; and

(z) payments of Additional Consideration, if any (and any imputed or stated interest thereon) will be excluded;

(ii) First Earn-Out. No later than March 31, 2001, Datum shall pay to the DDI Stockholders an amount equal to the sum of (y) the product of 15% of up to the first \$2 million of Net Operating Income Attributable to the Business during the period commencing on April 9, 1999, and concluding December 31, 2000, (the "First Earn Out Period") multiplied by six; and (z) the product of 15% of Net Operating Income Attributable to the Business in excess of \$2 million during the First Earn-Out Period multiplied by three, in the manner set forth in Section 2.2(v) below.

(iii) Second Earn-Out. No later than March 31, 2002, Datum shall pay to the DDI Stockholders an amount equal to the sum of (y) the product of 15% of up to the first \$5 million of Net Operating Income Attributable to the

Business during the period commencing January 1, 2001, and concluding December 31, 2001, (the "Second Earn Out Period") multiplied by six; and (z) the product of 15% of Net Operating Income Attributable to the Business in excess of \$5 million during the Second Earn-Out Period multiplied by three, in the manner set forth in Section 2.2(v) below.

(iv) Hardware Sales Earn-Out. Datum shall also pay to the DDI Stockholders an amount equal to 6% of revenue from sales Attributable to the Business (determined in accordance with GAAP consistently applied) of Datum's Trusted Local Clocks (Datum Part No. TLC-700), Trusted Third Party Clocks (Datum Part No. TMC-7000) and Time Serve Models (the Datum Part No. 2100 family of products) ("Designated Revenue") during the First and Second Earn Out Periods. The Hardware Sales Earn-Out for the First Earn-Out Period shall be paid no later than

4

<PAGE> 6

March 31, 2001, and the Hardware Sales Earn-Out for the Second Earn-Out Period shall be paid no later than March 31, 2002, both in the manner set forth in Section 2.2(v) below.

(v) Manner of Payment. Payments of Additional Consideration and Hardware Sales Earn-Outs, if any, will be made directly to the DDI Stockholders to the addresses set forth on, and in accordance with the Ownership Percentages of each shown on Schedule II. Datum may, at its sole discretion, make any payment of Additional Consideration to the DDI Stockholders in any combination of cash and Datum Common Stock. For purposes of such payments, Datum Common Stock shall be valued on a Twenty Day Rolling Basis. "Twenty Day Rolling Basis" means calculating the average of the closing prices of Datum Common Stock as reported on the Nasdaq National Market System for the twenty trading days ending on the trading day prior to the conclusion of the First Earn Out Period or the Second Earn Out Period, as applicable or, if shares of Datum Common Stock are not listed or admitted to trading on such exchange at such time of valuation, on the principal securities exchange on which such shares are listed or admitted to trading, or if no such sales are then being reported, the average of the highest reported bid and lowest reported asked prices as furnished by the National Association of Securities Dealers, Inc., through NASDAQ or another organization if NASDAQ is no longer reporting such information. If no price is determinable as described above for the purposes required herein, the fair value of such shares of Datum Common Stock, as reasonably determined by Datum's Board of Directors, shall be used. Notwithstanding the foregoing, (A) the cash component of any payment of Additional Consideration shall be no less than 25% and, unless necessary to comply with clause (B) below, no more than 75%; and (B) in no event shall the aggregate number of shares of Datum Common Stock issued to the DDI Stockholders as part of the Merger Consideration exceed 10% of the outstanding shares of Datum Common Stock as of the Closing Date, as adjusted for post-Closing stock dividends, stock splits and similar occurrences.

(d) Post-Closing Operations of DDI. Following the Closing, Datum shall in its sole discretion have complete control over all strategic and operational decisions concerning DDI, the Business and the Software Products, including without limitation decisions concerning the design, testing, manufacturing, pricing, warranting, marketing, advertising, and distribution of the Software Products, notwithstanding that such decisions may or will impact Net Operating Income Attributable to the Business or Designated Revenue. Datum agrees to use its discretion in making such decisions in good faith and without regard to any effect such decisions may have on the amount of Additional Consideration, if any, payable hereunder.

(e) Disputed Valuations. The DDI Representative (as described in Section 7.2(i) below) shall have the opportunity, after entering into a confidentiality agreement reasonably satisfactory to Datum, to inspect the books and records of Datum and DDI from time to time to verify the determinations of Additional Income made hereunder. In the event of any dispute, the dispute shall be determined in accordance with Section 2.4 below. The costs of such inspection shall be borne by the DDI Stockholders unless the amount of Additional Income determined in accordance with Section 2.4 is more than 105% of Datum's determination of Additional Income, in which event Datum shall bear such costs.

2.3 Adjustments to Merger Consideration for Indebtedness.

(a) Closing Balance Sheet. No later than three (3) business days prior to the Closing Date, DDI shall deliver to Datum DDI's unaudited balance sheet, dated the Closing Date (the "Closing Balance Sheet"). Datum may, within sixty (60) days after the Closing Date at its sole

5

<PAGE> 7

option with notice to the DDI Representative, prepare from DDI's books and records (in accordance with GAAP consistently applied) its own version of such Closing Balance Sheet, and if the two versions vary Datum and the DDI Representative shall meet to reconcile the versions and arrive at a final Closing Balance Sheet. In the event the parties cannot agree on a reconciled version, the dispute shall be determined in accordance with Section 2.4 below. The Closing Balance Sheet, if accepted by Datum at Closing, or in the alternative the reconciled Closing Balance Sheet resulting from the procedure described in the immediately preceding sentence, shall be the "Final Closing Balance Sheet".

(b) Merger Consideration Adjustment.

(i) If the Final Closing Balance Sheet reflects indebtedness of DDI in excess of the difference of (a) \$1 million plus DDI's aggregate accounts receivable created during the period beginning April 8, 1998 and ending on the Closing Date (such period, the "Pre-Merger Period"), less (b) any payments made against accounts payable shown on DDI's payables listing dated April 8, 1999 during the Pre-Merger Period (such payments, the "Restricted Payments", and such excess DDI indebtedness, the "Excess"), then the Primary Consideration shall be reduced dollar-for-dollar by the amount of the Excess (applying the Excess first against the Primary Cash Consideration until it is reduced to zero, then if necessary against the Primary Stock Consideration at a valuation of \$7.00 per share). If the Excess amount exceeds the aggregate Primary Consideration, it shall be grounds for termination of this Agreement pursuant to Section 8.1. For purposes of determining the Excess amount, indebtedness appearing on the Final Closing Balance Sheet representing amounts owing Datum under the Bridge Loan Agreement (as defined in Section 6.9 below) shall not be included, except if and to the extent any bridge loan proceeds ("Advances") were used to make Restricted Payments in which case such Advances and accrued unpaid interest thereon shall be included as DDI indebtedness in the calculation of the Excess.

(ii) The parties acknowledge and agree that (A) the part, if any, of the Advances which is not to be forgiven in accordance with Section 4(c) of the Bridge Financing Agreement, but is to be due and payable, with accrued interest thereon, on the Closing Date shall be deemed for the purposes of this Agreement and the Bridge Financing Agreement to equal the Restricted Payments, and DDI's obligations with respect to such indebtedness shall be deemed to be satisfied in full by the adjustment made to the Primary Consideration pursuant to this Section 2.3(b); (B) that such adjustment shall be deemed to have been made as of the Closing Date; (C) Datum has extended Fifty Thousand Dollars (\$50,000) more in Advances to DDI than the maximum "Loan Amount" provided for in the Bridge Financing Agreement, and the principal amount of the Advances outstanding thereunder on the date hereof equals Four Hundred Fifty Thousand Dollars (\$450,000); and (D) that the Bridge Financing Agreement is hereby amended by Datum and DDI to incorporate the foregoing acknowledgements and agreements as though originally incorporated into the terms thereof.

2.4 Valuation Dispute Resolution. To initiate a dispute between Datum and any DDI Stockholder with respect to any valuation made hereunder, the DDI Representative must notify Datum of such dispute within ten (10) business days of payment by Datum to the DDI Stockholders of the disputed amount, except that, if within such ten (10) business day period the DDI Representative requests to perform an inspection pursuant to Section 2.2(d), notification for the initiation of a dispute relating to such payment shall be made within ten (10) business days following the completion of such inspection. In the event the parties disagree as to the reconciliation of the Closing Balance Sheet under Section 2.3(a), this Section 2.4 shall be triggered automatically and the

<PAGE> 8

parties shall resolve the disagreement as set forth herein. In the case of such challenge or disagreement, the amount in dispute (the "Valuation") shall be determined as follows: (a) first, Datum and the DDI Representative shall engage in good faith discussions of the Valuation, following which a definitive Valuation may be agreed to; (b) if a definitive Valuation is not determined pursuant to the foregoing, Datum and the DDI Representative shall agree on a certified public accountant employed by a nationally recognized accounting firm ("CPA") to determine the calculation of the Valuation, in which case the amount so determined shall control; (c) if the definitive Valuation is not set pursuant to any of the foregoing, Datum and the DDI Representative shall each appoint their own CPA, each of whom shall determine the calculation of the Valuation. If the two calculations are within ten percent (10%) of each other, the average of the two shall be the definitive Valuation; (d) if the definitive Valuation is not set pursuant to any of the foregoing, the two CPAs shall together select a third CPA to determine the calculation of the Valuation. The definitive Valuation shall be equal to the average of the two closest calculations among the three. If the Valuation ultimately determined is equal to or less than the Valuation originally calculated by Datum (the "Original Price"), the DDI Stockholders shall bear the costs of such third CPA. If such amount is greater than the Original Price, but less than 105% of the Original Price, the costs of such third CPA shall be borne equally by Datum and the DDI Stockholders. If such amount is more than 105% of the Original Price, Datum shall bear the costs of such third CPA.

2.5 Dissenting Shares.

(a) Dissenters' Rights. Notwithstanding anything to the contrary in this Agreement, each share of DDI Stock issued and outstanding immediately prior to the Effective Time that is held by any DDI Stockholder who (i) has not voted in favor of the Merger, (ii) has perfected its right to an appraisal of its DDI Stock shares in accordance with the applicable provisions of the MBCL, and (iii) has not effectively withdrawn or lost such right to appraisal (a "Dissenting Share"), shall not be converted into the right to receive the Merger Consideration pursuant to Section 2.2, but shall be entitled only to such rights as are granted by the applicable provisions of the MBCL; provided, however, that any Dissenting Share held by a person at the Effective Time who shall, after the Effective Time, withdraw the demand for appraisal or lose the right of appraisal, in either case pursuant to the MBCL, shall be deemed to be converted into, as of the Effective Time, the right to receive the Merger Consideration pursuant to Section 2.2.

(b) Notice to Datum. DDI shall give Datum (i) prompt notice of any written demands for appraisal, withdrawals of demands for appraisal and any other instruments served pursuant to the applicable provision of the MBCL relating to the appraisal process received by DDI, and (ii) the opportunity to direct all negotiations and proceedings with respect to demands for appraisal under the MBCL, with the participation of DDI. DDI will not voluntarily make any payment with respect to any demands for appraisal and will not, except with the prior written consent of Datum, settle or offer to settle any such demands.

2.6 Fractional Shares. No fractional shares of Datum Common Stock shall be issued, but in lieu thereof each holder of shares of DDI Stock who otherwise would be entitled to receive a fraction of a share of Datum Common Stock (after aggregating all fractional shares of Datum Common Stock to be received by such holder) shall receive from Datum an amount of cash (rounded up to the nearest whole cent) equal to the product of the fraction of a share of Datum Common Stock to which such holder would otherwise be entitled times the valuation of the Datum Common Stock being used for the related payment.

<PAGE> 9

2.7 Exchange of Certificates.

(a) The Exchange. At the Closing, Datum shall deliver to each DDI Stockholder, in accordance with such DDI Stockholder's instructions, an amount equal to the sum of the Primary Cash Consideration due to such DDI Stockholder, as set forth on Schedule II (as adjusted pursuant to Section 2.3 above, if applicable). At the Closing, each DDI Stockholder shall deliver to Datum an investment letter, executed by such DDI Stockholder, containing customary representations and warranties to Datum with respect to the receipt of unregistered stock, substantially in the form attached hereto as Exhibit B (an "Investment Letter"). From and after the Closing, each DDI Stockholder shall deliver to ChaseMellon Shareholder Services, Datum's transfer agent ("ChaseMellon"), stock certificates representing the DDI Common Stock held by such DDI Stockholder, as set forth on Schedule II. Upon receipt of such DDI stock certificates, ChaseMellon shall deliver to the surrendering DDI Stockholder (i) certificates in the name of such DDI Stockholder representing such DDI Stockholder's Primary Stock Consideration, which shall be equal to the product of such DDI Stockholder's Ownership Percentage and 214,286 shares, as shown on Schedule II (as adjusted pursuant to Section 2.3 above, if applicable); provided, however, that the portion of such DDI Stockholder's Primary Stock Consideration that constitutes Escrow Shares shall be delivered to the escrow account; and (ii) the aggregate amount payable to such DDI Stockholder in lieu of fractional shares in accordance with Section 2.6. No transfer of ownership of DDI Stock which is not registered in the transfer records of DDI shall be recognized by Datum at the Closing, and Datum shall bear no liability with respect to such unrecorded transfer.

(b) No Further Ownership Rights in DDI Stock. Each holder of DDI Stock that has been converted into the Merger Consideration, upon surrender to Datum of the DDI Stock certificates in accordance with the terms hereof and other customary documentation, will be entitled to receive the Merger Consideration payable in respect of such DDI Stock. As of the Effective Time, all such DDI Stock shall no longer be outstanding and shall automatically be canceled, and each holder of DDI Stock certificates previously representing any such DDI Stock shall cease to have any rights with respect thereto, except the right to receive the Merger Consideration upon surrender of the certificates representing such DDI Stock as contemplated hereby. From and after the Effective Time, the stock transfer books of DDI shall be closed and there shall be no further registration of transfers on the stock transfer books of the Surviving Corporation of the shares of DDI Stock.

ARTICLE 3

REPRESENTATIONS AND WARRANTIES OF DDI

Except as disclosed on the DDI Disclosure Schedule attached hereto as Exhibit C (the "DDI Disclosure Schedule"), DDI represents and warrants to Datum and Sub as follows.

3.1 Organization and Qualification. DDI is a corporation duly organized, validly existing and in good standing under the laws of the Commonwealth of Massachusetts and has all requisite corporate power and authority to carry on its business as now conducted and as proposed to be conducted. DDI is duly qualified and licensed to do business and is in good standing in each jurisdiction in which the nature of its business or the ownership or leasing of its properties makes such qualification or licensing necessary, other than in such jurisdictions where the failure to be so qualified or licensed or to be in good standing (individually or in the aggregate) would not have a materially adverse effect on the business, condition (financial or otherwise), properties, assets

(including intangible assets), liabilities (including contingent liabilities), prospects, or results of operations (such effect, a "Material Adverse Effect") of DDI.

3.2 Subsidiaries. DDI does not own, directly or indirectly, any capital stock or other ownership interest in any corporation, partnership, joint

venture, or other entity.

3.3 Authority Relative to this Agreement. DDI has full corporate power and authority to enter into this Agreement, to perform its obligations hereunder and, subject to obtaining the approval of the DDI Stockholders, to consummate the transactions contemplated hereby. The execution, delivery and performance of this Agreement by DDI and the consummation by DDI of the transactions contemplated hereby have been duly and validly approved by DDI's Board of Directors, and DDI's Board of Directors has directed that this Agreement be submitted to the DDI Stockholders for their consideration and has recommended to the DDI Stockholders that the Agreement be approved. No other corporate proceedings on the part of DDI are necessary to authorize the execution, delivery and performance of this Agreement by DDI and the consummation by DDI of the transactions contemplated hereby other than such stockholder approval. This Agreement has been duly and validly executed by DDI and constitutes a valid and legally binding obligation of DDI, enforceable in accordance with its terms except (i) as limited by applicable bankruptcy, insolvency, reorganization, moratorium, and other laws of general application affecting enforcement of creditors' rights generally, and (ii) as limited by laws relating to the availability of specific performance, injunctive relief, or other equitable remedies (regardless of whether such enforceability is considered in a proceeding in equity or at law).

3.4 Capital Stock of DDI.

(a) Capitalization. The authorized capital stock of DDI consists solely of 200,000 shares of DDI Common Stock. As of the date hereof, 2,917.82 shares of DDI Common Stock were issued and outstanding, and owned as set forth in Schedule II, and no shares of DDI Common Stock are held as DDI treasury stock. All outstanding shares of capital stock of DDI are duly authorized, validly issued, fully paid, and nonassessable and not subject to preemptive rights. There are no bonds, debentures, notes, or other indebtedness of DDI having the right to vote (or convertible into securities having the right to vote) on any matters on which shareholders of DDI may vote. As of the date hereof, there are no securities, options, warrants, calls, rights, commitments, agreements, arrangements, or undertakings of any kind to which DDI is a party or by which it is bound obligating DDI to issue, deliver or sell, or cause to be issued, delivered or sold, additional shares of capital stock or other voting securities of DDI or obligating DDI to issue, grant, extend or enter into any such security, option, warrant, call, right, commitment, agreement, arrangement or undertaking (together, "DDI Options"). As of the date hereof, there are no outstanding contractual obligations of DDI to repurchase, redeem, or otherwise acquire any shares of capital stock of DDI. DDI has furnished to Datum true and correct copies of DDI's Article of Organization and Bylaws as in effect as of the date hereof. The offers and sales of all of the outstanding shares of capital stock of DDI were at all relevant times either registered under the Securities Act of 1933, as amended (the "Securities Act") and applicable state securities laws or exempt from such requirements.

(b) DDI Stockholders. Each DDI Stockholder is, and at the Closing will be the owner, beneficially and of record, of the number of shares of DDI Common Stock set forth opposite such DDI Stockholder's name on Schedule II (the "Shares"). All of the Shares are currently, and will be at the Closing, free and clear of all liens, claims, encumbrances, security interests, pledges,

equities, options, charges, restrictions and defects in title of any nature whatsoever ("Liens"), other than restrictions imposed by federal and applicable state securities laws which do not constitute an impediment to the exchange and cancellation described in this Agreement. Each DDI Stockholder has, and at the Closing will have, full legal right, capacity and power to deliver the Shares to Datum without obtaining the consent or approval of any other person or of any court, tribunal, arbitrator, authority, agency, commission, official or other instrumentality of the United States or any state, county, city or other political subdivision (a "Governmental or Regulatory Authority"). No DDI Stockholder has granted, and as of the Closing no DDI Stockholder shall have granted, and no DDI Stockholder is a party to, and as of the Closing no DDI Stockholder shall be a party to, any agreements, commitments or understandings

providing for the grant of any options to purchase or rights to acquire any of the Shares, obligating a DDI Stockholder to sell any of the Shares, or restricting such DDI Stockholder's right to transfer the Shares.

3.5 Non-Contravention; Consents.

(a) Non-Contravention. Except for the filing of the Articles of Merger and other appropriate merger documents required by the MBCL and appropriate documents with the relevant authorities of other states in which the Constituent Corporations are qualified to do business, the execution and delivery of this Agreement by DDI does not, and the performance by DDI of its obligations hereunder and the consummation of the transactions contemplated hereby will not, conflict with, result in a violation or breach of, constitute (with or without notice or lapse of time or both) a default under, result in or give to any person any right of payment or reimbursement, termination, cancellation, modification or acceleration of, or result in the creation or imposition of any lien upon any of the assets or properties of DDI under, any of the terms, conditions or provisions of (i) the Articles of Organization or Bylaws of DDI, or (ii)(A) any statute, law, rule, regulation or ordinance (together, "Laws"), or any judgment, decree, order, writ, permit or license (together, "Orders"), of any Governmental or Regulatory Authority applicable to DDI or any of their respective assets or properties, or (B) any note, bond, mortgage, security agreement, indenture, license, franchise, permit, concession, contract, lease or other instrument, obligation or agreement of any kind (together, "Contracts") to which DDI is a party or by which DDI or any of its assets or properties is bound, excluding from the foregoing clauses (A) and (B) conflicts, violations, breaches, defaults, payments, reimbursements, terminations, cancellations, modifications, accelerations and creations and impositions of liens which, individually or in the aggregate, could not be reasonably expected to have a Material Adverse Effect on DDI, taken as a whole, or on the ability of DDI to consummate the transactions contemplated by this Agreement.

(b) Consents. No consent, approval or action of, filing with or notice to any Governmental or Regulatory Authority or other public or private third party is necessary or required under any of the terms, conditions or provisions of any Law or Order of any Governmental or Regulatory Authority or any contract to which DDI is a party or by which DDI or any of its assets or properties is bound for the execution and delivery of this Agreement by DDI, the performance by DDI of its obligations hereunder or the consummation of the transactions contemplated hereby, other than such consents, approvals, actions, filings and notices which the failure to make or obtain, as the case may be, individually or in the aggregate, could not be reasonably expected to have a Material Adverse Effect on DDI, taken as a whole, or on the ability of DDI to consummate the transactions contemplated by this Agreement.

3.6 Financial Statements. DDI has delivered to Datum a true and complete copy of the following financial statements: (i) the unaudited balance sheets of DDI as of December 31, 1998 and

10

<PAGE> 12

the related unaudited statements of operations for the fiscal year then ended; and (ii) the unaudited balance sheet of DDI as of April 8, 1999 (the "DDI Financial Statements"). As of their respective dates and for the respective periods then ended, the DDI Financial statements (including, in each case, the notes, if any, thereto) (A) were prepared applying a tax-basis accounts method (as more fully described in the accountant's letter included in the DDI Disclosure Schedule) on a consistent basis during the periods involved (except as may be indicated therein or in the notes thereto); (B) fairly present the financial position of DDI as at the respective dates thereof and the results of its operations and cash flows for the respective periods then ended; and (C) did not contain any untrue statement of a material fact or omit to state a material fact required to be stated therein or necessary in order to make the statements therein, in light of the circumstances under which they were made, not misleading.

3.7 Absence of Changes. Since December 31, 1998, DDI has conducted its business only in the ordinary course, consistent with past practice and there

has been no change and no development in the business, properties, operations, condition (financial or otherwise), or results of operations of DDI taken as a whole, that had or could reasonably be expected to have a Material Adverse Effect other than those occurring as a result of general economic or financial conditions or other developments that are not unique to DDI but also affect other persons who participate or are engaged in the lines of business in which DDI participates or is engaged, or other than those occurring as a result of this Agreement and the transactions contemplated hereby.

3.8 Absence of Undisclosed Liabilities. Except for matters reflected or reserved against in the DDI Financial Statements, DDI did not have at December 31, 1998, nor has DDI incurred since that date, any liabilities or obligations (whether absolute, accrued, contingent, fixed or otherwise, or whether due or to become due) of any nature, except liabilities or obligations (a) which were incurred in the ordinary course of business consistent with past practice, and (b) which have not had, and could not be reasonably expected to have, individually or in the aggregate, a Material Adverse Effect on DDI.

3.9 Legal Proceedings. There are no actions, suits, arbitrations or proceedings pending or, to the knowledge of DDI, threatened against, relating to or affecting, nor are there any Governmental or Regulatory Authority investigations or audits pending, or to the knowledge of DDI, threatened against, relating to or affecting, DDI or any of its assets and properties which, individually or in the aggregate, could be reasonably expected to have a Material Adverse Effect on DDI, or on the ability of DDI to consummate the transactions contemplated by this Agreement.

3.10 Contracts and Commitments. The DDI Disclosure Schedule contains a true and complete list of each of the following types of written or oral contracts to which DDI is a party (such contracts, the "Material Contracts"):

(a) all contracts (excluding DDI Employee Benefit Plans (as defined below) which can be terminated at will without subjecting DDI to cost or penalty) providing for a commitment for employment or consultation services for a specified or unspecified term to, or otherwise relating to employment or the termination of employment of, any employee;

(b) all contracts with any person or entity containing any provision or covenant prohibiting or limiting the ability of DDI to engage in any business activity or compete with any person or entity in connection with their respective businesses or prohibiting or limiting the ability of any person or entity to compete with DDI in connection with their respective businesses;

11

<PAGE> 13

(c) all partnership, joint venture, shareholders' or other similar contracts with any person or entity in connection with DDI;

(d) all contracts relating to the future disposition or acquisition of assets of DDI, other than dispositions or acquisitions in the ordinary course of business;

(e) all other contracts with respect to DDI that (i) involve the payment or potential payment, pursuant to the terms of any such contract, by or to DDI of more than \$10,000 annually; and (ii) cannot be terminated within sixty (60) days after giving notice of termination without resulting in any material cost or penalty to DDI; and

(f) all contracts between DDI and any of (i) DDI's directors, officers, or employees, or any member of any such person's family, or (ii) the DDI Stockholders or any member of any such DDI Stockholder's family.

DDI has not received notice of a default under any Material Contract by any party thereto, nor has there occurred any event that with notice or lapse of time, or both, would constitute a material default by DDI under any of the Material Contracts to which it is a party. Each of the Material Contracts is enforceable against DDI thereto in accordance with its terms, except as such enforceability may be limited by general principles of equity or by bankruptcy, insolvency or other similar laws relating to rights of creditors. DDI has not

received notice that any party to any of the Material Contracts intends to cancel or terminate any of the Material Contracts or to exercise or not exercise any options under any of the Material Contracts

3.11 Taxes.

(a) Tax Returns. DDI has delivered to Datum correct and complete copies of all federal income tax returns, examination reports and statements of deficiencies assessed against or agreed to by DDI since its inception. No DDI tax returns have been audited by the Internal Revenue Service (the "IRS"), or are currently subject to an IRS audit.

(b) Timely Filing and Payment. DDI has filed all tax returns (including, without limitation, with respect to all property, income, payroll, sales, use, excise and franchise taxes) that are required to have been filed by it in any jurisdiction for all periods ending on or prior to the date hereof and such tax returns are true, correct and complete in all material respects, and DDI has paid all taxes shown to be due and payable on such returns and all other taxes and assessments payable by it to the extent the same have become due and payable and before they have become delinquent, except for any taxes and assessments the amount, applicability or validity of which is currently being contested in good faith by appropriate proceedings and with respect to which DDI has set aside on its books reserves (segregated to the extent required by GAAP, consistently applied throughout the specified period and in the immediately comparable period) deemed by it in its reasonable discretion to be adequate. DDI is not currently the beneficiary of any extension of time within which to file any tax return, nor has it waived any statute of limitations in respect of taxes nor agreed to any extension of time with respect to a tax assessment or deficiency. DDI has not received written notice of any claim made by any Governmental or Regulatory Authority in a jurisdiction where DDI does not file tax returns that DDI should file tax returns.

12

<PAGE> 14

(c) Withholding. DDI has withheld and paid all taxes required to have been withheld and paid in connection with amounts paid or owing to any employee, independent contractor, creditor, stockholder or other third party.

(d) Assessments and Liens. DDI has no knowledge of any proposed tax assessment, obligation or other claim against DDI and all tax liabilities of DDI are adequately provided for on the books of DDI. There are no liens for taxes upon any property or assets of DDI, except for liens for taxes not yet due.

(e) Controversies. There are no unresolved issues of law or fact arising out of a notice of deficiency, proposed deficiency or assessment from the IRS or any other Governmental or Regulatory Authority with respect to taxes of DDI which, if decided adversely, singly or in the aggregate, would have a Material Adverse Effect on DDI.

(f) Tax Sharing Agreements. DDI is not a party to any agreement providing for the allocation or sharing of taxes with any entity other than agreements the consequences of which are adequately reserved for in the DDI Financial Statements.

(g) Section 341(f). DDI has not filed a consent under Section 341(f) of the Code concerning collapsible corporations.

(h) Affiliated Group. DDI has never been a member of an "affiliated group" as that term is described under Section 1504 of the Code, filing a consolidated federal income tax return, and is not liable for the taxes of any other person under Treasury Regulation Section 1.4502-6 (or any similar provision of state, local or foreign law), as a successor or transferor, by contract or otherwise.

(i) Pending Rulings. There is no ruling issued to DDI (or closing agreement or gain recognition agreement to which DDI is a party) nor are any contemplated concerning taxes from or with any Governmental or Regulatory Authority which will have an effect on DDI after the Closing Date.

(j) Extraordinary Payments. DDI has not made any payments, and is not a party to any agreement that obligates it to make any payments, that would not be deductible, in whole or in part, under Sections 280G or 162(m) of the Code.

(k) Foreign Person. DDI is not a foreign person subject to withholding under Section 1445 of the Code.

3.12 Employee Benefit Plans; ERISA

(a) No prohibited transaction within the meaning of Section 406 or 407 of the Employee Retirement Income Security Act of 1974, as amended ("ERISA"), or Section 4975 of the Code with respect to any DDI Employee Benefit Plan (as defined below) has occurred during the five-year period preceding the date of this Agreement.

(b) There is no outstanding liability (except for premiums due) under Title IV of ERISA with respect to any DDI Employee Benefit Plan.

13

<PAGE> 15

(c) Neither the Pension Benefit Guaranty Corporation nor DDI has instituted proceedings to terminate any DDI Employee Benefit Plan.

(d) Full payment has been made of all amounts which DDI was required to have paid as a contribution to DDI Employee Benefit Plans as of the last day of the most recent fiscal year of each of DDI Employee Benefit Plans ended prior to the date of this Agreement, and none of DDI Employee Benefit Plans has incurred any "accumulated funding deficiency" (as defined in Section 302 of ERISA and Section 412 of the Code), whether or not waived, as of the last day of the most recent fiscal year of each such DDI Employee Benefit Plan ended prior to the date of this Agreement.

(e) The value on a termination basis of accrued benefits under each of DDI Employee Benefit Plans which is subject to Title IV of ERISA, based upon the actuarial assumptions used for funding purposes in the most recent actuarial report prepared by such DDI Employee Benefit Plan's actuary with respect to each such DDI Employee Benefit Plan, did not, as of its latest valuation date, exceed the then current value of the assets of such DDI Employee Benefit Plan.

(f) Each of DDI Employee Benefit Plans which is intended to be "qualified" within the meaning of Section 401(a) of the Code has been determined by the IRS to be so qualified and such determination has not been modified, revoked or limited.

(g) Each of DDI Employee Benefit Plans is, and its administration is and has been during the five-year period preceding the date of this Agreement in all material respects in compliance with, and DDI has not received any claim or notice that any such Company Employee Benefit Plan is not in compliance with, all applicable laws and orders and prohibited transaction exemptions, including, without limitation, the requirements of ERISA.

(h) There are no material pending or, to the knowledge of DDI, threatened or anticipated claims involving any of DDI Employee Benefit Plans other than claims for benefits in the normal course.

(i) To the knowledge of DDI, during the five-year period preceding the date of this Agreement, DDI has not entered into any transaction which could subject such entity to liability under Section 302(c)(ii), 4062, 4063, 4064, or 4069 of ERISA and no "reportable event" within the meaning of Section 4043 of ERISA has occurred with respect to any DDI Employee Benefit Plan.

(j) DDI is not in default in performing any of its contractual obligations under any DDI Employee Benefit Plan or any related trust agreement or insurance contract.

(k) There are no material outstanding liabilities of any DDI Employee Benefit Plan other than liabilities for benefits to be paid to participants in such DDI Employee Benefit Plan and their beneficiaries in

accordance with the terms of such DDI Employee Benefit Plan.

(l) DDI does not maintain and is not obligated to provide benefits under any life, medical or health plan which provides benefits to retirees or other terminated employees other than benefit continuation rights under the Consolidated Omnibus Reconciliation Act of 1985, as amended.

14

<PAGE> 16

(m) Neither the execution and delivery of this Agreement nor the consummation of the transactions contemplated hereby will accelerate benefits under any DDI Employee Benefit Plan.

As used herein:

(i) the term "DDI Employee Benefit Plan" means any Plan entered into, established, maintained, contributed to or required to be contributed to by DDI and existing on the date of this Agreement or at any time subsequent thereto and on or prior to the Effective Time and, in the case of a Plan which is subject to Part 3 of Title I of ERISA, Section 412 of the Code or Title IV of ERISA, at any time during the five-year period preceding the date of this Agreement; and

(ii) the term "Plan" means any employment, bonus, incentive compensation, deferred compensation, pension, profit sharing, retirement, stock purchase, stock option, stock ownership, stock appreciation rights, phantom stock, leave of absence, layoff, vacation, day or dependent care, legal services, cafeteria, life, health, medical, accident, disability, workers' compensation or other insurance, severance, separation, termination, change of control or other benefit plan, agreement, practice, policy or arrangement of any kind, whether written or oral, including, but not limited to any "employee benefit plan" within the meaning of Section 3(3) of ERISA.

3.13 Title to Assets. DDI is in possession of and has good title to, or has valid leasehold interests in or valid rights under contract to use, all of its properties and assets used in its business and material to the condition (financial or other) of such business, free and clear of all mortgages, liens, pledges, charges or encumbrances of any nature whatsoever, except (a) liens for current taxes, payments of which are not yet delinquent; (b) such imperfections in title and easements and encumbrances, if any, as are not substantial in character, amount or extent and do not materially detract from the value of or interfere with the present use of the property subject thereto or affected thereby, or otherwise materially impair DDI's business operations in the manner presently carried on by DDI; or (c) as disclosed in the DDI Financial Statements, and except for such matters which, individually or in the aggregate, would not have a Material Adverse Effect on DDI. All leases under which DDI leases any substantial amount of real or personal property have been delivered to Datum and are in good standing, valid and effective in accordance with their respective terms, and there is not, under any of such leases, any existing default by DDI or event which with notice or lapse of time or both would become a default by DDI, other than defaults under such leases which in the aggregate would not have a Material Adverse Effect on DDI.

3.14 Intellectual Property. In addition to the representations and warranties contained in Section 3.13 above and without duplication, DDI hereby represents and warrants to Datum and Sub as follows.

(a) Title to Intellectual Property. DDI owns a valid right, title, interest or license in and to the intellectual property set forth in the DDI Disclosure Schedule (except as disclosed thereon) (the "DDI Intellectual Property") and any Third Party Technology (as defined below) used in or necessary for the conduct of the business of DDI as presently conducted ("DDI's Operations"), including, without limitation, the right to bring actions for infringement of the DDI Intellectual Property. The conduct of DDI's Operations currently does not conflict with and in the past has not conflicted with the intellectual property rights of others and no person or entity other than DDI owns any right, title or interest in the DDI Intellectual Property, including without limitation any right to

<PAGE> 17

manufacture, use, copy, distribute or sublicense any object code or source code thereof. All DDI Intellectual Property used or held for use in the conduct of DDI's Operations which is owned by DDI is so owned free and clear of all liens and no other person, including any present or former employee, shareholder, officer of DDI, has any right whatsoever in such DDI Intellectual Property. DDI has the right to convey the DDI Intellectual Property being used or held for use to conduct DDI's Operations and such conveyance will not violate any of the intellectual property rights of any other person or entity. Neither DDI nor any present or former DDI employee has violated or, by conducting DDI's Operations in the ordinary course would violate, any of the intellectual property rights of any other person or entity. DDI does not have any obligation to compensate any person or entity for the use of any DDI Intellectual Property, nor has DDI granted to any person or entity any license, option or other rights to use in any manner any DDI Intellectual Property, whether requiring the payment of royalties or not.

(b) Third Party Technology. "Third Party Technology" shall mean all intellectual property and products owned by third parties and licensed pursuant to Third Party Licenses as defined below. Notwithstanding the foregoing, Third Party Technology shall not include any "off-the-shelf" software program if the use of such program by DDI is in accordance with any applicable shrink wrap license and no portion of such program is distributed or licensed by DDI to third parties or incorporated into products distributed by DDI or licensed to third parties. "Third Party License" shall mean all licenses and other agreements with third parties relating to any intellectual property or products that DDI is licensed or otherwise authorized by such third parties to use in connection with the DDI Intellectual Property identified as software in the DDI Disclosure Schedule (the "DDI Software") (including, without limitation, all quality assurance systems or technology), market or distribute along with or as part of the DDI Software, or to distribute or incorporate into the DDI Software, in each case as the DDI Software exists on the date hereof.

(c) Public Domain. No DDI Intellectual Property is in the public domain.

(d) Copyrights. All of DDI's copyright registrations related to any and all of DDI's copyrights relating to the Software are valid and in full force and effect. DDI has valid copyrights in all material copyrightable material included in the DDI Intellectual Property whether or not registered with the U.S. Copyright Office, and consummation of the transactions contemplated hereby will not alter or impair the validity of any such copyrights or copyright registrations.

(e) Claims. DDI has not received notice of any claims asserted against DDI by any person challenging DDI's use or distribution (including manufacture, marketing license, or sale) of the Software Products or any Third Party Technology, or challenging or questioning the validity or effectiveness of any license or agreement relating thereto (including, without limitation, the Third Party Licenses). To the knowledge of DDI, there is no valid basis for any such claim.

(f) Infringement. To DDI's knowledge, no third party is violating, infringing, or misappropriating any right or contract of DDI as related to DDI's Operations.

(g) Continuity of Rights. To DDI's knowledge, no party to any contract, commitment or restriction relating to any right of DDI, including any Third Party Technology, intends to cancel, withdraw, modify or amend such contract as related to DDI's Operations.

(h) Sole Right to Third Party Technology. No DDI Stockholder, employee or contractor, nor any of their respective affiliates, has any right, title or interest in or to any Third Party

<PAGE> 18

Technology, other than rights pertaining to the Third Party Technology obtained from one or more third party licensors.

(i) Sole Right to Intellectual Property and Software Products. (i) No third party has any right to manufacture, reproduce, distribute, sell, sublicense, market or exploit any of the DDI Intellectual Property rights, or any adaptations, translations, or derivative works based on such rights, or any portion thereof, other than rights pertaining to Third Party Technology obtained from the third party licensor; (ii) DDI has no agreements, contracts or commitments that provide for the manufacture, reproduction, distribution, sale, sublicensing, marketing, development, exploitation, or supply by DDI of the DDI Intellectual Property or Software Products or any adaptation, translation, or derivative work based on the DDI Intellectual Property or Software Products, or any portion thereof; (iii) DDI has not granted to any third party any exclusive rights of any kind with respect to any of the DDI Intellectual Property or Software Products, including territorial exclusivity or exclusivity with respect to particular versions, implementations or translations of any of the DDI Intellectual Property or Software Products; and (iv) DDI has not granted any third party any right to market any product utilizing any Software under any "private label" arrangements pursuant to which DDI is not identified as the source of such goods. Each document or instrument reflecting any such arrangements is listed in the DDI Disclosure Schedule and true and correct copies of such documents or instruments have been furnished to Datum. Except with respect to the rights of third parties to the Third Party Technology, no third party has any right to manufacture, reproduce, distribute, sublicense, market or exploit any works or materials of which any of the DDI Intellectual Property are a derivative work.

(j) Preservation of Software. DDI has not knowingly altered data related to the Software in a manner that may damage the Software, whether stored in electronic, optical, or magnetic or other form.

(k) End-User Documentation. DDI has furnished to Datum, or will furnish to Datum at Closing, true and accurate copies of all end user documentation that exists relating to the use, maintenance or operation of the DDI Software.

(l) Year 2000. The DDI Intellectual Property, the Third Party Technology used in DDI's Operations and the DDI Software (as it exists on the date hereof) shall record, store, transmit, receive, process (which includes calculations, comparisons, sequencing, display or storage), and present date data and leap year calculations from, into and between the 20th and 21st centuries, and during the years 1999 and 2000, in the same manner, and with the same functionality, as the same does for calendar dates on or before December 31, 1999.

3.15 Permits, Etc. DDI owns or validly holds all licenses, permits, certificates of authority, registrations, franchises and similar consents granted or issued by any applicable Governmental or Regulatory Authority, used or held for use which are required to conduct and material to the condition of their respective businesses.

3.16 Compliance with Laws. DDI is not in violation of, nor has it violated, any applicable provisions of any Laws or any term of any Order binding against it, except for violations which do not have and would not have, individually or in the aggregate, a Material Adverse Effect on DDI. The DDI Disclosure Schedule sets forth a complete list of DDI's licenses, permits and authorizations other than those not material to DDI's business or operations ("Permits"). No Governmental or Regulatory Authority has revoked or materially limited any Permit of DDI, and no investigation or

<PAGE> 19

proceeding is pending or, to DDI's knowledge, threatened, which involves the

revocation or material limitation of any Permit. DDI is not in possession of any information which would lead it to believe that any Permits will not remain in full force and effect for the complete duration of their respective terms. DDI has made available to Datum all material filings made to, and all inspection or compliance reports or correspondence received from, Governmental and Regulatory Authorities for the last three years and will make available to Datum all other Permits as requested by Datum. Each of such filings was in material compliance with all applicable laws and regulations.

3.17 Labor Controversies. There are no material controversies pending or, to the knowledge of DDI, threatened between DDI and any representatives of any of DDI's employees. There are no material organizational efforts presently being made involving any of the presently unorganized employees of DDI. DDI has complied in all material respects with all Laws relating to the employment of labor, including without limitation, any provisions thereof relating to wages, hours, collective bargaining, and the payment of social security and similar taxes. No person has asserted that DDI is liable in any material amount for any arrears of wages or any taxes or penalties for failure to comply with any of the foregoing, except for such controversies, organizational efforts, non-compliance and liabilities which, individually or in the aggregate, could not be reasonably expected to have a Material Adverse Effect on DDI.

3.18 Insurance. The DDI Disclosure Schedule lists all policies of fire, liability, life and employee health, environmental, errors and omissions, workers' compensation and other forms of insurance currently held and maintained by DDI ("DDI Insurance Policies"). The DDI Insurance Policies are commercially reasonable in amount and coverage. All DDI Insurance Policies are in full force and effect, all billed premiums with respect thereto covering all periods up to and including the Closing Date have been paid or will have been paid on or prior to the Closing Date and no written notice of cancellation or termination has been received with respect to any DDI Insurance Policy, except for failures to pay or cancellations or terminations which would not reasonably be expected to have a Material Adverse Effect on DDI.

3.19 Guaranties. DDI has not executed any guaranty or otherwise agreed to be a guarantor of any liability or obligation (including indebtedness) of any other person.

3.20 Brokers or Finders. Neither DDI nor the DDI Stockholders has any obligation to pay any agent, broker, investment banker, financial advisor or other firm or other person any broker's or finder's fee or any other commission or similar fee in connection with any of the transactions contemplated by this Agreement.

3.21 Full Disclosure. No information furnished by or on behalf of DDI to Datum pursuant to this Agreement and any information contained in the DDI Disclosure Schedule and the other schedules and exhibits to this Agreement, at any time prior to the Closing Date, contains nor will contain any untrue statement of a material fact and does not and will not omit to state any material fact necessary to make any statement, in light of the circumstances under which such statement is made, not misleading.

REPRESENTATIONS AND WARRANTIES OF DATUM AND SUB

18

<PAGE> 20

Except as disclosed on the Datum Disclosure Schedule attached hereto as Exhibit D (the "Datum Disclosure Schedule"), Datum and Sub jointly and severally represent and warrant to DDI as follows.

4.1 Organization and Qualification. Each of Datum and Sub is an entity duly organized, validly existing and in good standing under the laws of their respective jurisdictions. Datum and Sub each have full corporate power and authority to own or lease and to operate and use their respective properties and assets and to carry on their respective businesses as now conducted and as proposed to be conducted pursuant to this Agreement. Each of Datum and Sub are duly qualified or licensed to do business and is in good standing in each

jurisdiction in which the nature of their respective businesses or the ownership or leasing of their respective properties make such qualification or licensing necessary, other than in such jurisdictions where the failure to be so qualified or licensed or to be in good standing (individually or in the aggregate) would not have a Material Adverse Effect on Datum and its subsidiaries, taken as a whole.

4.2 Authorization. Each of Datum and Sub has full corporate power and authority to execute, deliver and perform this Agreement and to consummate the transactions contemplated hereby. The execution, delivery and performance of this Agreement by Datum and Sub has been duly authorized and approved by the respective Boards of Directors of Datum and Sub and does not require any further authorization or consent of Datum or Sub. This Agreement has been duly authorized, validly executed and delivered by both Datum and Sub and constitutes the legal, valid and binding obligations of each enforceable in accordance with its terms, except as the enforceability thereof may be subject to or limited by (i) bankruptcy, insolvency, reorganization, arrangement, moratorium or other similar laws now or hereafter in effect relating to or affecting creditors' rights, and (ii) general equitable principles, regardless of whether the issue of enforceability is considered in a proceeding in equity or at law.

4.3 Capital Stock of Datum and Sub.

(a) Datum. The authorized capital stock of Datum consists of 10,000,000 shares of Datum Common Stock and 1,000,000 shares of preferred stock. As of April 23, 1999, there were 5,549,264 shares of Common Stock and no shares of preferred stock issued and outstanding. No shares of Datum Common Stock are held by Datum in its treasury. Except for additional grants made in the ordinary course of business consistent with past practices, as of the Effective Time, outstanding options to purchase shares of Datum Common Stock and the shares of Datum Common Stock reserved for issuance upon the exercise of Datum Options (as defined below) shall be as disclosed in the Datum Reports (as defined below). All outstanding shares of capital stock of Datum are duly authorized, validly issued, fully paid, and nonassessable and not subject to preemptive rights, and such capital stock has been issued in full compliance with all applicable federal and state securities laws. There are no bonds, debentures, notes, or other indebtedness of Datum having the right to vote (or convertible into securities having the right to vote) on any matters on which stockholders of Datum may vote. Except as set forth above, as of the date hereof, there are no securities, options, warrants, calls, rights, commitments, agreements, arrangements, or undertakings of any kind to which Datum is a party or by which it is bound obligating Datum to issue, deliver or sell, or cause to be issued, delivered or sold, additional shares of capital stock or other voting securities of Datum or obligating Datum to issue, grant, extend or enter into any such security, option, warrant, call, right, commitment, agreement, arrangement or undertaking (together, "Datum Options"). Except as are entered into in the ordinary course of business consistent with past practices, as of the date hereof the outstanding contractual obligations of Datum to repurchase,

19

<PAGE> 21

redeem, or otherwise acquire any shares of capital stock of Datum are as disclosed in the Datum reports. Datum has furnished to DDI true and correct copies of Datum's Certificate of Incorporation and Bylaws as in effect as of the date hereof.

(b) Sub. The authorized capital stock of Sub consists solely of 100 shares of common stock, \$0.01 par value, all of which shares are issued and outstanding and owned of record by Datum. There are no outstanding options, warrants, or other rights to subscribe for or purchase from Datum any capital stock of Sub, or securities convertible into any capital stock of Sub.

4.4 Non-Contravention; Consents.

(a) Non-Contravention. Except for the filing of the Articles of Merger and other appropriate merger documents required by the MBCL with the Secretary of State and appropriate documents with the relevant authorities of other states in which the Constituent Corporations are qualified to do business, the execution and delivery of this Agreement by Datum and Sub does not, and the

performance by Datum and Sub of their respective obligations hereunder and the consummation of the transactions contemplated hereby will not conflict with, result in a violation or breach of, constitute (with or without notice or lapse of time or both) a default under, result in or give to any person any right of payment or reimbursement, termination, cancellation, modification or acceleration of, or result in the creation or imposition of any Liens upon any of the assets or properties of Datum under, any of the terms, conditions or provisions of (i) the Certificates of Incorporation or Bylaws of Datum, or the Articles of Incorporation or Bylaws of Sub, or (ii)(A) any Laws or Orders of any Governmental or Regulatory Authority applicable to Datum or Sub or any of their respective assets or properties, or (B) any Contracts to which Datum or Sub is a party or by which Datum or Sub or any of their respective assets or properties is bound, excluding from the foregoing clauses (A) and (B) conflicts, violations, breaches, defaults, payments, reimbursements, terminations, cancellations, modifications, accelerations and creations and impositions of Liens which, individually or in the aggregate, could not reasonably be expected to have a Material Adverse Effect on Datum and its subsidiaries, taken as a whole, or on the ability of Datum or Sub to consummate the transactions contemplated by this Agreement.

(b) Consents. No consent, approval or action of, filing with or notice to any Governmental or Regulatory Authority or other public or private third party is necessary or required under any of the terms, conditions or provisions of any Law or Order of any Governmental or Regulatory Authority or any contract to which Datum or Sub is a party or by which Datum or Sub or any of their respective assets or properties is bound for the execution and delivery of this Agreement by Datum and Sub, the performance by Datum and Sub of their respective obligations hereunder or the consummation of the transactions contemplated hereby, other than such consents, approvals, actions, filings and notices which the failure to make or obtain, as the case may be, individually or in the aggregate, could not reasonably be expected to have a Material Adverse Effect on Datum and its subsidiaries, taken as a whole, or on the ability of Datum or Sub to consummate the transactions contemplated by this Agreement.

4.5 No Litigation or Regulatory Action. Except as disclosed in the Datum Reports (as defined below), there are no actions, suits, arbitrations or proceedings pending or, to the knowledge of Datum, threatened against, relating to or affecting, nor are there any Governmental or Regulatory Authority investigations or audits pending, or to the knowledge of Datum, threatened against, relating to or affecting, Datum or Sub or any of their respective assets and properties which, individually or in the aggregate, could be reasonably expected to have a Material Adverse Effect on

20

<PAGE> 22

Datum and its subsidiaries, taken as a whole, or on the ability of Datum to consummate the transactions contemplated by this Agreement.

4.6 SEC Documents. Datum has filed with the SEC true and correct copies of each registration statement, report, definitive proxy statement or definitive information statement and all exhibits thereto filed (including exhibits and any amendments thereto) required under or pursuant to the Securities Act or the Securities Exchange Act of 1934, as amended (the "Exchange Act", and together with the Securities Act, the "Securities Laws"), (collectively, the "Datum Reports"). As of their respective dates, or as subsequently amended prior to the Closing Date, the Datum Reports complied in all material respects with the requirements of the Securities Laws applicable to such Datum Reports, and none of the Datum Reports contained any untrue statement of a material fact or omitted to state a material fact required to be stated therein or necessary in order to make the statements therein, in light of the circumstances under which they were made, not misleading. The financial statements of Datum included in the Datum Reports comply in all material respects with applicable accounting requirements in the published rules and regulations of the SEC with respect thereto, have been prepared in accordance with GAAP applied on a consistent basis (except as may be indicated in the notes thereto) and fairly present the consolidated financial position of Datum and its consolidated subsidiaries as of the dates thereof and the consolidated results of their operations and cash flows for the periods then ended (subject, in the case of unaudited statements, to normal year-end audit adjustments, the absence of notes and as permitted by

Form 10-Q of the Exchange Act). As of their respective dates, the Datum Reports complied as to form in all material respects with the applicable requirements of the Securities Laws.

4.7 Brokers and Finders. Neither Datum nor Sub have employed any broker, finder, consultant or intermediary in connection with the transactions contemplated by this Agreement who would be entitled to a broker's, finder's or similar fee or commission in connection therewith or upon the consummation thereof.

4.8 Datum Stock Issued in Merger. The shares of Datum Common Stock to be issued in the Merger will, when issued and delivered to the DDI Stockholders as a result of the Merger and pursuant to the terms of this Agreement, be duly and validly authorized and issued, fully paid, non-assessable and free of preemptive rights of any securityholder of Datum, and issued in compliance with applicable federal and state securities laws.

4.9 Datum Intellectual Property. To its knowledge Datum owns, or is licensed or otherwise has the full and exclusive right to use, all patents, trademarks, trade names, copyrights, technology, know-how and processes used in or necessary for the conduct of the Business as presently conducted and, other than with respect to those matters addressed in Section 9.2(e), as currently contemplated to be conducted by Datum and DDI (except for such property intended for use in the Business that is currently owned or licensed by DDI), and for the sale of the hardware referenced in Section 2.2(c)(iv).

4.10 Full Disclosure. No information furnished by or on behalf of Datum or Sub to DDI pursuant to this Agreement nor any information contained in the Datum Disclosure Schedule and other schedules and exhibits to this Agreement, at any time prior to the Closing Date contains nor will contain any untrue statement of a material fact and does not and will not omit to state any material fact necessary to make any statement, in light of the circumstances under which such statement is made, not misleading.

21

<PAGE> 23

ARTICLE 5

COVENANTS

5.1 Covenants of DDI. At all times from and after the date hereof until the Effective Time, DDI covenants and agrees that (except as expressly contemplated or permitted by this Agreement, or to the extent that Datum shall otherwise consent in writing):

(a) DDI shall conduct its business only in, and DDI shall not take any action except in, the ordinary course consistent with past practice.

(b) Without limiting the generality of paragraph (a) of this Section, except as otherwise disclosed in Section 5.1 of the DDI Disclosure Schedule, as applicable, and except as contemplated or permitted by this Agreement, (i) DDI shall preserve intact in all material respects its present business organization and reputation, keep available the services of T. Mark Hastings, use commercially reasonable efforts to keep available services of its other key officers and employees, maintain its assets and properties in good working order and condition (ordinary wear and tear excepted), maintain insurance on its tangible assets and business in such amounts and against such risks and losses as are currently in effect, use commercially reasonable efforts to preserve its relationships with customers and suppliers and others having significant business dealings with it and to comply in all material respects with all Laws and Orders of all Governmental or Regulatory Authorities applicable to them, and (ii) DDI shall not:

(A) amend or propose to amend its Articles of Organization or Bylaws;

(B) (w) declare, set aside or pay any dividends on or make other distributions in respect of any of its capital stock, (x) split, combine, reclassify or take similar action with respect to

any of its capital stock or issue or authorize or propose the issuance of any other securities in respect of, in lieu of or in substitution for shares of its capital stock, (y) adopt a plan of complete or partial liquidation or resolutions providing for or authorizing such liquidation or a dissolution, merger, consolidation, restructuring, recapitalization or other reorganization or (z) directly or indirectly purchase, redeem or otherwise acquire any shares of its capital stock or any DDI Option with respect thereto;

(C) issue, deliver or sell, or authorize or propose the issuance, delivery or sale of, any shares of its capital stock or any DDI Option with respect thereto, or modify or amend any right of any holder of outstanding shares of capital stock;

(D) acquire (by merging or consolidating with, or by purchasing a substantial equity interest in or a substantial portion of the assets of, or by any other manner) any business or any corporation, partnership, association or other business organization or division thereof or otherwise acquire or agree to acquire any assets which are individually or in the aggregate material to DDI;

22

<PAGE> 24

(E) other than dispositions of assets which are not individually or in the aggregate material to DDI, sell, lease, grant any security interest in or otherwise dispose of or encumber any of its assets or properties;

(F) except to the extent required by applicable law, (x) permit any material change in (I) any pricing, marketing, purchasing, investment, accounting, financial reporting, inventory, credit, allowance or tax practice or policy or (II) any method of calculating any bad debt, contingency or other reserve for accounting, financial reporting or tax purposes or (y) make any material tax election or settle or compromise any material income tax liability with any Governmental or Regulatory Authority;

(G) (x) incur any indebtedness for borrowed money or guarantee any such indebtedness other than in the ordinary course of its business consistent with past practice, or (y) purchase, cancel, prepay or otherwise provide for a complete or partial discharge in advance of a scheduled repayment date with respect to, or waive any right under, any indebtedness for borrowed money other than in the ordinary course of its business consistent with past practice;

(H) enter into, adopt, amend in any material respect (except as may be required by applicable law) or terminate any DDI Employee Benefit Plan or any other agreement or arrangement, plan or policy between DDI and one or more of its directors, officers or employees, or, except for normal increases in the ordinary course of business consistent with past practice that do not result in a material increase in benefits or compensation expense to DDI, increase in any manner the compensation or fringe benefits of any director, officer or employee or pay any benefit not required by any plan or arrangement in effect as of the date hereof;

(I) enter into any contract or amend or modify any existing contract, or engage in any new transaction, outside the ordinary course of business consistent with past practice and, with respect to any affiliate of DDI, on other than an arm's length basis;

(J) make any capital expenditures or commitments for additions to plant, property or equipment constituting capital assets except in the ordinary course of business consistent with past practice;

(K) make any change in the lines of business in which it participates or is engaged;

(L) file a consent under Section 341(f) of the Code concerning collapsible corporations; or

(M) enter into any contract, agreement, commitment or arrangement to do or engage in any of the foregoing.

5.2 Covenants of Datum. At all times from and after the date hereof until the Effective Time, Datum covenants and agrees as to itself and its subsidiaries that (except as expressly contemplated or permitted by this Agreement, or to the extent that DDI shall otherwise consent in

23

<PAGE> 25

writing): (a) Datum shall not make any material changes to its business or structure which could reasonably be expected to have a material adverse effect on the consideration to be received by DDI's stockholders; (b) Datum shall use all reasonable efforts to take all such actions as are necessary to effectuate the transactions contemplated hereby and to fulfill and cause to be fulfilled the conditions to Closing under this Agreement; and (c) Datum agrees to make all filings it is required to make pursuant to the Exchange Act on a timely basis.

5.3 Advice of Changes. Each party shall confer on a regular and frequent basis with the other with respect to its business and operations and other matters relevant to the Merger, and shall promptly advise the other, orally and in writing, of any change or event, including, without limitation, any complaint, investigation or hearing by any Governmental or Regulatory Authority (or communication indicating the same may be contemplated) or the institution or threat of litigation, having, or which, insofar as can be reasonably foreseen, could have, a Material Adverse Effect on DDI, or Datum and its subsidiaries taken as a whole, as the case may be, or on the ability of DDI or Datum and Sub, as the case may be, to consummate the transactions contemplated hereby.

ARTICLE 6

ADDITIONAL AGREEMENTS

6.1 Access to Information; Confidentiality.

(a) Access to Information. DDI shall, throughout the period from the date hereof to the Effective Time, (i) provide Datum and its directors, officers, employees, legal, investment banking and financial advisors, accountants and any other agents and representatives (collectively, "Datum Representatives") with full access, upon reasonable prior notice, and during normal business hours, to DDI and its assets, properties, books and records, but only to the extent that such access does not unreasonably interfere with DDI's Operations, and (ii) furnish promptly to the Datum Representatives (x) a copy of each material report, statement, schedule and other document filed or received by DDI pursuant to the requirements of federal or state securities laws or filed with any other Governmental or Regulatory Authority, and (y) all other information and data (including, without limitation, copies of Contracts and DDI Employee Benefit Plans and other books and records) concerning DDI's Operations as the Datum Representatives shall reasonably may request. No investigation pursuant to this paragraph or otherwise shall affect any representation or warranty contained in this Agreement or any condition to the obligations of the parties hereto.

(b) Confidentiality. Each party will hold, and will use its best efforts to cause its representatives to hold, in strict confidence, unless (i) compelled to disclose by judicial or administrative process or by other requirements of applicable Laws or Governmental or Regulatory Authorities (including, without limitation, in connection with obtaining the necessary approvals of this Agreement or the transactions contemplated hereby of Governmental or Regulatory Authorities), or (ii) disclosed in an action or

proceeding brought by a party hereto in pursuit of its rights or in the exercise of its remedies hereunder, all documents and information concerning the other party and its subsidiaries, if applicable, furnished to it by such other party or its representatives in connection with this Agreement or the transactions contemplated hereby, except to the extent that such documents or information can be shown to have been (x) previously known by DDI or Datum, as the case may be, or their respective representatives, (y) in the public domain (either prior to or after the furnishing of such documents or information hereunder) through no fault of DDI or Datum, as the case may be, or their respective representatives or (z) later acquired by DDI or Datum, as the case may be, or their

24

<PAGE> 26

respective representatives from another source if the recipient is not aware that such source is under an obligation to DDI or Datum, as the case may be, to keep such documents and information confidential. In the event that this Agreement is terminated without the transactions contemplated hereby having been consummated, upon the request of DDI or Datum, as the case may be, the other party will, and will cause its representatives to, promptly (and in no event later than five (5) business days after such request) redeliver or cause to be redelivered all copies of documents and information furnished by DDI or Datum, as the case may be, or their respective representatives to such party and its representatives in connection with this Agreement or the transactions contemplated hereby and destroy or cause to be destroyed all notes, memoranda, summaries, analyses, compilations and other writings related thereto or based thereon prepared by DDI or Datum, as the case may be, or their respective representatives.

6.2 Registration of Datum Common Stock. Datum shall use its best efforts to register for re-sale the shares of Datum Common Stock issued pursuant to the payment of the Merger Consideration (including Datum Common Stock issuable as Additional Consideration) and file a registration statement with respect to such registration with the SEC within ninety (90) business days after the Closing Date; provided, however, that, if the Board of Directors of Datum determines in good faith that such filing should in the best interests of Datum's stockholders be delayed past such period, then, upon written notice to the DDI Representative and the DDI Stockholders within such ninety (90) day period so stating, then Datum's obligation to file such registration statement shall be deferred, but such filing shall in any case be required within one hundred eighty (180) days after the Closing Date. Datum shall use its best efforts to cause the registration statement filed in accordance with the foregoing (the "Registration Statement") to become effective as promptly as practicable after filing and to keep the Registration Statement effective at least until March 31, 2003.

6.3 Nasdaq Listing. Datum shall file an application for original listing of the shares of Datum Common Stock that constitute Merger Consideration on the Nasdaq National Market prior to the issuance thereof.

6.4 Regulatory and Other Approvals. Subject to the terms and conditions of this Agreement, each of DDI and Datum will proceed diligently and in good faith and will use all commercially reasonable efforts to do, or cause to be done, all things necessary, proper or advisable to, as promptly as practicable, (i) obtain all consents, approvals or actions of, make all filings with and give all notices to Governmental or Regulatory Authorities or any other public or private third parties required of Datum, DDI or any of their Subsidiaries to consummate the Merger and the other matters contemplated hereby, and (ii) provide such other information and communications to such Governmental or Regulatory Authorities or other public or private third parties as the other party or such Governmental or Regulatory Authorities or other public or private third parties may reasonably request in connection therewith.

6.5 Employment Agreement. At and upon the Effective Time, Datum shall have entered into an employment agreement with Mark Hastings on substantially the terms as set forth in the form of employment agreement attached hereto as Exhibit E (the "Employment Agreement").

6.6 Expenses. Datum shall bear all of its costs and expenses incurred in connection with this Agreement and the transactions contemplated hereby;

provided, however, that if the Merger is not consummated due to DDI's failure to obtain Stockholder Approval, DDI shall reimburse the expenses of Datum incurred in connection with this Agreement and the Merger. DDI shall bear all of DDI's costs and expenses incurred in connection with this Agreement and the transactions

25

<PAGE> 27

contemplated hereby (the "DDI Merger Expenses") and all such expenses shall be paid by DDI at or prior to the Closing.

6.7 Notice and Cure. Each of Datum, Sub and DDI will notify the other in writing of, and contemporaneously will provide the other with true and complete copies of any and all information or documents relating to, and will use best efforts to cure before the Closing, any event, transaction or circumstance, as soon as practical after it becomes known to such party, occurring after the date of this Agreement that causes or will cause any covenant or agreement of Datum, Sub or DDI, as the case may be, under this Agreement to be breached or that renders or will render untrue any representation or warranty of Datum, Sub or DDI, as the case may be, contained in this Agreement as if the same were made on or as of the date of such event, transaction or circumstance. Each of Datum, Sub and DDI also will notify the other in writing of, and will use best efforts to cure, before the Closing, any violation or breach, as soon as practical after it becomes known to such party, of any representation, warranty, covenant or agreement made by Datum, Sub or DDI, as the case may be, in this Agreement, whether occurring or arising prior to, on or after the date of this Agreement. No notice given pursuant to this Section 6.7 shall have any effect on the representations, warranties, covenants or agreements contained in this Agreement for purposes of determining satisfaction of any condition contained herein.

6.8 Fulfillment of Conditions. Subject to the terms and conditions of this Agreement, each of Datum, Sub and DDI will take or cause to be taken all steps necessary or desirable and proceed diligently and in good faith to satisfy each condition to the other's obligations contained in this Agreement and to consummate and make effective the transactions contemplated by this Agreement, and neither Datum nor DDI will, nor will it permit any subsidiary, if any, to, take or fail to take any action that could be reasonably expected to result in the non-fulfillment of any such condition.

6.9 Bridge Financing Agreement. Datum and DDI have entered into that certain Bridge Financing Agreement, dated April 9, 1999 (the "Bridge Financing Agreement"). Any breach by DDI of the terms of the Bridge Financing Agreement shall be grounds for termination of this Agreement pursuant to Section 8.1.

ARTICLE 7

CONDITIONS

7.1 Conditions to Each Party's Obligation to Effect the Merger. The respective obligation of each party to effect the Merger is subject to the fulfillment, at or prior to the Closing, of each of the following conditions:

(a) No Injunctions or Restraints. No court of competent jurisdiction or other competent Governmental or Regulatory Authority shall have enacted, issued, promulgated, enforced or entered any Law or Order (whether temporary, preliminary or permanent) which is then in effect and has the effect of making illegal or otherwise restricting, preventing or prohibiting consummation of the Merger or the other transactions contemplated by this Agreement.

(b) Governmental and Regulatory Consents and Approvals. Other than the filing provided for by Section 1.2, all consents, approvals and actions of, filings with and notices to any Governmental or Regulatory Authority or any other public or private third parties or Datum or DDI

<PAGE> 28

Stockholders required of Datum, DDI or any Subsidiary which are to be taken prior to the Effective Time to consummate the Merger and the other matters contemplated hereby, shall have been obtained.

7.2 Conditions to Obligation of Datum and Sub to Effect the Merger. The obligation of Datum and Sub to effect the Merger is further subject to the fulfillment, at or prior to the Closing, of each of the following additional conditions (all or any of which may be waived in whole or in part by Datum and Sub in their sole discretion):

(a) Representations and Warranties. Each of the representations and warranties made by DDI in this Agreement shall be true and correct in all material respects as of the Closing Date as though made on and as of the Closing Date or, in the case of representations and warranties made as of a specified date earlier than the Closing Date, on and as of such earlier date, and DDI shall have delivered to Datum a certificate, dated the Closing Date and executed on behalf of DDI by its Chairman of the Board, Chief Executive Officer, President or any Executive or Senior Vice President, to such effect.

(b) Performance of Obligations. DDI shall have performed and complied with, in all material respects, each agreement, covenant and obligation required by this Agreement to be so performed or complied with by DDI at or prior to the Closing, and DDI shall have delivered to Datum a certificate, dated the Closing Date and executed on behalf of DDI by its Chairman of the Board, President or any Executive or Senior Vice President, to such effect.

(c) Orders and Laws. There shall not have been issued, enacted, promulgated or deemed applicable to DDI, the Surviving Corporation or the transactions contemplated by this Agreement any Order or Law of any Governmental or Regulatory Authority which is then in effect and which could be reasonably expected to result in a material diminution of the benefits of the Merger to Datum, and there shall not be pending or threatened on the Closing Date any action, suit or proceeding in, before or by any Governmental or Regulatory Authority which could be reasonably expected to result in any such issuance, enactment, promulgation or deemed applicability of any such Order or Law or of any Order or Law.

(d) Contractual Consents. DDI shall have received all consents (or in lieu thereof waivers) from parties to each Contract disclosed pursuant to Section 3.10, to the extent required pursuant to the terms of each such Contract.

(e) No Material Adverse Change. Since the date of this Agreement, there shall have been no changes in the business, condition (financial or otherwise), properties, assets (including intangible assets), liabilities (including contingent liabilities) or results of operations of DDI, which have had or may be reasonably expected to have, a Material Adverse Effect on DDI.

(f) Proceedings. All proceedings to be taken on the part of DDI in connection with the transactions contemplated by this Agreement and all documents incident thereto shall be reasonably satisfactory in form and substance to Datum, and Datum shall have received copies of all such documents and other evidences as Datum may reasonably request in order to establish the consummation of such transactions and the taking of all proceedings in connection therewith.

<PAGE> 29

(g) Opinion of Counsel. Datum shall have received the opinion of Lucash, Gesmer & Updegrave, LLP, counsel to DDI, dated the Closing Date, in form reasonably acceptable to Datum and covering the matters set forth on Exhibit F hereto.

(h) Employment Agreement. The Employment Agreement shall have been entered into by and between Datum and Mark Hastings.

(i) DDI Representative; Power of Attorney. Datum shall have received an instrument acceptable to it executed by the DDI Stockholders, naming T. Mark Hastings as the DDI Representative and authorizing such person to act on behalf of the DDI Stockholders for purposes of Sections 2.2(e), 2.3(a), 2.4, 6.2, 9.2(c) and 9.4 hereof, and to enter into agreements with Datum binding upon the DDI Stockholders for purposes of Section 2.4.

(j) DDI Disclosure Schedule. Datum shall have received the DDI Disclosure Schedule, true and complete as of the date hereof, and such DDI Disclosure Schedule shall remain true and complete as of the Closing Date.

(k) DDI Merger Expenses. Datum shall have received instruments reflecting the payment of, or the arrangements for payment of, DDI's Merger Expenses, in form and substance reasonably acceptable to Datum.

(l) Clerk Certificate. A copy of the votes of the Board of Directors and Stockholders of DDI, certified by its Clerk, authorizing and approving the execution, delivery and performance of this Agreement and the transactions contemplated hereby and the acts of the officers and employees of DDI in carrying out the terms and provisions hereof.

(m) Escrow Agreement. The Escrow Agreement shall have been executed by Datum, Mark Hastings and the DDI Stockholders.

7.3 Conditions to Obligation of DDI to Effect the Merger. The obligation of DDI to effect the Merger is further subject to the fulfillment, at or prior to the Closing, of each of the following additional conditions (all or any of which may be waived in whole or in part by DDI in its sole discretion):

(a) Representations and Warranties. Each of the representations and warranties made by Datum and Sub in this Agreement shall be true and correct in all material respects as of the Closing Date as though made on and as of the Closing Date or, in the case of representations and warranties made as of a specified date earlier than the Closing Date, on and as of such earlier date, and Datum and Sub shall each have delivered to DDI a certificate, dated the Closing Date and executed on behalf of Datum by its Chairman of the Board, Chief Executive Officer, President or any Executive or Senior Vice President and on behalf of Sub by its President or any Vice President, to such effect.

(b) Performance of Obligations. Datum and Sub shall have performed and complied with, in all material respects, each agreement, covenant and obligation required by this Agreement to be so performed or complied with by Datum, or Sub at or prior to the Closing, and Datum and Sub shall each have delivered to DDI a certificate, dated the Closing Date and executed on behalf of Datum by its Chairman of the Board, President or any Executive or Senior Vice

28

<PAGE> 30

President and on behalf of Sub by its Chairman of the Board, President or any Vice President, to such effect.

(c) Orders and Laws. There shall not have been issued, enacted, promulgated or deemed applicable to the Datum, its Subsidiaries, the Surviving Corporation or the transactions contemplated by this Agreement any Order or Law of any Governmental or Regulatory Authority which is then in effect and which could be reasonably expected to result in a material diminution of the benefits of the Merger to DDI or its stockholders, and there shall not be pending or threatened on the Closing Date any action, suit or proceeding in, before or by any Governmental or Regulatory Authority which could be reasonably expected to result in any such issuance, enactment, promulgation or deemed applicability of any such Order or Law or of any Order or Law.

(d) No Material Adverse Change. Since the date of this Agreement, there shall have been no changes in the business, condition (financial or otherwise), properties, assets (including intangible assets), liabilities (including contingent liabilities) or results of operations of Datum and its

Subsidiaries taken as a whole, which have had or may be reasonably expected to have, a Material Adverse Effect on Datum and its Subsidiaries taken as a whole.

(e) Proceedings. All proceedings to be taken on the part of Datum and Sub in connection with the transactions contemplated by this Agreement and all documents incident thereto shall be reasonably satisfactory in form and substance to DDI, and DDI shall have received copies of all such documents and other evidences as DDI may reasonably request in order to establish the consummation of such transactions and the taking of all proceedings in connection therewith.

(f) Employment Agreement. The Employment Agreement shall have been executed by Datum and delivered to Mark Hastings.

(g) Datum Disclosure Schedule. DDI shall have received the Datum Disclosure Schedule, true and complete as of the date hereof, and such Datum Disclosure Schedule shall remain true and complete as of the Closing Date.

(h) Opinion of Counsel. DDI and the DDI Stockholders shall have received the opinion of Stradling Yocca Carlson & Rauth, counsel to Datum, dated the Closing Date, in form reasonably acceptable to DDI and covering the matters set forth on Exhibit G hereto.

(i) Secretary/Clerk Certificate. A copy of the resolutions of the Board of Directors of Datum and the Board of Directors and stockholder of Sub, certified by their Secretary or Clerk, as the case may be, authorizing and approving the execution, delivery and performance of this Agreement and the transactions contemplated hereby and the acts of the officers and employees of Datum and Sub in carrying out the terms and provisions hereof.

ARTICLE 8

TERMINATION, AMENDMENT AND WAIVER

8.1 Termination. This Agreement may be terminated, and the transactions contemplated hereby may be abandoned, at any time prior to the Effective Time:

(a) by mutual written agreement of the parties hereto duly authorized by action taken by or on behalf of their respective Boards of Directors;

29

<PAGE> 31

(b) by either DDI or Datum upon notification to the non-terminating party by the terminating party:

(i) at any time after August 1, 1999, if the Merger shall not have been consummated on or prior to such date and such failure to consummate the Merger is not caused by a breach of this Agreement by the terminating party;

(ii) if any Governmental or Regulatory Authority, the taking of action by which is a condition to the obligations of either DDI or Datum to consummate the transactions contemplated hereby, shall have determined not to take such action and all appeals of such determination shall have been taken and have been unsuccessful;

(iii) if there has been a material breach of any representation, warranty, covenant or agreement on the part of the non-terminating party set forth in this Agreement which breach has not been cured within ten (10) business days following receipt by the non-terminating party of notice of such breach from the terminating party or assurance of such cure reasonably satisfactory to the terminating party shall not have been given by or on behalf of the non-terminating party within such ten (10) business day period; or

(iv) if any court of competent jurisdiction or other competent Governmental or Regulatory Authority shall have issued an Order making

illegal or otherwise restricting, preventing or prohibiting the Merger and such Order shall have become final and non-appealable; or

(c) by Datum, upon notification to DDI:

(i) if the requisite stockholder vote of DDI approving the principal terms of this Agreement, the Agreement of Merger and the Merger in accordance with applicable law and the Articles of Organization and Bylaws of DDI is not obtained; or

(ii) pursuant to Sections 2.3 and 6.9 hereof.

8.2 Effect of Termination. If this Agreement is validly terminated by either DDI or Datum pursuant to Section 8.1, this Agreement will forthwith become null and void and there will be no liability or obligation on the part of either DDI or Datum (or any of their respective representatives or affiliates), except that the provisions of Sections 6.1(b), 6.6 and 6.9 will continue to apply following any such termination.

8.3 Amendment. This Agreement may be amended, supplemented or modified by action taken by or on behalf of the respective Boards of Directors of the parties hereto at any time prior to the Effective Time. No such amendment, supplement or modification shall be effective unless set forth in a written instrument duly executed by or on behalf of each party hereto.

8.4 Waiver. At any time prior to the Effective Time any party hereto, by action taken by or on behalf of its Board of Directors, may to the extent permitted by applicable law (i) extend the time for the performance of any of the obligations or other acts of the other parties hereto, (ii) waive any inaccuracies in the representations and warranties of the other parties hereto contained herein or in any document delivered pursuant hereto or (iii) waive compliance with any of the covenants, agreements or conditions of the other parties hereto contained herein. No such extension or waiver shall be effective unless set forth in a written instrument duly executed by or on behalf of the party

30

<PAGE> 32

extending the time of performance or waiving any such inaccuracy or non-compliance. No waiver by any party of any term or condition of this Agreement, in any one or more instances, shall be deemed to be or construed as a waiver of the same or any other term or condition of this Agreement on any future occasion.

ARTICLE 9

GENERAL PROVISIONS

9.1 Sole Remedy; Survival.

(a) Sole Remedy. The indemnification provisions contained in this Article 9 shall serve as the only remedy of the parties hereto seeking recovery for claims arising under this Agreement.

(b) Survival of Representations, Warranties, Covenants and Agreements. The representations, warranties, covenants and agreements contained in this Agreement or in any instrument delivered pursuant to this Agreement shall survive the Effective Time and shall continue in full force and effect until December 31, 2001 (the "Indemnification Period"); provided, however, that Datum shall have until March 31, 2002, to assert any breach of the same that occurred before the expiration of the Indemnification Period.

9.2 Indemnification.

(a) Indemnification of Datum. Subject to the provisions of this Article 9, the DDI Indemnitors shall indemnify Datum from and against (i) subject to clause (d) below, any and all damage, loss, liability and expense (including without limitation reasonable expenses of investigation and

reasonable attorneys' fees and reasonable expenses in connection with any action, suit or proceeding) ("Damages") incurred or suffered by Datum arising out of any breach of the representations, warranties, covenants or agreements of DDI set forth herein; and (ii) any DDI Merger Expenses not paid pursuant to Section 6.6 or accounted for in any adjustment made to the Merger Consideration pursuant to Section 2.3 (collectively, "Datum Indemnifiable Damages"). Datum may obtain indemnification for any Datum Indemnifiable Damages to which this Section 9.2(a) relates only (A) if it makes a claim or claims for indemnification within the period specified in Section 9.1 above, and (B) solely with respect to Datum Indemnifiable Damages described in clause (i) above, such claim or claims aggregate in excess of Fifty Thousand Dollars (\$50,000) (the "Indemnification Threshold"); provided, that upon passing such Indemnification Threshold, all Datum Indemnifiable Damages in excess of Twenty-Five Thousand Dollars (\$25,000) shall be subject to indemnification hereunder. Any Datum Indemnifiable Damages shall be recovered first pro rata from any unpaid Additional Consideration owing to the DDI Stockholders, and thereafter from the DDI Indemnitors; provided, however, that the liability of each DDI Indemnitor for indemnification of any claim made hereunder shall be limited to an amount not to exceed the product of the aggregate liability of the DDI Indemnitors with respect to such claim and such DDI Indemnitor's Ownership Percentage; and provided, further, that the aggregate liability of each DDI Indemnitor for indemnification hereunder (such DDI Indemnitor's "Liability Cap"), including any indemnification pursuant to Section 9.2(d), shall not exceed the value of the Merger Consideration received by him pursuant to this Agreement. For purposes of determining a Liability Cap, the Merger Consideration shall be valued (i) for cash consideration, at face value, and (ii) for Datum Common Stock (A) if issued as Primary Stock Consideration, seven dollars (\$7) per share,

31

<PAGE> 33

and (B) if issued as Additional Consideration, the value of the shares as determined pursuant to Section 2.2(c)(v).

(b) Indemnification of DDI. Subject to the provisions of this Article 9, Datum agrees to indemnify the DDI Stockholders after the Effective Time from and against any and all Damages incurred or suffered by the DDI Stockholders arising out of any breach of the representation, warranties, covenants or agreements of Datum and Sub set forth herein (the "DDI Indemnifiable Damages"). The DDI Stockholders may obtain indemnification for any DDI Indemnifiable Damages to which this Section 9.2(b) relates only if (i) a claim or claims for indemnification is made within the Indemnification Period, and (ii) such claim or claims aggregate in excess of the Indemnification Threshold; provided, that upon passing such Indemnification Threshold, all DDI Indemnifiable Damages in excess of Twenty-Five Thousand Dollars (\$25,000) shall be subject to indemnification hereunder.

(c) Indemnification Procedures. A party seeking indemnification (the "Indemnitee") shall use its reasonable best efforts to minimize any liabilities, damages, deficiencies, claims, judgments, assessments, costs and expenses in respect of which indemnity may be sought under this Agreement. The Indemnitee shall give prompt written notice to the party from whom indemnification is sought (the "Indemnitor") of the assertion of a claim for indemnification, but in no event longer than twenty (20) days after service of process in the event litigation is commenced against the Indemnitee by a third party, or sixty (60) days after the assertion of such claim, whichever shall first occur. No such notice of assertion of a claim shall satisfy the requirements of this Section 9.2(c) unless it describes in reasonable detail and in good faith the facts and circumstances upon which the asserted claim for indemnification is based. If any action or proceeding shall be brought in connection with any liability or claim to be indemnified hereunder, the Indemnitee shall provide the Indemnitor (or, in the case the DDI Stockholders or the DDI Indemnitors are the Indemnitor, the DDI Representative) twenty (20) calendar days to decide whether to defend such liability or claim. During such period, the Indemnitee shall take all necessary steps to protect the interests of itself and the Indemnitor, including the filing of any necessary responsive pleadings, the seeking of emergency relief or other action necessary to maintain the status quo, subject to reimbursement from the Indemnitor of its expenses in doing so. The Indemnitor shall either (i) (with, if necessary, reservation of rights) defend such action or proceeding at its expense, using counsel selected

by the insurance company insuring against any such claim and undertaking to defend such claim, or by other counsel selected by it and approved by the Indemnatee, which approval shall not be unreasonably withheld or delayed, or (ii) decline to undertake to defend such action, in which case Indemnatee shall have sole discretion to defend or settle such claim and seek indemnification from the Indemnitor therefore. The Indemnitor shall keep the Indemnatee fully apprised at all times of the status of the defense and shall consult with the Indemnatee prior to the settlement of any indemnified matter. The Indemnatee agrees to use reasonable efforts to cooperate with the Indemnitor in connection with its defense of indemnifiable claims. In the event the Indemnatee has a claim or claims against any third party arising out of or connected with the indemnified matter, then upon receipt of indemnification, the Indemnatee shall fully assign to the Indemnitor the entire claim or claims to the extent of the indemnification actually paid by the Indemnitor and the Indemnitor shall thereupon be subrogated with respect to such claim or claims of the Indemnatee. Subject to Datum's right of set-off against Additional Consideration pursuant to Section 9.2(a) above, the Indemnitor shall pay any undisputed indemnity in immediately available funds no later than ten (10) business days after the later to occur of the making of a claim for such indemnity and such indemnity's assuming undisputed status. Notwithstanding any provision to the contrary in this Agreement, the DDI Indemnitors (or any of them) may, at their sole

32

<PAGE> 34

option, in lieu of payment in immediately available funds for any indemnification liability under this Agreement, indemnify Datum by transferring back to Datum shares of Datum Stock received by them as Merger Consideration (and only such shares), and for this purpose such returned shares shall be valued against such liability at the greater of their market value at the time of indemnification and their value as determined pursuant to the last sentence of Section 9.2(a) above.

(d) Indemnification by DDI with respect to Glassey-McNeil. In addition to, and notwithstanding anything to the contrary contained in Section 9.1(a) above, Datum shall be indemnified pursuant to this clause (d) for Damages incurred or suffered by it in the course of satisfying the claims of DDI and Glassey-McNeil arising from that certain Co-Inventor Agreement, dated October 26, 1998, by and among Glassey-McNeil and DDI (the "Glassey-McNeil/DDI Damages"). Pursuant to the terms of the Escrow Agreement, Datum shall be entitled to recover from the proceeds of the sale of all or any portion of the Escrowed Shares indemnification for Glassey-McNeil/DDI Damages, as follows:

(i) Datum shall be indemnified for fifty percent (50%) of the first Two Hundred Thousand Dollars (\$200,000) of Glassey-McNeil/DDI Damages incurred; and

(ii) Datum shall be indemnified in full for the next Two Hundred Thousand Dollars (\$200,000) of Glassey-McNeil/DDI Damages incurred.

For purposes of paying such indemnification, the share price of the Escrowed Shares shall be their share price as of the time the applicable Glassey-McNeil/DDI Damages are incurred, determined on a Twenty Day Rolling Basis. If no share price is determinable on such basis, the fair value of such shares of Datum Common Stock, as reasonably determined by Datum's Board of Directors, shall be used. In the event the Glassey-McNeil/DDI Damages aggregate an amount in excess of Four Hundred Thousand Dollars (\$400,000), Datum shall be entitled to indemnification for fifty percent (50%) of such excess Glassey-McNeil/DDI Damages pursuant to clause (a) above as though such excess damages were Datum Indemnifiable Damages. Datum shall use its reasonable best efforts to minimize the Glassey-McNeil/DDI Damages, and shall keep the DDI Representative fully apprised at all times of the status of the settlement efforts.

(e) Indemnification by Datum with respect to Glassey-McNeil. In addition to, and notwithstanding anything to the contrary contained in Section 9.1(b) above, the DDI Stockholders shall be indemnified pursuant to this clause (e) if and to the extent any Additional Compensation otherwise due them under this Agreement is reduced in the course of satisfying the claims of Glassey-McNeil against Datum arising from the relationship evidenced by those

certain Consulting Agreements, dated as of May 12, 1998, by and between among Glassey-McNeil (each as individuals) and Datum; provided, however, that any indemnification pursuant to this clause (e) shall not exceed Five Hundred Thousand Dollars (\$500,000) in the aggregate.

9.3 Knowledge. With respect to any representations or warranties contained herein which are made to the knowledge of DDI, Datum or Sub, as the case may be, the actual knowledge of the officers and directors of DDI, Datum or Sub, as the case may be, shall be imputed to DDI, Datum or Sub, as the case may be.

9.4 Notices. All notices, requests and other communications hereunder must be in writing and will be deemed to have been duly given only if delivered personally or by facsimile transmission or a nationally recognized overnight courier service (such as Federal Express) or

33

<PAGE> 35

mailed by registered or certified mail (postage prepaid) to the parties at the following addresses or facsimile numbers:

If to Datum, Sub or the Surviving Corporation, to:
Datum Inc.
9975 Toledo Way
Irvine, California 92618-1605
Facsimile No.: 949/598-7555
Attn: David A. Young
Vice President and Chief Financial Officer

with a copy to:

Stradling Yocca Carlson & Rauth
660 Newport Center Drive, Suite 1600
Newport Beach, California 92660-6441
Facsimile No.: 949/725-4100
Attn: Lawrence B. Cohn

If to DDI, to:
DDI Delivery, Inc.
54 Middlesex Turnpike
Bedford, MA 01730
Facsimile No.: 781/275-3883
Attn: Mark Hastings
Chief Executive Officer

with a copy to:
Lucash, Gesmer & Updegrove, LLP
40 Broad Street
Boston, MA 02109
Facsimile No.: 617/350-6878
Attn: William Contente, Esq.

If to the DDI Stockholders, to the addresses given for each on Schedule II, with a copy to the DDI Representative at the address given in the instrument referenced in Section 7.2(i) and to Lucash, Gesmer & Updegrove, LLP, at the address given above.

All such notices, requests and other communications will (i) if delivered personally to the address as provided in this Section, be deemed given upon delivery, (ii) if delivered by facsimile transmission to the facsimile number provided in this Section, but only (A) where the transmitting party includes a cover sheet identifying the name, location and identity of the transmitting party, the phone number of the transmitting device, the date and time of transmission and the number of pages transmitted (including the cover page), (B) where the transmitting device or receiving device records verification of receipt and the date and time of transmission receipt and the phone number of the other device, and (C) where the facsimile transmission is immediately followed by delivery of the original of the relevant notice in the manner provided in clause (i), (iii) or (iv) hereof, be deemed given upon

34

<PAGE> 36

receipt; (iii) if delivered by nationally recognized overnight courier to the address as provided in this Section 9.4, be deemed given the business day following mailing; and (iv) if delivered by mail in the manner described above to the address as provided in this Section 9.4, the fourth business day following mailing. Any party from time to time may change its address, facsimile number or other information for the purpose of notices to that party by giving notice specifying such change to the other parties hereto.

9.5 Entire Agreement. This Agreement supersedes all prior discussions and agreements among the parties hereto with respect to the subject matter hereof and contains the sole and entire agreement among the parties hereto with respect to the subject matter hereof.

9.6 Public Announcements. So long as this Agreement is in effect, DDI will not, and will not permit its representatives to, issue or cause the publication of any press release or make any other public announcement or otherwise cause or permit the release in any manner which could reasonably be expected to cause such information to be known to the public with respect to the transactions contemplated by this Agreement without the written consent of Datum; provided, however, that DDI may make such announcements and releases to the extent the content of such announcements or releases was contained in a prior approved announcement or release. Datum and DDI will cooperate with each other in the development and distribution of all press releases and other public announcements with respect to this Agreement and the transactions contemplated hereby, and Datum will furnish DDI with drafts of any such releases and announcements as far in advance as practicable.

9.7 No Third Party Beneficiary. The terms and provisions of this Agreement are intended solely for the benefit of each party hereto and their respective successors or permitted assigns, and it is not the intention of the parties to confer third-party beneficiary rights upon any other person.

9.8 No Assignment; Binding Effect.

(a) Prior to Closing. Prior to Closing, neither this Agreement nor any right, interest or obligation hereunder may be assigned by any party hereto without the prior written consent of the other parties hereto and any attempt to do so will be void, except that Sub may assign any or all of its rights, interests and obligations hereunder to another direct or indirect wholly-owned subsidiary of Datum.

(b) Post-Closing. After the Closing, Datum may transfer the Business or all or substantially all of the assets of the Business (a "Sale of the Business") in its sole discretion; provided, that in such event, Datum, pursuant to a written instrument delivered to the DDI Stockholders, shall assign to the transferee, and the transferee shall assume, the obligation to pay Additional Consideration as set forth herein; and provided, further, that Datum shall remain liable to the DDI Stockholders for such obligation to pay Additional Consideration in the event such transferee fails to perform such obligation. Notwithstanding the foregoing, Datum's aggregate liability for payments of Additional Consideration not made by such transferee shall be limited to an amount not to exceed thirty percent (30%) of the Profit received by Datum in the Sale of the Business. The term "Profit" shall mean the excess after taxes of the purchase price paid to Datum in the Sale of the Business over the sum of the Merger Consideration paid by Datum (net of Datum Indemnifiable Damages paid to Datum) through the effective date of the Sale of the Business plus

35

<PAGE> 37

net expenses Attributable to the Business incurred by Datum from April 8, 1999 through the effective date of the Sale of the Business.

(c) Successors and Assigns. Subject to the foregoing, this Agreement is binding upon, inures to the benefit of and is enforceable by the parties hereto and their respective successors and assigns.

9.9 Headings. The headings used in this Agreement have been inserted for convenience of reference only and do not define or limit the provisions hereof.

9.10 Invalid Provisions. If any provision of this Agreement is held to be illegal, invalid or unenforceable under any present or future law, and if the rights or obligations of any party hereto under this Agreement will not be materially and adversely affected thereby, (a) such provision will be fully severable, (b) this Agreement will be construed and enforced as if such illegal, invalid or unenforceable provision had never comprised a part hereof, (c) the remaining provisions of this Agreement will remain in full force and effect and will not be affected by the illegal, invalid or unenforceable provision or by its severance herefrom, and (d) in lieu of such illegal, invalid or unenforceable provision, there will be added automatically as a part of this Agreement a legal, valid and enforceable provision as similar in terms to such illegal, invalid or unenforceable provision as may be possible.

9.11 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Massachusetts applicable to a contract executed and performed there, without giving effect to the conflicts of laws principles thereof.

9.12 Counterparts. This Agreement may be executed by the parties in separate counterparts hereof and, provided that each party has executed and delivered a counterpart hereof, this Agreement shall be effective despite the fact that the parties have not executed the same counterpart hereof. All such counterparts shall constitute one and the same agreement.

9.13 Arbitration. All claims, controversies, differences or disputes between or among any of the parties hereto arising from or relating to this Agreement shall be determined solely and exclusively by arbitration in accordance with the rules of commercial arbitration then in effect of the American Arbitration Association, or any successors hereto ("AAA"), in Orange County, California, unless the parties otherwise agree in writing. Each of the parties consents to venue for such arbitrations in Orange County, California and to service of process by certified or registered mail. Upon commencement of any arbitration pursuant hereto, the parties shall jointly select an arbitrator. In the event the parties fail to agree upon an arbitrator within twenty (20) days, then each party shall select an arbitrator and such arbitrators shall then select a third arbitrator to serve as the sole arbitrator; provided, that if either party, in such event, fails to select an arbitrator within seven (7) days, such arbitrator shall be selected by the AAA upon application of either party. The arbitrator thus selected shall conduct a hearing within twenty (20) days of such selection, at which hearing the arbitrator shall, with the mutual agreement of the parties, (a) schedule pre-hearing conference, discovery and hearing dates, and (b) determine the scope and procedures to be used for discovery; provided, however, if the parties cannot mutually agree to such dates or discovery rules, they shall be set by the arbitrator. Judgment upon the award of the agreed upon arbitrator or the so chosen third arbitrator, as the case may be, shall be binding and shall be entered into by a court of competent jurisdiction. The parties agree to abide by any decision rendered in any such arbitration as final and binding and waive the right to submit the dispute to a public tribunal for a jury or non-jury trial. The

prevailing party shall be entitled to recover from the non-prevailing party reasonable attorneys' fees and expenses incurred by the prevailing party in connection with such arbitration.

[signature page to follow]

37

<PAGE> 39

IN WITNESS WHEREOF, each party hereto has caused this Agreement to be signed by its officer thereunto duly authorized, under seal, as of the date first above written.

DATUM INC.

DIGITAL DELIVERY, INC.

By: _____
Name: Erik van der Kaay
Title: President and Chief Executive Officer

By: _____
Name: Thomas Mark Hastings
Title: Chief Executive Officer,
President and Treasurer

DATUM ACQUISITION SUB, INC.

THE DDI INDEMNITORS

By: _____
Name: David A. Young
Title: President and Treasurer

Timothy Bowe

Gil Fishman

T. Mark Hastings

Steven D. Morlock

Ronald Rubbico

Ronald Subler

38

<PAGE> 40

EXHIBIT A
FORM OF ESCROW AGREEMENT

<PAGE> 41

EXHIBIT B
FORM OF INVESTMENT LETTER

<PAGE> 42

EXHIBIT D
DATUM DISCLOSURE SCHEDULE

<PAGE> 43

EXHIBIT E
FORM OF EMPLOYMENT AGREEMENT

<PAGE> 44

EXHIBIT F
FORM OF OPINION OF COUNSEL TO DDI

<PAGE> 45

EXHIBIT G
FORM OF OPINION OF COUNSEL TO DATUM

<PAGE> 46

SCHEDULE I
SURVIVING CORPORATION BOARD OF DIRECTORS AND OFFICERS

<PAGE> 47

SCHEDULE II
DDI STOCKHOLDERS

</TEXT>

</DOCUMENT>

</SEC-DOCUMENT>

-----END PRIVACY-ENHANCED MESSAGE-----

May it please the Court, the following is an extract from the SEARCH function inside the IETF.ORG Intellectual Property Rights Webpage (<http://www.ietf.org/ipr>) listing statements from search term "GLASSEY"; As you can see from the listing Glassey and McNeil filed numerous documents pertaining to Glassey's and McNeil's rights for the Standards Agency's unauthorized use of the protected Phase-II Intellectual Properties in its publications.

Patent Owner/Applicant Search Result

Total number of IPR disclosures found: 20

IPR that was submitted by *glassey*, and is related to ***RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"***

2013-10-27 • ID # 2224 "Todd S. Glassey's Statement about IPR related to RFC 3161"

IPR that was submitted by *glassey*, and is related to ***draft-ietf-geopriv-local-civic-03, "Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)"***

2012-07-18 • ID # 1829 "Glassey's Statement about IPR related to draft-ietf-geopriv-local-civic-03"

IPR that was submitted by *glassey*, and is related to ***draft-ietf-geopriv-deref-protocol-07, "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)"***

2012-07-15 • ID # 1825 "Todd S. Glassey's Statement about IPR related to draft-ietf-geopriv-deref-protocol-07"

IPR that was submitted by *glassey*, and is related to ***draft-ietf-geopriv-deref-protocol-06, "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)"***

2012-07-12 • ID # 1818 "Patent Recovery Corp (Glassey/McNeil)'s Statement about IPR related to draft-ietf-geopriv-deref-protocol-06 and (most all GeoPriv, DNSSec, and timestamping protocols will also infringe)"

IPR that was submitted by *glassey*, and is not related to a specific IETF contribution.

2012-01-24 • ID # 1669 "Todd Glassey's Statement about IPR related to Informational Publication"

IPR that was submitted by *glassey*, and is related to ***RFC 4776, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information"***

2008-06-24 • ID # 963 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4776 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"

2008-06-19 • ID # 954 IPR disclosure ID# 963 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4776 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey

GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 3694, "Threat Analysis of the Geopriv Protocol"**

- 2008-06-24 • ID # 962 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3694 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 962 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3694 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 5139, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)"**

- 2008-06-24 • ID # 961 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 5139 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 961 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 5139 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 3693, "Geopriv Requirements"**

- 2008-06-24 • ID # 960 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3693 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 960 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3693 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to **RFC 4589, "Location Types Registry"**

- 2008-06-24 • ID # 957 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4589 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 957 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4589 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital

Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to ***RFC 3825, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information"***

- 2008-06-24 • ID # 956 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3825 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 956 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 3825 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to ***RFC 4745, "Common Policy: A Document Format for Expressing Privacy Preferences"***

- 2008-06-24 • ID # 955 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4745 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models"
- 2008-06-19 • ID # 954 IPR disclosure ID# 955 "Todd S. Glassey, IP owner's Statement about IPR related to RFC 4745 and IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models" Updates Todd S. Glassey, IP owner's Statement about IPR related to IPR claimed in Glassey GeoSpatial Keying and Evidentiary Digital Testimony Models

IPR that was submitted by *glassey*, and is related to ***RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"***

- 2004-07-15 • ID # 461 "Glassey's Statement about possible IPR claimed in RFC 3161"

Additionally since the computers it operates to provide these publication services execute code which implements this 'description of the infringement' as real-world code, it directly infringes itself in its operations.

There is no copyright section 107 exemption for patent protected technologies whether enforced directly against the US patent or a license providing for those same controls to another party, as is the case in this shared-patent case.



Send a release
Become a member
For journalists
Member sign in
For bloggers
Global sites

Search
Products & Services
News Releases
Advanced Search

Products & Services

Knowledge Center

Browse News Releases

Contact PR Newswire

See more news releases in Computer Electronics | Acquisitions, Mergers and Takeovers

Datum Completes Acquisition of Digital Delivery

Acquisition of Leading Provider of Secure Information Distribution And

Management Software Provides Datum With a Gateway to E-Business Marketplace

Like 0

Follow

More

Print Email Share

IRVINE, Calif., July 29 /PRNewswire/ -- Datum Inc. (Nasdaq: DATM), a worldwide leader in synchronization and timing, today announced that it has closed its acquisition of privately held Digital Delivery, Inc., a leading provider of secure information distribution and management software. The acquisition will form the core of a new Datum business unit, titled E-business Solutions, demonstrating Datum's commitment to driving its core advanced timing solutions technology into emerging markets, including e-business applications. Mark Hastings, former President of Digital Delivery, will lead the new division.

Under the terms of the agreement, Datum acquired all of the outstanding shares of Digital Delivery for the initial purchase price of approximately \$4.0 million, which includes a combination of cash and stock and the assumption of liabilities in the aggregate amount of approximately \$1.0 million. In addition, Datum will be responsible for earn-out payments due on December 31 of 2000 and 2001, which will be valued by future profits and payable in a combination of cash and stock. The acquisition will be accounted for as a purchase and is expected to be accretive in calendar year 2000.

For more than thirty years, Datum has established itself as a leader in providing advanced timing solutions for the world's emerging technologies. Datum's Trusted Time initiative aims to use these advanced timing technologies as a comprehensive solution for authenticating, notarizing, tracking, distributing and securing electronically transmitted data. By integrating Datum's Trusted Time and Global Positioning System (GPS) technologies with Digital Delivery's Confidential Courier, a secure electronic information delivery solution, Datum will offer corporations one of the most secure methods for transferring information, regardless of the communication method.

One of the strategic initiatives that Datum plans to concentrate its efforts on is the e-business marketplace. Digital Delivery's proven secure distribution and management software provides Datum with the applications necessary to capitalize on the explosive use of the Internet, where security and authentication are critical success factors.

"We have signed a number of partnership agreements in the past year that have positioned Datum as the Trusted Time source for e-business security, but this acquisition marks our most aggressive and dramatic step to entering the marketplace," said Erik H. van der Kaay, President and Chief Executive Officer of Datum. "Increasing e-commerce transactions represents a tremendous opportunity to leverage Digital Delivery's technology to conduct business over the Internet. Datum has more than thirty years experience helping synchronize the world's most complex telecommunications and computer networks. It is a natural evolution for this technology to migrate to the next generation of business networks, specifically the Internet. We currently plan to demonstrate our first product at Networld + Interop in Atlanta in September 1999 followed by customer beta testing in the fourth quarter."

Mark Hastings stated, "The charter of the E-Business Solutions business unit is to provide software and hardware products that authenticate the exchange of information in the digital age by irrefutably binding transactions to times, users and locations. By merging Datum's trusted time technologies with Digital Delivery's expertise in secure information management, this new division is well positioned to lead the growing market for authentication and tracking of electronic transactions."

Datum designs, manufactures and markets high-performance timing and frequency solutions for telecommunications, computer networks, satellite systems, electronic commerce and test and measurement applications. Datum is the only company in the world that supplies the full range of timing technologies. Additional information about Datum is available at www.datum.com.

This press release contains forward-looking statements. The

Featured Video

Sanofi Pasteur Initiates Phase III Study of Investigational Clostridium difficile Vaccine in the United States

Journalists and Bloggers

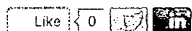


Visit PR Newswire for Journalists for releases, photos, ProfNet experts, and customized feeds just for Media.

View and download archived video content distributed by MultiVu on The Digital Center.

forward-looking statements, which reflect management's best judgment based on factors currently known, involve a number of risks and uncertainties, including the following: competition, uncertainty of intellectual property protection and uncertainty of acceptance of the Datum's products and technology. These factors and other risks inherent in Datum's business are described from time to time in datum's SEC filings, including its Annual Report Form 10-K for the year ended December 31, 1998 and Form 10-Q for the quarter ended March 31, 1999. Actual results may vary materially. Datum undertakes no obligation to revise the forward-looking statements contained herein to reflect events or circumstances after the date hereof or to reflect the occurrence of unanticipated events.

SOURCE Datum, Inc.



Next in Computer Electronics News

Custom Packages

Browse our custom packages or build your own to meet your unique communications needs.

Start today.

PR Newswire Membership

Fill out a PR Newswire membership form or contact us at (888) 776-0942.

Learn about PR Newswire services

Request more information about PR Newswire products and services or call us at (888) 776-0942.

[About PR Newswire](#) | [Contact PR Newswire](#) | [PR Newswire's Terms of Use Apply](#) | [Careers](#) | [Privacy](#) | [Site Map](#) | [RSS Feeds](#) | [Blog](#)
Copyright © 2013 PR Newswire Association LLC. All Rights Reserved.

A UBM plc company.

Dynamic Site Platform powered by Limelight Networks.

**BREACH OF CONTRACT and
COMPLIANCE DEMAND NOTICE**

Date: 7/23/2014
To: Custodian of Records, General Counsel and CEO through Service Channel
From: Todd S. Glassey
Re: Merger between Microsemi and Symmetricom has contractual requirements which must be agreed to PRIOR to the merger or the merger is not perfected.

To whom it may concern,

There is a very serious problem with the new Microsemi corporations status which breached the settlement contract between GLASSEY and your new corporation which apparently now is in breach of certain key provisions of the settlement agreement outlined in this breach notice.

Microsemi's Options

We need to clear this up immediately and have a number of proposals we would like to speak with corporate officers about without legal counsel (litigation support) involvement unless the corporation would rather take this immediately back into court.

These claims are caused by the improper transfer of the Patent US6370629 from Symmetricom to Microsemi in violation of the Settlement Terms in the attached document.

Notice of Breach

Please be advised under the Glassey/McNeil Settlement agreements (attached) that your company has a number of responsibilities it to date has failed to meet in managing the umbrella patent which protects our rights and perfects your role per the terms of the contract.

These must be completed PRIOR to Glassey and McNeil "certifying the merger" between Microsemi and Symmetricom.

These are as follows:

**Formal Notice of Assignment to a new party is required -
based on ongoing FIDUCIARY ROLE**

There is a direct requirement to accept the terms of this contract since under it the party in the FIDUCIARY ROLE (your company) sits now. Without accepting this role formally the merger is incomplete and is open to ongoing litigation pertaining to the fraudulent transfer of this contract to the new Microsemi in violation of the following term.

BREACH OF CONTRACT and COMPLIANCE DEMAND NOTICE

8.4 The parties may assign all rights and delegate all duties hereunder to an entity acquiring that portion of each parties' business to which this Agreement relates, or to any corporate successor by way of merger or consolidation, provided that the assignee delivers to DATUM or GMT/GLASSEY/MCNEIL, as appropriate, a statement that the assignee assumes the assigning party's obligations hereunder. GMT/GLASSEY/MCNEIL may assign its right to receive the royalty payments provided in paragraph 3.2 to any person or entity provided that DATUM receives notice in writing of such assignment signed by GMT, GLASSEY and MCNEIL.

The Roles were intended to be permanent - that's why all non-payment terms survive forever

The ROLES in this contract are **FIDUCIARY** (Microsemi) and **Benefiting Party** (Glassey and McNeil). In this role your company is required to protect and defend any basic claims to the IP you licensed back to us under the Settlement Agreement your predecessors (DATUM INC) are the sole authors of. This is setup forever by section 3.15 of the Settlement Agreement and is directly tied to performance of the roles.

The same is true of the IP codified as derivatives of Glassey's TTI or Trusted Timing Infrastructure which were built per the terms of the TTI Settlement itself.

All non-financial terms are permanent in form:

3.15 Termination of Payment Obligation and Survival of Non-Payment Terms: The parties agree and acknowledge that DATUM's royalty payment obligations terminate after the royalty payment derived from the third year of the royalty. Notwithstanding the foregoing, all other terms of this Agreement will remain in full force and effect after termination of DATUM's payment obligations.

This was done because the financial side of the settlement was structured to cover local use levels for all devices and had a number of traps to force the renegotiation or adjust the compensation for TTI and DDI technologies used by DATUM (and its successors) which it licensed from Glassey.

As such there are a number of continuing responsibilities for the FIDUCIARY role in this matter,

Microsemi must agree to accepting Fiduciary Role

Per section 8.4 of the Settlement Agreements Microsemi as successor to DATUM INC is tied to this agreement and per that clause in the Settlement Agreement Microsemi "must agree to become the formal IP Protector and assume the Fiduciary Role the transfer of the IP to Microsemi requires" prior to the completion of the Merger or the Merger is imperfect per US and Canadian law both. This requirement is codified in section 8 of the

BREACH OF CONTRACT and COMPLIANCE DEMAND NOTICE

settlement agreements.

Come Home to California Clause

Additionally Microsemi per sections 8.1 and 8.3 of the contract, on a yearly basis an affidavit is to be produced showing the agreement of the parties these technologies are sold to "to be bound by the 8.1 and 8.3 controls therein".

8.1 This Agreement is subject to, governed by, and shall be construed in accordance with the laws of the State of California.

and

8.3 This Agreement is enforceable and binding upon the parties hereto, their successors and assigns, and any agents or others under the control or direction of the parties. Moreover, both parties, as well as the signatories, hereby warrant and covenant that their respective representative signing this Agreement has full authority to bind the parties to the terms of this Agreement.

Periodic Reporting is required

What sections 8.4, 3.15, 8.1, and 8.3 require is a periodic reporting under section 8.8 of all parties status in enforcing this contract. This is true of both Settlement Agreements (DDI and TTI) and was put there to prevent the abuse of the limited use licensing paid by Datum to Glassey (and McNeil).

Requirements

As such, and based on a number of previous acts we require the production immediately (within 14 days) of the following:

- 1) A fully notarized copy of all wet signed originals of the Settlement Agreement with fully legible signatures of Mark Hastings and Gerald Willets for Digital Delivery and Erik Van Der Kaay for DATUM.
- 2) the below affidavit pertaining to third-party enforcement rights for PHASE-II Technologies under the Settlement agreement. This is to be produced for 'demonstration to any third parties' Glassey and McNeil's enforcement rights pertaining to PHASE-II technologies. ; said document to be executed and notarized and returned within 14 days per the terms of section 8.7 of this agreement.

Affidavit Text:

**BREACH OF CONTRACT and
COMPLIANCE DEMAND NOTICE**

"Under the perjury laws of the State of California I declare to the following to be true and correct.

Further under our settlement and its testimonial requirement per section 8.7 we declare that Todd Glassey and Michael McNeil are the lawful creators of all PHASE-II Technologies codified in the US6370629 patents and its foreign filings; and as such hold direct legal power of attorney pertaining to those IPs for all Third-Party and Sublicensing matters.

Witness my hand

// CEO or General Counsel (signer must also sit on corporations board as well as be a C level officer)"

- 3) Issue formal orders to Lathem Watkins its predecessor SYMMETRICOM's law firm to release to Glassey and McNeil any and all communications between Lathem Watkins and any corporation Glassey and McNeil tried to enforce the IP rights codified in the Settlement Agreement against.
- 4) Issue formal notice to each of those parties sending an executed copy of the above affidavit text and a note that "Glassey and McNeil in fact do control the sublicensing and all third-party enforcement rights for what are called PHASE-II technologies and as such any of those parties infringements would need to be licensed through Glassey and McNeils operations and not Microsemi".
- 4) Formal notice to the USPTO that "Datum licensed a derivative of IP which already existed from Glassey under the TTI Settlement and that he is the sole creator of the original IP which Datum licensed to create the components for which the US63393126 patent is filed for and as such is the true original inventor, something they discovered through their diligence after the merger was completed.

Other periodic documents and foreign submissions to the Patent Offices US63670629 will also be required to formally revive those filings. We will require those under ss8.7 of the contract as well. We await return and production of this first set of requirements.

Witness my hand

Todd S. Glassey Signatory to Settlement and sole inventor of US6370629 and US6393126.

CONTRACTS

CONSULTING AGREEMENT

1. INTRODUCTION

This agreement is entered into by Datum Inc., Bancomm-Timing Division; 6781 Via Del Oro; San Jose, CA 95119, herein after referred to as DATUM, and:
Name/Organization: Todd Glassey
Address: 109A Bluebonnet Lane, Scotts Valley, Ca 95066
TaxID/SSN#: 579-07-0748 herein after referred to as CONSULTANT for the purpose of securing technical consulting services as detailed in the STATEMENT OF WORK attached.

2. PERIOD

The period of this agreement is: 4th May 1998 to 4th July 1998. If either party wishes to discontinue this Agreement, either may do so upon thirty (30) days Notice to the other party. The "Termination Date" shall be the date on which the thirtieth (30th) day falls. If one party breaches this Agreement, however, or license provided herein, the non-breaching party may, at its option, provide the breaching party with Notice immediately and automatically terminating this Agreement. The date of Notice shall be the "Termination Date". All work shall be stopped on the Termination Date.

3. CONFIDENTIALITY

Each party shall exercise due diligence to preserve the confidentiality of Trade Secrets and other valuable proprietary information provided by the other in support of the contracted effort and during the term of the Consulting Agreement. All information designated as a Trade Secret or Confidential shall be maintained as confidential even after the termination of this Consulting Agreement.

3.1: "Trade Secret" means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listing of names, addresses or telephone numbers, or other information relating to any business of profession which is secret and of value. To be a Trade Secret the owner thereof must have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes. Information shall not be deemed to be a Trade Secret, confidential or proprietary which (1) is known to the other party before disclosure by owner of the information; (2) is now or hereafter becomes part of the public domain without fault of the other party; (3) is disclosed to the other party on a non-confidential basis by a third party under no legal disability to make such a disclosure; or (4) is disclosed pursuant to judicial action or Governmental regulation, providing efforts are made to ensure that further dissemination will not occur.

4. NON COMPETITION

During this Agreement and for a period of 6 months after the termination of this Agreement, CONSULTANT agrees not to provide any original, Intellectual Property newly developed for DATUM during the course of this Agreement, and not a Derivative Work of CONSULTANT's Intellectual Property, to DATUM's competitors as detailed below. These competitors are as follows:

Hewlett Packard, various locations.
Timing Solutions, Boulder, CO
True Time Inc, Santa Rosa, CA
Odetics, Anaheim, CA
Trak Microwave, various locations.
Arbiter Systems, San Luis Obispo, CA
DataChron, San Diego, CA

5. RIGHTS IN DATA

DATUM retains all rights in data including, but not limited to ownership of all materials, information, software in any format, and other properties generated in whole or in part by the CONSULTANT during the terms of this contract. Without limiting the prior sentence, the term properties includes specifications, documents, data, files, input/output, ideas, documentation and any related material. This paragraph shall survive the termination of this agreement.

If the CONSULTANT wants to retain data right ownership and license products and technologies to DATUM, a separate licensing agreement shall be executed. CONSULTANT shall identify these products and technologies to DATUM prior to initiating any work.

6. CHARGE RATE

CONSULTANT agrees to charge, and DATUM agrees to pay, \$ 75 per hour for CONSULTANT'S service. Further, DATUM shall reimburse to CONSULTANT any and all expenses, including travel, hotel, taxes, and or equipment purchases made in furtherance of this Agreement. CONSULTANT will invoice DATUM for services and expenses as outlined in Paragraph #7 below.

7. PAYMENT

CONSULTANT shall provide DATUM with an invoice based on completed milestones or bi-weekly work completed. This invoice shall include hours expended; a brief statement detailed the nature of the task completed; rate; total hourly billing; materials and service charges expended (included sales taxes, if any); travel and per diem as previously agreed; and total invoice amount.

Normal payment schedule:

Week_n Invoice processed at Bancomm-Timing San Jose and submitted to Accounting.
Week_{n+1} Invoice processed at Bancomm-Timing, CA, and mailed on Thursday or Friday.
Week_{n+2} Payment received.

8. LIMITATIONS OF LIABILITY

8.1 Limited per attached SpectraDynamics Limitation of Liability Statement.

9. GENERAL

9.1 CONSULTANT is, and shall hold itself out only as, an independent contractor of DATUM.

9.6 All Notices, requests, demands, applications, services of process, and other communications which are required to be or may be given under this Agreement shall be in writing and shall be deemed to have been duly given if sent by telecopy or facsimile transmission, answer back requested, or delivered by courier or mailed, certified first class mail, postage prepaid, return receipt requested, to the parties to this Agreement at the following addresses:

To DATUM:
6781 Via del Oro
San Jose, CA 95119

Attn.: President
Telephone: _____
Telecopy: _____

To CONSULTANT:
TODD GLASSEY
1054 R. Dineen
Scotts Valley CA 95066

Attn.: President
Telephone: (408) 439-7811
Telecopy: _____

This agreement is approved by:
Datum Inc, Bancomm-Timing Division

Mitch Stone

By: Mitch Stone
Title: Vice President
Date: 4th May 1998
FILE: j:\management\consult\glassey consulting Agreement.doc

Consultant:

Todd Glassey

By: TODD GLASSEY
Title: _____
Date: 12-11-98

CONSULTING AGREEMENT

1. INTRODUCTION

This agreement is entered into by Datum Inc., Bancomm-Timing Division; 6781 Via Del Oro; San Jose, CA 95119, herein after referred to as DATUM, and:

Name/Organization: Michael McNeil

Address: 1271 Lost Acre Drive, Felton, California 95018

TaxID/SSN#: 516 54 6307 herein after referred to as CONSULTANT for the purpose of securing technical consulting services as detailed in the STATEMENT OF WORK attached.

2. PERIOD

The period of this agreement is: 4th May 1998 to 4th July 1998. If either party wishes to discontinue this Agreement, either may do so upon thirty (30) days Notice to the other party. The "Termination Date" shall be the date on which the thirtieth (30th) day falls. If one party breaches this Agreement, however, or license provided herein, the non-breaching party may, at its option, provide the breaching party with Notice immediately and automatically terminating this Agreement. The date of Notice shall be the "Termination Date". All work shall be stopped on the Termination Date.

3. CONFIDENTIALITY

Each party shall exercise due diligence to preserve the confidentiality of Trade Secrets and other valuable proprietary information provided by the other in support of the contracted effort and during the term of the Consulting Agreement. All information designated as a Trade Secret or Confidential shall be maintained as confidential even after the termination of this Consulting Agreement.

3.1: "Trade Secret" means the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listing of names, addresses or telephone numbers, or other information relating to any business or profession which is secret and of value. To be a Trade Secret the owner thereof must have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes. Information shall not be deemed to be a Trade Secret, confidential or proprietary which (1) is known to the other party before disclosure by owner of the information; (2) is now or hereafter becomes part of the public domain without fault of the other party; (3) is disclosed to the other party on a non-confidential basis by a third party under no legal disability to make such a disclosure, or (4) is disclosed pursuant to judicial action or Governmental regulation, providing efforts are made to ensure that further dissemination will not occur.

4. NON COMPETITION

During this Agreement and for a period of 6 months after the termination of this Agreement, CONSULTANT agrees not to provide any original, Intellectual Property newly developed for Datum during the course of this Agreement, and not a Derivative Work of CONSULTANT's Intellectual Property, to DATUM's competitors as detailed below. These competitors are as follows:

Hewlett Packard, various locations.
Timing Solutions, Boulder, CO
True Time Inc, Santa Rosa, CA
Odetics, Anaheim, CA
Trak Microwave, various locations.
Arbiter Systems, San Luis Obispo, CA
DataChron, San Diego, CA

5. RIGHTS IN DATA

DATUM retains all rights in data including, but not limited to ownership of all materials, information, software in any format, and other properties generated in whole or in part by the CONSULTANT during the terms of this contract. Without limiting the prior sentence, the term properties includes specifications, documents, data, files, input/output, ideas, documentation and any related material. This paragraph shall survive the termination of this agreement.

If the CONSULTANT wants to retain data right ownership and license products and technologies to DATUM, a separate licensing agreement shall be executed. CONSULTANT shall identify these products and technologies to DATUM prior to initiating any work.

6. CHARGE RATE

CONSULTANT agrees to charge, and DATUM agrees to pay, \$ 75 per hour for CONSULTANT'S service. Further, DATUM shall reimburse to CONSULTANT any and all expenses, including travel, hotel, taxes, and or equipment purchases made in furtherance of this Agreement. CONSULTANT will invoice DATUM for services and expenses as outlined in Paragraph #7 below.

7. PAYMENT

CONSULTANT shall provide DATUM with an invoice based on completed milestones or bi-weekly work completed. This invoice shall include hours expended; a brief statement detailed the nature of the task completed; rate; total hourly billing; materials and service charges expended (included sales taxes, if any); travel and per diem as previously agreed; and total invoice amount.

Normal payment schedule:

Week _n	Invoice processed at Bancomm-Timing San Jose and submitted to Accounting.
Week _{n+1}	Invoice processed at Bancomm-Timing, CA, and mailed on Thursday or Friday.
Week _{n+2}	Payment received.

8. LIMITATIONS OF LIABILITY

8.1 Limited per attached SpectraDynamics Limitation of Liability Statement.

9. GENERAL

9.1 CONSULTANT is, and shall hold itself out only as, an independent contractor of DATUM.

9.6 All Notices, requests, demands, applications, services of process, and other communications which are required to be or may be given under this Agreement shall be in writing and shall be deemed to have been duly given if sent by telecopy or facsimile transmission, answer back requested, or delivered by courier or mailed, certified first class mail, postage prepaid, return receipt requested, to the parties to this Agreement at the following addresses:

To DATUM:
6781 Via del Oro
San Jose, CA 95119

To: CONSULTANT:
1271 Lost Acre Dr.
Felton, CA 95018

Attn.: President
Telephone: _____
Telecopy: _____

Attn.: President
Telephone: 408 335-2069
Telecopy: _____

This agreement is approved by:
Datum Inc, Bancomm-Timing Division

Mitch Stone

By: Mitch Stone
Title: Vice President
Date: 4th May 1998
FILE: j:\management\consult\glassey consulting Agreement.doc

Consultant:

Michael McNeil

By: Michael McNeil
Title: _____
Date: 5/12/98

CO-INVENTOR AGREEMENT

This is Co-Inventor Agreement ("Agreement"), is made this 26th day of October, 1988 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, 1987 (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.

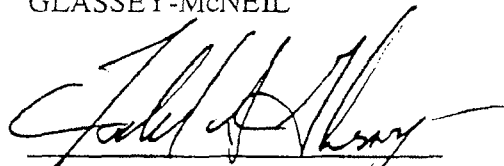
IN WITNESS WHEREOF, the parties hereto have executed this Agreement the day and year first above written.

DIGITAL DELIVERY


[Signature]

T. Mack Hastings President
[Please Print Name/Title]

GLASSEY-McNEIL


TODD S. GLASSEY

Michael McNeil
MICHAEL E. McNEIL

SETTLEMENT AGREEMENT AND MUTUAL RELEASE

This Settlement Agreement and Release ("Agreement") is entered into by and between DATUM, INC. ("DATUM") and DIGITAL DELIVERY INC. ("DDI"), on the one hand, and GLASSEY-MCNEIL TECHNOLOGIES ("GMT"), TODD GLASSEY ("GLASSEY") and MICHAEL E. MCNEIL ("MCNEIL") (collectively referred to as "GMT/GLASSEY/MCNEIL"), on the other hand.

SECTION ONE
BACKGROUND

1.1 GLASSEY and MCNEIL and DDI entered into a Co-Inventor Agreement, dated October 26, 1998 (the "Co-Inventor Agreement"), pursuant to which those parties agreed, on an interim basis, to certain rights and interests in intellectual property and to certain future payment obligations of DDI, pending the execution of a definitive agreement with respect to such intellectual property.

1.2 On or about July 29, 1999, DATUM consummated a merger whereby DDI became a wholly owned subsidiary of DATUM.

1.3 On or about August 20, 1999, DATUM filed a complaint (the "COMPLAINT") stating claims against GMT/GLASSEY/MCNEIL for, among other things, Breach of Contract, Breach of the Covenant of Good Faith and Fair Dealing, Misappropriation of Trade Secrets and Proprietary Business Information, Trade Libel, Slander and Declaratory Relief.

1.4 DATUM, DDI and GMT/GLASSEY/MCNEIL desire to definitively resolve and terminate the interim arrangements arising from the Co-Inventor Agreement, to avoid the risks and expenses attendant upon litigation and to reach a mutual, full and final compromise and settlement of the parties' matters, claims, causes of action and the like with respect the Co-Inventor Agreement, the Assembly, Distribution and Use of Digital Information Patent, the Controlling Access Patent and the Phase II Technology (as defined below).

DOCSOC696435v3\19250.0043

Exhibit E - Controlling Access Settlement

SYM00001

1.5 This Settlement Agreement is a mutual and complete compromise between the parties and is intended as a complete and final resolution and settlement of the respective differences, positions and claims of DDI, DATUM and GMT/GLASSEY/MCNEIL, with respect to the Co-Inventor Agreement, the Assembly, Distribution and Use of Digital Information Patent, the Controlling Access Patent and the Phase II Technology.

SECTION TWO

DEFINITIONS

2.1 The Assembly, Distribution and Use of Digital Information Patent: U.S. Patent No. 5,646,992 issued to DDI on July 8, 1997 for certain data and file protection and encryption technology. One of the products produced under this patent is called the Confidential Courier, which is described as an electronic transmittal envelope which can be opened only by specifically designated persons having the encoded passwords.

2.2 Controlling Access Patent: A US and certain foreign countries patent pending covering the expansion of technology covered by the Assembly, Distribution and Use of Digital Information Patent to include the new technology of geo-positioning and time/data encryption with respect to digital data and file assembly, distribution, use and access.

2.3 Phase II Technology - Phase II Technology refers to the method of authentication, encryption and transmission of date/time and/or location data for the purpose of linking together two or more disparate electronic components, such that a trust model is established between them. Such physical elements must individually be capable of computational and cryptographic functionality, but computationally may be isolated from one another. Such electronic components must be physically secure, and communicate with each other over communications channel(s) which may themselves be insecure.

SECTION THREE
TERMS OF SETTLEMENT

3.1 In consideration of the mutual covenants set forth herein, and in full settlement of the claims and causes of action asserted or held by DDI and/or GMT/GLASSEY/MCNEIL under the Co-Inventor Agreement, the parties agree as follows:

3.2 Assignment of Controlling Access Patent: GMT/GLASSEY/MCNEIL assign all rights, title and interest in the Controlling Access Patent and the application therefor, to DATUM.

3.3 Ownership of and License to Use Phase II Technology: DDI and DATUM acknowledges that GMT/GLASSEY/MCNEIL owns all rights, title and interest in the Phase II Technology, but GMT/GLASSEY/MCNEIL hereby grants DATUM a perpetual, non-exclusive, irrevocable, assignable, sub-licensable, worldwide license for use of the Phase II Technology and derivatives thereof, with rights to sublicense, in connection with the Confidential Courier product and other products and technology covered by the Controlling Access Patent.

3.4 Payment: DATUM will pay to GMT/GLASSEY/MCNEIL \$300,000 upon full execution of this Agreement. Payment shall be wired within 24 hours of execution as follows:

Bank Routing No. 121139096

Bank Account No. 01-49350-5

Bank Name: Coast Commercial Bank

Bank Address: 720 Front Street
Santa Cruz, California 95060

3.5 Dismissal of Complaint: DATUM agrees to dismiss with prejudice the COMPLAINT within ten (10) days of the full execution of this Agreement

3.6 Acknowledgment of Rights Under the Assembly, Distribution and Use of Digital Information Patent GMT/GLASSEY/MCNEIL disclaim and waive any rights to the Assembly,

Distribution and Use of Digital Information Patent and the technology described therein and agree not to make, use or sell any products developed using or derived from the Phase II Technology which also include the technology described in or covered by the Assembly, Distribution and Use of Digital Information Patent. GMT/GLASSEY/MCNEIL explicitly acknowledge that they had no participation in the invention or patent application process which resulted in the U.S. Patent No. 5,646,992 issued to DDI on July 8, 1997.

3.7 Co-Inventor Agreement Terminated. In addition and without duplication, upon the execution of this Agreement and payment of the amount specified in paragraph 3.4, above the Co-Inventor Agreement shall be terminated, and this Agreement shall be the only agreement of the parties with respect to the subject matter of the Co-Inventor Agreement and this Agreement. Such subject matter includes without limitation the future payment obligations and division of intellectual property rights set forth in the Co-Inventor Agreement. The parties hereto acknowledge and agree that the settlement payment constitutes the satisfaction in full of any claims by GMT/GLASSEY/MCNEIL for compensation of any kind pursuant to the Co-Inventor Agreement.

3.8 Availability of Injunctive Relief: GMT/GLASSEY/MCNEIL acknowledge and agree that the covenants of GMT/GLASSEY/MCNEIL and the restrictions on GMT/GLASSEY/MCNEIL contained in this Agreement are reasonable and necessary in order to protect the legitimate interests of DATUM, and that any violation thereof by GMT/GLASSEY/MCNEIL or any affiliates would result in irreparable injuries to DATUM, for which damages would not, in and of themselves, be an adequate remedy. Therefore, GMT/GLASSEY/MCNEIL acknowledge and agree that, in the event of a violation or breach by GMT/GLASSEY/MCNEIL or any affiliates of any of the covenants or any of the restrictions contained in this Agreement, DATUM shall be entitled to obtain, from any court of competent jurisdiction, temporary, preliminary and permanent injunctive relief, in addition to any other rights or remedies to which DATUM may be entitled under applicable law or equitable principles, without the necessity on the part of DATUM of having to post a bond or other security and without thereby limiting any other rights and remedies, including the recovery of monetary damages, that DATUM may have hereunder or under applicable law by reason of such violation or breach.

3.9 Release of Claims:

3.9.1 GMT/GLASSEY/MCNEIL's Release of Claims Against DATUM and DDI

GMT, GLASSEY and MCNEIL, for themselves and for themselves and for and on behalf of GMT and any affiliates, related entities, assigns and successors in interest, if any, now or in the future, hereby irrevocably release, forgive and discharge DATUM and DDI and all of their officers, directors, shareholders, partners, agents, employees, representatives, affiliates, parent, subsidiaries, and related entities, assigns and successors in interest, if any, now or in the future (collectively, the "Datum Parties"), from any and all obligations, responsibilities and liabilities relating to or arising out of the Co-Inventor Agreement against the Datum Parties. Notwithstanding the foregoing, DATUM's obligations under this Agreement are expressly excepted from the foregoing release.

3.9.2 DATUM's and DDI's Release of Claims Against

GMT/GLASSEY/MCNEIL: DATUM and DDI agree and acknowledge for themselves and for themselves and for and on behalf of DATUM and any affiliates, related entities, assigns and successors in interest, if any, now or in the future, that GMT/GLASSEY/MCNEIL are released and fully discharged from any and all obligations, responsibilities and liabilities to DATUM or DDI relating to or arising out of the Co-Inventor Agreement. Notwithstanding the foregoing, GMT/GLASSEY/MCNEIL's obligations under this Agreement are expressly excepted from the foregoing release.

3.9 Civil Code Section 1542: With respect to the matters herein stated as the subject of release, the parties hereto do hereby mutually waive and relinquish any and all rights which any of them may have under the provisions of Section 1542 of the Civil Code of the State of California, which Section reads as follows:

**"A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS
WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT
TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING
THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE
MATERIALLY AFFECTED HIS SETTLEMENT WITH THE
DEBTOR."**

3.10 Attorney's Fees: DATUM, DDI and GMT/GLASSEY/MCNEIL shall bear their own costs and attorneys' fees in connection with their respective disputes and claims settled herein.

SECTION FOUR
WARRANTIES AND REPRESENTATIONS

4.1 The parties hereto warrant and represent that no promise or inducement has been offered or made for this Agreement except as herein set forth, that this Agreement is executed without reliance on any statements or any representations not contained herein, and that this Agreement reflects the entire settlement among the parties. The attorneys of record warrant and represent that they are satisfied that their respective clients fully understand the effect, significance and consequence of this Agreement. The terms, acknowledgments, warranties and representations made herein shall survive the execution and delivery of this Agreement, and shall be binding upon the respective heirs, representatives, and assigns and successors of each of the parties and their attorneys.

SECTION FIVE
NO ADMISSION OF LIABILITY

5.1 The parties hereto acknowledge and agree that this Agreement is entered into as a mutual compromise and settlement which is not in any respect or for any purpose to be deemed or construed as an admission or concession of any liability whatsoever on the part of any of the parties hereto.

SECTION SIX
CONFIDENTIALITY

6.1 The parties agree that this Agreement and its terms are confidential. The parties further agree that the confidentiality of this Agreement and its terms is a material term of this Agreement without which the parties would not have consented to the Agreement. The parties expressly agree that they will not disclose or discuss the terms of this Agreement with any person. GMT/GLASSEY/MCNEIL shall notify DATUM's legal counsel, in writing, of the receipt of any request for the disclosure of any confidential information. GMT/GLASSEY/MCNEIL shall cooperate with the efforts of DATUM to quash such subpoena or other legal process or to obtain a protective order, as DATUM deems appropriate. The parties shall have the right to provide required information concerning this Agreement to investors and potential investors, and to Affiliates in order to enable them to carry out the activities contemplated hereunder and in connection with strategic business needs. Any such disclosure shall be pursuant to a separate agreement of confidentiality between DATUM or GMT/GLASSEY/MCNEIL and any such third parties.

6.2 The parties further agree to maintain the confidentiality of any document or information which has been or is designated as confidential.

SECTION SEVEN
ENFORCEMENT OF AGREEMENT

7.1 If any legal action or other proceeding is brought for the enforcement of this Agreement, or because of an alleged dispute, breach, default, or misrepresentation arising out of or relating to any of the provisions of this Agreement, the successful or prevailing party or parties shall be entitled to recover reasonable attorneys' fees and other costs incurred in that action or proceeding, in addition to any other relief to which it or they may be entitled.

SECTION EIGHT
MISCELLANEOUS

8.1 This Agreement is subject to, governed by, and shall be construed in accordance with the laws of the State of California.

8.2 GMT/ GLASSEY/MCNEIL represent and warrant that they are the sole and rightful owners of the claims asserted in the dispute described in this Agreement and that any such claims have not been assigned or transferred to any unnamed party. DATUM and DDI represent and warrant that DATUM is the sole and rightful owner of the claims asserted in the COMPLAINT and otherwise herein and that any such claims have not been assigned or transferred to any unnamed party.

8.3 This Agreement is enforceable and binding upon the parties hereto, their successors and assigns, and any agents or others under the control or direction of the parties. Moreover, both parties, as well as the signatories, hereby warrant and covenant that their respective representative signing this Agreement has full authority to bind the parties to the terms of this Agreement.

8.4 The parties may assign all rights and delegate all duties hereunder to an entity acquiring that portion of each parties' business to which this Agreement relates, or to any corporate successor by way of merger or consolidation, provided that the assignee delivers to DATUM or GMT/GLASSEY/MCNEIL, as appropriate, a statement that the assignee assumes the assigning party's obligations hereunder.

8.5 This Agreement constitutes and contains the entire understanding and agreement of the parties and cancels and supersedes any and all prior negotiations, correspondence and understandings and agreements, whether verbal or written, between the parties respecting the subject matter hereof. No waiver, modification or amendment of any provision of this Agreement shall be valid or effective unless made in writing and signed by a duly authorized officer of each of the parties.

8.6 The provisions of this Agreement are severable, and if one or more provisions should be determined to be judicially unenforceable, in whole or in part, the remaining provisions shall nevertheless be binding and enforceable. The provisions of this Agreement shall be construed as separate provisions covering their subject matter in each of the separate counties and states in the United States in which DATUM transacts its business; to the extent that any provision shall be judicially unenforceable in any one or more of those counties or states, that provision shall not be affected with respect to each other county or state, each provision with respect to each county and state being construed as severable and independent.

8.7 The parties agree to take any acts, and execute any further documents, that may be reasonably necessary to accomplish and effect the terms of this Agreement.

8.8 This Agreement may be executed in counterparts and by fax, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, this Agreement has been executed by the undersigned on the dates below indicated.

Dated: November 14, 1999


TODD GLASSEY

Dated: November 19, 1999


MICHAEL MCNEIL

Dated: November 14, 1999


GLASSEY MCNEIL TECHNOLOGIES

Dated: November __, 1999

DATUM, INC.

Dated: November __, 1999

DIGITAL DELIVERY, INC.

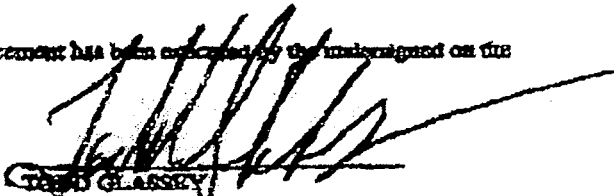
8.6 The provisions of this Agreement are severable, and if one or more provisions should be determined to be judicially unenforceable, in whole or in part, the remaining provisions shall nevertheless be binding and enforceable. The provisions of this Agreement shall be construed as separate provisions covering their subject matter in each of the separate countries and states in the United States in which DATUM transacts its business; to the extent that any provision shall be judicially unenforceable in any one or more of those countries or states, that provision shall not be affected with respect to each other country or state, each provision with respect to each country and state being construed as severable and independent.

8.7 The parties agree to take any acts, and execute any further documents, that may be reasonably necessary to accomplish and effect the terms of this Agreement.

8.8 This Agreement may be executed in counterparts and by fax, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, this Agreement has been executed by the undersigned on the dates below indicated.

Dated: November 11, 1999


THOMAS GLASSEY

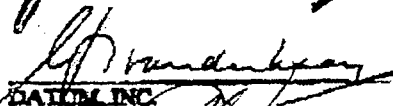
Dated: November 19, 1999


MICHAEL MCNEIL

Dated: November 19, 1999


GLASSEY MCNEIL TECHNOLOGIES

Dated: November 29, 1999


DATUM, INC.

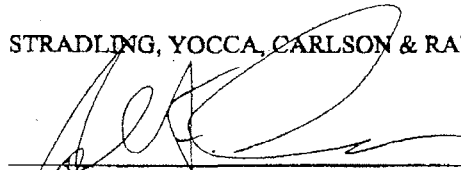
Dated: November 29, 1999


DIGITAL DELIVERY, INC.

APPROVED AS TO FORM AND CONTENT:


STRADLING, YOCCA, CARLSON & RAUTH

Dated: November __, 1999 By:


John F. Cannon
Attorneys for DATUM, Inc. and Digital Delivery Inc.

BOSSO, WILLIAMS SACHS, BOOK, ATACK &
GALLAGHER

Dated: November 19, 1999 By:


Jason R. Book, Esq.
Attorneys for Glassey-McNeil Technologies, Inc.
Todd Glassey, and Michael McNeil.

7

SETTLEMENT AGREEMENT AND MUTUAL RELEASE

This Settlement Agreement and Release ("Agreement") is entered into by and between DATUM, INC. ("DATUM"), on the one hand, and GLASSEY-MCNEIL TECHNOLOGIES ("GMT"), TODD GLASSEY ("GLASSEY"), and MICHAEL MCNEIL ("MCNEIL"), (sometimes collectively referred to as "GMT/GLASSEY/MCNEIL"), on the other hand.

SECTION ONE

BACKGROUND

1.1 This Agreement is a mutual and complete compromise between the parties and is intended as a complete and final resolution and settlement of the respective differences, positions and claims of DATUM and GMT/GLASSEY/MCNEIL, as described below.

1.2 All parties hereto desire to avoid the risks and expenses attendant upon further litigation and to reach a mutual, full and final compromise and settlement of the parties' disputes, claims, causes of action and the like.

1.3 In or about February 1998 the parties began collaborating on the development of certain technologies related to electronic commerce and time verification, which included the development of certain intellectual property, technologies, trade secrets and confidential and proprietary information. The parties also collaborated on the development of marketing efforts related to electronic commerce and time verification. The parties' collaborative efforts continued through the end of 1998/early 1999.

1.4 From the parties' business relationship a dispute arose between DATUM and GMT/GLASSEY/MCNEIL. Among other things, the parties dispute ownership in and other rights to certain of the intellectual property, technologies, trade secrets and confidential and proprietary information developed or contributed during the parties relationship, including the Protected Technology, defined below. When the parties were unable to resolve the dispute informally, on or around August 20, 1999, DATUM filed a complaint (the "COMPLAINT") stating claims for, among other things, Breach of Contract, Breach of the Covenant of Good Faith and Fair Dealing,

Misappropriation of Trade Secrets and Proprietary Business Information, Trade Libel, Slander and Declaratory Relief.

SECTION TWO

DEFINITIONS

2.1 Protected Technology: Protected Technology includes any information, data, method, product, software, hardware, trade secrets, copyrights, documents, e-mails, technology, ideas, or inventions, disclosed, provided, produced, created in any form by GMT/GLASSEY/MCNEIL to, for, or in conjunction with DATUM between the initiation of the parties' relationship on February 1, 1998 through March 1, 1999, including any derivatives thereof, and any information, data, method, product, software, hardware, trade secrets, copyrights, documents, e-mails, technology, ideas, or inventions, disclosed, provided, produced, created in any form by DATUM to which GMT/GLASSEY/MCNEIL had, or was provided access to, or gained knowledge of or worked on between February 1, 1998 through March 1, 1999, including all derivatives thereof, including the Trusted Time Infrastructure ("TTI"), TTI II, or any further derivative or variation thereof, including but not limited to the Trusted Local Clocks and Trusted Master Clocks defined below.

2.2 Trusted Local Clocks: The Trusted Local Clock ("TLC") is a particular implementation of a trusted clock that is periodically certified to an upper clock, typically a Trusted Master Clock (TMC). The TLC provides time stamp tokens and temporal tokens. The TLC is a PCiv2.1 compliant card and assumed to be operating in an insecure host in an insecure environment. It uses a real time operating system to control the on-card functions.

2.3 Trusted Master Clocks: The Trusted Master Clock ("TMC") is a particular implementation of a trusted clock, synchronized to Coordinated Universal Time and made comparable to the time offered by a National Time Standard such as the National Institute of Science and Technology, which generates trusted time data which is sent to TLCs for time stamping and other certification purposes. The TMC also monitors and calibrates the TLCs.

2.4 Trusted Time Infrastructure: The term Trusted Time Infrastructure ("TTI") describes

a particular system and process developed by Datum by which time can be affixed to an e-commerce document or transaction, or any other electronically transmitted information, in such a way that it can be free from outside alteration, thus providing a universal, secure and reliable way to ascertain when a transaction occurred or a document was received or sent.

John L. Hyslop
Michael M. Hyslop

2.5 Net Sales: Net Sales shall mean the amount invoiced for sales of Trusted Local Clocks and Trusted Master Clocks (collectively the "Licensed Products") by DATUM less the following deductions (to the extent they are not already reflected in the amount billed):

- (i) Discounts, refunds, and wholesaler chargebacks allowed and taken in amounts customary in the trade;
- (ii) Import, export, excise, sales or use taxes, tariffs and duties directly imposed and with reference to particular sales;
- (iii) Outbound transportation prepaid or allowed, including insurance.
- (iv) Amounts allowed or credited on rebates, returns or retroactive price deductions.

Licensed Products shall be considered "sold" when the amount billed out or invoiced to a third party has been received by DATUM. Licensed Products shall not be sold for less than commercially reasonable amounts, provided however, DATUM may provide Licensed Products as samples and promotional items in the normal course of business for no charge or reduced charge. If a Licensed Product is incorporated into another product or is sold in combination with other products or services and not invoiced separately, such Licensed Products shall be included in the Net Sales at the then current list price for such quantities of such Licensed Products with any discount from list price being applied proportionately to the discount from list price of the product into which the Licensed Product was incorporated or the list price of the other product sold, as the case may be. If there is then no current list price for such Licensed Product, the Net Sales will be based on the separate value of such Licensed Product and such other products or services.

SECTION THREE
TERMS OF SETTLEMENT

3.1 In consideration of the mutual covenants set forth herein, and in full settlement of the claims and causes of action asserted or held by DATUM and/or GMT/GLASSEY/MCNEIL, the parties agree as follows:

3.2 Royalty:

(a) DATUM agrees to pay to GMT/GLASSEY/MCNEIL a three percent (3%) royalty upon the Net Sales by DATUM of any DATUM Trusted Local Clocks and Trusted Master Clocks. The royalty shall be calculated based upon final sales as of the end of the calendar year in which a royalty may be calculated. The royalty shall be due within sixty (60) days of the end of each year the royalty is due.

(b) The duration of the royalty shall be three (3) years (years 2000, 2001 and 2002).

(c) The royalty shall be subject to a ceiling of \$150,000 per year. Under no circumstances shall DATUM be obligated to pay more than \$150,000 in royalties in any calendar year irrespective of the amount of its Net Sales in any calendar year. GMT/GLASSEY/MCNEIL has no rights to any payment other than the 3% royalty and subject to the ceiling of \$150,000.

(d) DATUM agrees to advance \$50,000 of its royalty payment at the commencement of each year for which a royalty may be paid. The first advance payment shall be made per the wiring instructions below on or before January 7, 2000. Thereafter, the advance shall be paid within the first thirty days of each calendar year per the instructions below. Each of the three (3) \$50,000 advances shall be nonrefundable and shall not be subject to whether DATUM generates sufficient sales to generate the royalty payments but shall be creditable against the royalty earned pursuant to this section. All other royalty payments are subject to DATUM achieving sales of the two (2) products subject of the royalty.

(e) The first advance payment, due on or before January 7, 2000, shall be made by wire transfer to the following account:

(Correct #)
Bank Acc. # —

01-49530-5

Name on Account —

Bosso Williams
attorney Trust
Account.

Bank Routing No. 121139096
Bank Account No. 01-49350-5
Bank Name: Coast Commercial Bank
Bank Address: 720 Front Street
Santa Cruz, California 95060

All further payments shall be by wire transfer to the following account:

Bank Routing No.: 121139096
Bank Account No.: 04-50823-8
Bank Account Name: Glassey-McNeil Technologies
Bank Name: Coast Commercial Bank
Bank Address: 203 Mount Harmon Road
Scotts Valley, CA 95066

(f) Unless notified in a writing signed by GMT, GLASSEY and MCNEIL, and their legal counsel, changing the payees and/or destination of payment, DATUM will follow these instructions for all payments and will not be subject to liability for following such instructions.

3.2.1 Currency of Payments. All payments under this Agreement shall be made U.S. Dollars by wire transfer to such bank account as designated herein. Any payments due hereunder on Net Sales outside of the United States shall be payable in U.S. Dollars at the average of the rate of exchange of the currency of the country in which the Net Sales are made as reported in the New York edition of The Wall Street Journal, for the last three (3) business days of the period for which the royalties are payable.

3.2.2 Tax Withholding. If laws or regulations require the withholding of income taxes owed on account of royalties accruing under this Agreement, such taxes shall be deducted on a country-by-country basis by DATUM from such remittable royalty and will be paid by it to the proper taxing authority. Proof of payment shall be secured and sent to GMT/GLASSEY/MCNEIL as evidence of such payment.

3.2.3 Audit Rights re Royalty Payments: To the extent GMT/GLASSEY/MCNEIL in good faith dispute the amount of royalties to which they are entitled pursuant to this Agreement, GMT/GLASSEY/MCNEIL may request an inspection of DATUM's accounting records reflecting the calculation of Net Sales. Such request may be made once per year while Datum's royalty payment obligations continue under this Agreement. Unless such request is made within thirty (30) days of GMT/GLASSEY/MCNEIL's receipt of a royalty payment from DATUM, the right to audit that payment is waived. The inspection shall be made only by a Certified Public Accountant ("CPA"), subject to DATUM's approval, which will not unreasonably be withheld, and conditioned upon execution of a confidentiality agreement regarding the review of DATUM's records, which shall include, among other things, a provision which prohibits the disclosure by the CPA of any information disclosed, learned or reviewed during the audit to GMT/GLASSEY/MCNEIL except for the final calculation of the amount that the CPA contends DATUM owes under this Agreement. Unless otherwise mutually agreed to in writing, the inspection by the CPA shall take place at the law offices of Stradling, Yocca Carlson & Rauth in Newport Beach, California during normal business hours. No information inspected during the audit may be removed from the premises, other than that which is expressly permitted by this paragraph. For purposes of this audit, the CPA may review only the computer generated accounting records necessary to make a final calculation of royalties owed and shall not be given access to manufacturing documents, inventory records or any underlying invoices and records. GMT/GLASSEY/MCNEIL shall bear all its own costs and expenses incurred to conduct any audits. If the audit determines that an amount is owed by DATUM to GMT/GLASSEY/MCNEIL and that amount is within ten percent (10%) of the original amount paid by DATUM, GMT/GLASSEY/MCNEIL, or if the audit determines that no amount is owed, or if DATUM has overpaid, GMT/GLASSEY/DATUM shall also reimburse DATUM for all of DATUM's cost and expenses in handling any audit. DATUM shall have the right to offset any right to reimbursement under this provision from any future royalty payments.

3.3 Dismissal of Complaint: DATUM agrees to dismiss with prejudice the COMPLAINT within ten (10) days of the full execution of this Agreement.

3.4 Intellectual Property Rights Regarding the Protected Technology:

GMT/GLASSEY/MCNEIL disclaim any ownership in, or rights to, the Protected Technology and hereby acknowledge, represent and warrant that such Protected Technology is owned solely and exclusively by DATUM as its intellectual property, trade secrets and proprietary information. GMT/GLASSEY/MCNEIL agrees not to contest DATUM's ownership of any Protected Technology or the labeling of the Protected Technology as intellectual property, trade secrets, and/or proprietary information.

3.5 Other Agreements Superseded and Terminated: GMT/GLASSEY/MCNEIL further

agree that, with the exception of this Agreement, which supersedes the terms of any prior agreements of the parties, all terms of all other agreements between the parties including, but not limited to any consulting agreements between the parties, any confidentiality or non-disclosure agreements, any value added reseller agreements and any other express, implied or oral agreements are hereby terminated and hereafter void. The parties mutually agree that as between DATUM and GMT/GLASSEY/MCNEIL no provision of any agreement between the parties, other than this Agreement and the settlement agreement relating to the parties' prior co-inventor agreement, shall be deemed to survive.

3.6 Protection of DATUM's Trade Secrets and Proprietary Information: From the

execution date of this Agreement and at all times thereafter, GMT/GLASSEY/MCNEIL shall not, and shall not permit any representatives, agents, assigns or affiliates, to use or disclose to any person or entity any Protected Technology. GMT/GLASSEY/MCNEIL expressly agree, represent and acknowledge that they shall not engage in, or be associated with, any business which uses, in any manner, any Protected Technology.

3.7 Availability of Injunctive Relief: Given the nature of DATUM's business,

GMT/GLASSEY/MCNEIL's involvement in DATUM's business and in the formulation and implementation of its business plans and strategies relating to the Protected Technology, and GMT/GLASSEY/MCNEIL's direct involvement with DATUM clients, GMT/GLASSEY/MCNEIL acknowledge and agree that the covenants of GMT/GLASSEY/MCNEIL and the restrictions on GMT/GLASSEY/MCNEIL contained in this Agreement are reasonable and necessary in order to protect the legitimate interests of DATUM, and that any violation thereof by

GMT/GLASSEY/MCNEIL or any affiliates would result in irreparable injuries to DATUM, for which damages would not, in and of themselves be an adequate remedy. Therefore, GMT/GLASSEY/MCNEIL acknowledge and agree that, in the event of a violation or breach by GMT/GLASSEY/MCNEIL or any affiliates of any of the covenants or any of the restrictions contained in this Agreement, DATUM shall be entitled to obtain, from any court of competent jurisdiction, temporary, preliminary and permanent injunctive relief, in addition to any other rights or remedies to which DATUM may be entitled under applicable law or equitable principles, without the necessity on the part of DATUM of having to post a bond or other security and without thereby limiting any other rights and remedies, including the recovery of monetary damages, that DATUM may have hereunder or under applicable law by reason of such violation or breach.

3.8 Representation of Non-disclosure: GMT/GLASSEY/MCNEIL represent and warrant that they have not disclosed any Protected Technology to any party other than Datum, its employees, agents, representatives.

3.9 Communication with Datum: GMT/GLASSEY/MCNEIL agree to refrain from any contact or communication with DATUM or any affiliated entities, including any officers, employees, former employees, agents, or representatives of DATUM or its affiliated entities. All communication on behalf of GMT/GLASSEY/MCNEIL which is directed at DATUM, its employees, agents or representatives must be directed to DATUM's legal counsel: John F. Cannon, Esq., Stradling, Yocca, Carlson & Rauth, 660 Newport Center Drive, Suite 1600, Newport Beach, California, 92660-6441. Further, all such communications must be made by legal counsel for GMT/GLASSEY/MCNEIL who is designated as follows: Jason Book, Esq., Bosso, Williams, Sachs, Book, Attack & Gallagher, 133 Mission Street, Suite 280, Santa Cruz, California 95061-1822.

3.10 No Communication Regarding Datum: GMT/GLASSEY/MCNEIL agree that they will not discuss any aspect of DATUM, including but not limited to DATUM's business, officers, employees, former employees, representatives, affiliated entities, transactions, or products with any person or entity, other than as expressly contemplated by this Agreement.

3.11 Release of Claims:

3.11.1 GMT/GLASSEY/MCNEIL's Release of Claims Against DATUM: GMT, GLASSEY and MCNEIL, for themselves and for and on behalf of GMT and any affiliated or related entities, assigns and successors in interest, if any, now or in the future, hereby irrevocably release, forgive and discharge DATUM and all of its current and former officers, directors, shareholders, partners, agents, employees, representatives, affiliates, parent, subsidiaries, and related entities, assigns and successors in interest, if any, now or in the future (collectively, the "DATUM Parties"), from any and all claims, demands, contracts, causes of action, obligations, debts, liabilities of any kind or nature whatsoever, whether known or unknown, which they now have or may have in the future, against the DATUM Parties. This release expressly includes any claims for which DATUM would bear an obligation of indemnity, pursuant to contract statute or otherwise to the person against whom GMT/GLASSEY/MCNEIL would have a claim. This release may be asserted by any of the Datum Parties and shall be a complete defense to any claim for which Datum would bear an indemnity obligation. Notwithstanding the foregoing, DATUM's obligations under this Agreement are expressly excepted from the foregoing release.

3.11.2 DATUM's Release of Claims Against GMT/GLASSEY/MCNEIL: DATUM agrees and acknowledges that DATUM on behalf of itself and any affiliated or related entities, assigns and successors in interest, if any, hereby irrevocably releases, forgives and discharges GMT/GLASSEY/MCNEIL and all of its officers, directors, shareholders, partners, agents, employees, representatives, affiliates, parents, subsidiaries, and related entities, assigns and successors in interest, if any, now or in the future (collectively, the "GMT Parties"), from any and all claims, demands, contracts, causes of action, obligations, debts, liabilities of any kind or nature whatsoever, whether known or unknown, which they now have or may have in the future, including those claims stated in the COMPLAINT, against the GMT Parties. This release expressly includes any claims for which GMT/GLASSEY/MCNEIL would bear an obligation of indemnity because such claim arose during and out of GMT/GLASSEY/MCNEIL's employment of the person against whom DATUM would have a claim. Notwithstanding the foregoing, GMT/GLASSEY/MCNEIL's obligations under this Agreement are expressly excepted from the foregoing release.

3.12 Civil Code Section 1542: With respect to the matters herein stated as the subject of release, the parties hereto do hereby mutually waive and relinquish any and all rights which any of

them may have under the provisions of Section 1542 of the Civil Code of the State of California, which Section reads as follows:

"A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR."

3.13 Settlement of Claims Against DATUM: GMT/GLASSEY/MCNEIL agree and acknowledge that, upon performance of this Agreement, DATUM shall have no further obligations under any consulting agreements, non-disclosure agreements, value added reseller agreements or any other agreement with GMT/GLASSEY/MCNEIL and that GMT/GLASSEY/MCNEIL waive any claims or causes of action any of them may have against DATUM arising out of such agreements, including, but not limited to, claims for damages and claims for the return of any intellectual properties allegedly disclosed to DATUM by GMT/GLASSEY/MCNEIL.

3.14 Attorney's Fees: DATUM and GMT/GLASSEY/MCNEIL shall bear their own costs and attorneys' fees in connection with their respective disputes and claims settled herein.

3.15 Termination of Payment Obligation and Survival of Non-Payment Terms: The parties agree and acknowledge that DATUM's royalty payment obligations terminate after the royalty payment derived from the third year of the royalty. Notwithstanding the foregoing, all other terms of this Agreement will remain in full force and effect after termination of DATUM's payment obligations.

SECTION FOUR

WARRANTIES AND REPRESENTATIONS

4.1 The parties hereto warrant and represent that no promise or inducement has been offered or made for this Agreement except as herein set forth, that this Agreement is executed without reliance on any statements or any representations not contained herein, and that this

Agreement reflects the entire settlement among the parties. The attorneys of record warrant and represent that they are satisfied that their respective clients fully understand the effect, significance and consequence of this Agreement. The terms, acknowledgments, warranties and representations made herein shall survive the execution and delivery of this Agreement, and shall be binding upon the respective heirs, representatives, and assigns and successors of each of the parties and their attorneys.

SECTION FIVE

NO ADMISSION OF LIABILITY

5.1 The parties hereto acknowledge and agree that this Agreement is entered into as a mutual compromise and settlement which is not in any respect or for any purpose to be deemed or construed as an admission or concession of any liability whatsoever on the part of any of the parties hereto.

SECTION SIX

CONFIDENTIALITY

6.1 The parties agree that this Agreement and its terms are confidential. The parties further agree that the confidentiality of this Agreement and its terms is a material term of this Agreement without which the parties would not have consented to the Agreement. The parties expressly agree that they will not disclose or discuss the terms of this Agreement with any person. GMT/GLASSEY/MCNEIL shall notify DATUM's legal counsel, in writing, of the receipt of any request for the disclosure of any confidential information. GMT/GLASSEY/MCNEIL shall cooperate with the efforts of DATUM to quash such subpoena or other legal process or to obtain a protective order, as DATUM deems appropriate. The parties shall have the right to provide required information concerning this Agreement to investors and potential investors, and to Affiliates in order to enable them to carry out the activities contemplated hereunder and in connection with strategic business needs. Any such disclosure shall be pursuant to a separate agreement of confidentiality between DATUM or GMT/GLASSEY/MCNEIL and any such third parties.

6.2 The parties further agree to maintain the confidentiality of any document or information which has been or is designated as confidential, including Protected Technology.

SECTION SEVEN

ENFORCEMENT OF AGREEMENT

7.1 If any legal action or other proceeding is brought for the enforcement of this Agreement, or because of an alleged dispute, breach, default, or misrepresentation arising out of or relating to any of the provisions of this Agreement, the successful or prevailing party or parties shall be entitled to recover reasonable attorneys' fees and other costs incurred in that action or proceeding, in addition to any other relief to which it or they may be entitled.

SECTION EIGHT
MISCELLANEOUS

8.1 This Agreement is subject to, governed by, and shall be construed in accordance with the laws of the State of California.

8.2 GMT/ GLASSEY/MCNEIL represent and warrant that they are the sole and rightful owners of the claims asserted in the dispute described in this Agreement and that any such claims have not been assigned or transferred to any unnamed party. DATUM represents and warrants that it is the sole and rightful owner of the claims asserted in the COMPLAINT and otherwise herein and that any such claims have not been assigned or transferred to any unnamed party.

8.3 This Agreement is enforceable and binding upon the parties hereto, their successors and assigns, and any agents or others under the control or direction of the parties. Moreover, both parties, as well as the signatories, hereby warrant and covenant that their respective representative signing this Agreement has full authority to bind the parties to the terms of this Agreement.

8.4 The parties may assign all rights and delegate all duties hereunder to an entity acquiring that portion of each parties' business to which this Agreement relates, or to any corporate successor by way of merger or consolidation, provided that the assignee delivers to DATUM or GMT/GLASSEY/MCNEIL, as appropriate, a statement that the assignee assumes the assigning party's obligations hereunder. GMT/GLASSEY/MCNEIL may assign its right to receive the royalty payments provided in paragraph 3.2 to any person or entity provided that DATUM receives notice in writing of such assignment signed by GMT, GLASSEY and MCNEIL.

8.5 This Agreement constitutes and contains the entire understanding and agreement of the parties and cancels and supersedes any and all prior negotiations, correspondence and understandings and agreements, whether verbal or written, between the parties respecting the subject matter hereof. No waiver, modification or amendment of any provision of this Agreement shall be valid or effective unless made in writing and signed by a duly authorized officer of each of the parties.

8.6 The provisions of this Agreement are severable, and if one or more provisions should be determined to be judicially unenforceable, in whole or in part, the remaining provisions shall nevertheless be binding and enforceable. The provisions of this Agreement shall be construed as separate provisions covering their subject matter in each of the separate counties and states in the United States in which DATUM transacts its business; to the extent that any provision shall be judicially unenforceable in any one or more of those counties or states, that provision shall not be affected with respect to each other county or state, each provision with respect to each county and state being construed as severable and independent.

8.7 The parties agree to take any acts, and execute any further documents, that may be reasonably necessary to accomplish and effect the terms of this Agreement.

8.8 This Agreement may be executed in counterparts and by fax, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, this Agreement has been executed by the undersigned on the dates below indicated.

Dated: November 19, 1999


TODD GLASSEY

Dated: November 19, 1999


MICHAEL MCNEIL

Dated: November 17, 1999


GLASSEY MCNEIL TECHNOLOGIES

Dated: November __, 1999

DATUM, INC.

APPROVED AS TO FORM AND CONTENT:

8.6 The provisions of this Agreement are severable, and if one or more provisions should be determined to be judicially unenforceable, in whole or in part, the remaining provisions shall nevertheless be binding and enforceable. The provisions of this Agreement shall be construed as separate provisions covering their subject matter in each of the separate counties and states in the United States in which DATUM transacts its business; to the extent that any provision shall be judicially unenforceable in any one or more of those counties or states, that provision shall not be affected with respect to each other county or state, each provision with respect to each county and state being construed as severable and independent.

8.7 The parties agree to take any acts, and execute any further documents, that may be reasonably necessary to accomplish and effect the terms of this Agreement.


8.8 This Agreement may be executed in counterparts and by fax, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, this Agreement has been executed by the undersigned on the dates below indicated.

Dated: November 19, 1999


TODD GLASSEY

Dated: November 19, 1999


MICHAEL MCNEIL

Dated: November 17, 1999


GLASSEY MCNEIL TECHNOLOGIES

Dated: November 29, 1999

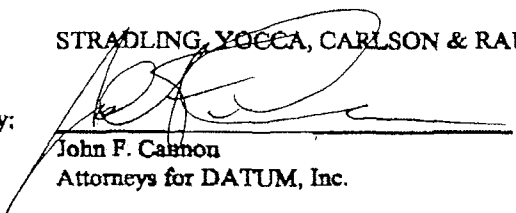

DATUM, INC.

APPROVED AS TO FORM AND CONTENT:

Dated: November ____, 1999

By:

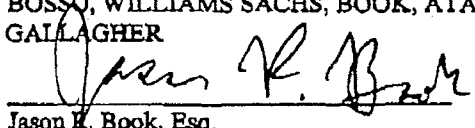
STRADLING, YOECCA, CARLSON & RAUTH


John F. Cannon
Attorneys for DATUM, Inc.

Dated: November 9, 1999

By:

BOSSO, WILLIAMS SACHS, BOOK, ATACK &
GALLAGHER


Jason K. Book, Esq.
Attorneys for Glassey-McNeil Technologies, Inc.
Todd Glassey, and Michael McNeil.

package pickup
age online - Gc

SS FIRMLY



UNITED STATES POSTAL SERVICE®		Click-N-Ship®	
P	usps.com 9405 5036 9930 0365 1573 49 0052 5000 0002;0005		
	\$5.25		
	US POSTAGE Legal Flat Rt Env		
	08/28/14	Commercial Base Pricing	Mailed from 95031 062S0000001311
PRIORITY MAIL 2-DAY™			
TODD S GLASSEY PATENT RECOVERY CORP PO BOX 1000 LOS GATOS CA 95031-1000		Expected Delivery Date: 08/30/2014 0006	
		C030	
SHIP TO: INTERNET SOCIETY C/O CORPORATION SERVICE COMPANY 1090 VERMONT AVE NW WASHINGTON DC 20005-4905			
USPS TRACKING #			
9405 5036 9930 0365 1573 49			
Electronic Rate Approved #038555749			

SE PRESS FIRMLY



POSTAGE REQUIRED.