Todd S. Glassey, In Pro Se
305 McGaffigan Mill Road
Boulder Creek, CA. 95006
(408) 890-7321
tglassey@earthlink.net

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

Microsemi Inc, US Government, et Al;, Appellee, vs. Todd S. Glassey, In Pro Se, and , Michael E. McNeil, In Pro Se, Appellants	Case No.: No. 14-17574 On Appeal from the US District Court, San Francisco, CA, CASE 14-CV-03629, Before his Honor Judge Alsup Notice of Motion and Motion for Limited En Banc Reconsideration of "Motions Dismissed without Hearing" from US_CAND-14-CV-03629_WHA • DOCKET 122 Determination of Fraud Loss Standing for Patent Agent actions • DOCKET 123 Review of |Settlement Document Template, and TTI and DDI Settlements for TALBOT and GELLMAN sufficiency • DOCKET 138 2nd Motion for 3-Judge Panel • DOCKET 139 - Establishment and confirmation of PERFORMANCE RIGHTS under Copyright Standards for PHASE-II Technologies in various systems and Industry Standards; • DOCKET 141 - Review actual Inventorship of US6393126 *(and US6370629)

Notice of Motion and Motion for Limited En Banc Reconsideration of "Motions Dismissed without Hearing" from US_CAND-14-CV-03629_WHA.

1. This is a Motion and Petition for a Limited En Banc Review of just the five (5) Motions which were denied in the District Court matter without review. The Motions and their Docketing is attached here for the convenience of the Appellate Court's review herein.

Review of the Motions

2. We ask that the Appellate Court specifically review them in the following order

1) The Empanelling of a 3-Judge Panel Motion - DOCKET 138;

3. For the first review requested, we ask the Appellate Court to review the dismissal without review of the 3-Judge Empanelling Motions.

4. This motion should have been granted if for no other reason than this matter pertains to both the Patent and Software Copyright Controls on Digital Timestamping which through the US6370629 and subsidiary copyrighted technology specifications published by Appellant Glassey created the proper method under the Mazer v Stein ruling from the Supreme Court to support this.

5. The District Court refused to look at COPYRIGHT CONTROLS which exist both under the Patent Filing and independently; these Copyright Controls protect computer Programs

which use the Appellant/Plaintiff's PHASE-II Location Based Service Technologies without compensation.

6. Simply put, this Intellectual Property control set constrains the operations of automated voting systems of all types in America so it impacts and constrains Apportionment as it is mechanically performed today.

7. Since that is irrefutable in fact, this matter directly impacts both the actual apportionment and the operations of every elected position in the US today and based on the Copyright Act's terminus will until sometime in 2085. As such under various Federal and State Election's Acts and the Fifth Amendment's Takings Clause the Election Results from a Constrained System are directly controlled by the Section 3 and Section 8 Settlement Terms and the full Copyright Control that Appellant's enjoy against that same set of PHASE-II Intellectual Properties when they are used in commercial systems today.

2) Determination of Fraud Loss Standing for Patent Agent actions - DOCKET 122;

8. This motion is to "Confirm that the CO-INVENTOR AGREEMENT is specifically a 'Patent Agent retainer-agreement with a contingency-based payment rider' and that as such HASTINGS when US6370629 stood as Appellant's Patent Agent for the Filing and Administration of US6370629. These losses also pertain to instances of US6370629 filed in Japan, South Korea, Australia, Brazil, Canada, and the EU without any formal releases or authorizing from Appellant's as was done for the South African Filing.

9. All of the instances of US6370639 filed in foreign nations were abandoned making them total enforcement losses for Appellant's and further those abandonment's created what are

subsidiary damages in Appellant's Copyright Protections which were derived from those Patents in those Nations.

In the Case of the Fraudulent (Sherman Act) Transfer of the US6370629 Patent to Datum

10. That any subsequent standing they have after HASTINGS sold Appellant's patent to DATUM and then himself took a job at DATUM constituted a fraud against Appellant's property and the services they were contracting with HASTINGS for, and as such the "Settlement for the DDI Patent provides Appellant's less control and less value than they would have had, if HASTINGS conversion of their Property illegally had never happened.

3) Review of |Settlement Document Template, and TTI and DDI Settlements for TALBOT and GELLMAN sufficiency - Docket 123

11. Appellant have asked the District Court for a formal review of the terms and conditions included in the two Settlement Agreements for a clarification of certain processes; also to make a determination as to whether the Informational-Notice and Area-of-Responsibility for the Enforcement and Defense of PHASE-II IP inside the US6370629 Patent was denied without any review. We seek that Review as the Trial Court erred in its dismissal

Talbot/Gellman Sufficiency

12. Appellants sought a formal review of the actual terms in the DDI Settlement Contract *(the Contract for US6370629) and the fact that Datum and later its successor Symmetricom withheld the executed copy of that contract from the Date of its Signing in

1999 until they delivered the first executed copy to Appellant/Plaintiffs on 2-26-2013. In the interim they (Datum and its Successors) denied through their Law Firm Lathem Watkins and their Counsel Peter Chen that said Settlement existed. That there was no settlement and that they and only they owned PHASE-II IP. Appellant's sought review of that pretty obvious fraud on Datum and its successors parts.

Under the Talbot/Gellman Question: Does the DDI (*and TTI) Settlement Agreement Template meet the minimum necessary standard for a shared Intellectual Property Transfer and Sublicensing per Talbot and Gellman Standards?

13. The Terms of the Contract are permanent per section 3 and there are specific requirements for adding "the missing pieces of that contract" per section 8.7 of the contract which TALBOT requires. For instance if someone sues Microsemi over US6370629's use of PHASE-II IP who is responsible for that litigation? How for instance is an infringement which is informed to APPELLANT/PLAINTIFF'S served on Microsemi? How are Copyright-Infringement's against Software Programs using the Protected Intellectual Properties licensed to Microsemi addressed? The Settlement has a number of voids in it which Appellant/Plaintiff's believe render it void as well or at least so incomplete as to be unenforceable in form. It is a review of that the Appellant/Plaintiff's sought from the District Court and which they were summarily denied without cause.

14. Further in our original Motion to the District Court we raised the proper question as that under Gellman is there anything in either agreement which "allows the filing of a Patent in any nation without a formal release against the filing of said patent application?"

*4) Review actual Inventorship of US6393126 *(and US6370629)*

15. Appellant have asked the District Court for a formal review of Appellant's being the actual inventor's of the Trusted Timing Infrastructure ("TTI") which a subset of (3 of 32 components in the larger technology suite) were licensed to DATUM for use along with the actual Term of Art "TTI" itself;

16. As the parties licensing the use of the Term and Technology used in the US6393126 Patent to the parties who filed said patent application claiming themselves to be the sole inventors of the Trusted Timing Infrastructure; this review is both simple, timely and warranted.

17. As such we sought review of the actual TTI inventorship and correction of the named inventors to US6393126 and its foreign filings. Also for the USPTO to notice that "No Patent Application Releases were signed for this technology filing nor will they be without a release payment for the use of that technology

18. Since that technology happens to control the NSA's PRISM system the US DOJ has a problem in they just impacted the integrity of every PRISM Data Request filed by the FBI in this, the Land of the Free and the Home of the Brave.

5) Establishment and confirmation of PERFORMANCE RIGHTS under Copyright Standards for PHASE-II Technologies in various systems and Industry Standards;

19. Appellant have asked the District Court for a formal review of Appellant's standing to enforce their Derivative Copyrights against the IETF and other parties placing their PHASE-II IP inside of their Computer Programs without compensating Appellant/Plaintiffs for the use of their PHASE-II IP.

20. The Appellant/Plaintiffs asked the District Court to review their standing both under a Derivative Copyright Claim and through a Natural Copyright Claim for publications submitted containing PHASE-II IP to a Copyright Protected IP stream.

21. Appellants raised the following questions

22. **Q1:** Does protected material which is included in a subsequent protected Intellectual Property obtain the Co-Copyright Standing. I.e. if pieces of another Computer Program are included in another Program which is protected by the Authors copyright, what happens to the enforcement rights of the Original Code-Snippet Owner?

23. And as an aspect of this larger question, does a Patent IP Owner's IP get instant Copyright Protection when it is included in Copyright Protected Computer Programs? or is there another step necessary like the filing of a specific Copyright Protection Statement or other effort necessary to obtain this standing?

24. **Q2:** Does the publication of a copyright protected statement inside the mailing lists of a Standards Organization constitute proper notice to the Industry or not?

25. and again, as an aspect of that, answering that "If the US Government (both DoJ and DoC are parties to those mailings and members of that organization) does this also constitute Government Standing behind that Standards Agency Action?"

26. **Q3:** Finally what are Appellant's enforcement rights against their copyright protected IP which is Patent Protected as well.

Relief Requested

27. These five Motions can be reviewed and Appellant's believe their claims are all properly grantable. We therefore ask for review of the individual motions in the order requested; and that in reviewing these motions en banc that the Appellate Court grant relief in the form of granting the motion as it was originally submitted.

28. We also find however that in these motions that we believe that a finding of flaw in any one of them is grounds for voiding the Dismissal with Prejudice and returning this matter to the District Court;

Dated this Monday, May 04, 2015

/s/ Todd S. Glassey

Todd S. Glassey, In Pro Se
305 McGaffigan Mill Road
Boulder Creek, CA. 95006
(408) 890-7321
tglassey@earthlink.net

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

Michael E McNeil In Pro Se
Michael E McNeil In Pro Se
PO Box 640
Felton CA, 95018-0640
831-246-0998
memcneil@juno.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

TODD S. GLASSEY, In Pro Se

And

MICHAEL E. MCNEIL, In Pro Se

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

2nd MOTION FOR THE EMPANELING OF A THREE JUDGE PANEL

Judge: His Honor, Judge ALSUP
Where: Court Room 8, 19th Fl
When: January 15th, 8AM, 2015

I. <u>NOTICE OF MOTION</u>

1. On January 15th at 8 AM (after the Planned CMC Conference) Plaintiffs based on the 2281 through 2284 issues in the State's GIS and IT Infrastructure used to manage the actual Apportionment of Congressional and Judicial Districts of the State Court System, will move the Court for the

empanelling of a three judge panel in this matter based these issues in both the State of California and pertaining to the Constitutional Standing of FISA and the AG's ability to decline a prosecution for TRIPS and PCT violations as described in the Second Amended Complaint.

2. This Motion is made up of this Notice of Motion and Motion, Attached and referenced Exhibits, Declarations and testimony to be given at the time of the Hearing.

II. 2ND MOTION FOR THREE JUDGE PANEL

3. May it please the Court, with the Filing of the Second Amended Complaint, the Plaintiffs cured the failings of the First Motion for a Three Judge Panel by properly identifying the key questions of Constitutional Law, State Apportionment issues pertaining to GIS and Infrastructure which Plaintiffs claim in the Second Amended Complaint is a Constitutional Violation.
4. We therefore after the Second Amended Complaint was filed resubmit the motion for the Assignment of a Three Judge Panel per 28 USC 2284.

CASES

STATUTES

MEMORANDUM OF POINTS AND AUTHORITIES

I. Plaintiffs request a Three Judge Panel because of a confluence of enabling factors which make this case perfect for the application of a three-judge review.

5. Three Judge Panels were a mechanism added to the review process to enable the control of a Single Federal Judge being able to hog-tie a State; So matters asking for Injunctive relief against a State were generally granted this standing in deference to honoring the separation of Federal and States' rights. The Kessler Test and its successor precedents indicate there is a long history on further tightening the constraints which a Three Judge Panel is required (or even desirable) for.

6. Plaintiffs state that this is a very important factor in this case because Plaintiffs have accused California of wholesale creation of a new set of Intellectual Property enforcement precedents, that it has apparently made deals with the Nation of China in the form of Joint Economic Agreements as well, and considering this patent they refuse to enforce not only controls apportionment but

everything relying on computer networking in the State, this case is ripe for the application of the Three Judge Panel even with the added costs and complexity this brings to a Case.

II. This case focuses on three key questions of constitutional law

7. The Three points of Constitutional Law are

   a. 1) Can FISA be used in a Civil Case Matter to functionally stop the litigation by making it impossible for Attorneys to represent their Clients once served by this type of instrument (as Alleged in this Case); A purely Constitutional Law issue;

   b. 2) Does the Congressional Standing in the TRIPS, PCT and WTO agreements eliminate the prosecutorial discretion of the US and California State Attorneys General with regard to the Patent Frauds happening both in the US and in foreign Nations tied to US parties; and

   c. 3) Does the inclusion of a PATENT (Title 35) PROTECED SOFTWARE SYSTEM in a SOFTWARE PROGRAM which is Copyright Protected create a PERFORMANCE RIGHT under the Copyright Code (Title 17) for that Program?? And if so who owns it? The Patent IP Owner?

III. States Rights, Apportionment, and Commerce vs Supremacy Claus conflict

8. Finally with the State of California as a party to this matter and we are seeking permanent Injunctive relief against it for its Unconstitutional refusal to enforce US Patent Law and its own Patent Related precedents in the apportionment of the State's Voting, Judicial, Power and Sewage Districts through GIS (the Graphic Information Services);

9. Plaintiffs assert that the State of California cannot properly operate any of its Elections Controls Equipment including its Districting and Census services without committing a Sherman Act (ss2) as well as Clayton Act (ss4) Violations. As such it cannot provide apportionment for its Congressional

Districts based on the Constitutional Questions raised in this Patent Infringement and Antitrust Action at the Federal Level.

10. As such it is appropriate under both 28 USC 2281 (1970) and 2284 to order the empanelling of a Three Judge Panel[1]; The constitutional matter threshold is met in the three points listed above and it totally supported by Bailey v Patterson (39 US 31 (1962)) as both Substantial and certainly not a fictitious issue, there are clearly seven abandoned instances of US6370629 to contend with regard to those actions and the damages those caused Plaintiffs.

11. Summarizing: Plaintiffs assert this matter fully passes the old Kessler Test because it pertains to "a sole (set) of immediate Constitutional Questions without any need for Statutory Review" but also the extended standard set in Swift and Co v Wickham 382 US 111 86 S. Ct. 258 (meeting Buder[2]-Bransford) and as such, because of the unique type of matter and all of the US Government's reliance on infringing equipment and systems for its daily operations, this matter deserves absolute transparency at each step of its path through the US Judicial Framework,

[1] See Idlewild Bon Boyage Liquor Corp. v. Rohan. 289 F.2d 426 (1961), see also Bon Voyage Liquor Corp. v. Epstein, 370 U.S. 713 (1962); Schack-man v. Arnebergh, 387 U.S. 427 (1967)

[2] Ex parte Buder, 271 U.S. 461, 46 S.Ct. 557, 70 L.Ed. 1036,

IV. In closing

12. Plaintiffs assert the Empanelment of a Three Judge panel is uniquely warranted because at the State level this is a pure question of whether the State of California has to violate US Law (Patent and Copyright) issues, which it cannot set aside to determine its voting districts, conduct its elections, collect its taxes, pay its debts, operate its power grid, or any number of other functions without continuing to Infringe on Plaintiffs' PHASE-II Technologies both as a set of services it uses internally and as a source of "Tax Revenue from Infringers the State is functionally protecting by its actions", which are thus an unconstitutional setting aside of Plaintiffs' Property and Due.

13. As to how this fits together, while California itself may enjoy its own 11th Amendment Protections, when it itself purchases infringing equipment and services from someone infringing on Plaintiff's PHASE-II Enforcement Rights and who causes their customers to become infringers, the State, in refusing to Prosecute the Underlying Infringement and Inducement to Infringe Fraud became a direct ongoing party to the Fraud.

14. When this loss from the State of California protecting the Infringers turns into hundreds of billions of dollars yearly in the form of both systems and services the State spends money on as well as its then collecting larger amounts of State Income and Sales Taxes from those Parties "the State is actively protecting in their infringement on Plaintiffs' IP", this thereby becomes in effect a paid protection scheme run by the Office of the Governor of the State of California. The US Constitution never anticipated the State of California rewriting US Patent and Antitrust Escape-hatches into the framework of US Law, and should be stopped from this activity.

1. Because US6370629 controls secured Location Based Services it is a key component of the National Commerce Framework

15. Functionally, Plaintiffs' rights in PHASE-II technology control all key components of the computer based Apportionment Practice used in all states, not just California but in any State running a Computer based GIS practice as part of the State Emergency and Mapping Efforts.

16. Plaintiffs finally state that this matter brings into review multiple conflicts in the Commerce and Supremacy Clauses of the Constitution with regard to the State of California and its refusal to enforce both US national Patent Law and its own policies as set in California v Beninsig while continuing to collect Tax and Political Contributions from Companies and their Tech Sector Executives who are infringers on Plaintiffs' PHASE-II IPs.

V. Relief Requested

A. Empanel a Three Judge Panel

17. At the very least to meet Fifth Circuit's Jackson v. Choate 404 F.2d 910 (5th Cir. 1969) standard by which a Three Judge Panel was convened to determine the threshold value issues pertaining to this matter. Plaintiffs assert there are grounds on the State Apportionment issues pertaining to its refusal to enforce Title 35 and other key aspects of Federal Law or acknowledge its actions in taking monies from parties it is blocking prosecutorial claims against.

. eSigned, 11/27/2014

/s/ Todd S. Glassey
Todd S. Glassey, In Pro Se
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

/s/Michael E. McNeil
Michael E McNeil In Pro Se
PO Box 640
Felton CA, 95018-0640
831-246-0998
memcneil@juno.co

VI. ECF FILING DECLARATION

This filing was made on this day from my ECF account and as such was properly served on all parties with the exception of the State of California who still refuses to answer the complaint. The State is as such being mailed a paper-copy for their review.

/s/ Todd S. Glassey, Plaintiff
11/27/2014

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

Michael E. McNeil, In Pro Se
Michael E. McNeil In Pro Se
PO Box 640
Felton CA 95018-0640
831-246-0998
memcneil@juno.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Todd S. Glassey In Pro Se and Michael E. McNeil In Pro Se, Plaintiff, vs. Microsemi, et Al, Defendant	Case No. 14-CV-03629-WHA DECLARATION IN SUPPORT OF 2ND MOTION FOR THREE JUDGE PANEL Judge: His Honor, Judge ALSUP Where: Court Room 8, 19th Fl. When: January 15th, 2015, 8AM

DECLARATION IN SUPPORT MOTION TO QUASH FISA OR RELATED

1. I declare the following under the penalty of perjury of the laws of the United States of America, that the following statements (1-9) are true and correct, and to those things I rely on information and belief, they are also true and correct.
2. This case qualifies for the appointment of a Three Judge Panel and it should be done before any of the other motions already on file and those about to be filed are addressed by the court. The reasons are the matter at hand not only controls the use of Apportionment Controls on the State and Federal Judiciary, it controls the use of GIS data in all

secured applications meaning it controls things which rely on that technology today.

3. Apportionment, specifically the actual mechanisms of how Vote Tabulation, District Census, and Utility/Commerce weightings are all factored into a set of data called GIS models.

4. GIS Systems are based on LOCATION and TIME information, the two key control factors that US6370629 is setup to use. So it is no wonder that so many of today's GIS based systems naturally infringe on US6370629's PHASE-II IP.

5. The same is actually true of many of the components of the practices used in a number of Digital Balloting Stations (including but not limited to the Premier one and the Diebold ATM's it was evolved from as well).

6. Today all of the paper-based processes are so slow they were retied a decade or two ago.

7. In the US today there is no way to use a GIS data model which includes a time and location constraint over a secured network without infringing on Claims 19-32 of the US6370629, aka the PHASE-II IP Components. As such, the Practice of operating these services constitutes a wholesale conversion of Plaintiffs Property Rights and should be stopped.

8. Governments have authority to use private citizens IP for certain limited purposes within the Government. Private Companies do not. Governments also are not allowed (Under property and Treaty with the other Nations) to sell it to third parties or to provide coverage for those third parties infringements in exchange for both Tax Moneys to the Government (State and Federal) pertaining to the Sales of those Technologies without compensating the Plaintiffs under Eminent Domain.

9. I have asked my Government numerous times to prosecuted these alleged frauds, the actual frauds the review of the co-inventor agreement and the DDI settlements first three statements confesses, they generally don't acknowledge anything and they have certainly not contacted me about Victims Assistance or the Loss Implications.

//

eSigned, 11/28/2014

/s/ Todd S. Glassey
Todd S. Glassey, In Pro Se
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

I. ECF FILING DECLARATION

This filing was made on this day from my ECF account and as such was properly served on all parties with the exception of the State of California who still refuses to answer the complaint. The State is as such being mailed a paper-copy for their review.

/s/ Todd S. Glassey, Plaintiff

Dated this 28th day of November, 2014

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

[PROPOSED] ORDER

Appointment of Three Judge Panel

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: December 19th, 8AM

For good cause the Plaintiffs 2nd Motion for the Appointment of a Three Judge Panel is Granted; Case is referred to the Clerk for assignment of the Panel under Ninth Circuit, USDC, and Local Court Policy.

Witness my hand, Judge WH Alsup, ___________________, Dated ________ 2014

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

Michael E McNeil In Pro Se
PO Box 640
Felton CA, 95018-0640
831-246-0998
memcneil@juno.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

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 PLAINTIFFS, vs. Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES Defendants.	Case No.: 14-CV-3629-WHA Date: December 26th 2014 Time: 8 AM Courtroom 8, 19th Fl Judge W.H. Alsup NOTICE OF MOTION FOR EXPIDETED REVIEW AND SUMMARY MOTION FOR PARTIAL SUMMARY JUDGEMENT OF COUNT 1 ACKNOWLEDGING IRC165 FRAUD LOSSES ON SOUTH AFRICAN, JAPANESE, KOREAN, AUSTRALIAN, BRAZILIAN, CANADIAN and EU FILINGS OF US6370629

May it please the Court;

A. Expedited Review under Local Rules

1. May it please the Court, we in this motion are requesting an expedited ruling for Summary Judgment so that this Ruling will have effect in the

2014 Calendar Tax Year and support the existence of said same losses for previous years filings;

B. Notice of Motion and Motion

2. Be advised, on December 26th 2014 at 8AM in Courtroom 8 before his Honor Judge Alsup, Plaintiffs will move for a partial summary judgment acknowledging their IRC165 eligible fraud losses for the loss of access to their PHASE-II IP Enforcement Rights protected under US6370629 seven other and other abandoned foreign patents today;

3. The Motion is composed of this Notice of Motion and Motion, the associated Declarations as well as precedent and any testimony from experts or others at the time of the hearing.

4.

C. This Motion has no impact on Case Schedules or other CMC related matters

1. This motion pertains to a function of acknowledging that someone filed seven patents with PLAINTIFFS NAMES on them and then abandoned them; That however that happened, Plaintiffs would have been able to file those same patents on their own without any other parties names or claims against them if the Microsemi had never purchased Plaintiffs PATENT AGENT and started this continuing offense.

D. Plaintiffs Scope of requested Fraud Losses - Excludes Classified Uses

5. We apologize to the Court for this filing it will clearly cause concerns, but it is critical for PLAINTIFFS and their Calendar 2014 Filings with IRS, that means we acknowledge that our technology is critical to Department of Defense and National Intelligence systems everywhere. We for those reasons are only requesting against NON CLASSIFIED INFRINGEMENTS at this time.

6. In this ruling we seek acknowledgment of enforcement losses for the seven abandoned instances as complete losses and the US instance to date for all

- all NON-CLASSIFIED USES of the PHASE-II Intellectual Properties in the following areas: - *Database Timestamp Triggered transactions*; *Agribusiness Operations*; Software Branding [of Operating System instances for entitlement controls]; and
- Media Delivery Services using our secured data-stream transactions including both on-demand (downloads of porn, cable tv, BitTorrant and eBook) systems; and
- Multicast FX and Unicast FX event control practices [matching and trading engine operations] for LIGHT POOLS in use in the US per SEC and DTCC reporting as well as SAVVIS reporting streams; and
- additionally on most all mobile cellular or pad type device based GPS navigator applications and use of "Location Based Services interfaces across the encrypted MODEM Chips used to connect the Cell Phone to the Cell Tower" and "Cellphone to encrypted network transports delivered across WiFi or WiMax interfaces"; and finally
- "the PCI-DSS Payment Card Model which is owned and licensed by the PCI SSC (www.pcissc.org). PCI-DSS Sections 10.4(A), (B), and (C) with their cryptographic signing mandate forces all Credit Card vendors using Crypto-Enhanced Cards to infringe directly as do entities using Card Capture Terminals and ATM's from virtually all manufacturers, there are none of these devices systems or programs which can run without infringing in one or more direct instances on processes which infringe on CLAIMS 19-32 of US6370629; and

- Additionally most banking transactions done both online over the Internet and with retail banking systems including those with PAYPAL and the other payment processors infringe on claims 19-32 as well.

E. Notice of Motion and Summary Motion

7. May it further please the Court, on December 26th at 8AM in Court Room 8 of the US District Court in San Francisco before his Honor, Judge Wayne Alsup, Plaintiffs will move and seek a Summary Judgment *acknowledging the scope of the Fraud Losses under IRC165 for use in TAX YEAR 2014* in the proceedings herein.

F. The Motion

May it please the Court, as soon as may be reviewed or on December 26th 2014 the PLAINTIFFS seek the Courts acknowledgement of the filings of the seven foreign US6370629 instances so that PLAINTIFFS may take those loses on their CALENDAR 2014 Tax Filings; as such time is of the essence in this ruling.

Plaintiffs have filed evidence instances of unconformed but easily confirmed full copies of each of the seven patent instances (filed again with this motion for completeness). The US Patent from which they were filed is also included as the proof of US Government publication of the original instance.

As such Plaintiffs move the court to summarily issue a Judgment that all seven instances of the US6370629 patent are total losses to date. And that PLAINTIFFS have suffered some financial loss yet to be determined for each of them in each jurisdiction;

TABLE OF CONTENTS

MEMORANDUM OF POINTS AND AUTHORITIES

A. Plaintiffs Fraud Losses stands alone from any other claims

8. Without ruling on any other merits of the PLAINTIFFS claims, there are clearly seven abandoned instances of US6360629 filed that PLAINTIFFS have through the process of the Settlement extortion and Microsemi's continuing offense have been deprived of their rightful access to enforce against.

9. Plaintiffs are the uncontested owners and sole creators of what is called PHASE-II IP. Since US6370629 is all PHASE-II IP Plaintiffs assert that it is the Patent they would have been able to file without the actions Microsemi did behind closed doors to prevent Plaintiffs recovery or use of their IP over the last decade. The fact that there are formally unauthorized filings which were intentionally abandoned documents the mechanics of the frauds perfectly.

10. As such the losses for the areas of identified infringements are reasonable as is adding more loss for newly discovered and documented infringements in the future against things which infringed.

B. Fraud Loss is Fraud Loss - and FISA doesn't change that

11. Because the Plaintiffs are entitled to (irrelevant of whether Classified by FISA or some other instrument like PD12333) to file those losses under the IRC165 provisions, especially the 2009/09 "Madoff Extensions for victims of unprosecuted frauds" the Court should grant and order this loss acknowledged.

12. Plaintiffs have fully complied with all legal requirements, notified IRS, Treasury, SEC, FBI, California State AG, USAA Antitrust Team, Customs over unlawful importation of tech systems violating the TTI Settlement and DDI settlements, State of California AG's office Bob Morgester SAAG; the County of Santa Cruz DA's office, Bill Atkins ADA

so all requirements for taking a formal fraud loss against an UNPROSECUTED FRAUD have been fully met by PLAINTIFFS.

C. Plaintiffs are entitled to all Non-Classified Fraud Losses they can document for all Patent Jurisdictions for their PHASE-II Enforcement Rights

13. The PLAINTIFFS are entitled to the difference under IRC165 of anything they could have licensed their IP for relative to what they have been allowed to license their IP for (nothing to date).

14. As such for these non-classified uses of the IP the PLAINTIFFS are entitled for full write-down losses under IRC165 for this fraud loss based on the simple legal precedent that if the Plaintiffs had filed those on their own instead of hiring HASTINGS and MICROSEMI they would own all rights to those patents outright and be the only party licensing any parts of it. This litigation would never had happened; and enforcement would have started 12 years ago meaning there would be no brutal realization today that a single US Patent controls a number of key commerce-centric applications.

15. Because of this, the PLAINTIFFS seek a ruling from this the Court that they are as such entailed to the Physical Damage Amount that they can document infringements for based on a set of proposed loss models.

II. The Patents (Exhibits)

A. US 992 Patent

As a historical basis the 992 patent as extracted from the USPTO website is included as a reference point here.

B. EPO report from 11-16-2014

16. The attached Exhibits from the following PATENT AGENCIES (WIPO, EPO, South African, Japanese, Brazilian, Korean, Canadian, US and IP Australia) showing printouts for each of the following FOREIGN FILINGS of US6370629 – JAPAN, SOUTH AFRICA, REPUBLIC OF SOUTH KOREA, AUSTRALIA, CANADA, BRAZIL, THE EU AND THE US6370629 MASTER PATENT INSTANCE taken from the following hyperlink:

http://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=0&ND=5&at=8&locale=en_EP&FT=D&CC=AU&NR=5401599A&KC=A

1. Verifiable as "Government Agency Representations across an Internet Channel" from a Court Evidence Perspective (Sedona and Paul Grimm Evidence Standards)

17. All EPO IMAGES of PATENT FRONT PAGES are available for Court Verification at the following URLS. These are included here with the attached images to allow the Court to meet the EASILY VERIFIED AS A STATEMENT FROM ANOTHER GOVERNMENT AGENCY requirement herein.

III. US6370629 Foreign Instances

ALL FOREIGN FILINGS OF US6370629 that we have found to date are abandoned, as late as in 2004 and 2007.

1. URL for EPO Report showing front page (filing information) for Australian US6370629 Patent instance

http://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=0&ND=5&at=8&locale=en_EP&FT=D&CC=AU&NR=5401599A&KC=A

2. URL for EPO Report showing front page (filing information) for South Korean US6370629 instance

http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20000626&DB=EPODOC&locale=en_EP&CC=KR&NR=20000035093A&KC=A&ND=6

3. URL for EPO Report showing front page (filing information) for Japanese US6370629 instance

http://worldwide.espacenet.com/publicationDetails/originalDocument;jsessionid=69D78C7A856FC5D37E1114C3703304A5.espacenet_levelx_prod_1?FT=D&date=20000616&DB=EPODOC&locale=en_EP&CC=JP&NR=2000163379A&KC=A&ND=6

4. URL for EPO Report showing front page (filing information) for the Canadian 6370629 instance

http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20000429&DB=EPODOC&locale=en_EP&CC=CA&NR=2287596A1&KC=A1&ND=6

5. URL for EPO Report showing front page (filing information) for EU US6370629 instance

http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20020102&DB=EPODOC&locale=en_EP&CC=EP&NR=0997808A3&KC=A3&ND=6

6. URL for EPO Report showing front page (filing information) for South African US6370629 instance

http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20000621&DB=EPODOC&locale=en_EP&CC=ZA&NR=9906799A&KC=A&ND=6

7. URL for EPO Report showing front page (filing information) for Brazilian US6370629 instance

http://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20001219&DB=EPODOC&locale=en_EP&CC=BR&NR=9904979A&KC=A&ND=6

B. MICROSEMI Contracts Exhibits (Co-Inventor Agreement, DDI Settlement, TTI Settlement)

18. Attached are the CO-INVENTOR Agreement and the two Settlements currently being moved as void under the Talbot precedent.

C. MICROSEMI 992 and 629 Patent Exhibits

19. Attached is the original 992 Patent and the 629 Patent's conformed copy

IV. Foreign IP Websites operated by Governments which corroborate the EPO statements of the jurisdictions Filed in.

A. CANADIAN GOVERNMENT IP WEBSITE FILING

20. The following example website operated by a Foreign Government (Canadian) shows an instance of US6370629 natively filed in that Jurisdiction and corroborates the Information provided from the EPO Website PLAINTIFFS are asking the Court to take Judicial Notice of. As such this supports the request fully.

http://brevets-patents.ic.gc.ca/opic-cipo/cpd/eng/patent/2287596/summary.html?query=2287596&start=1&num=50&type=basic_search

B. SOUTH AFRICAN GOVERNMENT IP WEBSITE FILING

21. As another example the following website operated by a Foreign Government (South African) shows an instance of US6370629 natively filed in that Jurisdiction and corroborates the Information provided from the EPO Website PLAINTIFFS are asking the Court to take Judicial Notice of. As such this supports the request fully.

URL = http://patentsearch.cipc.co.za/patents/patentsearch.aspx?search=basic

SEARCH TERMS = controlling access to stored information

Results show a filing which was abandoned in 2000 for non-payment. Image is included as ZA REPORT here. The same type of thing was done for all of them, filed and then abandoned.

V. Conclusion/Relief Requested

Motion for recognition of the Loss of Enforcement against Australian, Japanese, Korean, South African Brazilian, EU and Canadian instances of US6370629 are total losses to date and while they may be revivable that has not happened and so PLAINTIFFS are entitled to total losses against their enforcement potentials herein for their PHASE-II Technologies components and their licensing potentials as a Market Power under the Sherman (ss-2) and Foreign Antitrust Acts.

A. Proposed FRAND Securities Industry Loss Level

22. Plaintiffs agree Fair and Reasonable ("FRAND") per-event licensing for coming up with Loss Numbers is key here.

23. Plaintiffs proposed Loss Level is ONE MILL PER FX TRANSACTION IN A SECURITIES FRAMEWORK. This is 1/5 to 1/3 the costing the NYSE charges for their implementation of our technology (3 mils to 5 mils per transaction event) without licensing of any type to us and has for the last 8 years or so based on adoption rates for the updated IETF protocols and the underlying products from CISCO, JUNIPER and many others.

24. The same is true of every other LIGHT and DARK POOL FX Stream Operator in the US today and these rights were lost in those nations the Patents were filed in such that PLAINTIFFS are entitled to take that as a fraud loss.

B. Proposed FRAND Media-Download Fee

25. Plaintiffs proposed Loss Level is ONE MILL PER MEDIA FILE Downloaded using the BITTORRANT data protocol in its current uses as of 11/29/2014. The same is set as a FRAND level for operations of CASINOS in the US as well as all online Gaming of all types. One mil per event.

C. Proposed FRAND Gaming Operations Fee

26. In a Casino the following events and systems all infringe on Claims 19-32 of US6370629, the geotagging of an image in the surveillance and tracking systems, its special-persons tracking and other control events (noticing that the AC or Power changed in the logging is an infringement) constitute discrete events. As does every actuation of every gaming device in or electronically attached to the Casino or which are run under any of its licenses. Proposed Loss Level is ONE MIL PER EVENT;

D. Proposed FRAND CABLE TV PROVIDER Use Fee

27. Cable TV providers with their streaming interfaces and on-demand capabilities allow parties to select time-sensitive media files with location controls setup to route them wherever they are needed, whether over a Cell Phone, the Internet, or the Cable System itself, all media delivery types are supported. This workflow has a number of infringing technologies which force per use infringements for damage estimation Proposed Loss Level is ONE MIL PER ON DEMAND SECURED DOWNLOAD PROCESS EVENT; This same loss extends to Porn and eBook Downloads online as well.

E. Proposed FRAND Credit/Payment Card Use Fee

28. In a PCI-DSS standard based Credit and Payment Card transaction processes *(the capture of the card data, the encrypted verification of the card in the data capture station, the sending of the transaction event

token and its info to the server, the server triggering timestamps which then trigger secondary events over encrypted transports to queue payment acknowledgment and accounting events in later batch streams is an infringement in three or more areas of this workflow into IP protected by Claims 19-32 of the US6370629 patent. Proposed Loss Level is ONE MIL PER PCI PROCESS EVENT;

29. We ask the Court to accept these loss numbers or supply ones of its own in granting this motion to recognize Plaintiffs loss of IP enforcement rights to date herein granting status to this loss for use with IRS under Section IRC 165 as a fully harvestable fraud loss complete with permanent carry forward.

.

Dated this 23rd day of November, 2014

/s/ Todd S. Glassey
Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321

/s/ Michael E. McNeil
Michael E. McNeil, In Pro Se
Michael E. McNeil In Pro Se,
PO Box 640
Felton CA 95018
831-246-0998

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

[PROPOSED] **Order Acknowledging IRC 165 Fraud Losses**

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: December 26th, 8AM

For good cause the motion is hereby and Plaintiffs are granted acknowledgment

_______ of their IRC165 Fraud Losses for all filings of US6370629 to date for claims pertaining to any and all infringements against PLAINTIFFS PHASE-II Technologies;

_______Further Plaintiffs Loss Models of ONE MIL PER EVENT TYPE as noticed are also Accepted for use in all related IRC165 filings with IRS pertaining to this or related matters.

Witness my hand, Judge WH Alsup, __________________, Dated ________ 2014

(12) PATENT APPLICATION **(11)** Application No. **AU 199954015 A1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Controlling access to stored information

(51)7 International Patent Classification(s)
G06F 012/14 **G11B 031/00**
G07F 019/00

(21) Application No: **199954015** (22) Application Date: **1999.10.14**

(30) Priority Data

(31)	Number **09182342**	(32)	Date **1998.10.29**	(33)	Country **US**

(43) Publication Date : **2000.05.04**
(43) Publication Journal Date : **2000.05.04**

(71) Applicant(s)
Datum, Inc.

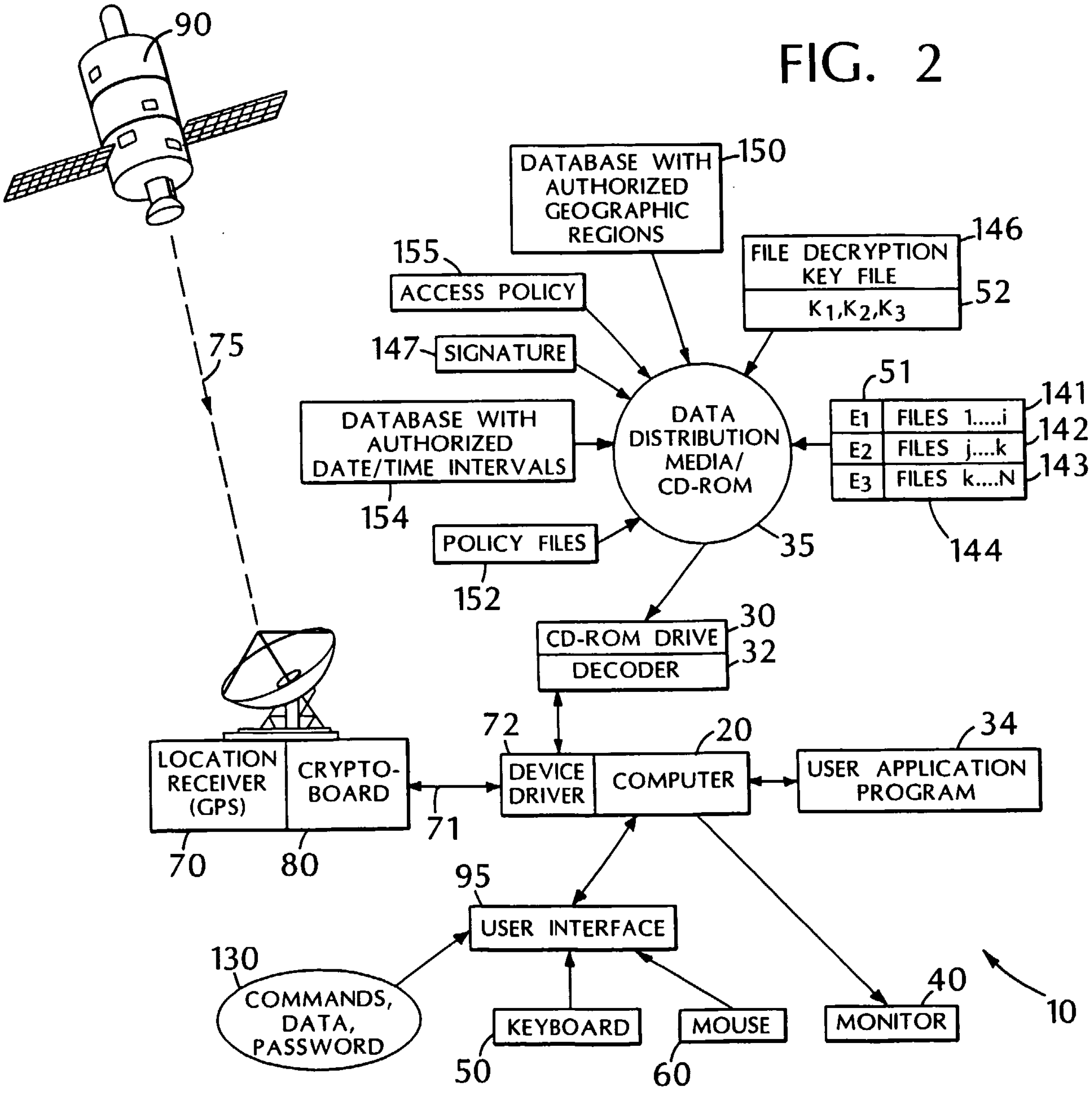
(72) Inventor(s)
Thomas Mark Hastings; Gerald L. Willett; Todd S. Glassey; Michael E. Mcneil

(74) Agent/Attorney
DAVIES COLLISON CAVE,1 Little Collins Street,MELBOURNE VIC 3000

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.

FIG. 2


90
DATABASE WITH AUTHORIZED GEOGRAPHIC REGIONS
150
FILE DECRYPTION KEY FILE
146
K1,K2,K3
52
155
ACCESS POLICY
147
SIGNATURE
75
51
E1
FILES 1.....i
141
E2
FILES j....k
142
E3
FILES k....N
143
DATABASE WITH AUTHORIZED DATE/TIME INTERVALS
DATA DISTRIBUTION MEDIA/ CD-ROM
154
POLICY FILES
35
144
152
CD-ROM DRIVE
30
DECODER
32
72
20
34
LOCATION RECEIVER (GPS)
CRYPTO-BOARD
DEVICE DRIVER
COMPUTER
USER APPLICATION PROGRAM
71
70
80
95
USER INTERFACE
130
COMMANDS, DATA, PASSWORD
KEYBOARD
MOUSE
MONITOR
40
10
50
60

AUSTRALIA

PATENTS ACT 1990

COMPLETE SPECIFICATION

NAME OF APPLICANT(S):

Datum, Inc.

ADDRESS FOR SERVICE:

DAVIES COLLISON CAVE
Patent Attorneys
1 Little Collins Street, Melbourne, 3000.

INVENTION TITLE:

Controlling access to stored information

The following statement is a full description of this invention, including the best method of performing it known to me/us:-

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. 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 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 crytographically 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 differnt sections of information which are applicable to corresponding specific countries and/or regions. A user may be permitted to see only the portion of the information which is applicable to his current geographic location. Likewiese, access to a sensitive corpoarte report may be limited to specific plant location. Access to time-sensitive information may be denied before or after a certain date or limited to a permitted period. By associating information about authorized geographic regions and time intervals with policy files stored on the CD-ROM and accessed with a user password, the CD-ROM producer can issue a new password to permit the user to access a particular set of policy files, and therefore the information authorized, for a corresponding region and date/time.

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

Description

FIG. 1 is a perspective view of a computer system;

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

FIGS. 3 through 5 are flow diagrams;

FIG. 6 is a block diagram of cryptographic elements.

As seen in FIGS. 1 to 3, access to information which is stored on a portable computer-readable CD-ROM which 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 authenication and encrypted data transmission between the receiver 70 and the decoder 32. The computer 20 can then be any commerical 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 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 access, or can be a one-time password. Alternately, the producer can associate specific geographic region/date/time information of lists 150 and 154 with the files 141, 142 and 143 via the policy files 152. A valid user password 130 may unlock one or more policy files 152. If the user's actual geographic position and the current date and time are within the authorized geographic region and the authorized date/time corresponding to the user password 150, then the user can access the selected files via the user interface 95. The selected information is then displayed on output device 40.

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

Table 1

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

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

As seen in FIGS. 4 and 5, to gain access to the signed/encrypted files 144, the user obtains a password 130 (FIG. 2) from the producer (step 400), and enters the password 130 via the keyboard 50 (step 410). The password 130 is assumed to be a one-time password, although user passwords valid for more than one session can also be used.

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.

Throughout this specification and the claims which follow, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

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;

comparing said actual geographic position with 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. The method of claim 1, further comprising:

cryptographically signing said 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 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. 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. 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; 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. The apparatus of claim 12, the receiver further comprising a receiver encryption mechanism providing a receiver encryption key for cryptographically signing the actual geographic position.

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

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

17. The apparatus of claim 16, further comprising a reader encryption mechanism providing a reader encryption key for cryptographically signing the position offset, wherein said position offset signature is verified by the receiver with a corresponding reader

decryption key before the position offset is added to the actual geographic position.

18. 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;

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. 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 which 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. 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;

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. 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 a inertial navigation system.

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

29. A method for controlling access to stored information, or to a subset of files substantially as hereinbefore described with reference to the drawings and/or Examples.

30. Apparatus for controlling access to stored information substantially as hereinbefore described with reference to the drawings and/or Examples.

31. The steps, features, compositions and compounds disclosed herein or referred to or indicated in the specification and/or claims of this application, individually or collectively, and any and all combinations of any two or more of said steps or features.

DATED this FOURTEENTH day of OCTOBER 1999

Datum, Inc.

by DAVIES COLLISON CAVE
Patent Attorneys for the applicant(s)

1/6

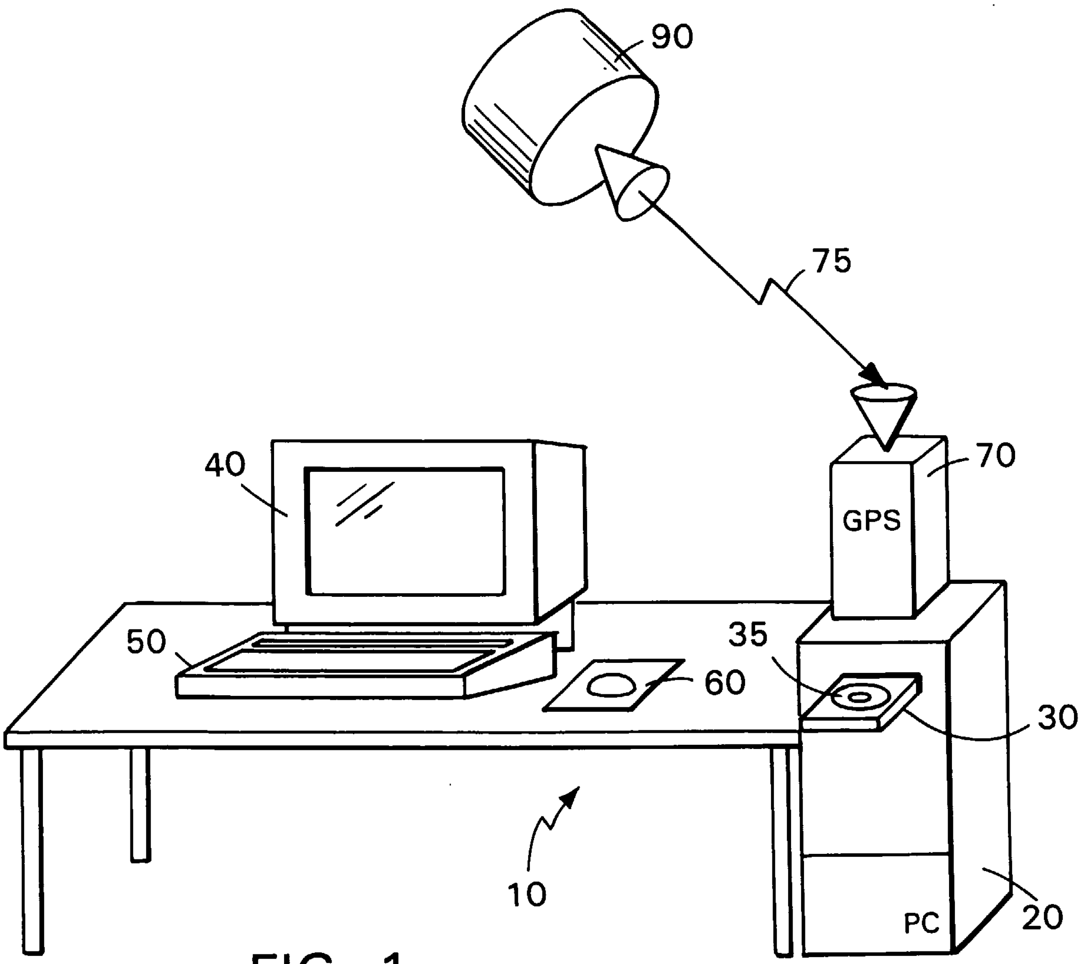
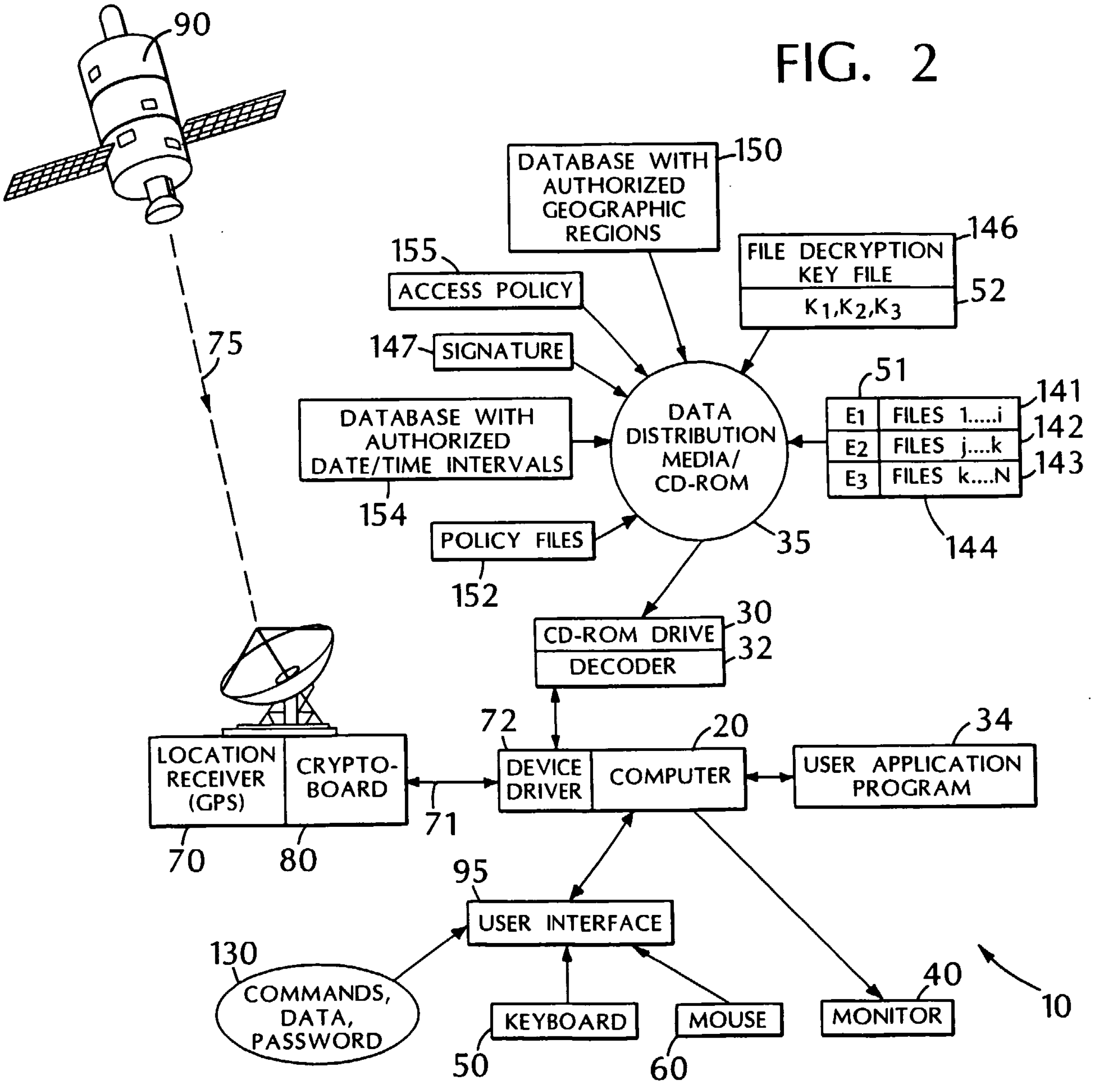


FIG. 1

FIG. 2


90
DATABASE WITH AUTHORIZED GEOGRAPHIC REGIONS
150
FILE DECRYPTION KEY FILE
K1,K2,K3
146
52
155
ACCESS POLICY
147
SIGNATURE
75
DATABASE WITH AUTHORIZED DATE/TIME INTERVALS
154
DATA DISTRIBUTION MEDIA/ CD-ROM
35
51
E1 FILES 1.....i
E2 FILES j....k
E3 FILES k....N
141
142
143
144
POLICY FILES
152
CD-ROM DRIVE
DECODER
30
32
LOCATION RECEIVER (GPS)
CRYPTO-BOARD
70
80
71
72
DEVICE DRIVER
COMPUTER
20
USER APPLICATION PROGRAM
34
95
USER INTERFACE
130
COMMANDS, DATA, PASSWORD
KEYBOARD
MOUSE
MONITOR
50
60
40
10

3/6

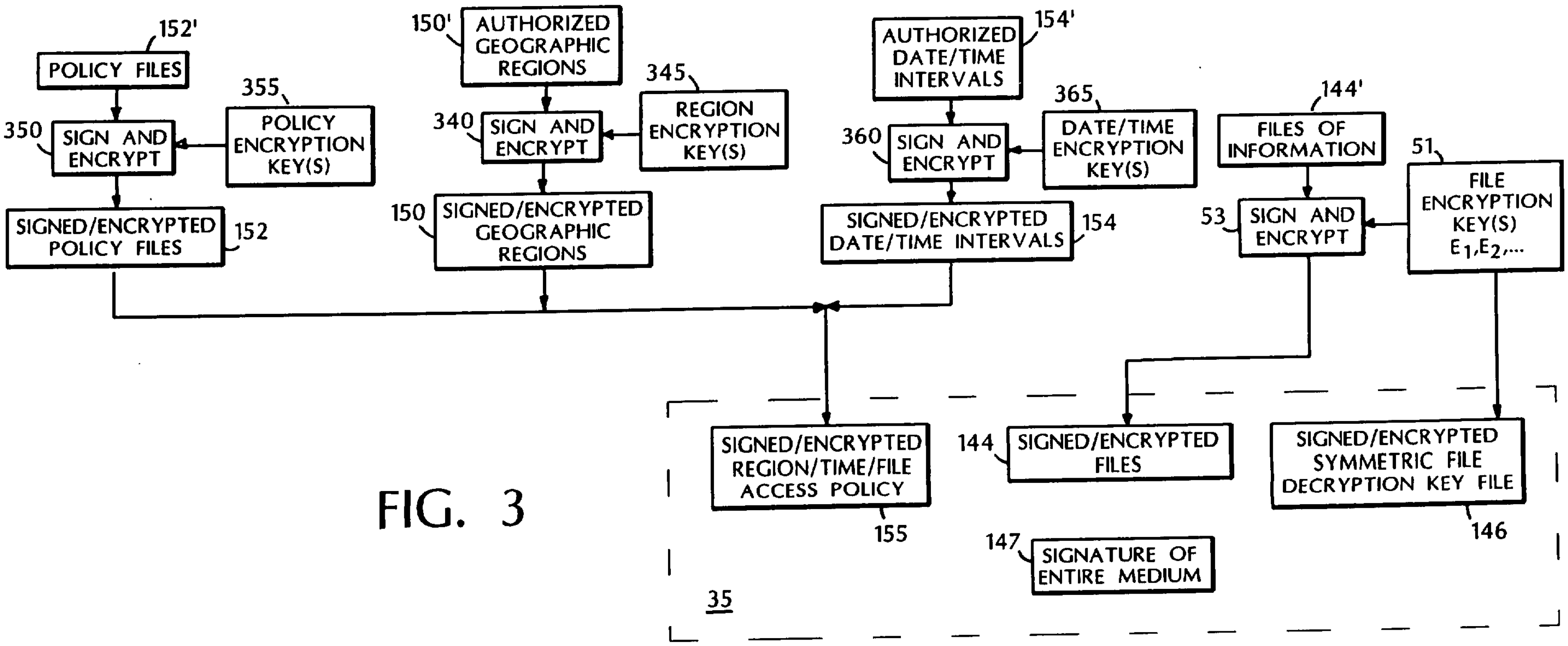
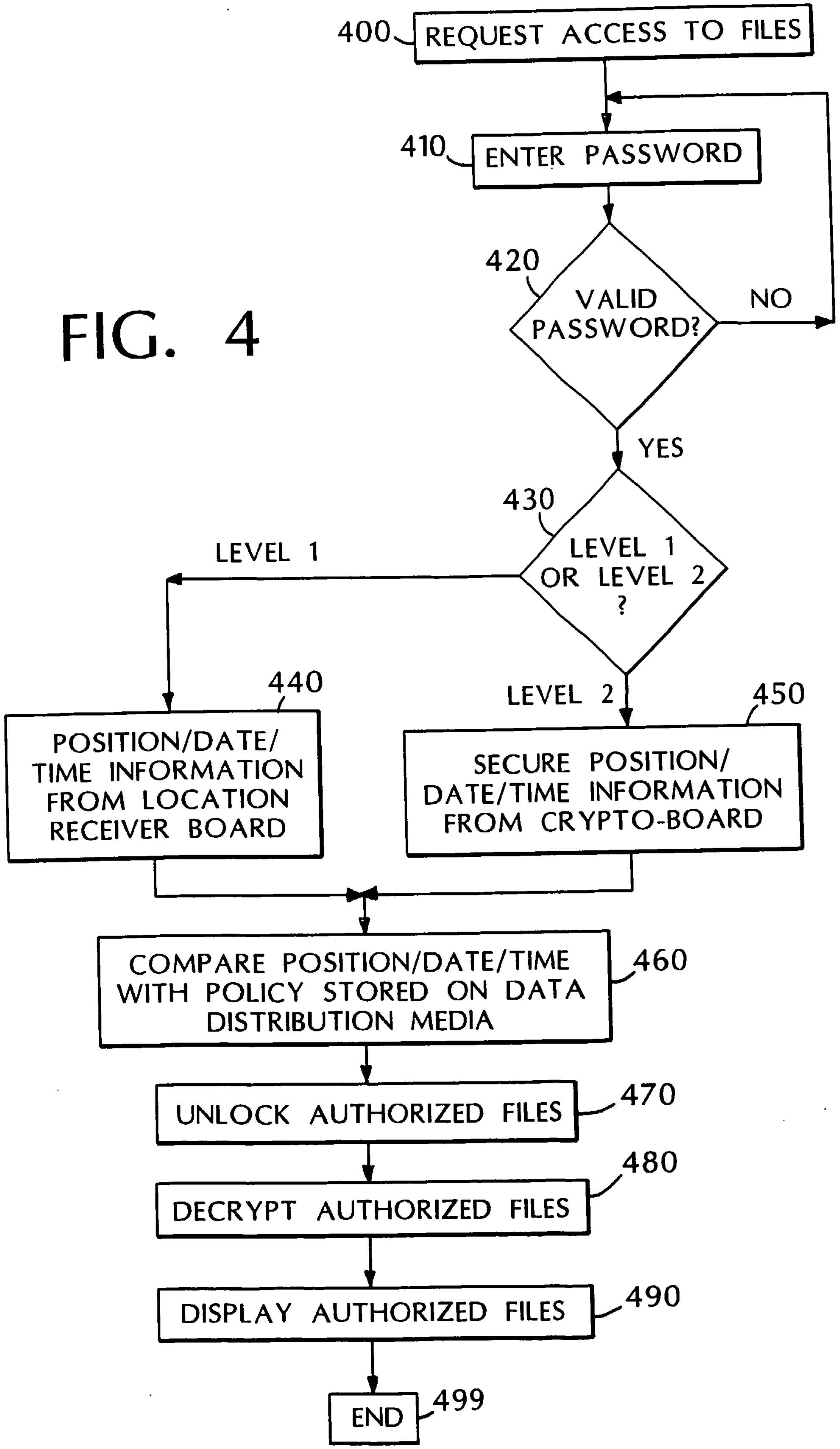

152'
POLICY FILES
350
SIGN AND ENCRYPT
355
POLICY ENCRYPTION KEY(S)
SIGNED/ENCRYPTED POLICY FILES
152
150'
AUTHORIZED GEOGRAPHIC REGIONS
340
SIGN AND ENCRYPT
345
REGION ENCRYPTION KEY(S)
150
SIGNED/ENCRYPTED GEOGRAPHIC REGIONS
AUTHORIZED DATE/TIME INTERVALS
154'
360
SIGN AND ENCRYPT
365
DATE/TIME ENCRYPTION KEY(S)
SIGNED/ENCRYPTED DATE/TIME INTERVALS
154
144'
FILES OF INFORMATION
53
SIGN AND ENCRYPT
51
FILE ENCRYPTION KEY(S) $E_1, E_2, \ldots$
SIGNED/ENCRYPTED REGION/TIME/FILE ACCESS POLICY
155
144
SIGNED/ENCRYPTED FILES
SIGNED/ENCRYPTED SYMMETRIC FILE DECRYPTION KEY FILE
146
147
SIGNATURE OF ENTIRE MEDIUM
35

FIG. 3

FIG. 4


400
REQUEST ACCESS TO FILES
410
ENTER PASSWORD
420
VALID PASSWORD?
NO
YES
430
LEVEL 1 OR LEVEL 2 ?
LEVEL 1
LEVEL 2
440
POSITION/DATE/ TIME INFORMATION FROM LOCATION RECEIVER BOARD
450
SECURE POSITION/ DATE/TIME INFORMATION FROM CRYPTO-BOARD
460
COMPARE POSITION/DATE/TIME WITH POLICY STORED ON DATA DISTRIBUTION MEDIA
470
UNLOCK AUTHORIZED FILES
480
DECRYPT AUTHORIZED FILES
490
DISPLAY AUTHORIZED FILES
499
END

5/6

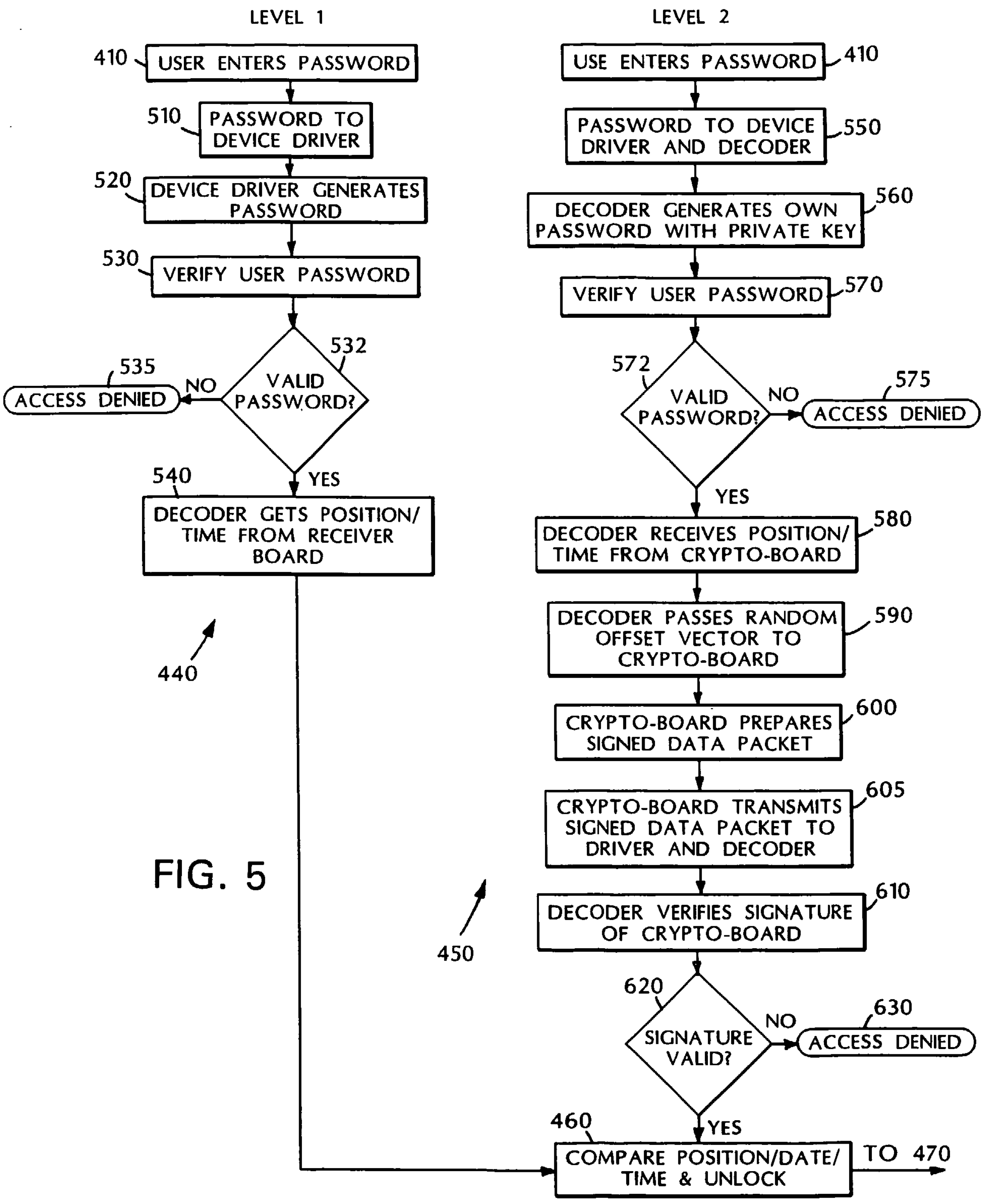

LEVEL 1
410
USER ENTERS PASSWORD
510
PASSWORD TO DEVICE DRIVER
520
DEVICE DRIVER GENERATES PASSWORD
530
VERIFY USER PASSWORD
532
VALID PASSWORD?
NO
535
ACCESS DENIED
YES
540
DECODER GETS POSITION/ TIME FROM RECEIVER BOARD
440
LEVEL 2
410
USE ENTERS PASSWORD
550
PASSWORD TO DEVICE DRIVER AND DECODER
560
DECODER GENERATES OWN PASSWORD WITH PRIVATE KEY
570
VERIFY USER PASSWORD
572
VALID PASSWORD?
NO
575
ACCESS DENIED
YES
580
DECODER RECEIVES POSITION/ TIME FROM CRYPTO-BOARD
590
DECODER PASSES RANDOM OFFSET VECTOR TO CRYPTO-BOARD
600
CRYPTO-BOARD PREPARES SIGNED DATA PACKET
605
CRYPTO-BOARD TRANSMITS SIGNED DATA PACKET TO DRIVER AND DECODER
610
DECODER VERIFIES SIGNATURE OF CRYPTO-BOARD
620
SIGNATURE VALID?
NO
630
ACCESS DENIED
YES
450
460
COMPARE POSITION/DATE/ TIME & UNLOCK
TO 470

FIG. 5

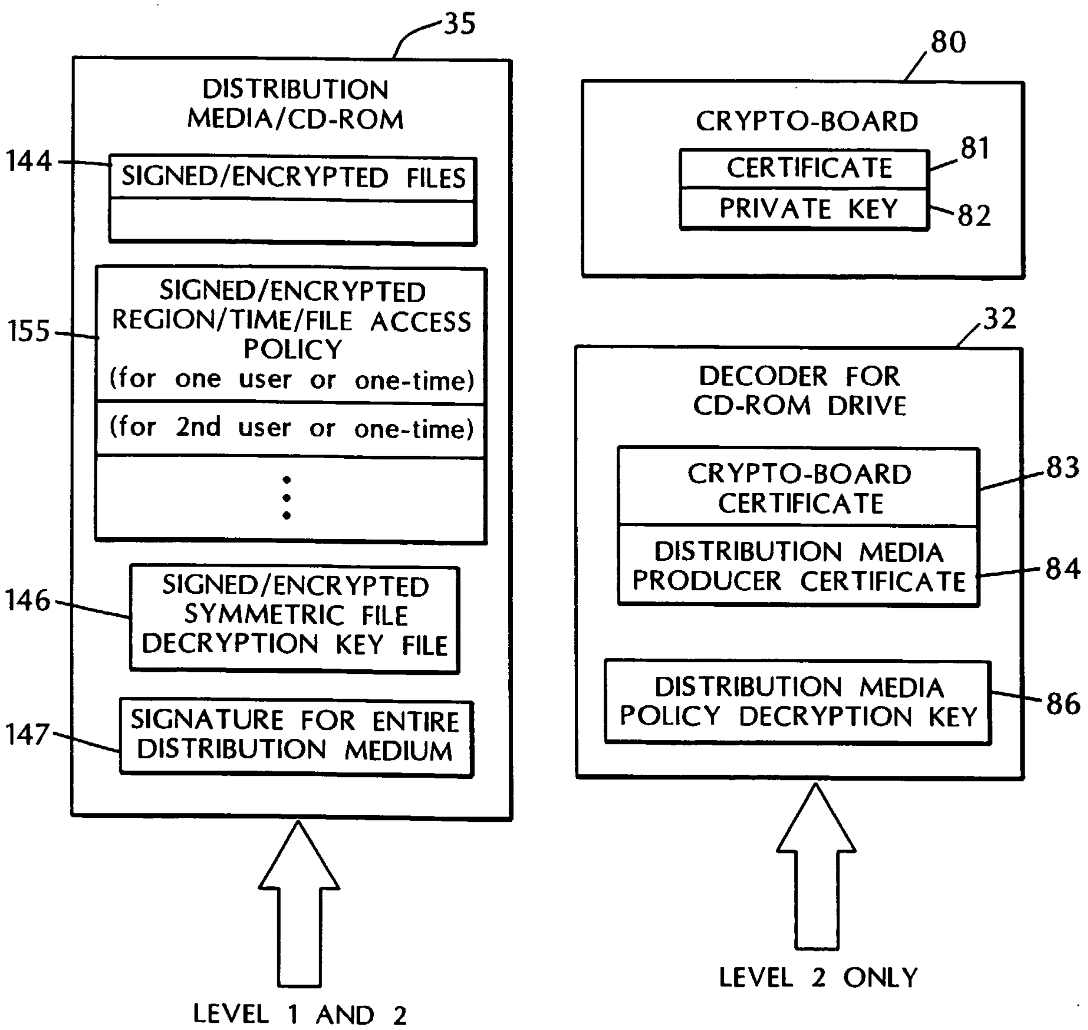

35
DISTRIBUTION MEDIA/CD-ROM
144
SIGNED/ENCRYPTED FILES
155
SIGNED/ENCRYPTED REGION/TIME/FILE ACCESS POLICY
(for one user or one-time)
(for 2nd user or one-time)
⋮
146
SIGNED/ENCRYPTED SYMMETRIC FILE DECRYPTION KEY FILE
147
SIGNATURE FOR ENTIRE DISTRIBUTION MEDIUM
LEVEL 1 AND 2
80
CRYPTO-BOARD
81
CERTIFICATE
PRIVATE KEY
82
32
DECODER FOR CD-ROM DRIVE
CRYPTO-BOARD CERTIFICATE
83
DISTRIBUTION MEDIA PRODUCER CERTIFICATE
84
DISTRIBUTION MEDIA POLICY DECRYPTION KEY
86
LEVEL 2 ONLY

FIG. 6

República Federativa do Brasil
Ministério do Desenvolvimento, Industria 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**

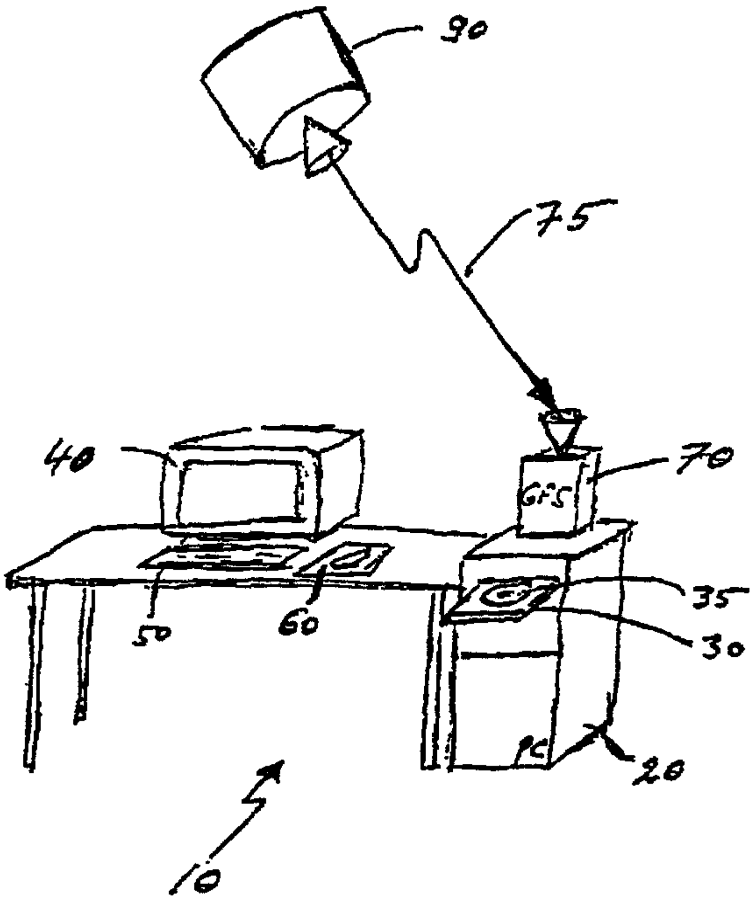
(30) Prioridade Unionista 29/10/1998 US 09/182,342

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

(72) Inventor(es) Thomas Mark Hastings, Michael E Mcneil, 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 esta 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 e 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 desencriptar 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 descriptografia 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 chave de criptografia de receptor e verificando a assinatura do receptor com uma chave de descriptografia 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 com uma chave de descriptografia 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 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 descriptografia 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 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 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 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 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 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

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,

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 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

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 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 descriptografia 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 descriptografia de política 86 desencripta 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 / descriptografia 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 incluir 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

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 descriptografia 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 descriptografia de arquivo correspondentes 52 (K_1, K_2, K_3) são armazenados no CD-ROM 35 no arquivo de chave de desencriptação de arquivo 146 A informação adicional sobre as chaves de descriptografia e o arquivo de chave de descriptografia 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 preciso 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 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 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 desbloquear 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

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 descriptografia 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 descriptografia de arquivo K1, por exemplo, uma senha, pode desencriptar o Manual A nas regiões geográficas L1 e L3 no tempo T1 O mesmo usuário também pode desencriptar 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 desencriptar 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

Tabela 1

Arquivo Cripto-grafado	Chave de Des-criptografia de Arquivo	Regiões Geográfi-cas 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 arquívos 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 assınados / criptografados 144, o usuário obtém uma senha 130 (FIG 2) a partır do produtor (etapa 400), e ıntroduz a senha 130 vıa o teclado 50 (etapa 410) É assumıdo que a senha 130 seja uma senha para uma única vez, embora as senhas de usuário válıdas por maıs de uma sessão também possam ser usadas

Como vısto na FIG 4, as porções ınıcıaıs do fluxo de processo para o Nível 1 e o Nível 3 são quase ıdêntıcas

A etapa 420 verıfıca a senha 130 e o processo então executa a etapa 440 (para o Nível 1, sem nenhuma segurança adıcıonal) ou a 450 (para o Nível 2, com segurança de receptor / drıve de CD-ROM), dependendo da confıguração do sıstema Os detalhes das etapas 440 e 450 são mostradas na FIG 5 e serão dıscutıdos agora

Como vısto na FIG 5, no processo 440, a senha de usuárıo 130 é envıada para o controlador de dıspositıvo 72 (etapa 510) Em resposta à senha de uso únıco 130, o controlador de dıspositıvo 72 gera a partır da senha de usuárıo 130 sua própria senha de uso únıco (etapa 520) e verıfıca (etapa 530) que o usuárıo de fato ıntroduzıu uma senha de uso único correto 130, desse modo autentıcando o usuárıo para a sessão ınteratıva (etapa 532) Caso contrárıo, o acesso é negado (etapa 535)

Uma vez que a senha 130 tenha autentıcado o usuárıo, o controlador de dıspositıvo 72 ınterroga o receptor 70 quanto à posıção e à data / tempo atuaıs (etapa 540) O controlador de dıspositıvo 72 então compara os dados de tempo e posıção retornados pelo receptor 70 com a polítıca 155, a qual se aplıca aos arquıvos 144 ou a um subconjunto 141, 142 e 143 dos arquıvos (etapa 460) Se o usuárıo estıver autorızado a acessar os arquıvos 144, então, o dado é desbloqueado, descrıptografado (etapa 470, FIG 3) com as chaves de descrıptografia 52 (etapa 480) e suprıdo para o programa aplıcatıvo de usuárıo 34 (etapa 490) e exıbıdo

Em um sıstema de Nível 2, o receptor 70 ıncluı a placa de receptor crıptográfıco 80, a partır deste ponto referıda como a "crıpto-placa" Como mencıonado antes, a crıpto-placa 80 pode assınar e encrıptar / desencrıptar mensagens O drıve de CD-ROM 30 ınclui o decodıfıcador 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) 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)

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

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

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 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 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

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 além das senhas

REIVINDICAÇÕES

1 Método para controle de acesso a informação armazenada, que compreende·

determinação de uma posição geográfica real onde a referida 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

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

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 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 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

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

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

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

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 informação 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

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

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 descriptografia de receptor, para verificação da referida posição real assinada de forma criptográfica

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

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 descriptografia de leitor correspondente, antes do deslocamento de posição ser adicionado à posição geográfica real

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,

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

provisão de uma chave de descriptografia de arquivo, a qual autoriza o acesso e permite a descriptografia 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

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 autorizada associada aos arquivos

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

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,

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

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 permitido, e ainda permitindo acesso ao referido arquivo se a referida data ou tempo real ocorrer no referido intervalo de data ou tempo autorizado associado

24 Método, de acordo com a reivindicação 21,a onde a referida informação armazenada é dividida em subconjuntos de informação e onde pelo menos um dos subconjuntos tem um intervalo de data ou tempo autorizado diferente dos outros subconjuntos, de modo que o acesso seja autorizado 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

25 Método para controle de acesso a uma informação armazenada, 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 referida 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 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 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 Órbita 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 localização baseado em satélite

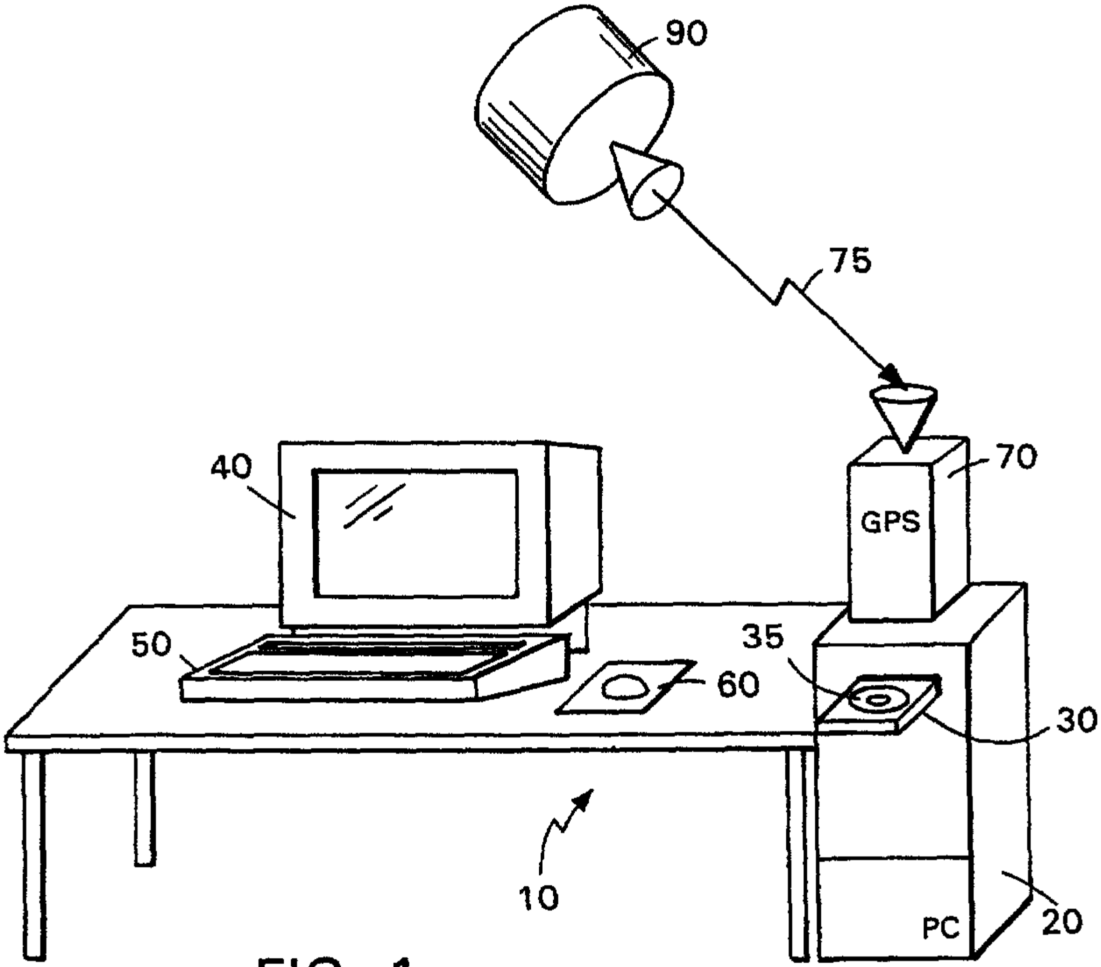
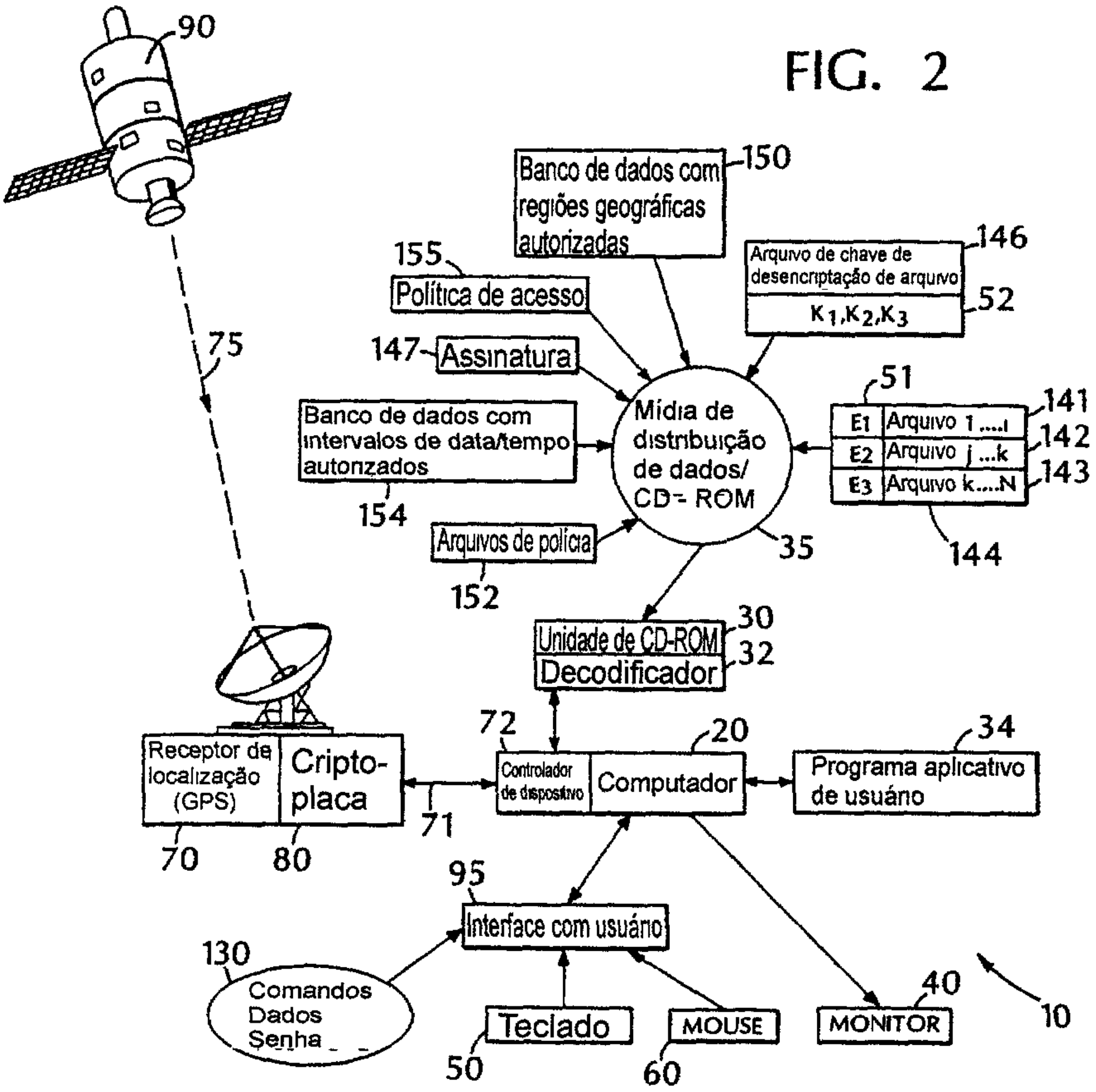


FIG. 1

FIG. 2


90
Banco de dados com regiões geográficas autorizadas
150
155
Política de acesso
Arquivo de chave de desencriptação de arquivo
146
K1,K2,K3
52
75
147
Assinatura
51
Banco de dados com intervalos de data/tempo autorizados
Mídia de distribuição de dados/ CD- ROM
E1 Arquivo 1 i
E2 Arquivo j ...k
E3 Arquivo k....N
141
142
143
154
Arquivos de polícia
35
144
152
Unidade de CD-ROM
Decodificador
30
32
72
20
34
Receptor de localização (GPS)
Cripto-placa
Controlador de dispositivo
Computador
Programa aplicativo de usuário
71
70
80
95
Interface com usuário
130
Comandos
Dados
Senha
40
10
Teclado
MOUSE
MONITOR
50
60

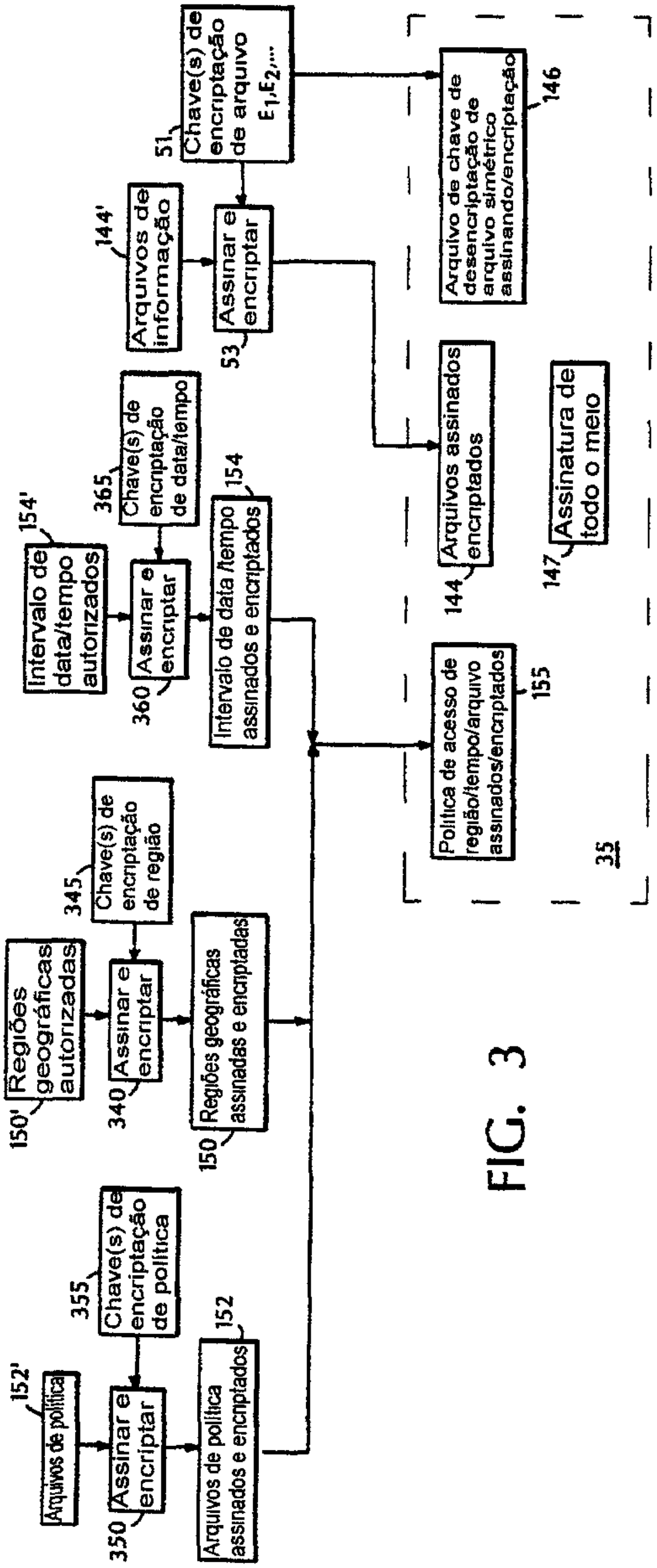
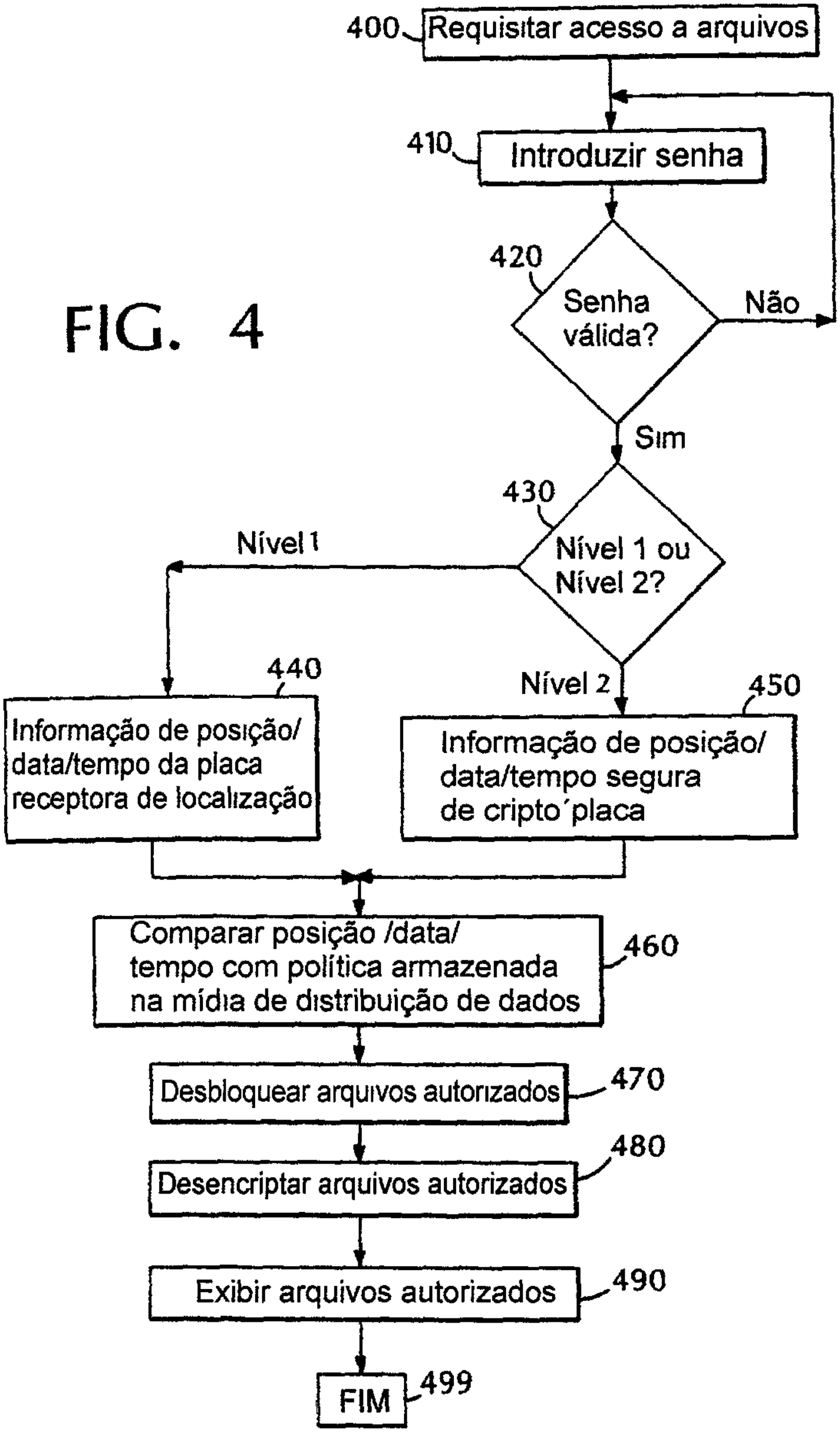

Chave(s) de encriptação de arquivo E1,E2,...
51
Arquivos de informação
144'
Assinar e encriptar
53
Arquivo de chave de desencriptação de arquivo simétrico assinando/encriptação
146
Arquivos assinados encriptados
144
Assinatura de todo o meio
147
Intervalo de data/tempo autorizados
154'
Chave(s) de encriptação de data/tempo
365
Assinar e encriptar
360
Intervalo de data /tempo assinados e encriptados
154
Política de acesso de região/tempo/arquivo assinados/encriptados
155
35
Regiões geográficas autorizadas
150'
Chave(s) de encriptação de região
345
Assinar e encriptar
340
Regiões geográficas assinadas e encriptadas
150
Arquivos de política
152'
Chave(s) de encriptação de política
355
Assinar e encriptar
350
Arquivos de política assinados e encriptados
152

FIG. 3

FIG. 4


400
Requisitar acesso a arquivos
410
Introduzir senha
420
Senha válida?
Não
Sim
430
Nível 1 ou Nível 2?
Nível 1
Nível 2
440
Informação de posição/ data/tempo da placa receptora de localização
450
Informação de posição/ data/tempo segura de cripto´placa
Comparar posição /data/ tempo com política armazenada na mídia de distribuição de dados
460
Desbloquear arquivos autorizados
470
Desencriptar arquivos autorizados
480
Exibir arquivos autorizados
490
FIM
499

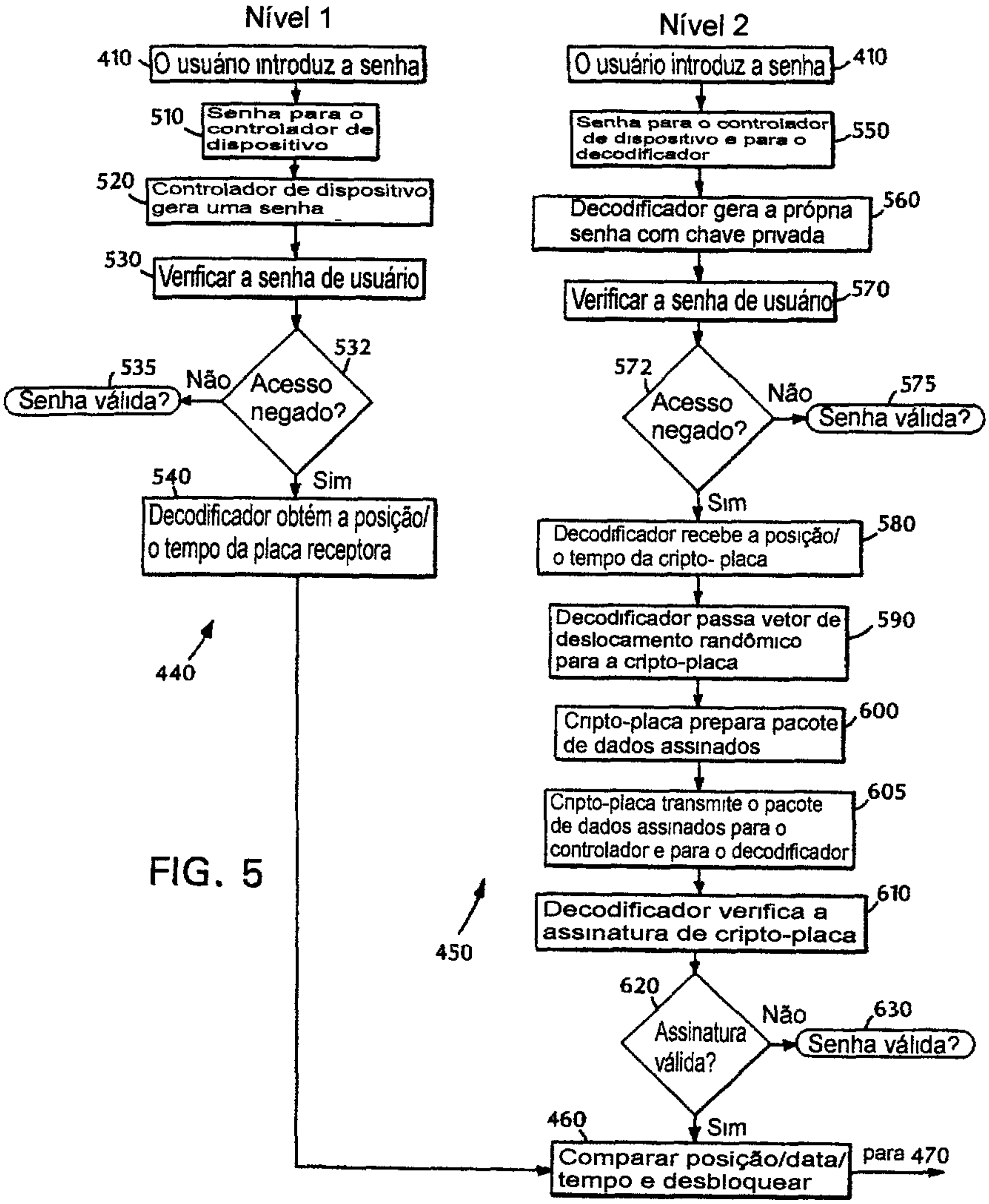

Nível 1
410
O usuáno introduz a senha
510
Senha para o controlador de dispositivo
520
Controlador de dispositıvo gera uma senha
530
Verıficar a senha de usuário
532
Acesso negado?
Não
535
Senha válida?
Sim
540
Decodificador obtém a posição/ o tempo da placa receptora
440
Nível 2
410
O usuário introduz a senha
550
Senha para o controlador de dispositivo e para o decodificador
560
Decodıficador gera a própna senha com chave pnvada
570
Verificar a senha de usuáno
572
Acesso negado?
Não
575
Senha válıda?
Sım
580
Decodificador recebe a posição/ o tempo da cripto- placa
590
Decodıficador passa vetor de deslocamento randômıco para a crıpto-placa
600
Cnpto-placa prepara pacote de dados assınados
605
Cnpto-placa transmıte o pacote de dados assınados para o controlador e para o decodıficador
610
Decodificador verıfica a assınatura de cripto-placa
620
Assinatura válida?
Não
630
Senha válida?
Sım
460
Comparar posição/data/ tempo e desbloquear
para 470
450

FIG. 5

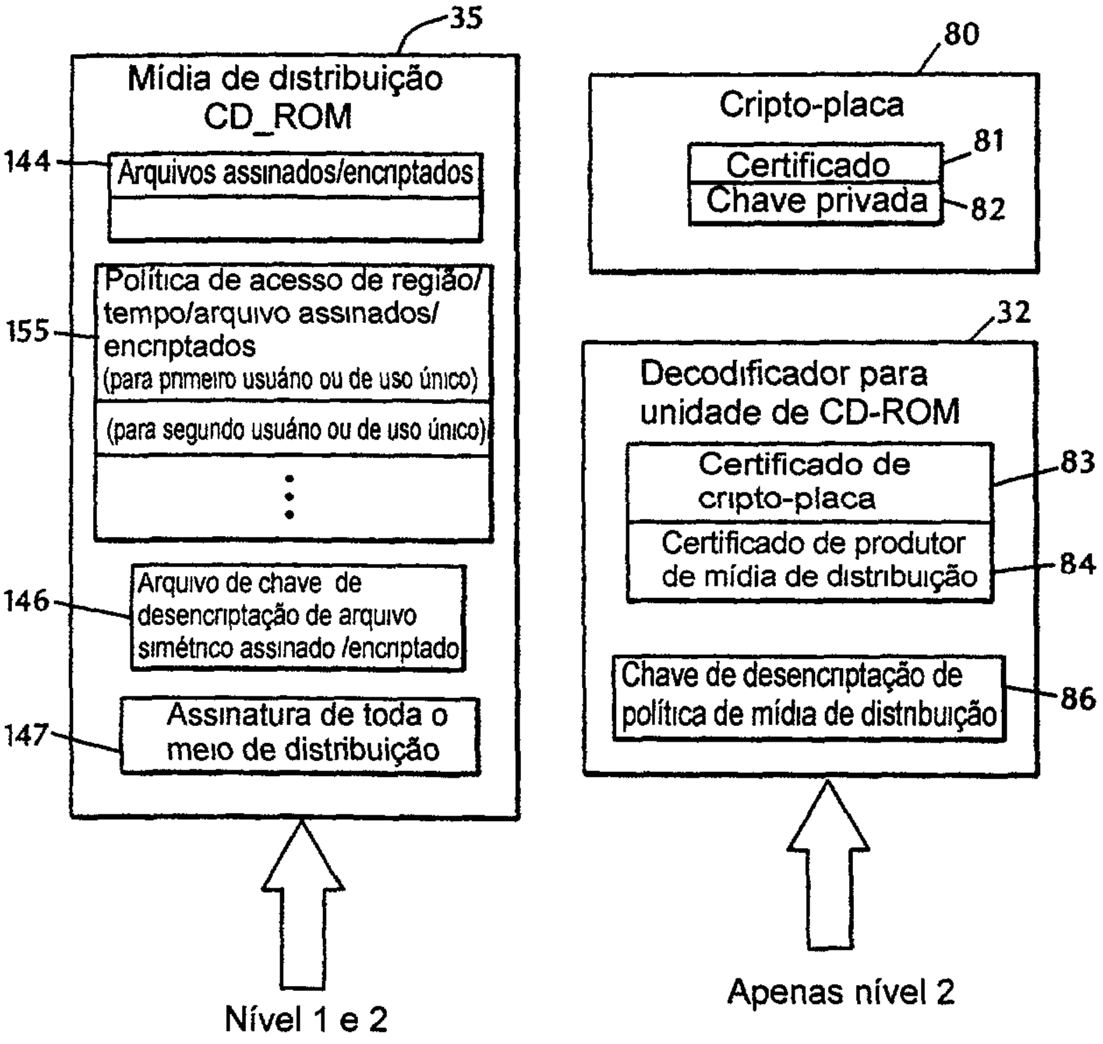

35
Mídia de distribuição CD_ROM
144
Arquivos assinados/encriptados
155
Política de acesso de região/ tempo/arquivo assinados/ encriptados
(para primeiro usuário ou de uso único)
(para segundo usuário ou de uso único)
146
Arquivo de chave de desencriptação de arquivo simétrico assinado /encriptado
147
Assinatura de toda o meio de distribuição
Nível 1 e 2
80
Cripto-placa
81
Certificado
Chave privada
82
32
Decodificador para unidade de CD-ROM
83
Certificado de cripto-placa
84
Certificado de produtor de mídia de distribuição
Chave de desencriptação de política de mídia de distribuição
86
Apenas nível 2

FIG. 6

PI9904979

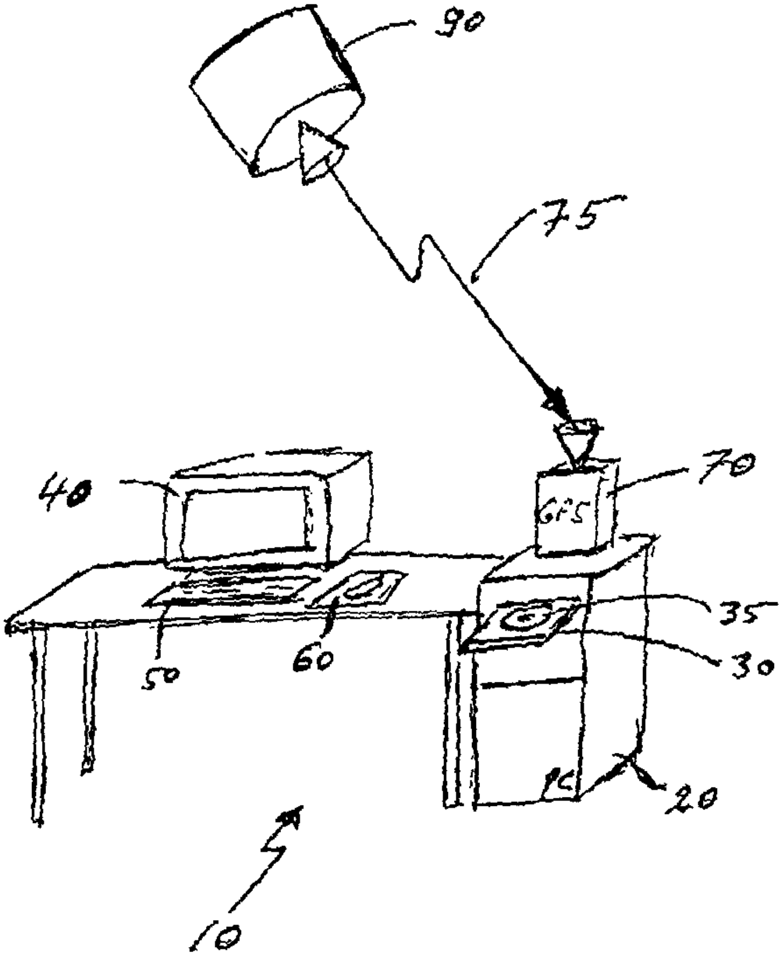


Fig. 1

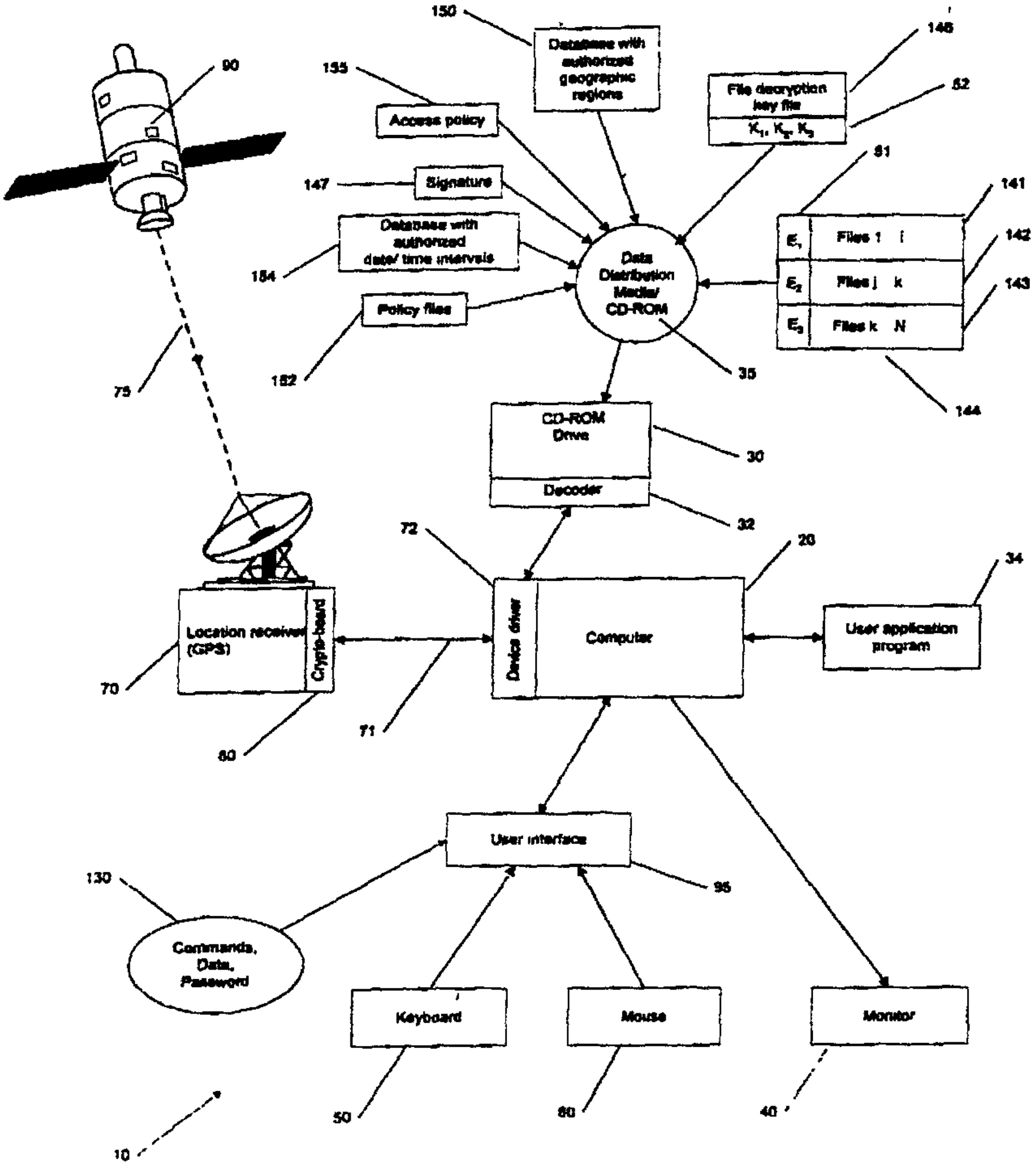

150
Database with authorized geographic regions
146
File decryption key file
K1, K2, K3
52
90
155
Access policy
51
147
Signature
141
Database with authorized date/ time intervals
154
Data Distribution Media/ CD-ROM
E1
Files 1 i
142
E2
Files j k
143
E3
Files k N
Policy files
152
75
35
144
CD-ROM Drive
30
Decoder
32
72
20
34
Location receiver (GPS)
Crypto-board
Device driver
Computer
User application program
70
71
80
User interface
130
95
Commands, Data, Password
Keyboard
Mouse
Monitor
50
60
40
10

FIG 2

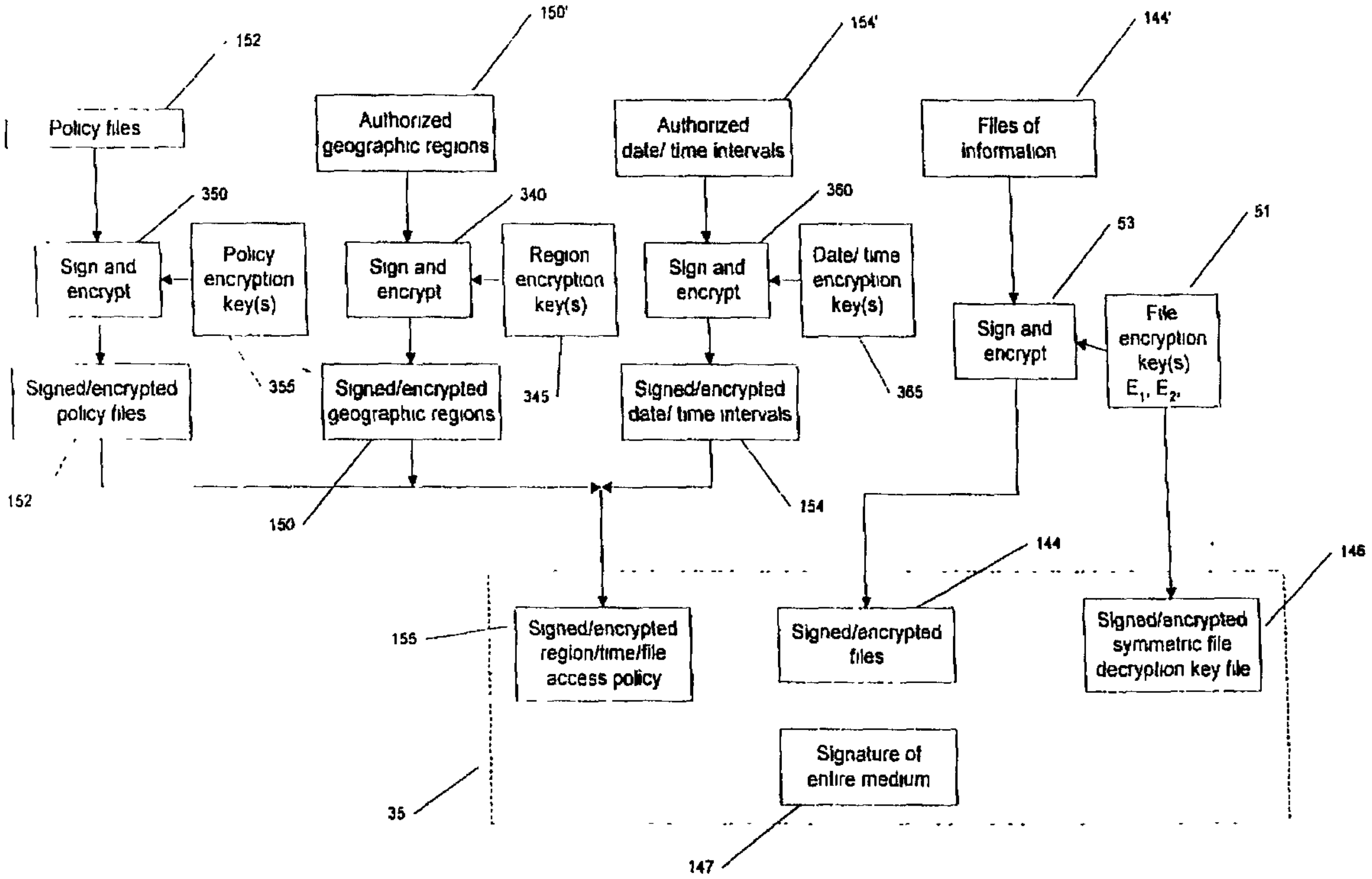

Policy files
152
Authorized geographic regions
150'
Authorized date/ time intervals
154'
Files of information
144'
Sign and encrypt
350
Policy encryption key(s)
Sign and encrypt
340
Region encryption key(s)
Sign and encrypt
360
Date/ time encryption key(s)
53
Sign and encrypt
51
File encryption key(s) E_1, E_2,
Signed/encrypted policy files
355
Signed/encrypted geographic regions
345
Signed/encrypted date/ time intervals
365
152
150
154
144
146
155
Signed/encrypted region/time/file access policy
Signed/encrypted files
Signed/encrypted symmetric file decryption key file
Signature of entire medium
35
147

FIG. 3

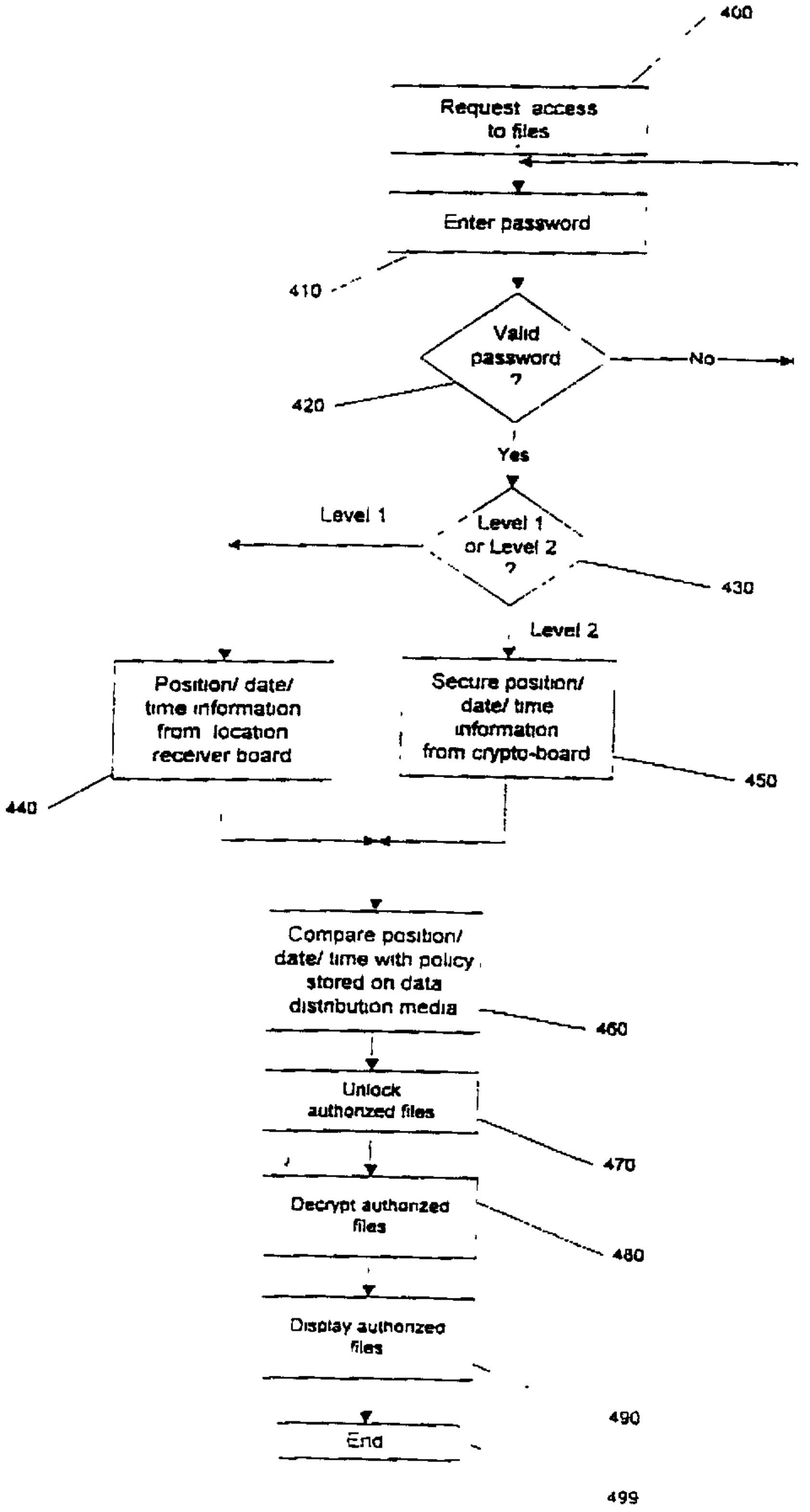

400
Request access to files
Enter password
410
Valid password ?
No
420
Yes
Level 1
Level 1 or Level 2 ?
430
Level 2
Position/ date/ time information from location receiver board
Secure position/ date/ time information from crypto-board
440
450
Compare position/ date/ time with policy stored on data distribution media
460
Unlock authorized files
470
Decrypt authorized files
480
Display authorized files
490
End
499

FIG. 4

PI9904979

5/6

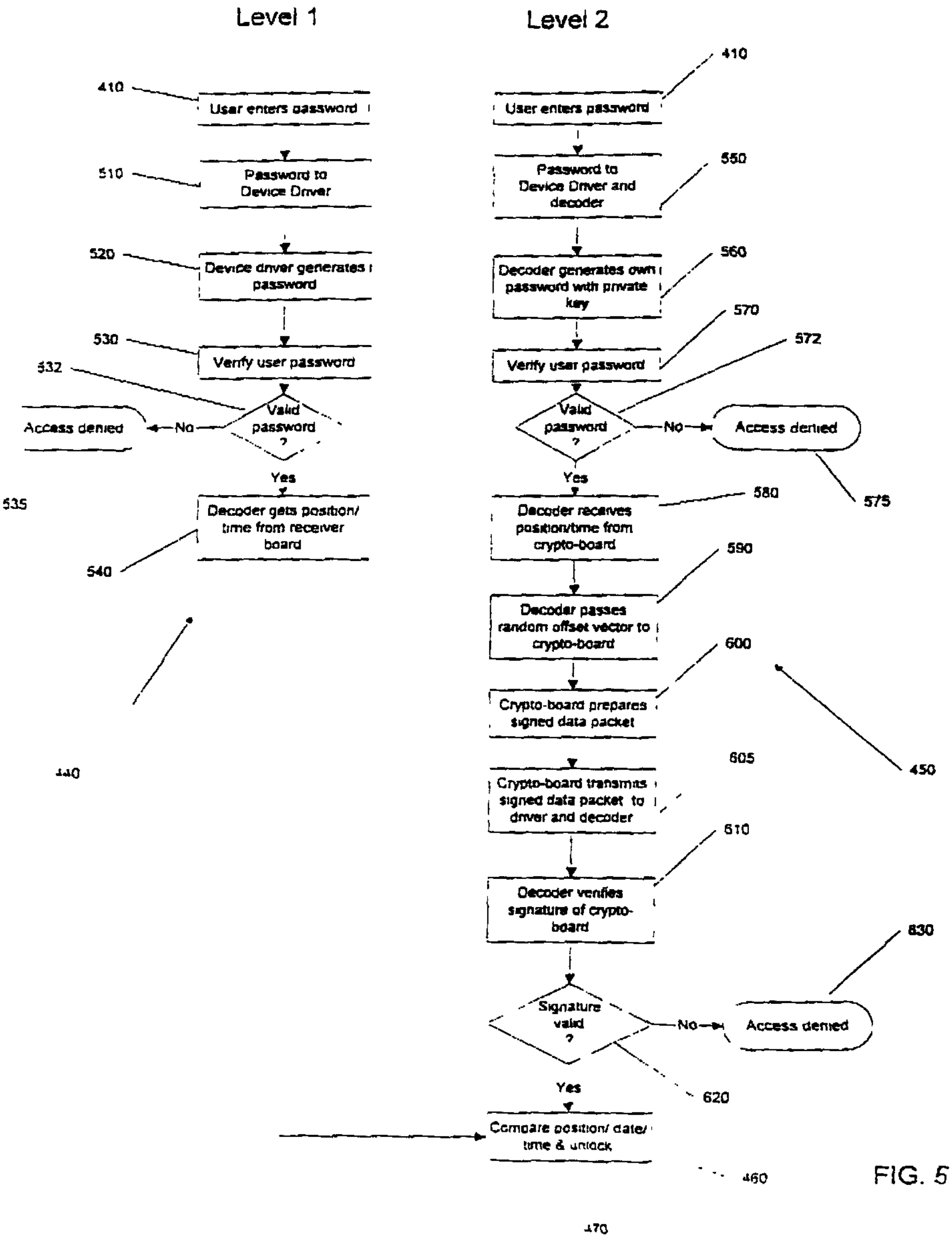

Level 1
Level 2
410
User enters password
510
Password to Device Driver
520
Device driver generates password
530
Verify user password
532
Valid password ?
No
Access denied
Yes
535
Decoder gets position/ time from receiver board
540
440
410
User enters password
550
Password to Device Driver and decoder
560
Decoder generates own password with private key
570
Verify user password
572
Valid password ?
No
Access denied
575
Yes
580
Decoder receives position/time from crypto-board
590
Decoder passes random offset vector to crypto-board
600
Crypto-board prepares signed data packet
450
605
Crypto-board transmits signed data packet to driver and decoder
610
Decoder verifies signature of crypto-board
630
Signature valid ?
No
Access denied
620
Yes
Compare position/ date/ time & unlock
460
470

FIG. 5

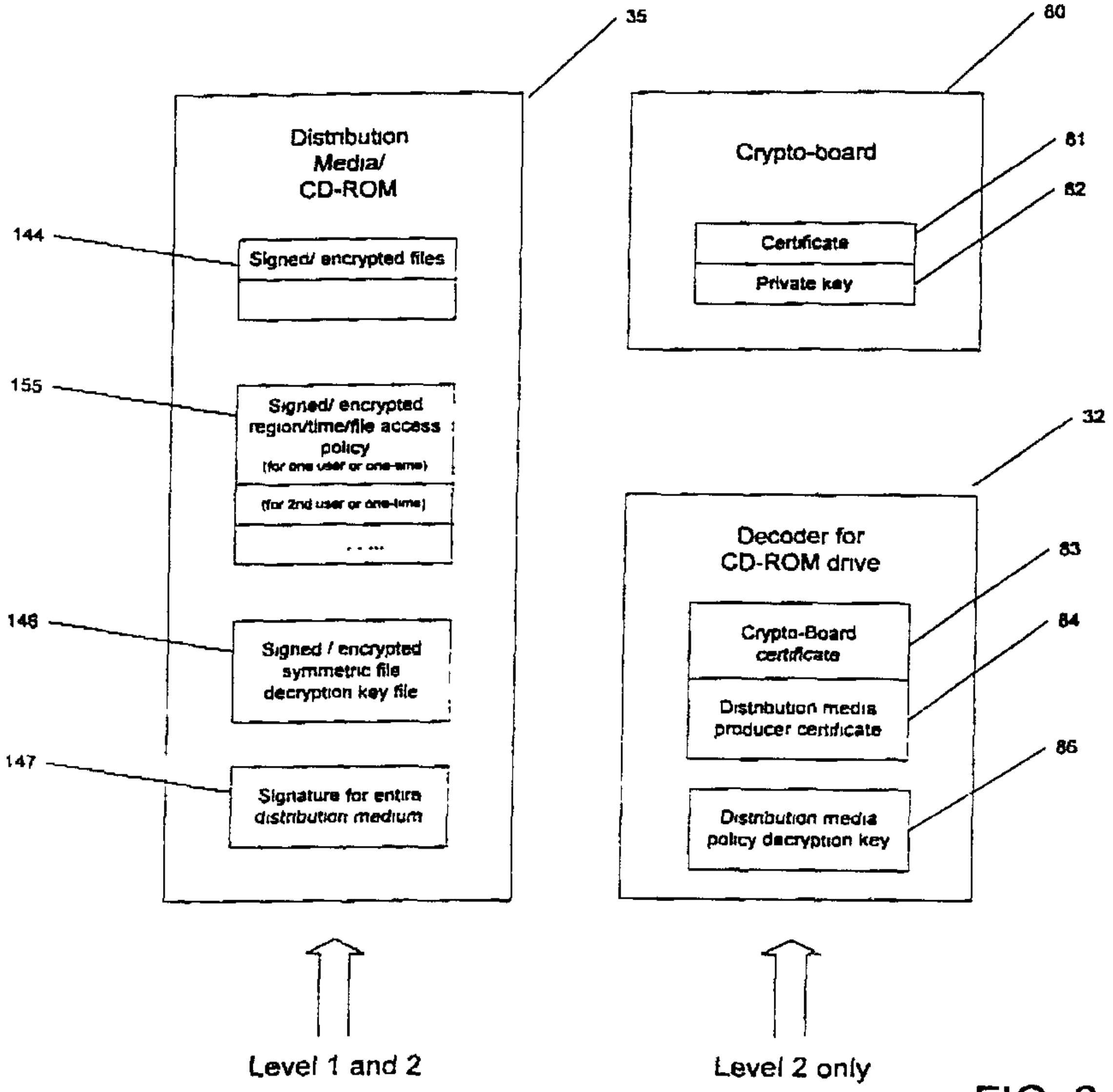

35
80
Distribution
Media/
CD-ROM
Crypto-board
144
Signed/ encrypted files
Certificate
Private key
81
82
155
Signed/ encrypted
region/time/file access
policy
(for one user or one-time)
(for 2nd user or one-time)
. . ...
32
Decoder for
CD-ROM drive
146
Signed / encrypted
symmetric file
decryption key file
Crypto-Board
certificate
83
Distribution media
producer certificate
84
147
Signature for entire
distribution medium
Distribution media
policy decryption key
86
Level 1 and 2
Level 2 only

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

(19) Canadian Intellectual Property Office

An Agency of
Industry Canada

Office de la Propriété Intellectuelle du Canada

Un organisme
d'Industrie Canada

(11) **CA 2 287 596** (13) **A1**

(43) **29.04.2000**

(12)

(21) **2 287 596**

(51) Int. Cl.^{6}: **G06F 012/14**, H04L 009/32

(22) **26.10.1999**

(30) **09/182,342 US 29.10.1998**

(71)
DATUM, INC.,
54 Middlesex Turnpike, BEDFORD, XX (US).

(72)
HASTINGS, THOMAS MARK (US).
MCNEIL, MICHAEL E. (US).
GLASSEY, TODD S. (US).
WILLETT, GERALD L. (US).

(74)
SMART & BIGGAR

(54) CONTROLE D'ACCES A DE L'INFORMATION STOCKEE
(54) CONTROLLING ACCESS TO STORED INFORMATION

(57)

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.

OPIC
Office de la propriété
intellectuelle du Canada

CIPO
Canadian Intellectual
Property Office

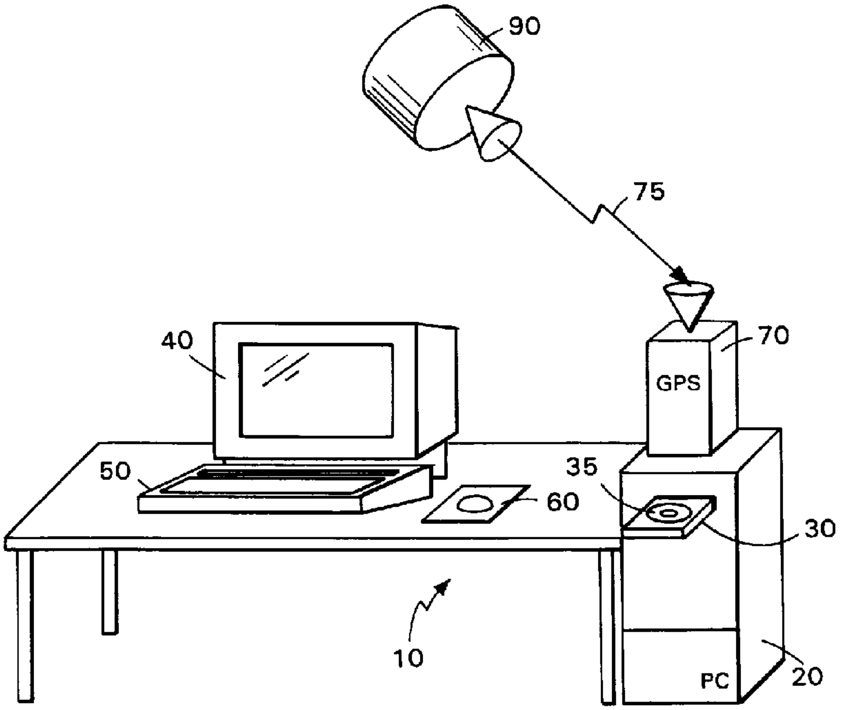
(12) (19) (CA) **Demande-Application**

(21) (A1) **2,287,596**
(22) 1999/10/26
(43) 2000/04/29

(72) HASTINGS, THOMAS MARK, US
(72) MCNEIL, MICHAEL E., US
(72) GLASSEY, TODD S., US
(72) WILLETT, GERALD L., US
(71) DATUM, INC., US

(51) Int.Cl.^{6} G06F 12/14, H04L 9/32
(30) 1998/10/29 (09/182,342) US

(54) **CONTROLE D'ACCES A DE L'INFORMATION STOCKEE**
(54) **CONTROLLING ACCESS TO STORED INFORMATION**



(57) 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.

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.

PATENT

ATTORNEY DOCKET NO: 06157/006001

CONTROLLING ACCESS TO STORED INFORMATION

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. 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 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 crytographically 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 differnt sections of information which are applicable to corresponding specific countries and/or regions. A user may be permitted to see only the portion of the information which is applicable to his current geographic location. Likewiese, access to a sensitive corpoarte report may be limited to specific plant location. Access to time-sensitive information may be denied before or after a certain date or limited to a permitted period. By associating information about authorized geographic regions and time intervals with policy files stored on the CD-ROM and accessed with a user password, the CD-ROM producer can issue a new password to permit the user to access a particular set of policy files, and therefore the information authorized, for a corresponding region and date/time.

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

Description

FIG. 1 is a perspective view of a computer system;

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

FIGS. 3 through 5 are flow diagrams;

FIG. 6 is a block diagram of cryptographic elements.

As seen in FIGS. 1 to 3, access to information which is stored on a portable computer-readable CD-ROM which 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 authenication and encrypted data transmission between the receiver 70 and the decoder 32. The computer 20 can then be any commerical 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 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 access, or can be a one-time password. Alternately, the producer can associate specific geographic region/date/time information of lists 150 and 154 with the files 141, 142 and 143 via the policy files 152. A valid user password 130 may unlock one or more policy files 152. If the user's actual geographic position and the current date and time are within the authorized geographic region and the authorized date/time corresponding to the user password 150, then the user can access the selected files via the user interface 95. The selected information is then displayed on output device 40.

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

Table 1

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

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

As seen in FIGS. 4 and 5, to gain access to the signed/encrypted files 144, the user obtains a password 130 (FIG. 2) from the producer (step 400), and enters the password 130 via the keyboard 50 (step 410). The password 130 is assumed to be a one-time password, although user passwords valid for more than one session can also be used.

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.

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;

comparing said actual geographic position with 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. The method of claim 1, further comprising:

cryptographically signing said 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 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. 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. 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; 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. The apparatus of claim 12, the receiver further comprising a receiver encryption mechanism providing a receiver encryption key for cryptographically signing the actual geographic position.

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

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

17. The apparatus of claim 16, further comprising a reader encryption mechanism providing a reader encryption key for cryptographically signing the position offset, wherein said position offset signature is verified by the receiver with a corresponding reader

decryption key before the position offset is added to the actual geographic position.

18. 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;

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. 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 which 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. 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;

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. 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 a inertial navigation system.

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

Smart & Biggar
Ottawa, Canada
Patent Agents

1/6

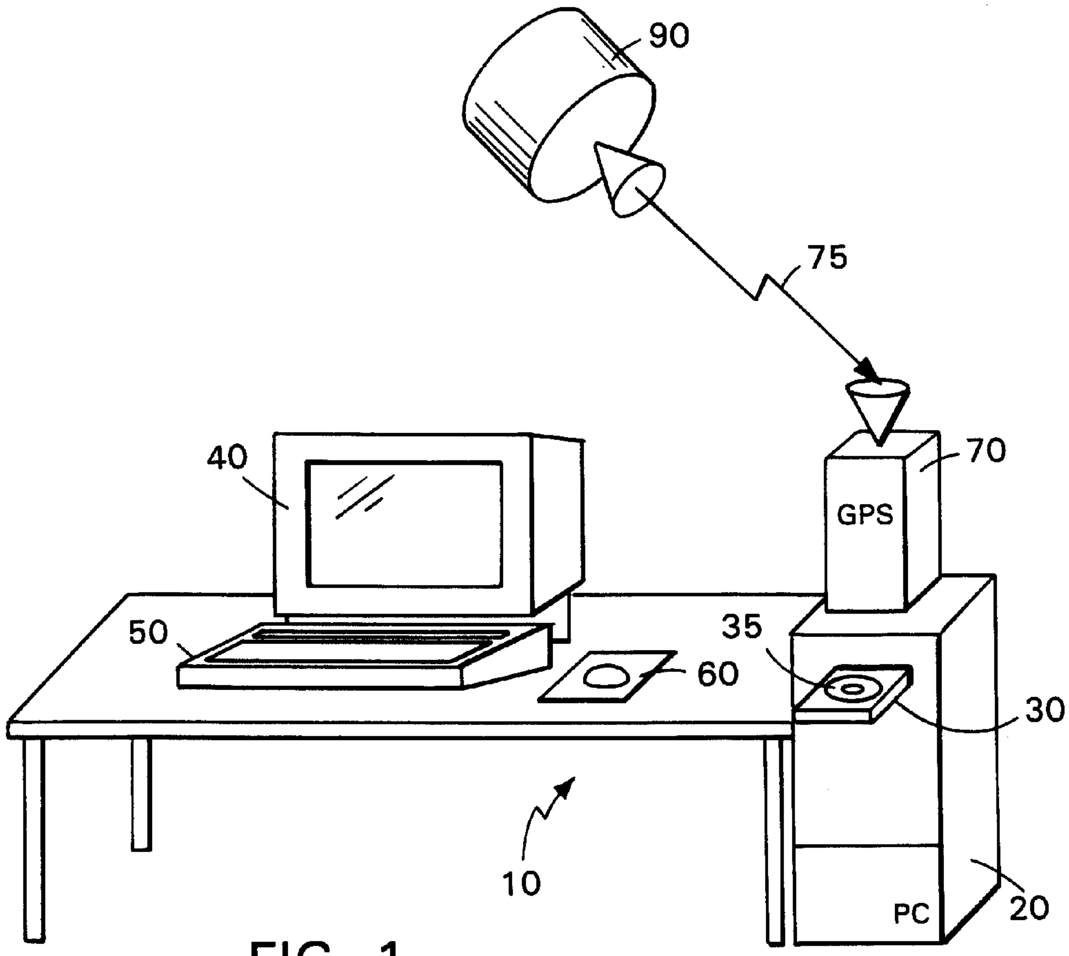
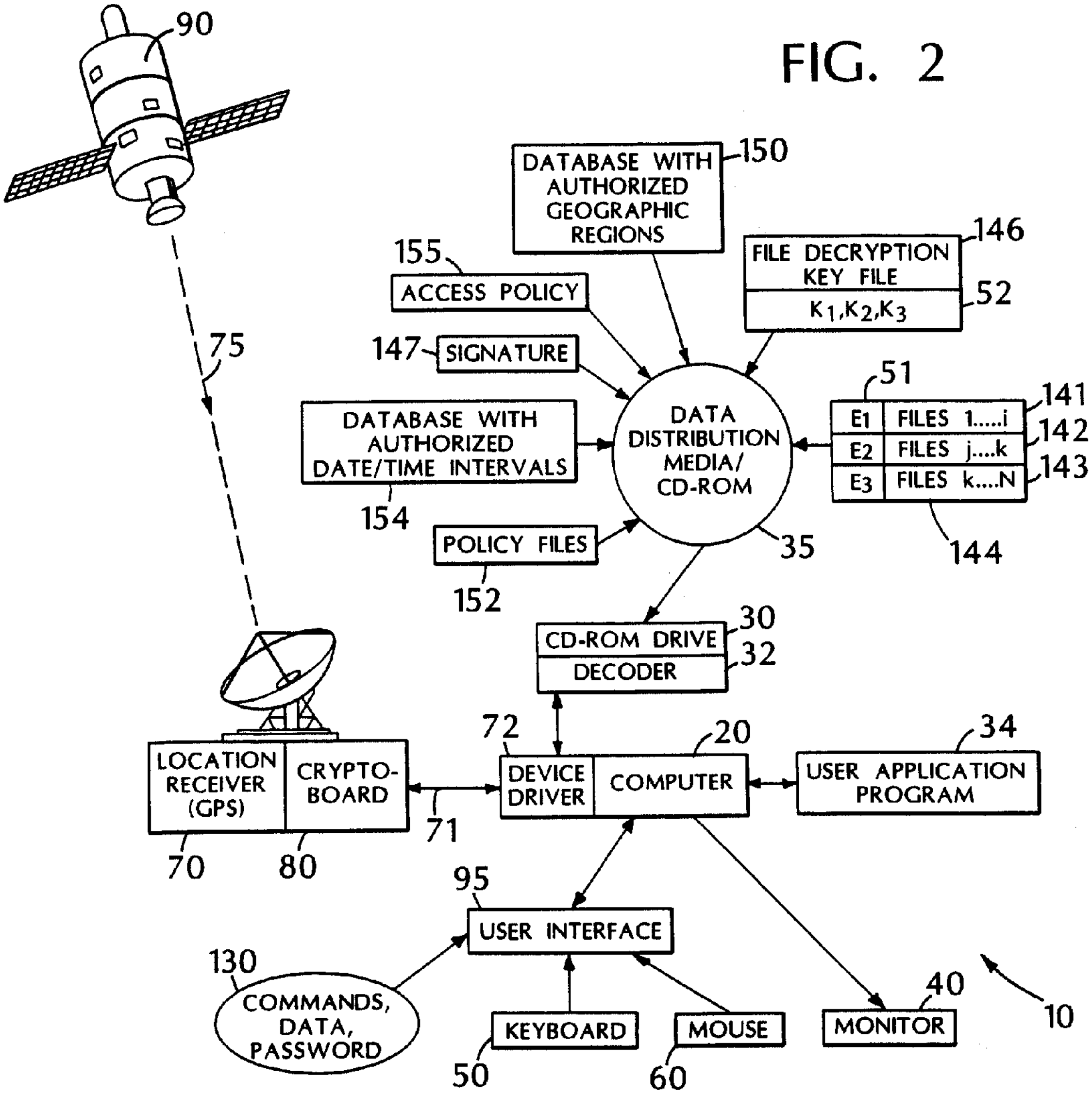


FIG. 1

FIG. 2


90
75
DATABASE WITH AUTHORIZED GEOGRAPHIC REGIONS
150
155
ACCESS POLICY
FILE DECRYPTION KEY FILE
146
K_1,K_2,K_3
52
147
SIGNATURE
51
DATABASE WITH AUTHORIZED DATE/TIME INTERVALS
DATA DISTRIBUTION MEDIA/ CD-ROM
E1
FILES 1.....i
141
E2
FILES j....k
142
E3
FILES k....N
143
154
POLICY FILES
35
144
152
CD-ROM DRIVE
30
DECODER
32
72
20
34
LOCATION RECEIVER (GPS)
CRYPTO-BOARD
DEVICE DRIVER
COMPUTER
USER APPLICATION PROGRAM
71
70
80
95
USER INTERFACE
130
COMMANDS, DATA, PASSWORD
KEYBOARD
MOUSE
MONITOR
40
10
50
60

3/6

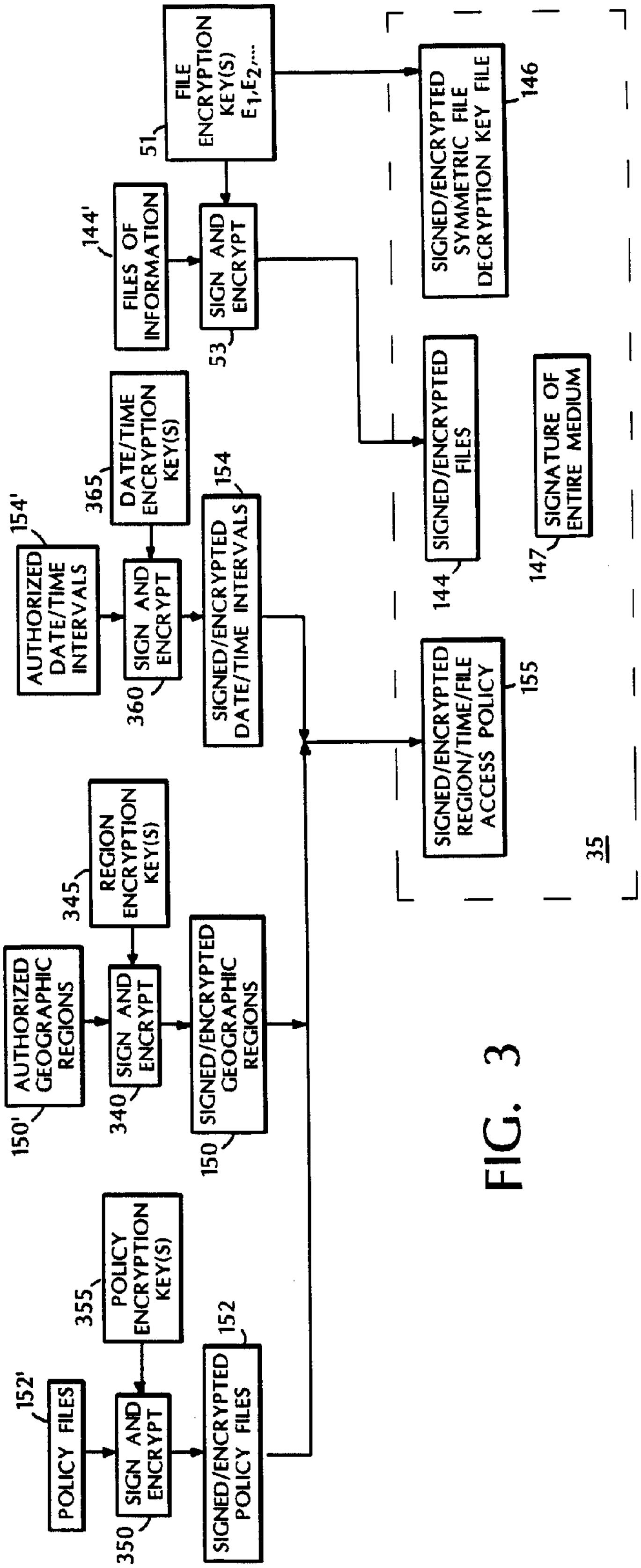

FILE ENCRYPTION KEY(S) $E_1,E_2,...$
51
FILES OF INFORMATION
144'
SIGN AND ENCRYPT
53
SIGNED/ENCRYPTED SYMMETRIC FILE DECRYPTION KEY FILE
146
SIGNED/ENCRYPTED FILES
144
SIGNATURE OF ENTIRE MEDIUM
147
AUTHORIZED DATE/TIME INTERVALS
154'
DATE/TIME ENCRYPTION KEY(S)
365
SIGN AND ENCRYPT
360
SIGNED/ENCRYPTED DATE/TIME INTERVALS
154
SIGNED/ENCRYPTED REGION/TIME/FILE ACCESS POLICY
155
35
AUTHORIZED GEOGRAPHIC REGIONS
150'
REGION ENCRYPTION KEY(S)
345
SIGN AND ENCRYPT
340
SIGNED/ENCRYPTED GEOGRAPHIC REGIONS
150
POLICY FILES
152'
POLICY ENCRYPTION KEY(S)
355
SIGN AND ENCRYPT
350
SIGNED/ENCRYPTED POLICY FILES
152

FIG. 3

4/6

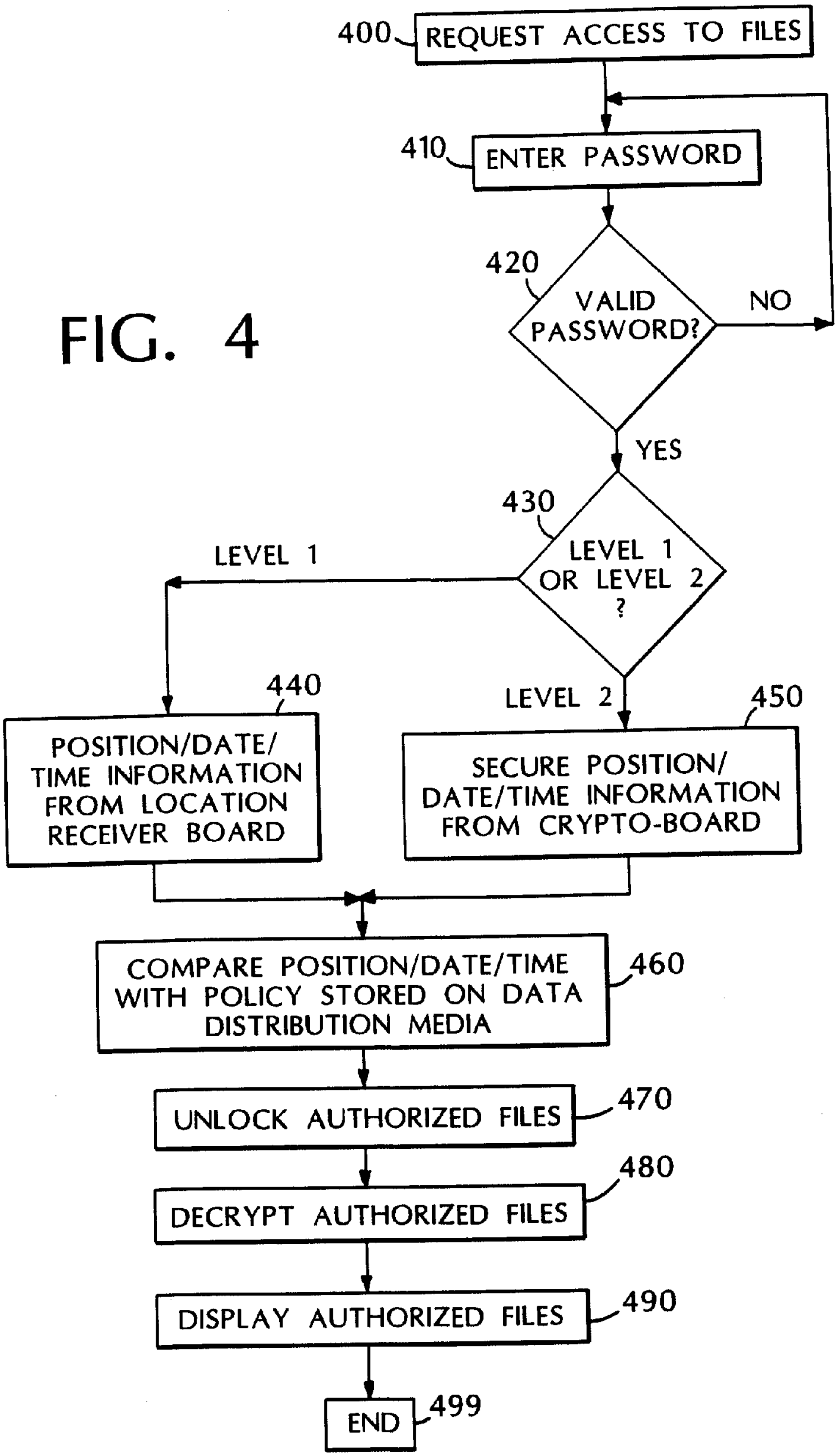

400
REQUEST ACCESS TO FILES
410
ENTER PASSWORD
420
VALID PASSWORD?
NO
YES
430
LEVEL 1 OR LEVEL 2 ?
LEVEL 1
LEVEL 2
440
POSITION/DATE/ TIME INFORMATION FROM LOCATION RECEIVER BOARD
450
SECURE POSITION/ DATE/TIME INFORMATION FROM CRYPTO-BOARD
460
COMPARE POSITION/DATE/TIME WITH POLICY STORED ON DATA DISTRIBUTION MEDIA
470
UNLOCK AUTHORIZED FILES
480
DECRYPT AUTHORIZED FILES
490
DISPLAY AUTHORIZED FILES
499
END

FIG. 4

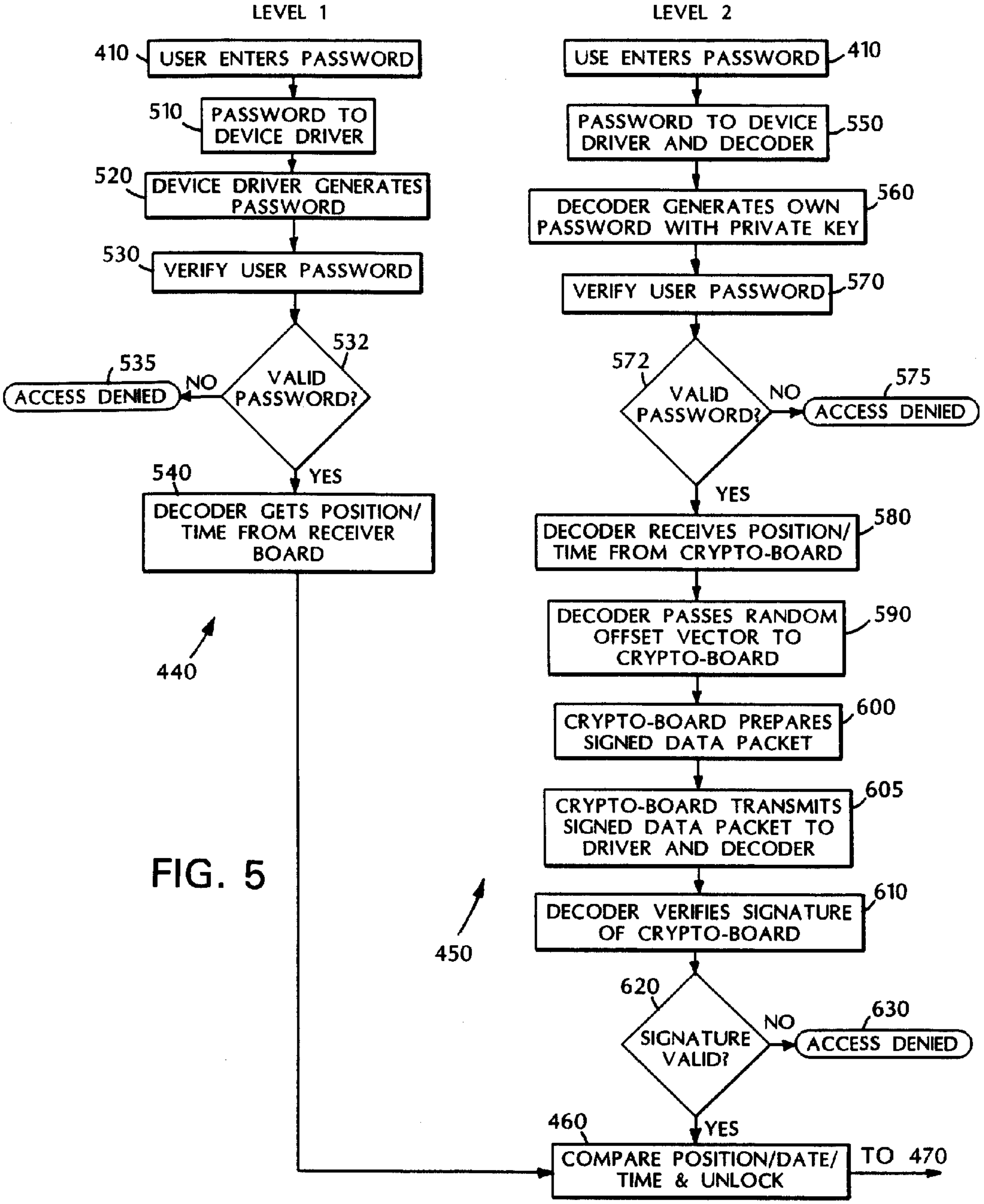

LEVEL 1
410
USER ENTERS PASSWORD
510
PASSWORD TO DEVICE DRIVER
520
DEVICE DRIVER GENERATES PASSWORD
530
VERIFY USER PASSWORD
532
VALID PASSWORD?
535
NO
ACCESS DENIED
540
YES
DECODER GETS POSITION/ TIME FROM RECEIVER BOARD
440
LEVEL 2
410
USE ENTERS PASSWORD
550
PASSWORD TO DEVICE DRIVER AND DECODER
560
DECODER GENERATES OWN PASSWORD WITH PRIVATE KEY
570
VERIFY USER PASSWORD
572
VALID PASSWORD?
NO
575
ACCESS DENIED
YES
580
DECODER RECEIVES POSITION/ TIME FROM CRYPTO-BOARD
590
DECODER PASSES RANDOM OFFSET VECTOR TO CRYPTO-BOARD
600
CRYPTO-BOARD PREPARES SIGNED DATA PACKET
605
CRYPTO-BOARD TRANSMITS SIGNED DATA PACKET TO DRIVER AND DECODER
610
DECODER VERIFIES SIGNATURE OF CRYPTO-BOARD
450
620
SIGNATURE VALID?
NO
630
ACCESS DENIED
460
YES
COMPARE POSITION/DATE/ TIME & UNLOCK
TO 470

FIG. 5

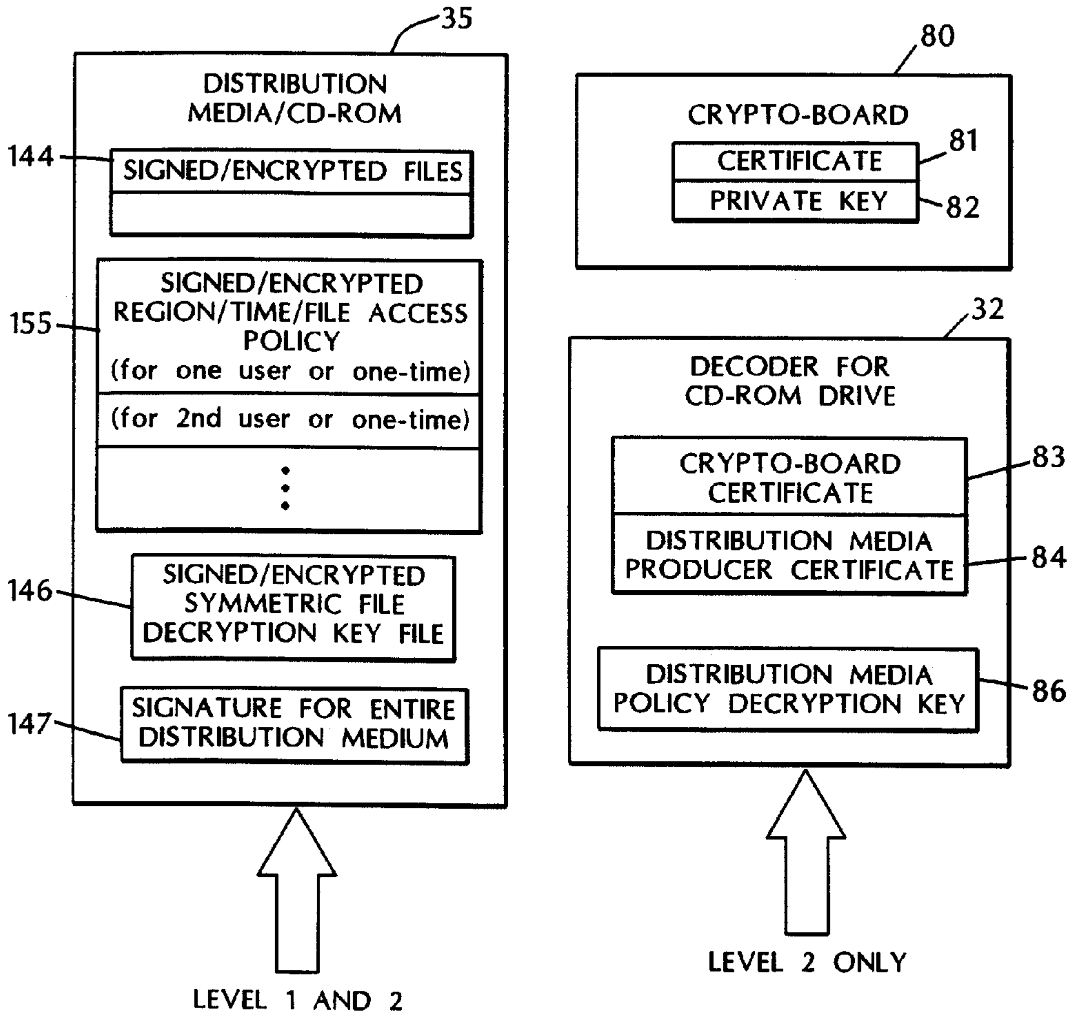

35
DISTRIBUTION MEDIA/CD-ROM
144
SIGNED/ENCRYPTED FILES
155
SIGNED/ENCRYPTED REGION/TIME/FILE ACCESS POLICY
(for one user or one-time)
(for 2nd user or one-time)
146
SIGNED/ENCRYPTED SYMMETRIC FILE DECRYPTION KEY FILE
147
SIGNATURE FOR ENTIRE DISTRIBUTION MEDIUM
LEVEL 1 AND 2
80
CRYPTO-BOARD
CERTIFICATE
81
PRIVATE KEY
82
32
DECODER FOR CD-ROM DRIVE
CRYPTO-BOARD CERTIFICATE
83
DISTRIBUTION MEDIA PRODUCER CERTIFICATE
84
DISTRIBUTION MEDIA POLICY DECRYPTION KEY
86
LEVEL 2 ONLY

FIG. 6

(19)日本国特許庁（ＪＰ）　(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	ＦＩ			テーマコード°(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｄ	
Ｇ０１Ｓ	5/14		Ｇ０１Ｓ	5/14		
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ａ	
	12/14	３１０		12/14	３１０Ｋ	
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ	

審査請求　未請求　請求項の数28　ＯＬ　（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)

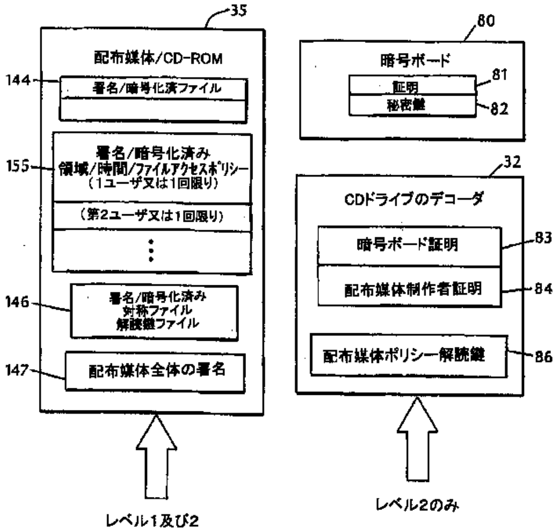
(31)優先権主張番号　０９／１８２３４２
(32)優先日　平成10年10月29日(1998.10.29)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　599153541
デイタム　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、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。

【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】

【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。

【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、周回する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、１４６、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の範囲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Ｌ３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の期間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つ以上の日時の期間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。

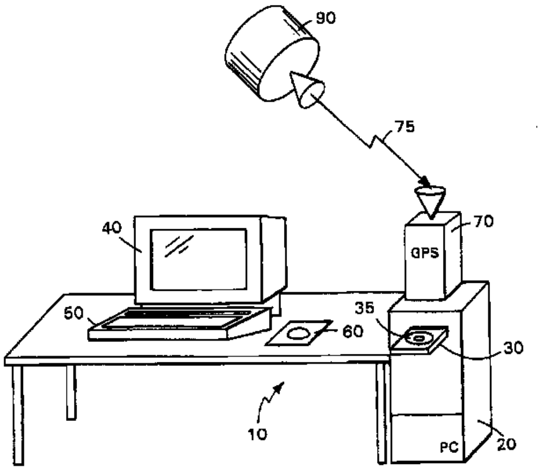
【図６】暗号の構成要素を示すブロック図である。

【主要部分の符号の説明】

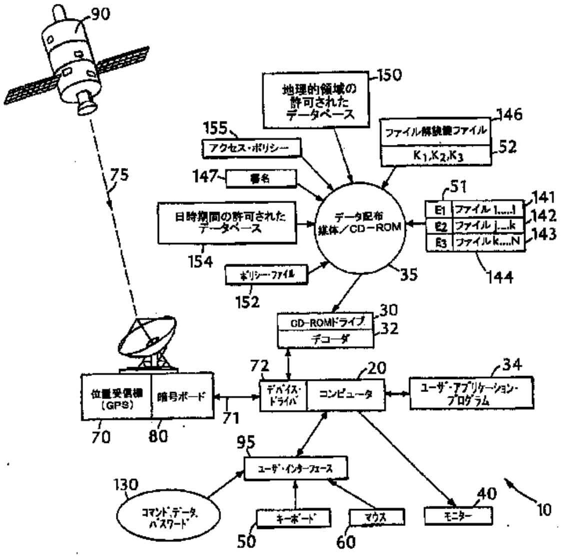
１０	コンピュータ・システム
２０	コンピュータ
３２	デコーダ
３５	データ配布媒体
７０	ＧＰＳ受信機
８０	暗号ボード
８１	証明書

８２	秘密鍵	１４４	情報ファイル
８３	暗号ボード公開鍵証明	１４６	ファイル解読鍵ファイル
８４	製作者証明	１４７	配布媒体の署名
８６	配布媒体ポリシー解読鍵	１５５	アクセス・ポリシー
９０	ＧＰＳ衛星		

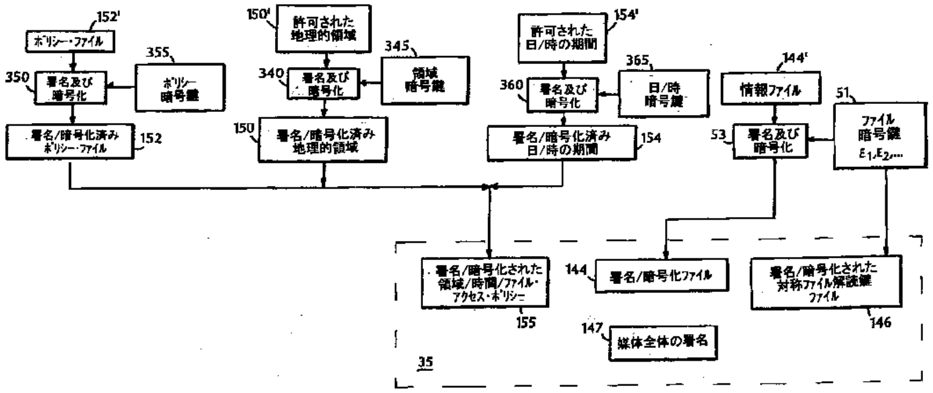
【図１】



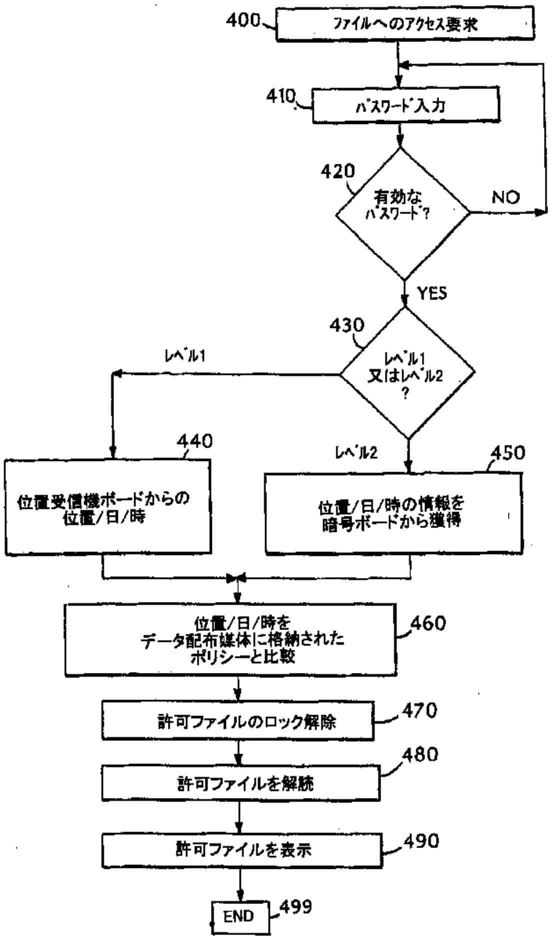
【図２】



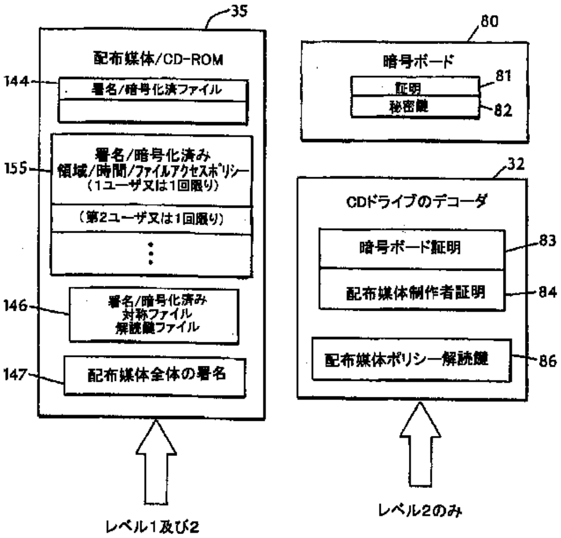
【図３】



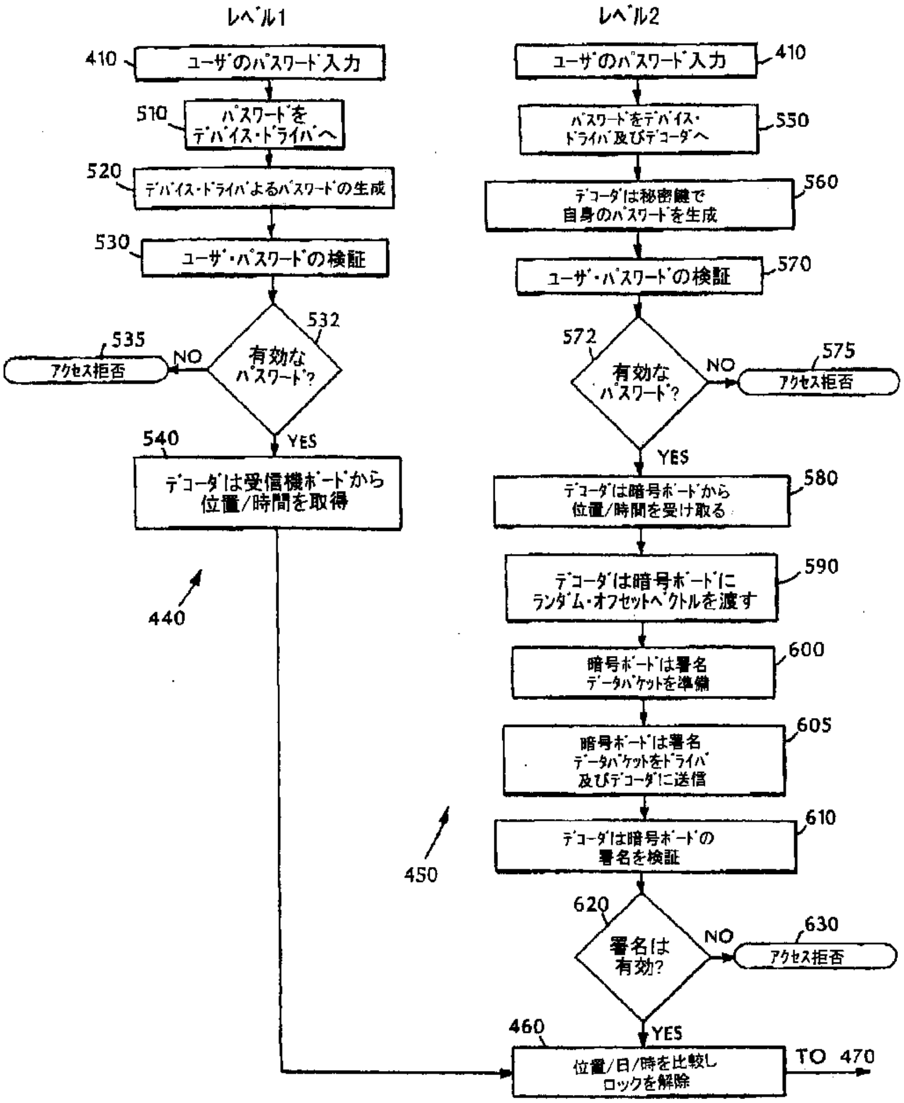
【図4】


400
ﾌｧｲﾙへのｱｸｾｽ要求
410
ﾊﾟｽﾜｰﾄﾞ入力
420
有効な
ﾊﾟｽﾜｰﾄﾞ?
NO
YES
430
ﾚﾍﾞﾙ1
又はﾚﾍﾞﾙ2
?
ﾚﾍﾞﾙ1
ﾚﾍﾞﾙ2
440
位置受信機ボードからの
位置/日/時
450
位置/日/時の情報を
暗号ボードから獲得
位置/日/時を
データ配布媒体に格納された
ポリシーと比較
460
許可ファイルのロック解除
470
480
許可ファイルを解読
490
許可ファイルを表示
END
499

【図6】


35
配布媒体/CD-ROM
144
署名/暗号化済ファイル
155
署名/暗号化済み
領域/時間/ファイルアクセスﾎﾟﾘｼｰ
(1ユーザ又は1回限り)
(第2ユーザ又は1回限り)
146
署名/暗号化済み
対称ファイル
解読鍵ファイル
147
配布媒体全体の署名
レベル1及び2
80
暗号ボード
81
証明
秘密鍵
82
32
CDドライブのデコーダ
暗号ボード証明
83
配布媒体制作者証明
84
配布媒体ポリシー解読鍵
86
レベル2のみ

【図５】



フロントページの続き

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/14		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．　グラッシィ
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

SPOOR AND FISHER

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978

FORM P.8
(To be lodged in duplicate)

PUBLICATION PARTICULARS AND ABSTRACT

(Section 32(3)(a) – Regulation 22(1)(g) and 31)

OFFICIAL APPLICATION NO.
21 01 99/6799

LODGING DATE
22 28-10-1999

ACCEPTANCE DATE
43 21·6·2000

INTERNATIONAL CLASSIFICATION
51 G 06 F

NOT FOR PUBLICATION
CLASSIFIED BY: SPOOR AND FISHER

FULL NAME(S) OF APPLICANT(S)
71 DATUM, INC.

FULL NAME(S) OF INVENTOR(S)
72 HASTINGS, Thomas Mark; MCNEIL, Michael E.; GLASSEY, Todd S.; WILLETT, Gerald L.

EARLIEST PRIORITY CLAIMED

COUNTRY	NUMBER	DATE
33 US	31 09/182,342	32 29-10-1998

TITLE OF INVENTION
54 CONTROLLING ACCESS TO STORED INFORMATION

57 ABSTRACT (NOT MORE THAT 150 WORDS)

NUMBER OF SHEETS 28

If no classification is finished, Form P.9 should accompany this form.
The figure of the drawing to which the abstract refers is attached.

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.

DATUM, INC.
APPLICATION NO 99/6799

FOR PUBLICATION
FIGURE 1

1/6

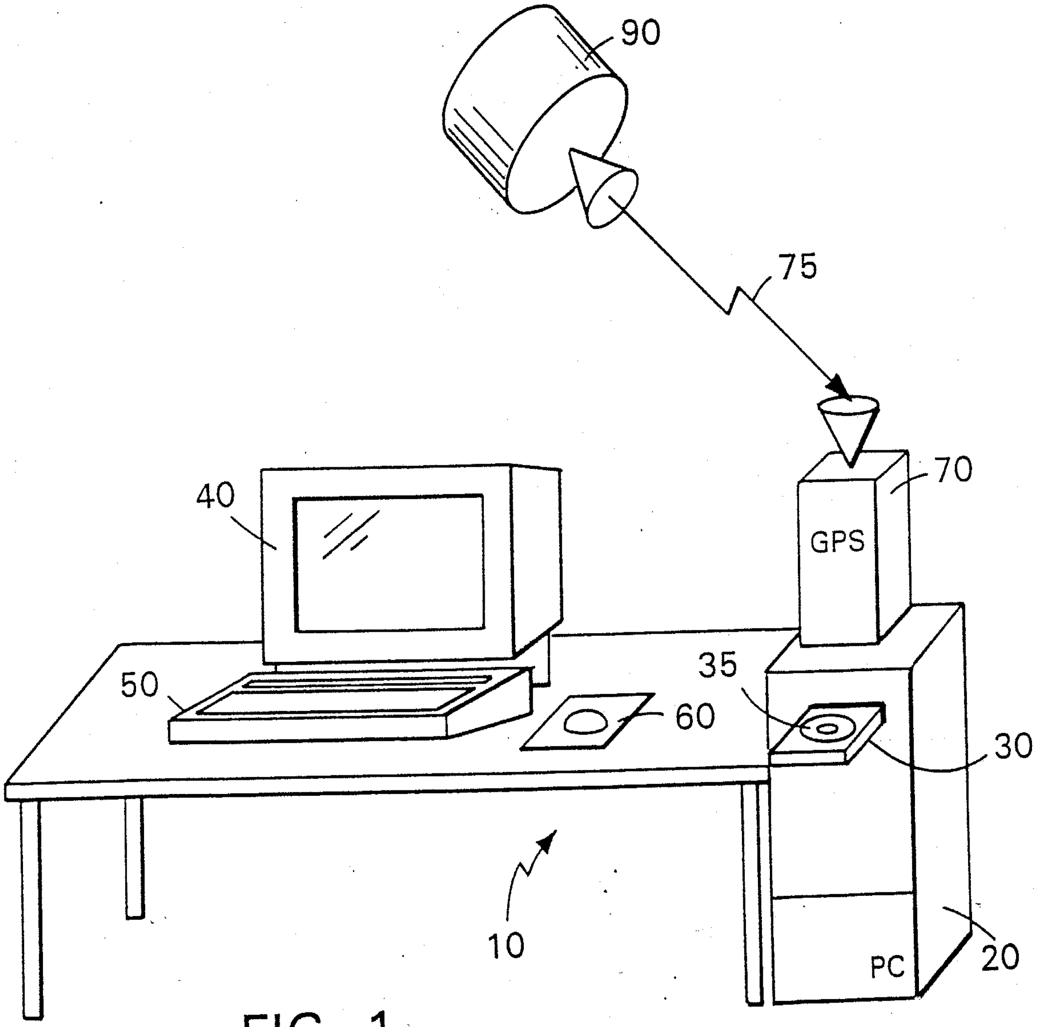


FIG. 1

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. 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 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 crytographically 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 differnt sections of information which are applicable to corresponding specific countries and/or regions. A user may be permitted to see only the portion of the information which is applicable to his current geographic location. Likewiese, access to a sensitive corpoarte report may be limited to specific plant location. Access to time-sensitive information may be denied before or after a certain date or limited to a permitted period. By associating information about authorized geographic regions and time intervals with policy files stored on the CD-ROM and accessed with a user password, the CD-ROM producer can issue a new password to permit the user to access a particular set of policy files, and therefore the information authorized, for a corresponding region and date/time.

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

Description

FIG. 1 is a perspective view of a computer system;

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

FIGS. 3 through 5 are flow diagrams;

FIG. 6 is a block diagram of cryptographic elements.

As seen in FIGS. 1 to 3, access to information which is stored on a portable computer-readable CD-ROM which 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 authenication and encrypted data transmission between the receiver 70 and the decoder 32. The computer 20 can then be any commerical 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 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 access, or can be a one-time password. Alternately, the producer can associate specific geographic region/date/time information of lists 150 and 154 with the files 141, 142 and 143 via the policy files 152. A valid user password 130 may unlock one or more policy files 152. If the user's actual geographic position and the current date and time are within the authorized geographic region and the authorized date/time corresponding to the user password 150, then the user can access the selected files via the user interface 95. The selected information is then displayed on output device 40.

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

Table 1

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

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

As seen in FIGS. 4 and 5, to gain access to the signed/encrypted files 144, the user obtains a password 130 (FIG. 2) from the producer (step 400), and enters the password 130 via the keyboard 50 (step 410). The password 130 is assumed to be a one-time password, although user passwords valid for more than one session can also be used.

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.

CLAIMS:

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;

comparing said actual geographic position with 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. The method of claim 1, further comprising:

cryptographically signing said 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 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. 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. 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; 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. The apparatus of claim 12, the receiver further comprising a receiver encryption mechanism providing a receiver encryption key for cryptographically signing the actual geographic position.

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

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

17. The apparatus of claim 16, further comprising a reader encryption mechanism providing a reader encryption key for cryptographically signing the position offset, wherein said position offset signature is verified by the receiver with a corresponding reader

decryption key before the position offset is added to the actual geographic position.

18. 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;

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. 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 which 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. 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;

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. 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 reliable position information is received from a Global Orbiting Navigational Satellite System.

27. The method of claim 1, wherein said reliable position information is received from a inertial navigation system.

28. The method of claim 1, wherein said reliable position information is received from a satellite based location determination system.

DATED THIS 28TH DAY OF OCTOBER 1999

SPOOR AND FISHER
APPLICANTS PATENT ATTORNEYS

AMENDED THIS 23RD DAY OF DECEMBER 1999

SPOOR AND FISHER
APPLICANTS PATENT ATTORNEYS

DATUM, INC.
COMPLETE SPECIFICATION
APPLICATION NO 99/6799

6 SHEETS
SHEET 1

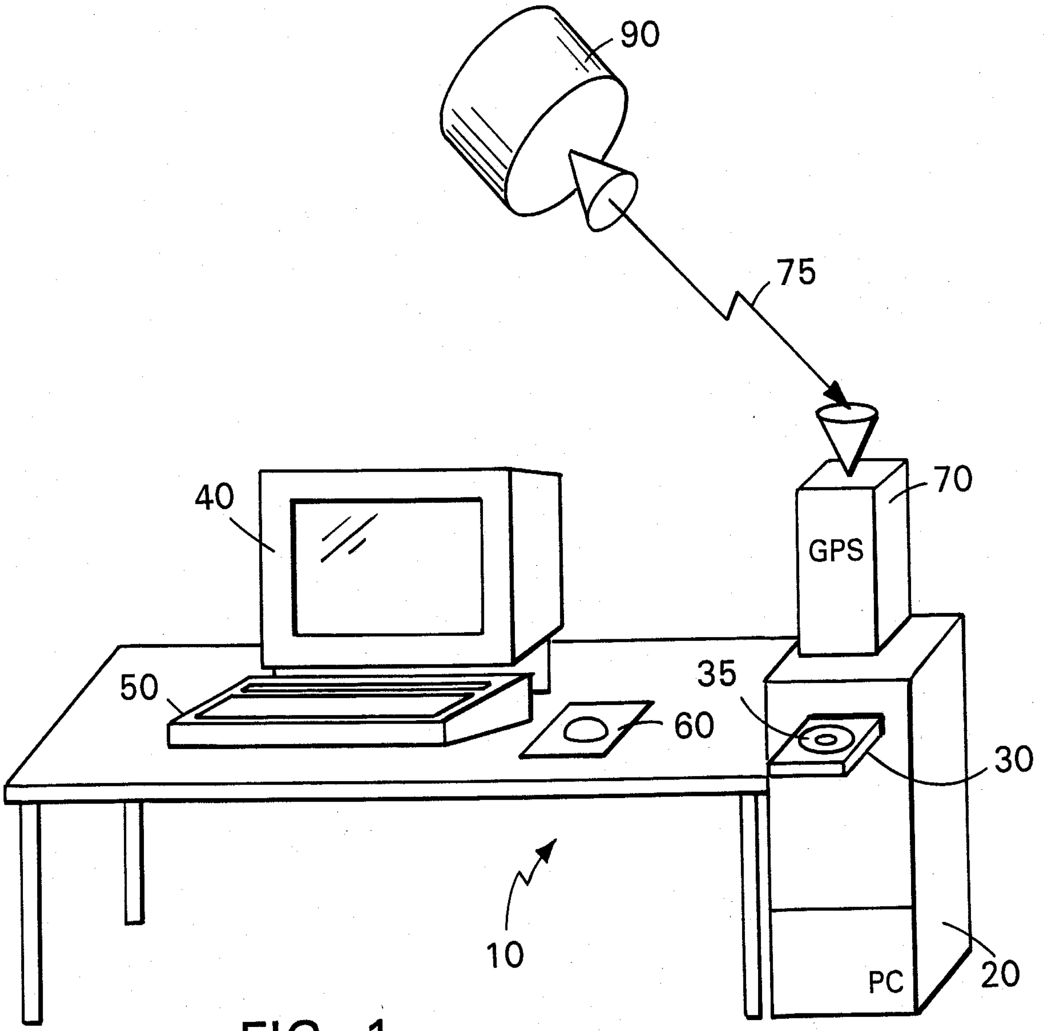


FIG. 1

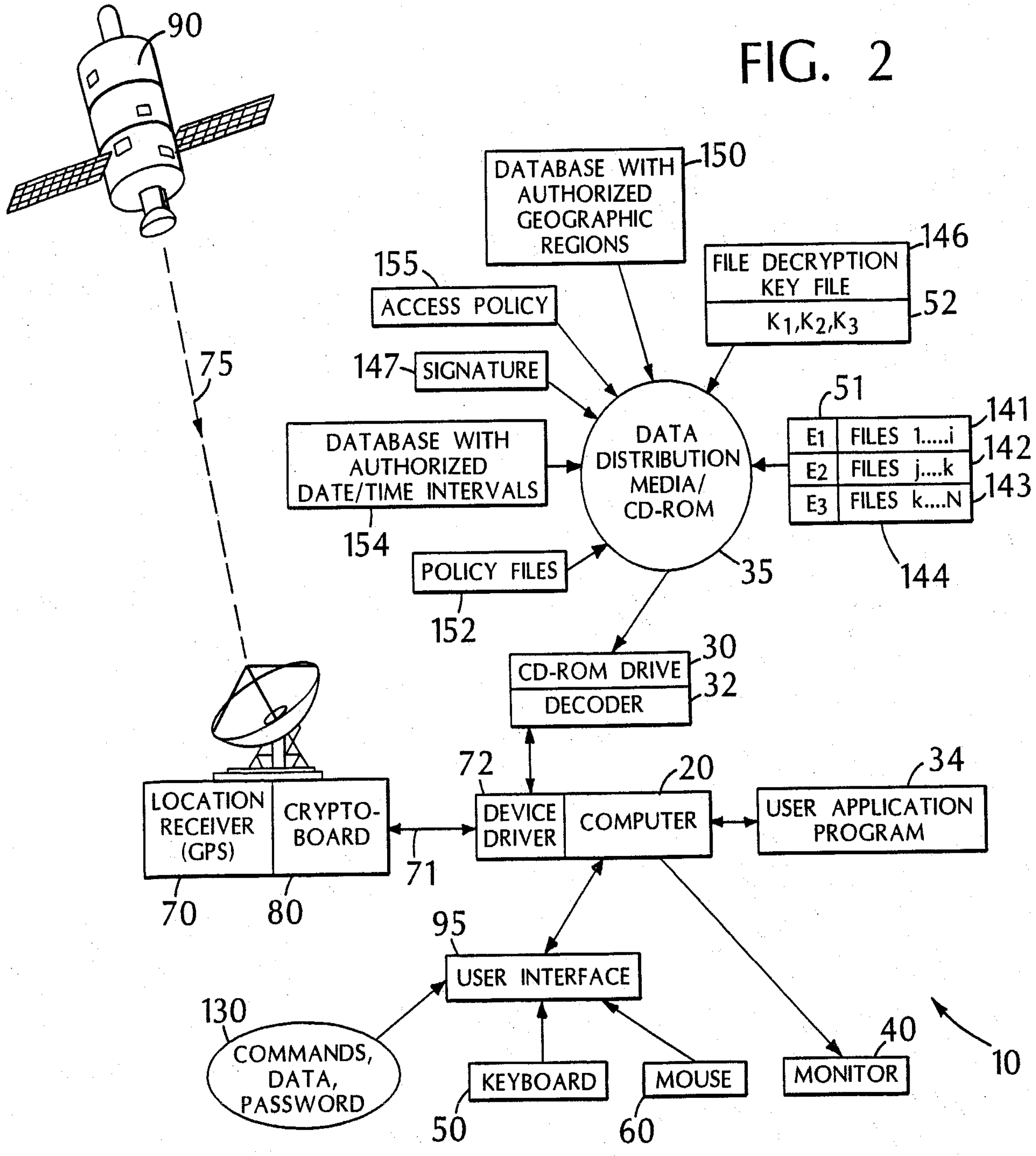
SPOOR AND FISHER
APPLICANTS PATENT ATTORNEYS

DATUM, INC.
COMPLETE SPECIFICATION
APPLICATION NO 99/6799

6 SHEETS
SHEET 2

2/6

FIG. 2



SPOOR AND FISHER

DATUM, INC.
COMPLETE SPECIFICATION
APPLICATION NO 99/6799

3/6

6 SHEETS
SHEET 3

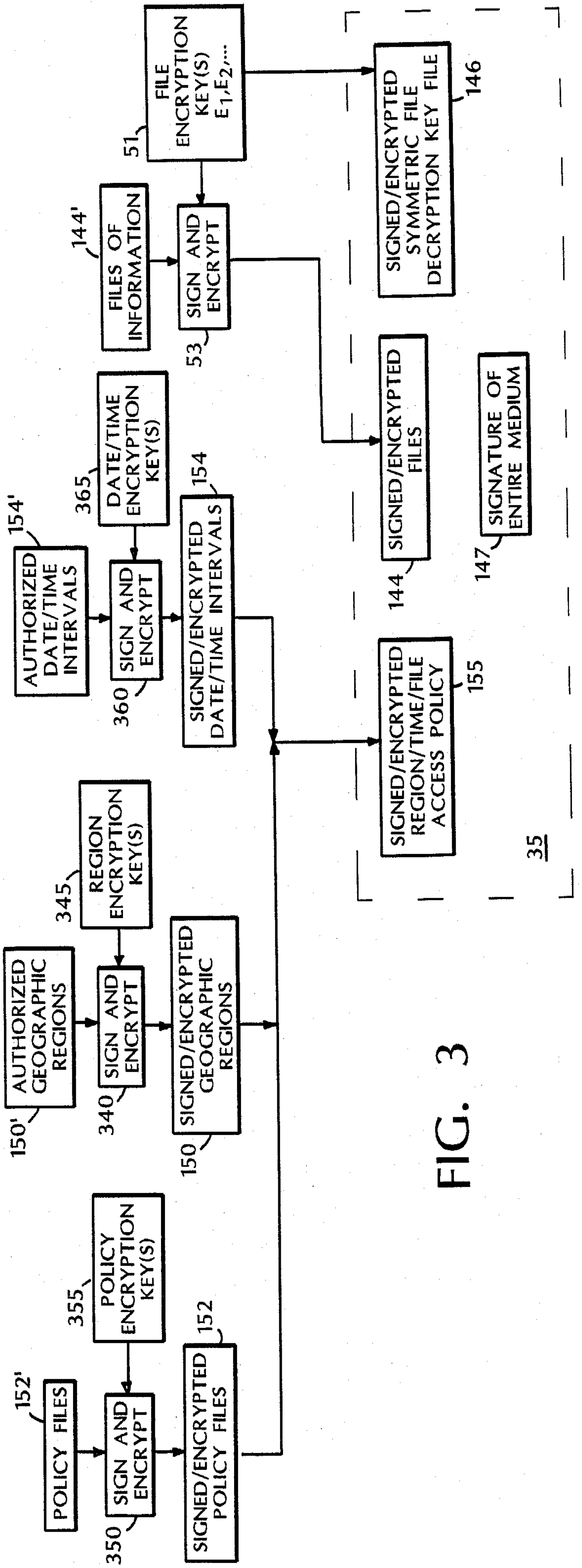

FILE ENCRYPTION KEY(S) $E_1, E_2, \ldots$
51
FILES OF INFORMATION
144'
SIGN AND ENCRYPT
53
SIGNED/ENCRYPTED SYMMETRIC FILE DECRYPTION KEY FILE
146
SIGNED/ENCRYPTED FILES
144
SIGNATURE OF ENTIRE MEDIUM
147
AUTHORIZED DATE/TIME INTERVALS
154'
DATE/TIME ENCRYPTION KEY(S)
365
SIGN AND ENCRYPT
360
SIGNED/ENCRYPTED DATE/TIME INTERVALS
154
SIGNED/ENCRYPTED REGION/TIME/FILE ACCESS POLICY
155
35
AUTHORIZED GEOGRAPHIC REGIONS
150'
REGION ENCRYPTION KEY(S)
345
SIGN AND ENCRYPT
340
SIGNED/ENCRYPTED GEOGRAPHIC REGIONS
150
POLICY FILES
152'
POLICY ENCRYPTION KEY(S)
355
SIGN AND ENCRYPT
350
SIGNED/ENCRYPTED POLICY FILES
152

FIG. 3

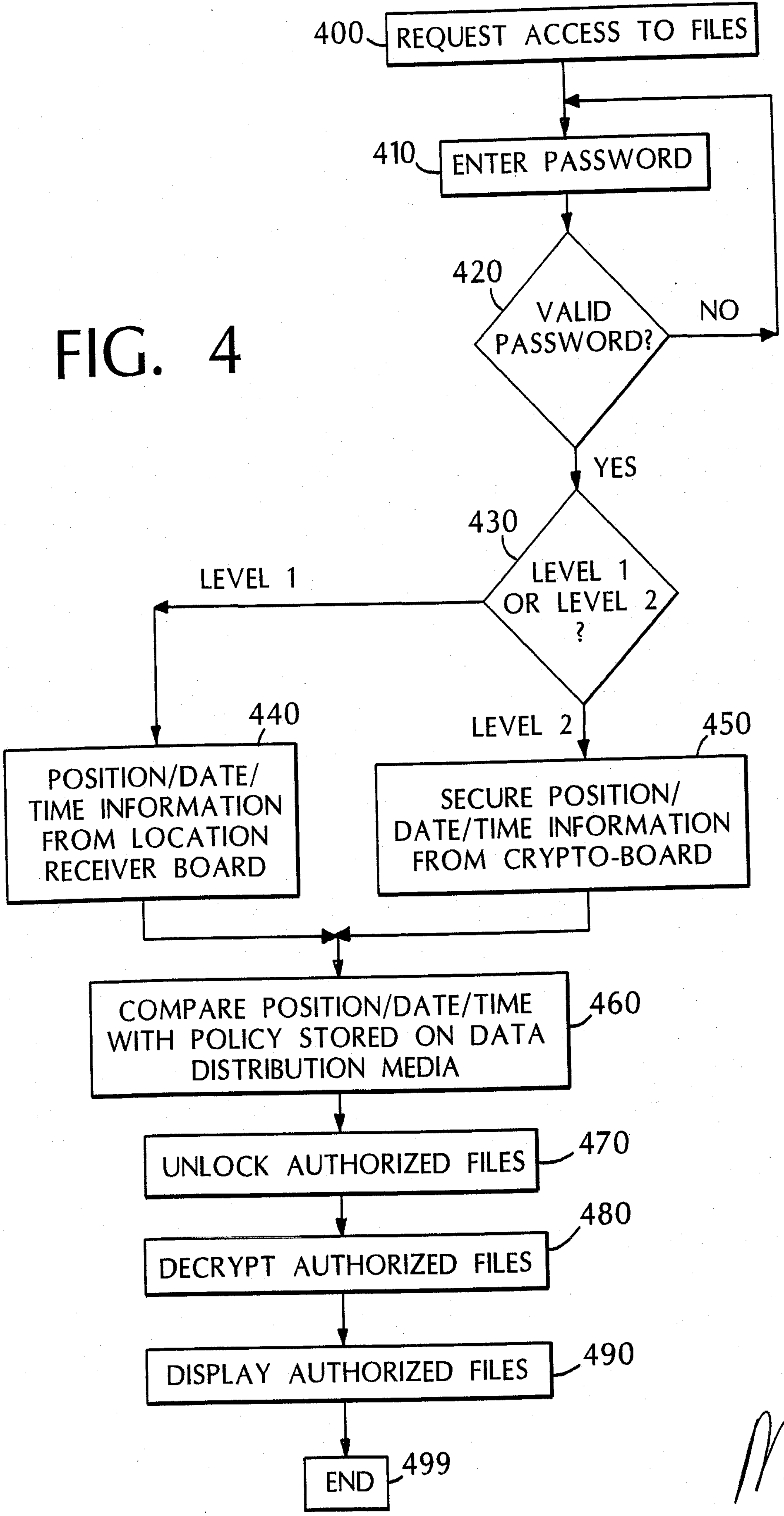
SPOOR AND FISHER

DATUM, INC.
COMPLETE SPECIFICATION
APPLICATION NO 99/6799

4/6

6 SHEETS
SHEET 4

FIG. 4



SPOOR AND FISHER

DATUM, INC.
COMPLETE SPECIFICATION
APPLICATION NO 99/6799

6 SHEETS
SHEET 5

5/6

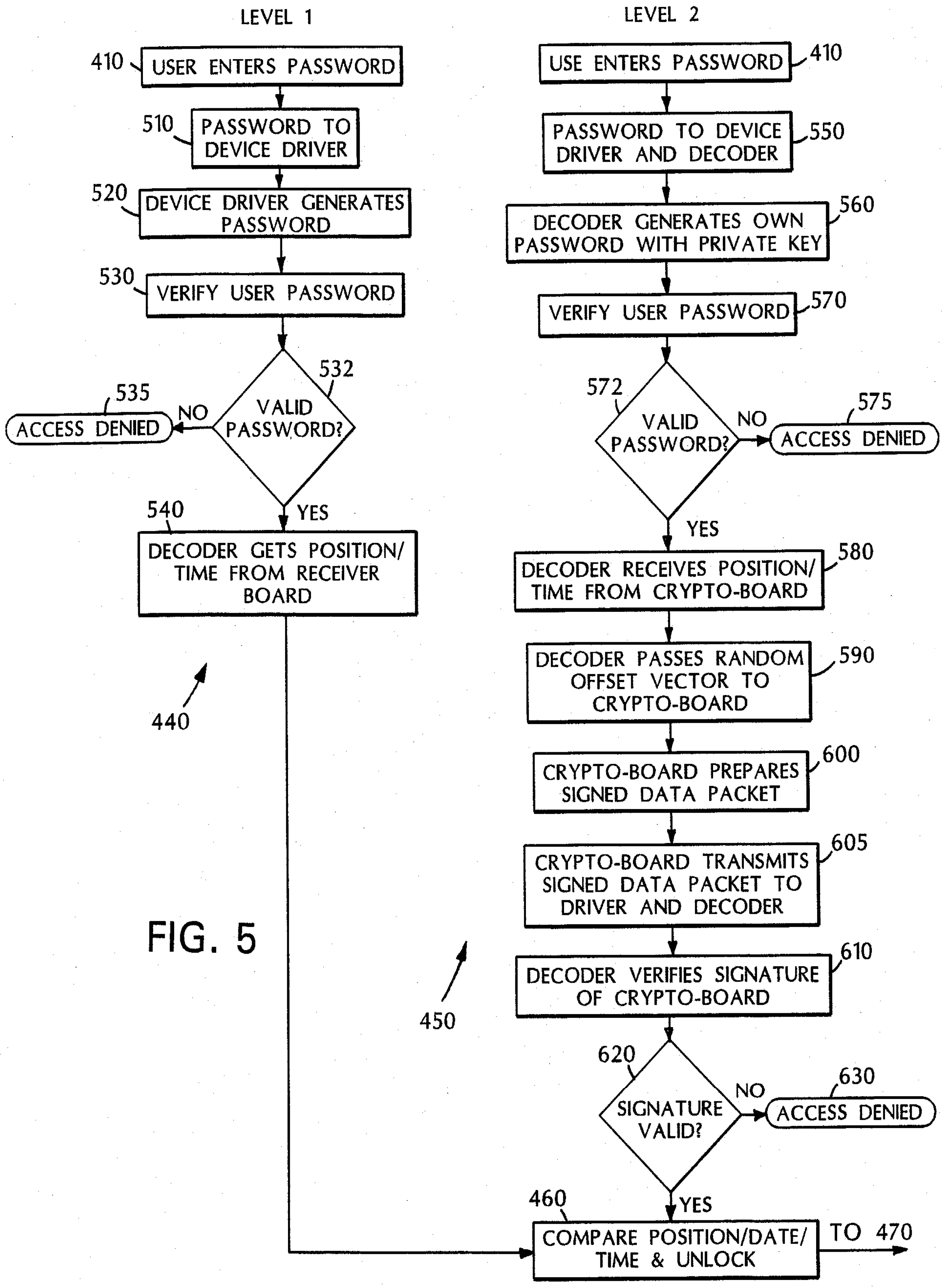

LEVEL 1
410
USER ENTERS PASSWORD
510
PASSWORD TO DEVICE DRIVER
520
DEVICE DRIVER GENERATES PASSWORD
530
VERIFY USER PASSWORD
532
VALID PASSWORD?
NO
535
ACCESS DENIED
540
YES
DECODER GETS POSITION/ TIME FROM RECEIVER BOARD
440
LEVEL 2
USE ENTERS PASSWORD
410
PASSWORD TO DEVICE DRIVER AND DECODER
550
DECODER GENERATES OWN PASSWORD WITH PRIVATE KEY
560
VERIFY USER PASSWORD
570
572
VALID PASSWORD?
NO
575
ACCESS DENIED
YES
DECODER RECEIVES POSITION/ TIME FROM CRYPTO-BOARD
580
DECODER PASSES RANDOM OFFSET VECTOR TO CRYPTO-BOARD
590
CRYPTO-BOARD PREPARES SIGNED DATA PACKET
600
CRYPTO-BOARD TRANSMITS SIGNED DATA PACKET TO DRIVER AND DECODER
605
DECODER VERIFIES SIGNATURE OF CRYPTO-BOARD
610
450
620
SIGNATURE VALID?
NO
630
ACCESS DENIED
460
YES
COMPARE POSITION/DATE/ TIME & UNLOCK
TO 470

FIG. 5

SPOOR AND FISHER

DATUM, INC.
COMPLETE SPECIFICATION
APPLICATION NO 99/6799

6 SHEETS
SHEET 6

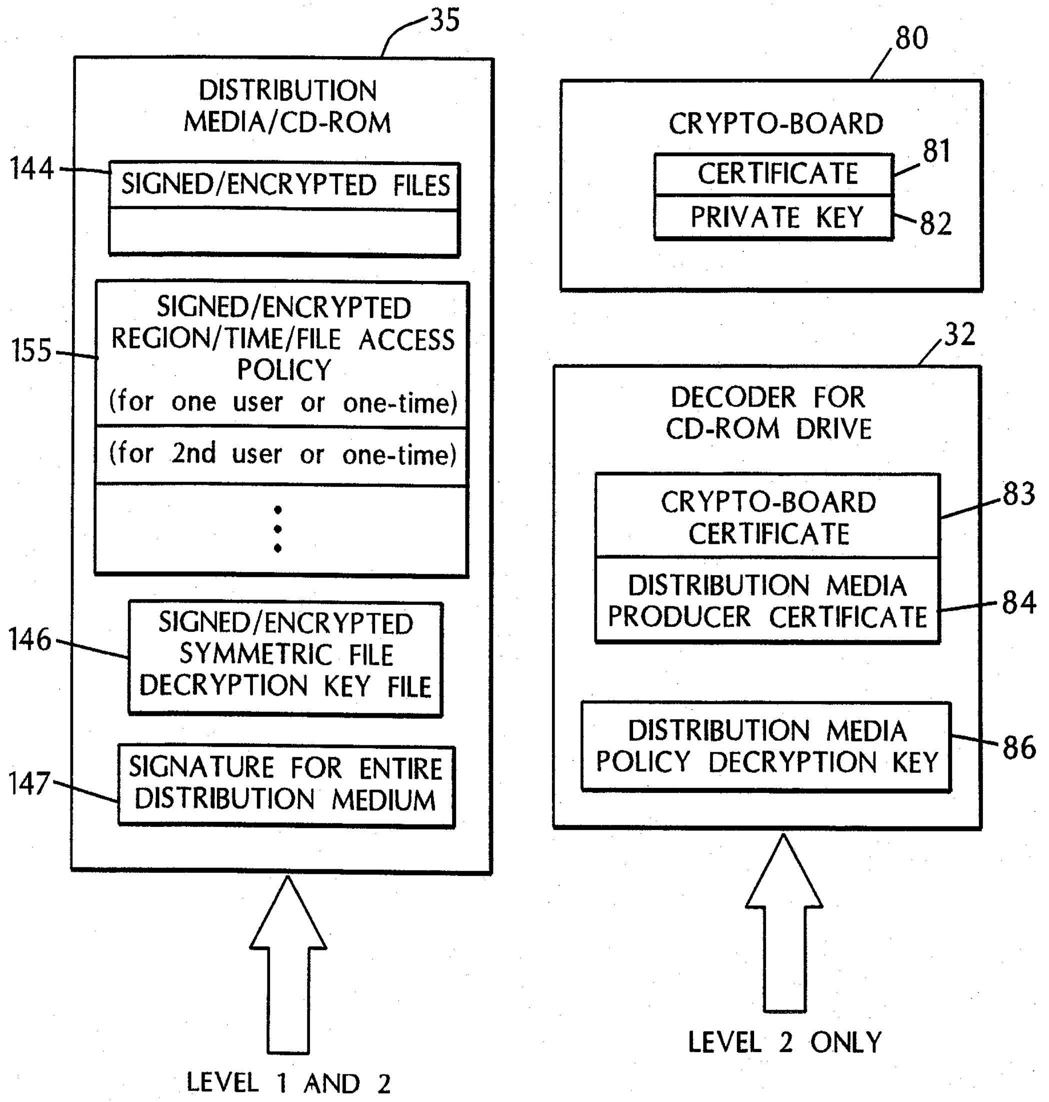

35
DISTRIBUTION MEDIA/CD-ROM
144
SIGNED/ENCRYPTED FILES
155
SIGNED/ENCRYPTED REGION/TIME/FILE ACCESS POLICY
(for one user or one-time)
(for 2nd user or one-time)
146
SIGNED/ENCRYPTED SYMMETRIC FILE DECRYPTION KEY FILE
147
SIGNATURE FOR ENTIRE DISTRIBUTION MEDIUM
LEVEL 1 AND 2
80
CRYPTO-BOARD
CERTIFICATE
81
PRIVATE KEY
82
32
DECODER FOR CD-ROM DRIVE
CRYPTO-BOARD CERTIFICATE
83
DISTRIBUTION MEDIA PRODUCER CERTIFICATE
84
DISTRIBUTION MEDIA POLICY DECRYPTION KEY
86
LEVEL 2 ONLY

FIG. 6

SPOOR AND FISHER

7402753

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 18, 2013

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE
DEPARTMENT OF COMMERCE

Certified by

David J. Kappos

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

FISH & RICHARDSON P.C.

225 Franklin Street
Boston, Massachusetts
02110-2804

Telephone
617 542-5070

Facsimile
617 542-8906

Web Site
www.fr.com

Frederick P. Fish
1855-1930

W.K. Richardson
1859-1951

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

October 29, 1998

Attorney Docket No.: **06175/006001**

Box Patent Application
Assistant Commissioner for Patents
Washington, DC 20231

Presented for filing is a new original patent application of:

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

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

	Pages
Specification	13
Claims	7
Abstract	1
Declaration	2
Drawing(s)	6

Enclosures:

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

"EXPRESS MAIL" Mailing Label Number EM529182920US

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 Mean

Ambrose Mean

October 29, 1998
Page 2

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

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

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

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

Please send all correspondence to:

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

Respectfully submitted,

David L. Feigenbaum
Reg. No. 30,378

Enclosures

330306.B11

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: CONTROLLING ACCESS TO STORED INFORMATION

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

"EXPRESS MAIL" Mailing Label Number EM529182192US

Date of Deposit OCTOBER 29, 1998

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

Ambrose Mean

AMBROSE MEAN

CONTROLLING ACCESS TO STORED INFORMATION

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. 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 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 crytographically 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 differnt sections of information which are applicable to corresponding specific countries and/or regions. A user may be permitted to see only the portion of the information which is applicable to his current geographic location. Likewiese, access to a sensitive corpoarte report may be limited to specific plant location. Access to time-sensitive information may be denied before or after a certain date or limited to a permitted period. By associating information about authorized geographic regions and time intervals with policy files stored on the CD-ROM and accessed with a user password, the CD-ROM producer can issue a new password to permit the user to access a particular set of policy files, and therefore the information authorized, for a corresponding region and date/time.

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

Description

FIG. 1 is a perspective view of a computer system;

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

FIGS. 3 through 5 are flow diagrams;

FIG. 6 is a block diagram of cryptographic elements.

As seen in FIGS. 1 to 3, access to information which is stored on a portable computer-readable CD-ROM which 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 authenication and encrypted data transmission between the receiver 70 and the decoder 32. The computer 20 can then be any commerical 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 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 access, or can be a one-time password. Alternately, the producer can associate specific geographic region/date/time information of lists 150 and 154 with the files 141, 142 and 143 via the policy files 152. A valid user password 130 may unlock one or more policy files 152. If the user's actual geographic position and the current date and time are within the authorized geographic region and the authorized date/time corresponding to the user password 150, then the user can access the selected files via the user interface 95. The selected information is then displayed on output device 40.

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

Table 1

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

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

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

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

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.

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;

comparing said actual geographic position with 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. The method of claim 1, further comprising:

cryptographically signing said 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 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. 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. 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; 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. The apparatus of claim 12, the receiver further comprising a receiver encryption mechanism providing a receiver encryption key for cryptographically signing the actual geographic position.

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

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

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

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

18. 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;

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. 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 which 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. 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;

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. 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 a inertial navigation system.

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

CONTROLLING ACCESS TO STORED INFORMATION

Abstract

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

318943.B11

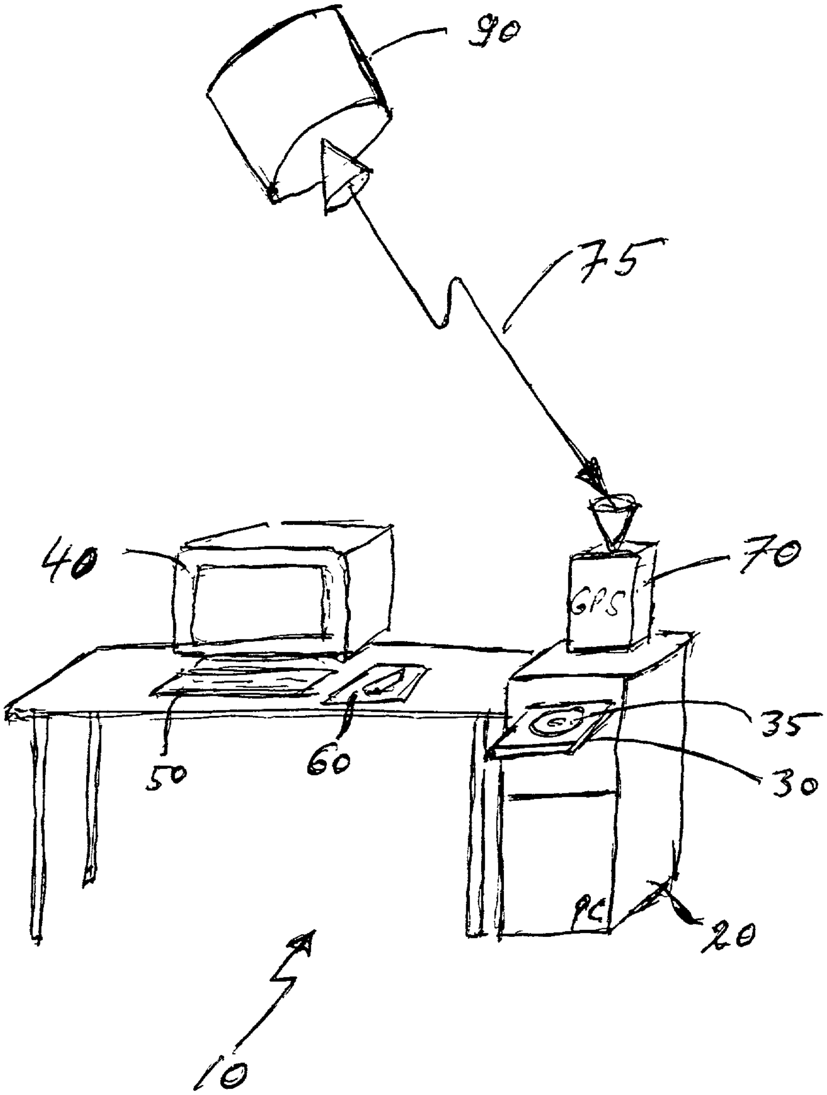


Fig. 1

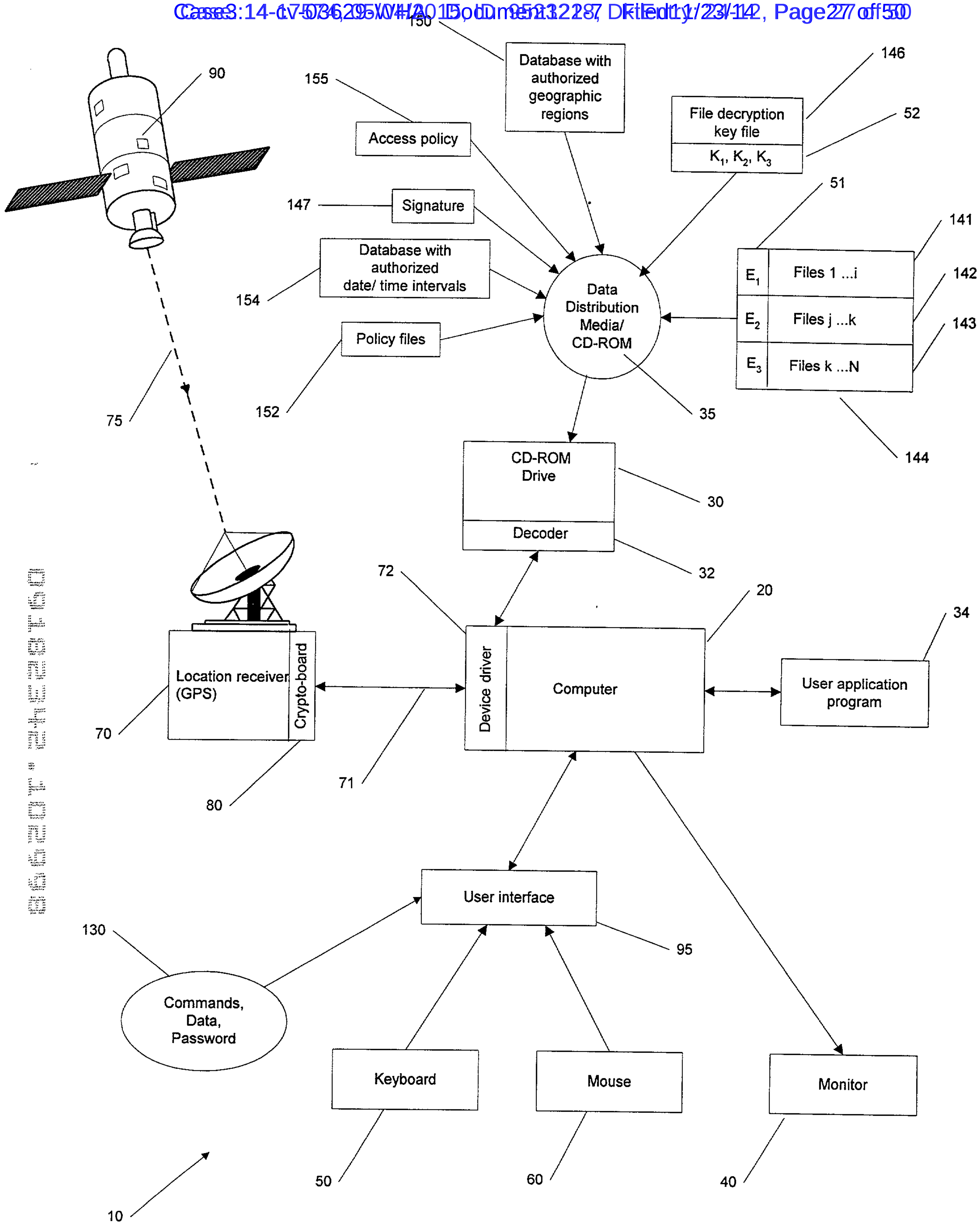

150
90
155
Database with authorized geographic regions
146
File decryption key file
52
K_1, K_2, K_3
Access policy
147
Signature
51
141
Database with authorized date/ time intervals
154
Data Distribution Media/ CD-ROM
E_1
Files 1 ...i
142
E_2
Files j ...k
143
E_3
Files k ...N
Policy files
152
75
35
144
CD-ROM Drive
30
Decoder
32
72
20
34
Location receiver (GPS)
Crypto-board
Device driver
Computer
User application program
70
71
80
User interface
130
95
Commands, Data, Password
Keyboard
Mouse
Monitor
50
60
40
10

FIG. 2

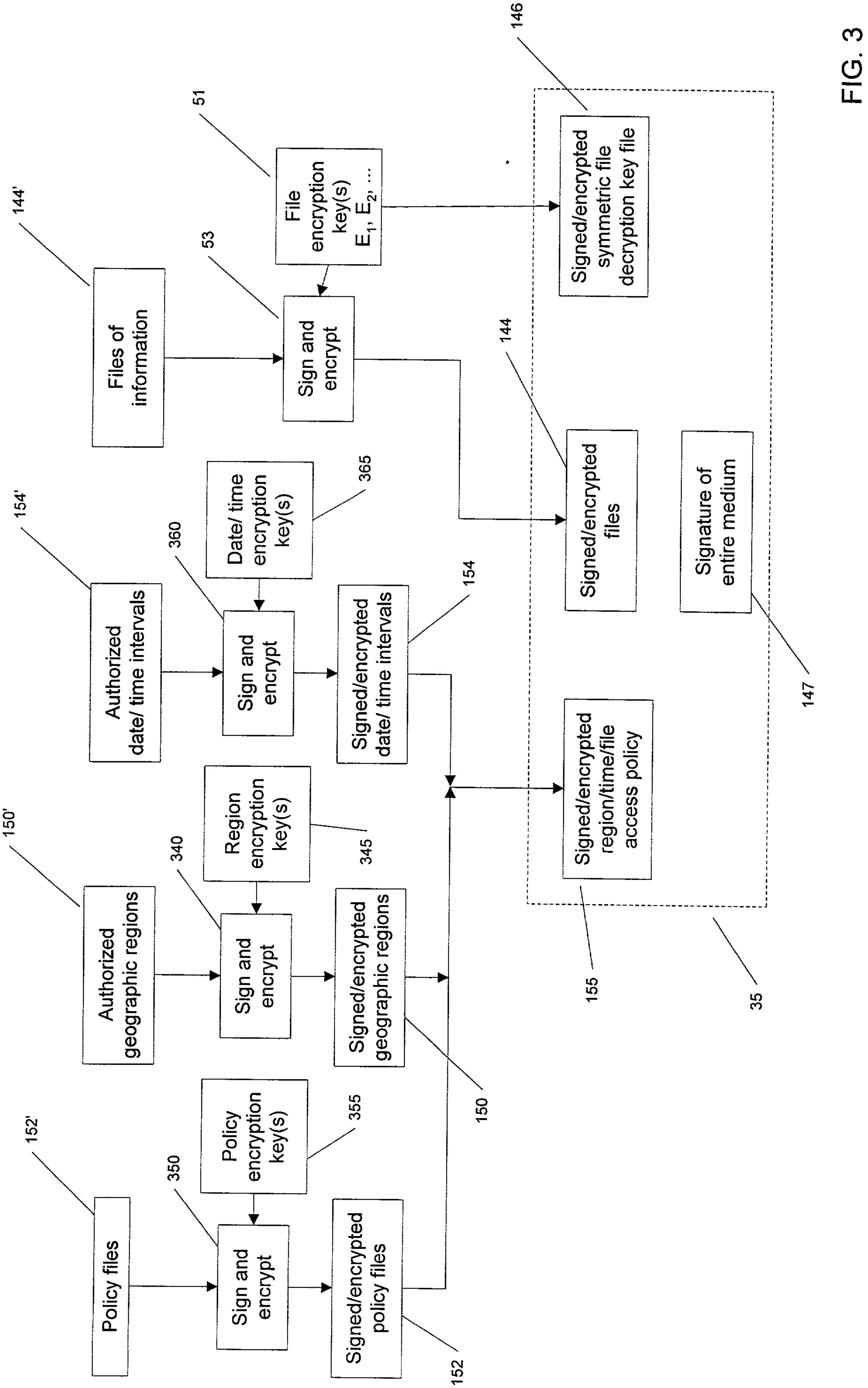

Files of information
144'
Sign and encrypt
53
File encryption key(s) $E_1, E_2, \ldots$
51
Signed/encrypted symmetric file decryption key file
146
Signed/encrypted files
144
Signature of entire medium
147
Authorized date/ time intervals
154'
Sign and encrypt
360
Date/ time encryption key(s)
365
Signed/encrypted date/ time intervals
154
Signed/encrypted region/time/file access policy
155
35
Authorized geographic regions
150'
Sign and encrypt
340
Region encryption key(s)
345
Signed/encrypted geographic regions
150
Policy files
152'
Sign and encrypt
350
Policy encryption key(s)
355
Signed/encrypted policy files
152

FIG. 3

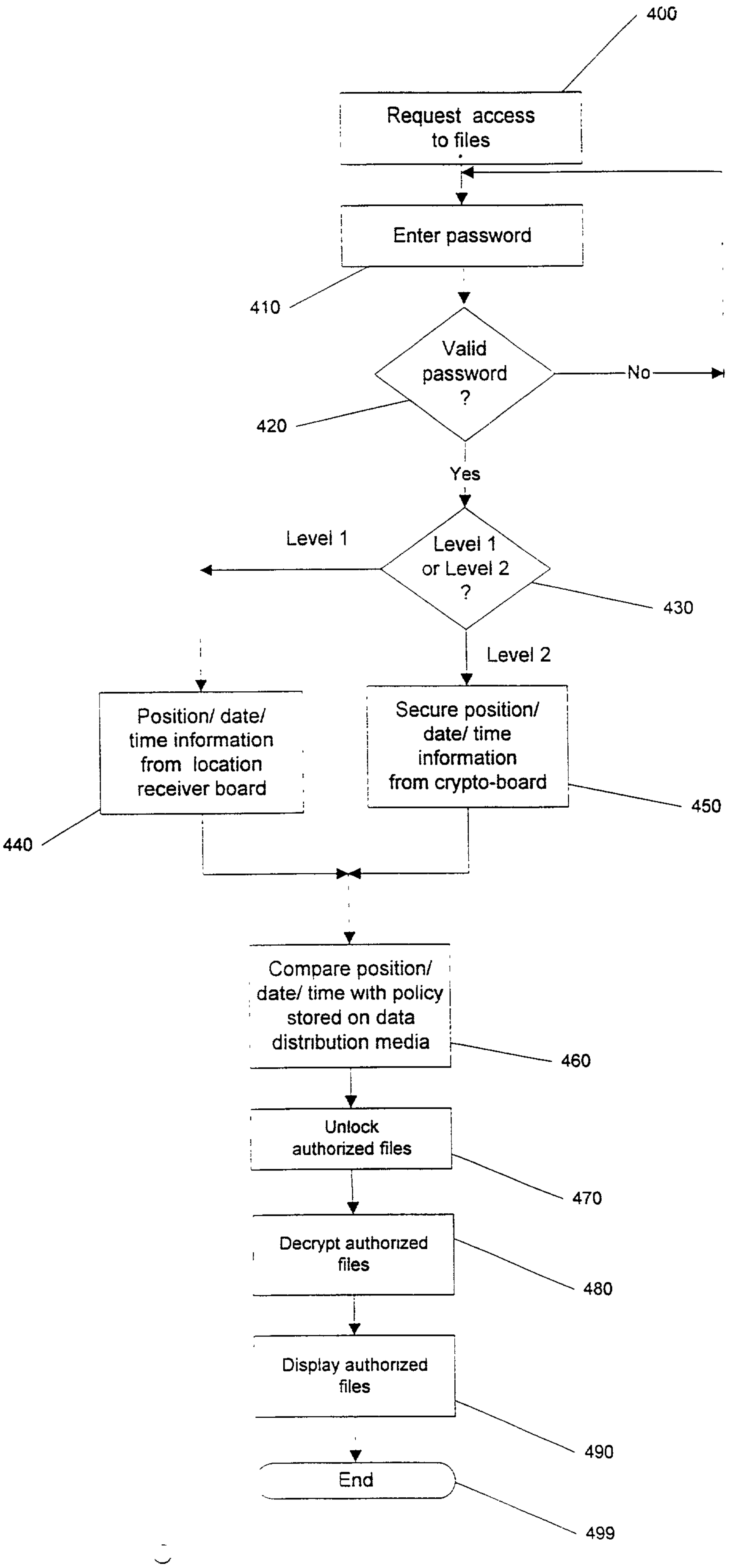

400
Request access to files
Enter password
410
Valid password ?
No
420
Yes
Level 1
Level 1 or Level 2 ?
430
Level 2
Position/ date/ time information from location receiver board
Secure position/ date/ time information from crypto-board
440
450
Compare position/ date/ time with policy stored on data distribution media
460
Unlock authorized files
470
Decrypt authorized files
480
Display authorized files
490
End
499

FIG. 4

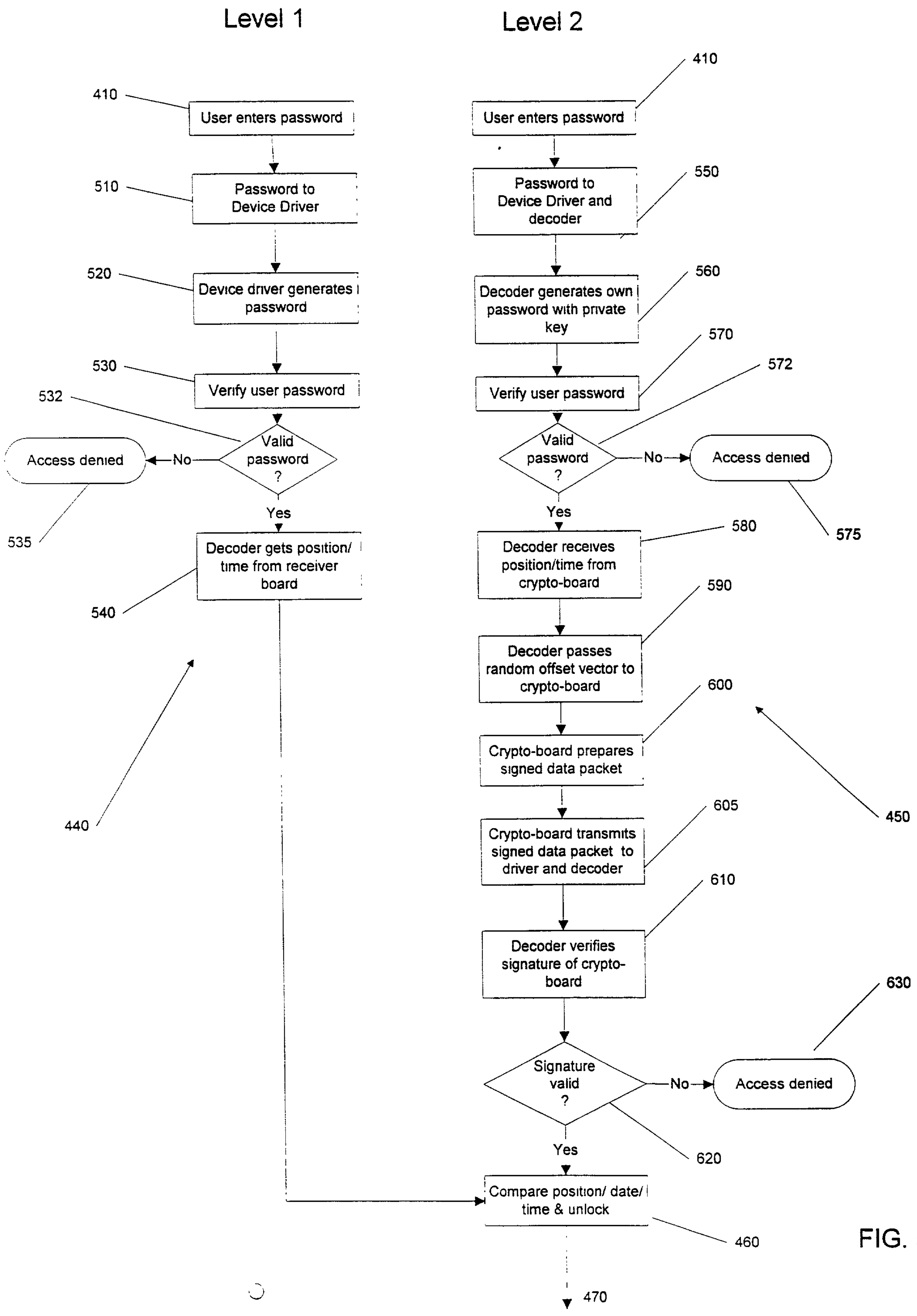

Level 1
Level 2
410
User enters password
510
Password to Device Driver
520
Device driver generates password
530
Verify user password
532
Valid password ?
No
Access denied
535
Yes
Decoder gets position/ time from receiver board
540
440
410
User enters password
550
Password to Device Driver and decoder
560
Decoder generates own password with private key
570
Verify user password
572
Valid password ?
No
Access denied
575
Yes
580
Decoder receives position/time from crypto-board
590
Decoder passes random offset vector to crypto-board
600
Crypto-board prepares signed data packet
450
605
Crypto-board transmits signed data packet to driver and decoder
610
Decoder verifies signature of crypto-board
630
Signature valid ?
No
Access denied
620
Yes
Compare position/ date/ time & unlock
460
470

FIG. 5

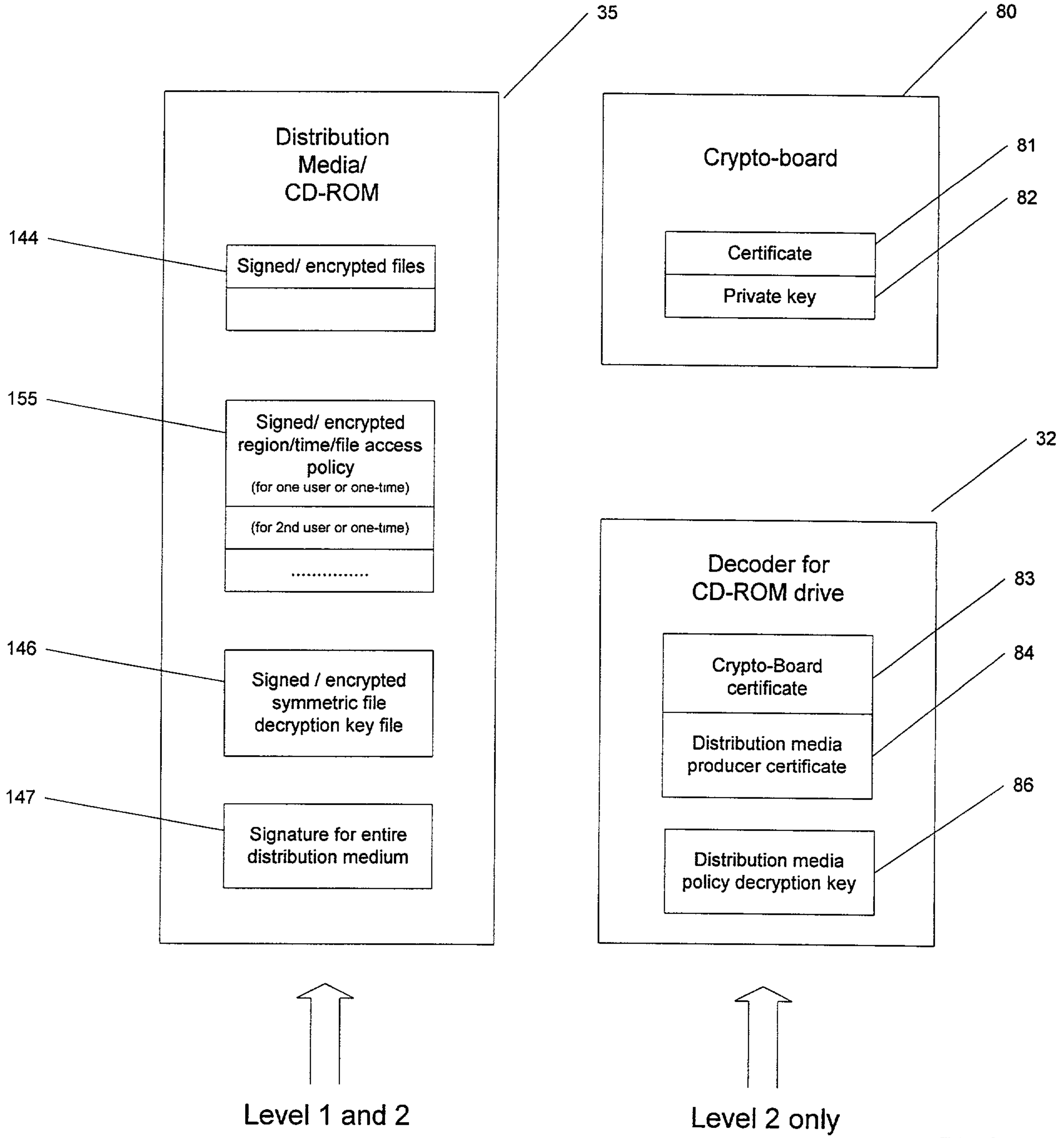

35
80
Distribution Media/ CD-ROM
144
Signed/ encrypted files
155
Signed/ encrypted region/time/file access policy
(for one user or one-time)
(for 2nd user or one-time)
....
146
Signed / encrypted symmetric file decryption key file
147
Signature for entire distribution medium
Crypto-board
81
82
Certificate
Private key
32
Decoder for CD-ROM drive
83
84
86
Crypto-Board certificate
Distribution media producer certificate
Distribution media policy decryption key
Level 1 and 2
Level 2 only

FIG. 6

PATENT
ATTORNEY DOCKET NO: 06157/006001

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

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

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

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

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

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

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

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

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

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

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

Full Name of Inventor: Thomas Mark Hastings

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

Residence Address: Lexington, MA

Citizen of: United States

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

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: Date: 27-Oct-98

Residence Address: Scotts Valley, CA

Citizen of: United States

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

Full Name of Inventor: Gerald L. Willett

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

Residence Address: Malden, MA

Citizen of: United States

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

330287.B11

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:
[x] an official of the small business concern empowered to act on behalf of the concern identified below:

Name of Small Business Concern: DIGITAL DELIVERY, INC.

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

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

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

[x] the specification filed herewith.
[ ] application serial no. , filed .
[ ] patent no. , issued .

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

Full Name: DIGITAL DELIVERY, INC.

Address: 54 Middlesex Turnpike, Bedford, MA 01730

[ ] INDIVIDUAL [x] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

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

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

Name: Thomas Mark Hastings

Title: President & CEO

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

Signature: Thomas Mark Hastings Date: 10/29/1996

PTO/SB/123 (01-06)
Approved for use through 12/31/2008. OMB 0651-0035
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Patent

Address to:

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

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

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

☒ The address associated with Customer Number 26290

OR

□ **Firm *or* Individual Name**

Address

City	**State**	**ZIP**
Country		
Telephone	**Email**	

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

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

I am the :

□ Patentee.

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

□ Attorney or agent of record. Registration Number ______.

Signature			
Typed or Printed Name	William Slater		
Date	Sept 4, 2007	Telephone	(408) 433-0910

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

☒ *Total of 1 forms are submitted.

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

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

PTO/SB/96 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Hastings, et al.

Application No./Patent No.: 09/182,342 Filed/Issue Date: April 9, 2002

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

SYMMETRICOM, INC. , a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

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

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

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

OR

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

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

2. From : Digital Delivery, Inc. To: Datum, Inc.
   The document was recorded in the United States Patent and Trademark Office at Reel 010456, Frame 0059, or for which a copy thereof is attached.

3. From: Datum, Inc. To: Symmetricom, Inc.
   The document was recorded in the United States Patent and Trademark Office at Reel 014120, Frame 0637, or for which a copy thereof is attached.

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

□ Copies of assignments or other documents in the chain of title are attached.
[NOTE: A separate copy (i.e., a true copy of the original document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

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

	Sept 4, 2007
Signature	Date
William Slater	(408) 433-0910
Printed or Typed Name	Telephone Number
Executive VP and CFO	
Title	

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

Electronic Acknowledgement Receipt

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

Payment information:

Submitted with Payment	no

File Listing:

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

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Change of Address	1	1
	Assignee showing of ownership per 37 CFR 3.73(b).	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	98753	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

SUBMISSION TYPE:	CORRECTIVE ASSIGNMENT
NATURE OF CONVEYANCE:	Corrective Assignment to correct the improper assignment w/o the missing Co-Inventor Agreement; makes assignment appear as Sale rather than Fiduciary Retainer previously recorded on Reel 009555 Frame 0985. Assignor(s) hereby confirms the (replace the Co-Inventor Agreement as part of the Assignment).

CONVEYING PARTY DATA

Name	Execution Date
Todd S Glassey	10/27/1998
Michael E McNeil	10/27/1998

RECEIVING PARTY DATA

Name:	Digital Delivery Inc
Street Address:	54 MIDDLESEX TURNPIKE
City:	Bedford
State/Country:	MASSACHUSETTS
Postal Code:	01730

PROPERTY NUMBERS Total: 1

Property Type	Number
Patent Number:	6370629

CORRESPONDENCE DATA

Fax Number:
Correspondence will be sent via US Mail when the fax attempt is unsuccessful.

Phone:	408-890-7321
Email:	tglassey@earthlink.net
Correspondent Name:	Todd Glassey
Address Line 1:	305 McGaffigan Mill Rd
Address Line 4:	Boulder Creek, CALIFORNIA 95006

ATTORNEY DOCKET NUMBER:	CV165643
NAME OF SUBMITTER:	Todd S. Glassey
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 10

source=DDI-Co-Inventor Agreement#page1.tif
source=DDI-Co-Inventor Agreement#page2.tif
source=DDI-Co-Inventor Agreement#page3.tif
source=DDI-Co-Inventor Agreement#page4.tif
source=DDI-Co-Inventor Agreement#page5.tif
source=DDI-Co-Inventor Agreement#page6.tif
source=Assignment#page1.tif
source=Assignment#page2.tif
source=assignment abstract for 6370629#page1.tif
source=assignment abstract for 6370629#page2.tif

CO-INVENTOR AGREEMENT

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

RECITALS

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

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

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

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

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

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

1. PATENT APPLICATION TECHNOLOGY

For purposes of this Agreement, the term:

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

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

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

2. AGREEMENT IN PRINCIPLE

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

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

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

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

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

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

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

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

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

3. FAILURE TO MAKE DEFINITIVE AGREEMENT

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

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

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

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

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

4. DEFAULT IN COMPENSATION

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

5. NONASSIGNABILITY

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

6. NOTICES

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

7. ATTORNEY FEES

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

8. INTEGRATION

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

9. SEVERABLILITY

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

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 34 Middlesex Turnpike, Bedford, Massachusetts, and its successors and assigns (collectively hereinafter called "the Assignee"), the entire right, title and interest throughout the world in the inventions and improvements which are subject of an application for United States Patent signed by us, entitled CONTROLLING ACCESS TO STORED INFORMATION, filed ______ ______, and assigned U.S. Serial Number ______________, and we authorize and request the attorneys appointed in said application to hereafter complete this assignment by inserting above the filing date and serial number of said application when known; this assignment including said application, any and all United States and foreign patents, utility models, and design registrations granted for any of said inventions or improvements, and the right to claim priority based on the filing date of said application under the International Convention for the Protection of Industrial Property, the Patent Cooperation Treaty, the European Patent Convention, and all other treaties of like purposes; and we authorize the Assignee to apply in all countries in our name or in its own name for patents, utility models, and design registrations and like rights of exclusion and for inventors' certificates for said inventions and improvements; and we agree for ourselves and our respective heirs, legal representatives and assigns, without further compensation to perform such lawful acts and to sign such further applications, assignments, Preliminary Statements and other lawful documents as the Assignee may reasonably request to effectuate fully this assignment.

IN WITNESS WHEREOF, I hereto set my hand and seal at Burlington Massachusetts, this 28 day of October, 1998

______________________________ L.S.
Thomas Mark Hastings

STATE OF Massachusetts :
: ss.
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.

____
Notary Public

My Commission Expires: 2/04/2005

[Notary's Seal Here]

this 27th day of October, 1998.

Michael McNeil L.S.
Michael E. McNeil

STATE OF California :
:ss.
COUNTY OF Santa Cruz :

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

[Notary's Seal Here]

My Commission Expires:
July 9, 2002

CHRIS REHN
Comm. # 1188423
NOTARY PUBLIC - CALIFORNIA
Santa Cruz County
My Comm. Expires July 9, 2002

IN WITNESS WHEREOF, I hereto set my hand and seal at Scotts Valley,
this 27 day of October 1998

Todd S. Glassey L.S.
Todd S. Glassey

STATE OF Ca :
:ss.
COUNTY OF Santa Cruz :

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

[Notary's Seal Here]

My Commission Expires:
July 9, 2002

CHRIS REHN
Comm. # 1188423
NOTARY PUBLIC - CALIFORNIA
Santa Cruz County
My Comm. Expires July 9, 2002

United States Patent and Trademark Office

Home | Site Index | Search | Guides | Contacts | eBusiness | eBiz alerts | News | Help

Assignments on the Web > Patent Query

Patent Assignment Abstract of Title

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

Total Assignments: 4

Patent #: 6370629 **Issue Dt:** 04/09/2002 **Application #:** 09182342 **Filing Dt:** 10/29/1998

Inventors: THOMAS MARK HASTINGS, MICHAEL E. MCNEIL, TODD S. GLASSEY, GERALD L. WILLET

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

Assignment: 1

Reel/Frame: 009555/0985 **Recorded:** 10/29/1998 **Pages:** 4

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors:	HASTINGS, THOMAS MARK	**Exec Dt:** 10/28/1998
	MCNEIL, MICHAEL E.	**Exec Dt:** 10/27/1998
	GLASSEY, TODD S.	**Exec Dt:** 10/27/1998
	WILLETT, GERALD L.	**Exec Dt:** 10/28/1998

Assignee: DIGITAL DELIVERY, INC.
54 MIDDLESEX TURNPIKE'
BEDFORD, MASSACHUSETTS

Correspondent: FISH & RICHARDSON P.C.
DAVID L. FEIGENBAUM
225 FRANKLIN STREET
BOSTON, MA 02110-2804

Assignment: 2

Reel/Frame: 010456/0059 **Recorded:** 12/15/1999 **Pages:** 2

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: DIGITAL DELIVERY, INC. **Exec Dt:** 11/08/1999

Assignee: DATUM, INC.
54 MIDDLESEX TURNPIKE
BEDFORD, MASSACHUSETTS 01730

Correspondent: FISH & RICHARDSON P.C.
DAVID L. FEIGENBAUM
225 FRANKLIN STREET
BOSTON, MA 02110-2804

Assignment: 3

Reel/Frame: 012721/0294 **Recorded:** 03/26/2002 **Pages:** 9

Conveyance: SECURITY INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: DIGITAL DELIVERY, INC **Exec Dt:** 07/07/2000

Assignee: WELLS FARGO BANK, N.A.
2030 MAIN ST

ORANGE COAST RCBO
IRVINE, CALIFORNIA 92614

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

Assignment: 4

Reel/ Frame: 014120/0637 **Recorded:** 06/02/2003 **Pages:** 15

Conveyance: MERGER (SEE DOCUMENT FOR DETAILS).

Assignor: DATUM, INC. **Exec Dt:** 02/03/2003

Assignee: SYMMETRICOM, INC.
2300 ORCHARD PARKWAY
SAN JOSE, CALIFORNIA 95131-1017

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

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

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

| .HOME | INDEX| SEARCH | eBUSINESS | CONTACT US | PRIVACY STATEMENT

STRADLING YOCCA CARLSON & RAUTH

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
660 NEWPORT CENTER DRIVE, SUITE 1600
NEWPORT BEACH, CA 92660-6422
TELEPHONE (949) 725-4000
FACSIMILE (949) 725-4100

JOHN F. CANNON
DIRECT DIAL: (949) 725-4107
JCANNON@SYCR.COM

SAN FRANCISCO OFFICE
44 MONTGOMERY STREET, SUITE 4200
SAN FRANCISCO, CALIFORNIA 94104
TELEPHONE (415) 283-2240
FACSIMILE (415) 283-2255

SANTA BARBARA OFFICE
302 OLIVE STREET
SANTA BARBARA, CALIFORNIA 93101
TELEPHONE (805) 564-0065
FACSIMILE (805) 564-1044

May 4, 2000

By Federal Express

Mr. Todd S. Glassey
Mr. Michael E. McNeil
1271 Los Acre Drive
Felton, CA 95018-9179

Re: *Datum, Inc.*

Dear Messrs. Glassey and McNeil:

On April 12, 2000 I sent you a letter requesting your signatures on an Assignment of Invention for the South African Patent Office relating to the Controlling Access Patent. Two weeks have passed and I have not received any response from either of you.

Section 8.7 of the Co-Inventor Agreement under which each of you acknowledged assignment of the Controlling Access patent to Datum, signed by both of you, requires you to "take any acts, and execute any further documents, that may be reasonably necessary to accomplish and effect the terms of this Agreement." Signing this form confirming the assignment of the Controlling Access Patent as required by the South African Patent Office for Datum to acquire an effective patent in that country clearly is an act contemplated by Section 8.7 of the Co-Inventor Agreement. Thus, your failure to sign the assignment confirmation or respond in any way to our April 12, 2000 correspondence is a violation of the Co-Inventor Agreement for which Datum may seek to recover damages and/or injunctive relief and recover its attorney's fees in enforcing its rights.

However, litigation should not be necessary to compel your performance of such a simple and quick task. We have enclosed a self-addressed Federal Express envelope to facilitate the process. My client does not want to have to resort to further litigation, however, we must have the signature as soon as possible. Thus if we do not receive the signed form by May 9, 2000, be assured that we will do everything necessary to protect our client's rights under the Co-Inventor Agreement.

Mr. Todd S. Glassey
Mr. Michael E. McNeil
May 4, 2000
Page Two

If you have any questions please give me a call at (949) 725-4107.

Very truly yours,

STRADLING YOCCA CARLSON & RAUTH

John F. Cannon

JFC:jmv
Enclosure

cc: Erik H. van der Kaay
Thomas Mark Hastings

CO-INVENTOR AGREEMENT

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

RECITALS

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

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

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

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

Exhibit C - Co-Inventor Agreement

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. SEVERABLILITY

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

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

Michael E McNeil In Pro Se
Michael E McNeil In Pro Se
PO Box 640
Felton CA, 95018-0640
831-246-0998
memcneil@juno.com

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No.: 14-CV-3629-WHA

Date: December 26th 2014
Time: 8 AM
Courtroom 8
Judge W.H. Alsup

RENOTICE OF MOTION AND MOTION FOR PARTIAL SUMMARY JUDGEMENT VOIDING DDI (US6370629) SETTLEMENT AND TTI (US6393126) SETTLEMENT

RENOTICE OF MOTION AND MOTION FOR PARTIAL SUMMARY JUDGEMENT VOIDING DDI (US6370629) SETTLEMENT AND TTI (US6393126) SETTLEMENT

1. May it please the Court, to consolidate all Plaintiffs pre-CMC Motions, On December 26th 2014 at 8AM or as soon as may be considered, the Plaintiffs will move the Court for a finding BOTH the TTI Settlement (pertaining to US Patent US6393126) and its carbon copy the DDI Settlement (pertaining to US Patent US6370629) as VOID based on their being missing the key components pertaining to infringement and noticing therein being missing as well as other important components.

2. Be advised this refiling replaces DOCKET 118 and as such is associated with DOCKET 119 and 120; we request Judicial Notice of those matters herein.

3. Plaintiffs believe in the case of the TTI Settlement additional grounds for declaring the Settlement void exist per the Gellman Precedent which supports that there is and was no intent to allow Microsemi to file any patent from the Settlement Rights in the US or Abroad, and as such we ask that the Court additionally take that into consideration in ordering the TTI settlement voided with the DDI settlement. As such a Partial Summary Judgment against Count-1 for the claims as listed is requested.

Plaintiffs Recovery of the executed contract for the DDI settlement

Plaintiffs had a set of settlements extorted from them which the parties who extorted the settlements then made one of the two settlements invalid by withholding it from Plaintiffs and claiming to Defendants named herein that it didnt exist.

Finally after 12 and 3/4 years Symmetricom (Microsemi) external lawyer John Burton "refused" we believe to continue to be an active part of the fraud going on and forced his client to turn over the document.

Today after 13 years Plaintiff's finally have had the DDI Settlement Contract withheld from them by MICROSEMI. In that period Clients allege that Microsemi committed ongoing frauds with its partners. What Plaintiffs seek here is a formal court review on the enforceability of the Settlement Contracts in light of their apparently being Voided based on the standard in Talbot.

Talbot v Quaker State should void both Settlements

Now that Plaintiffs have an executed copy of the DDI Settlement Agreement we need to enforce its terms in providing Plaintiffs third party enforcement rights or have it declared void under the Standard and Precedent set in Shared-Use Patent Contracts by the US Supreme Court in the 1939 TALBOT v QUAKER STATE OIL REFINERY Case.

Filing is Timely

This is a key question which probably should have been filed in this matter first. Further its timely in its filing as the Recovery of the first executed copy of the DDI Settlement document from Microsemi lawyers happened Feb 26th 2013. It had been withheld from Plaintiffs and its existence denied by Microsemi Lawyers and Corporate Officers for 12 years previous.

CONCLUSION

Plaintiffs ask the Court declare both Settlements VOID for cause and precedent, ordering that PLAINTIFFS be awarded full custody of both the 629 and 992 patents per the terms of the CO-INVENTOR AGREEMENT.

x // Todd S. Glassey, In Pro Se 10-23-2014
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321

x // Michael E McNeil In Pro Se, 10-23-2014
Michael E McNeil In Pro Se
PO Box 640
Felton CA, 95018-0640

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

[PROPOSED] ORDER Granting Plaintiffs Motion for Partial Summary Judgment Voiding Settlements

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: December 26th, 8AM
Date: 9th December 2014

For good cause the motion is hereby granted. The following CONTRACT Settlements are reviews and found void by this the Trial Court under TALBOT and other related standards.

_____ DDI Settlement pertaining to US6370629 and all of its associated filings

_____ TTI Settlement pertaining to US6393126 and the Trusted Timing Infrastructure

Witness my hand, Judge WH Alsup, ___________________, Dated ________ 2014

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

SUPPLEMENTAL EVIDENCE - CONTRACTS FOR DOCKET 118 REVIEW

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: December 9th, 8AM
Date: 9th December 2014

I Todd S. Glassey declare under the Penalty of Perjury of the Laws of the United States Of America the following.

The Attached CO-INVENTOR AGREEMENT is necessary for review of DOCKET 118-120.

The Attached Copies of the TWO CONTRACTS are the SETTLEMENT AGREEMENTS to be reviewed for DOCKET118-120 matters. They were not filed with 118 because they will be used with multiple motions and so are being attached to the 118 matter through this filing (*DOCKET 121).

/s/ Todd S. Glassey, 11/222014

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

Todd S. Glassey In pro Se
305 McGaffigan Mill Road
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

Michael E. McNeil
PO Box 640
Felton CA 95018-0640
831-246-0998
memcneil@juno.com

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case Number: C3:14-CV-03629-WHA

Date: December 19th 2014
Time: 8 AM
Courtroom 8
Judge W.H. Alsup

MEMORANDUM OF POINTS AND AUTHORITIES PERTAINING TO CALIFORNIA STATE CONTRACT RESCISSION STANDARDS AND THE SETTLEMENT AGREEMENTS

Table of Contents

Cases

Statutes

Memorandum of Points and Authorities

1. Microsemi's failure to perform cause PLAINTIFFS to notice Microsemi all Settlements were noticed as rescinded under California Rescission Standards including the Assignment Documents with USPTO which were executed under the umbrella of this California Law-framed Contract.

Framing events

2. Over the last 12 years PLAINITFFS have repeated tried to get Microsemi (as Datum, then as Symmetricom, and now as Microsemi) to honor specific terms required by various agreements between the parties. They have in all instances been either Ultra Vires in their actions against Plaintiffs as well as Deceptive in their Practices as evidenced by a number of unauthorized global filings for US6370629 and all of the unauthorized filings for

US6393126. As such Plaintiffs formally notified Attorney Peter Chen in 2010 that they wert formally triggering the Arbitration Clause in one last desperate effort to get the contracts terms met and Microsemi refused to participate in that Arbitration at all. In doing so Plaintiffs finally exhausted their possible remedies and rescinded both the Settlement and Interim Assignment Documents per the Below California Law precedent which each of those documents are fully controlled by.

HISTORY: June 2009 Notice

3. Microsemi was noticed to stop using any PHASE-II IP outside of the authorized limited uses provided in the Licensing Statements in the TTI Settlement and that they were to stop all uses of DDI technologies outside of Confidential Courier Products entirely.

HISTORY: Arbitration and Rescission Notice

4. 12 months later in June of 2010 Plaintiffs served Microsemi Attorney Peter Chen of Lathem Watkins LLP in Menlo Park (now his Honor AL Judge Peter Chen of USPTO) that all Settlements were formally rescinded and with the arbitration demand in them PLAINTFFS were invoking that clause, which Microsemi ignored triggering the FINAL SETTLEMENT terms in the failure to perform section.

REMEDY PRECEDENTS

5. Remedy Precedents in California provide for direct rescission of th3 assignment documents and any subsidiary documents filed with US Government based on those agreements, and even though no notice of this is necessary it was given to MICROSEMI several times and was ignored in all instances.

Rescission (Nelson v. Sperling, 270 Cal. App. 2d 194, 195, 76 Cal. Rptr. 481, 482 (1969) (failure of consideration for rescinding party's obligation, in a material respect and from any cause, is sufficient basis for unilateral rescission)).

The withholding of the settlement contract for 12 years was grounds for its rescission alone, The unlawful filing of the patents in six foreign nations is additionally grounds for this rescission.

No Notice of Rescission Required (Benson v. Andrews, 138 Cal. App. 2d 123, 136, 292 P.2d 39, 47 (1955) (defendant was not required to give notice of rescission after discovering that plaintiff builder abandoned his construction obligations); see also Russ Lumber & Mill Co. v. Muscupiabe Land & Water Co., 120 Cal. 521, 527, 52 P. 995, 997 (1898)).

Plaintiffs have no obligation to notice anyone other than PTO and they were formally noticed in 2010 and 2011 with complaints filed with the Commissioner of Patents for USPTO.

Plaintiffs rights in rescinding contract returned the Patents to their Control

6. Under California Precedent Plaintiffs noticed Defendants to stop using their IP that the Assignment Documents were void for incomplete and ineffective because they were formally rescinded under California Law Precedent as show below.

7. Plaintiffs had suffered damages warranting rescission based on Microsemi's refusal to turn over the executed copy of the DDI settlement; An act PLAINTIFFS assert was done to prevent this Court from reviewing the enforceability and other actions done by Microsemi as

evidenced in Patent Filing Reports as attached to this Memorandum of Points and Authorities.

Delay in Performance/"Time Is of the Essence"

8. As defined in Holland a mere delay in performing a contract is not a material breach unless the delay is such as to warrant the conclusion that the party does not intend to perform. In this case though the breach is to egregious and so damaging to Plaintiffs rescission was the only course of action since Plaintiffs withheld executed contract from plaintiffs so they could not obtain formal court review of its effectiveness or requirements in ongoing maintenance for the parties therein. This violated the standard set in Hofland v. Gustafson, 132 Cal. App. 2d Supp. 907, 909-10, 282 P.2d 1039, 1041 (1955) (eight-day delay in plaintiff's receipt of insurance proceeds after signing release form was not such a material breach as to give plaintiff right to rescind release).

9. Under California Precedent the failures to meet the terms of the Settlement Agreements caused them to be able to be able to be rescinded in form fully. The un-noticed filings in foreign nations, the refusal to fully define what components inside the US6370629 claims were part of 992 and which were part of PHASE-II technologies owned by PLAINTIFFS, and the actions in concert with their Resellers in adding PLAINTIFFS other IP's to products they sell now or have sold off to other entities (Thales Group) fully supports this as well

PRECEDENT: Willful Failure to Perform

10. A willful default may be material even though the innocent party suffers no economic loss. Coleman v. Mora, 263 Cal. App. 2d 137, 150, 69 Cal. Rptr. 166, 173 (1968) (owner was justified in rescinding exclusive listing agreement where broker did not produce any prospective buyers and made only

nominal efforts to advertise property); Wilson v. Corrugated Kraft Containers, Inc., 117 Cal. App. 2d 691, 697, 256 P.2d 1012, 1016 (1953) (fact that seller might have sold its product elsewhere did not diminish the materiality of buyer's failure to purchase its requirements from seller).

11. The Willful Failure to Perform on the Settlement Contract Terms and its unlawful extortion from Plaintiffs in the first place as an act mandating rescission of the underlying agreement is fully supported.

PRECEDENT: Failure to Execute a Promise

12. That the contracts are missing pieces is key, those components form other parts of the agreement which was breached.

> **<u>The promise that is breached need not be expressly stated in the contract.</u>** Bliss v. California Coop. Producers, 30 Cal. 2d 240, 249, 181 P.2d 369, 374 (1947) (even in absence of express promise and fixed time for performance in contract, court implied promise by corporation to market and process growers' agricultural products and pay insurance premiums for at least ten years where growers had given corporation notes payable in annual installments over ten years as an extension of credit to corporation).

13. PLAINTIFFS were entitled to demand rescission based the scope of the Settlement, how it was obtained, and the breeches of the Settlement itself along the initial acts and certainly for the unauthorized filings of Patents in foreign nations not included in those listed WITH the settlement at the time of its signing, another of the amendments to the contract which disappeared over the years. The supporting grounds are that a party may rescind for partial failure of consideration even if

there has been partial performance by the party against whom the rescission is sought. Coleman v. Mora, 263 Cal. App. 2d 137, 150-51, 69 Cal. Rptr. 166, 173-74(1968) (principal had right to rescind brokerage agreement after broker had had a reasonable time to perform his obligations and failed to do so).

14. PLAINTIFFS were entitled to demand rescission based on the Coleman v Mora standard in California Courts alone.

> For a breach to justify abandonment of the contract, the promise must “go to the root of the contract,” so that a failure to perform it would render the performance of the rest of the contract different in substance from what was contracted. Walker v. Harbor Bus. Blocks Co., 181 Cal. 773, 780, 186 P. 356, 359 (1919).

15. The breach in this instance is simply total denial of access to PLAINTIFFS IP RIGHTS causing an IRC Fraud Loss of staggering size for the enforcement losses against US6370629 along the Pacific Rim and European as well as South American and US/Canadian Commerce centers those abandoned and rights withheld patents inflicted on PLAINTIFFS.

Plaintiffs Rights are further strengthened by Associated Lathing and Plastering

16. A key California Precedent called Associated Lathing and Plastering is key here. In Associated we read:

> The timing of the breach is relevant in determining the materiality of the breach. A breach prior to or at the outset of performance may justify rescission when the same breach late in performance would not be significant. When the failure to perform is at the outset, it is helpful to consider whether it would be more just to

> free the injured party or to require him to perform his promise, in both cases giving the injured party a right of action if the failure to perform was wrongful. Associated Lathing and Plastering Co. v. Louis C. Dunn, Inc., 135 Cal. App. 2d 40, 50, 286 P.2d 825, 830 (1955) (subcontractor materially breached contract by failing to cooperate with general contractor on several occasions, even though dollar amounts involved were relatively minor, because contract provided that time was of the essence, and all indications were that subcontractor's delay and failure to cooperate were going to continue throughout term of contract).

17. In the context of the Rescission Demands, PLAINTIFFS have asserted that the Assignments were formally rescinded under the above and below precedents and they were to stop using the IP. USPTO was also formally noticed of this as well as various frauds pertaining to US6393126 as well as those pertaining to US6370629 the DDI/GMT Controlling Access Patent.

Microsemi's failure to pay for the foreign Patent Filings is a willful default.

18. Per the following standard, Microsemi's willful refusal to pay the publication fee on several of the foreign patents including JAPAN, CANADA, the EU, South Korea, and South Africa on violated the Timely Payment Requirements in the management of the patents. The Payment Demand to Microsemi from the PATENT AGENCIES from those governments named triggered this responsibility per the below precedent

> When no time is specified for doing an act, other than paying money, a demand for performance is necessary to put the promisor in default. Johnson v. Alexander, 63 Cal. App. 3d 806, 813, 134 Cal. Rptr. 101, 105 (1976).

COMPENSATORY DAMAGE PRECEDENT

19. Plaintiffs are entitled to compensatory damages under the Associated Plaster precedent in California Courts

> Compensatory Damages (Associated Lathing and Plastering Co. v. Louis C. Dunn, Inc., 135 Cal. App. 2d 40, 51, 286 P.2d 825, 831 (1955) (where subcontractor failed to perform, general contractor was entitled to damages equal to difference between price for which subcontractor agreed to do lathing and plastering work and reasonable cost of completing job); Hofland v. Gustafson, 132 Cal. App. 2d Supp. 907, 909, 282 P.2d 1039, 1041 (1955) (where the failure of consideration is not material, damages are plaintiff's sole remedy and rescission is not available)).

20. Because of the fraud around the filings and then abandonment of the seven foreign instances of US6370629 and all of the instances of US6393126, PLAINTIFFS are entitled to compensatory damages for each of the patent families, their licensing potential and the damages done to plaintiffs in their unlawful filings.

STATUTE OF LIMITATIONS

21. This matter is timely because DDI contract was just recovered after being withheld for 12 3/4 years. Under California Law Precedent the recovery of the DDI contract in February of 2013 and the USPTO resetting the original filing of US6370629 to CONDITIONALLY FILED per the correction to the Federal Record they published in August of 2013, this matter is timely filed.

The statute of limitations is four years for claims based on a written instrument. Cal. Civ. Proc. Code §337(1). For claims based on an oral agreement, the limitations period is two years. Cal. Civ. Proc. Code §339(1).

/s/ Todd S. Glassey Wednesday, November 19, 2014, Boulder Creek California

Witness my hand, Todd S. Glassey,
Todd S. Glassey In pro Se
305 McGaffigan Mill Road
Boulder Creek CA 95006
408-890-7321

CO-INVENTOR AGREEMENT

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

RECITALS

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

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

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

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

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

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

1. PATENT APPLICATION TECHNOLOGY

For purposes of this Agreement, the term:

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

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

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

2. AGREEMENT IN PRINCIPLE

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

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

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

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

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

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

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

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

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

3. FAILURE TO MAKE DEFINITIVE AGREEMENT

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

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

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

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

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

4. DEFAULT IN COMPENSATION

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

5. NONASSIGNABILITY

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

6. NOTICES

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

7. ATTORNEY FEES

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

8. INTEGRATION

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

9. SEVERABLILITY

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"), 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.

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:

Bank Acc. # (Correct #) —

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. Nothwithstanding 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.

<u>SECTION SEVEN</u>
<u>ENFORCEMENT OF AGREEMENT</u>

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
MICHAEL MCNEIL

Dated: November 19, 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 17, 1999

TODD GLASSEY

Dated: November 19, 1999

Michael McNeil
MICHAEL MCNEIL

Dated: November 17, 1999

GLASSEY MCNEIL TECHNOLOGIES

Dated: November 29, 1999

DATUM, INC.

APPROVED AS TO FORM AND CONTENT:

STRADLING, YOCCA, CARLSON & RAUTH

Dated: November ____, 1999 By: ________________________

John F. Cannon
Attorneys for DATUM, Inc.

BOSSO, WILLIAMS SACHS, BOOK, ATACK & GALLAGHER

Dated: November 19, 1999 By: Jason R. Book

Jason R. Book, Esq.
Attorneys for Glassey-McNeil Technologies, Inc.
Todd Glassey, and Michael 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).

Exhibit E - Controlling Access Settlement

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 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 19, 1999

TODD GLASSEY

Dated: November 19, 1999

Michael McNeil
MICHAEL MCNEIL

Dated: November 19, 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 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
MICHAEL MCNEIL

Dated: November 14, 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

Jason R. Book, Esq.
Attorneys for Glassey-McNeil Technologies, Inc.
Todd Glassey, and Michael McNeil.

Todd S. Glassey, In Pro Se
Todd S., Glassey
305 McGaffigan Mill Road
Boulder Creek CA, 95006
408-890-7321
tglassey@earthlink.net

Michael E. McNeil, In Pro Se
Michael E. McNeil
PO Box 640
Felton CA, 95018
831-246-0998
memcneil@juno.com

Plaintiffs,

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

Notice of Motion and Partial Summary Motion for US6393126 Patent Inventorship Correction

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: January 15th 2015 8AM

Notice of Motion and Partial Summary Motion for

CORRECTING INVENTORSHIP ON US6393126

May it please the Court, on January 15th 2015 before his Honor Judge Alsup, if the Court has not already ruled on this Motion, Plaintiffs will move the Trial Court to review in summary the proper INVENTORS named in US6393126 Patent Filing and Plaintiffs standing as the true "Inventors of the TRUSTED TIMING INFRASTUCTURE", the technology that US6393126 patent filed protection for claiming ERIK VAN DER KAAY and others as the "named inventors"; And to properly issue a ruling ordering the correction of the US Patent 6393126 INVENTORS to read Todd S. Glassey and Michael E. McNeil.

This motion is composed of Notice of Motion and Motion, Exhibits, Declarations and supporting Testimony to be given at the time of the Hearing.

Table of Contents

CASES

"); ROBERT L. HARMON, PATENTS AND THE FEDERAL CIRCUIT § 3.3, at 51 (2d ed. 1991)	8
474 U.S. 976 (1985)	8
Board of Trustees of the Leland Stanford Junior Univ. v. Roche Molecular Systems, Inc., 583 F.3d 832, 841–42 (Fed. Cir. 2009)	14
C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1353 (Fed. Cir. 1998)	8
Checkpoint Sys., Inc. v. All-Tag Sec. S.A., 412 F.3d 1331, 1338-40 (Fed. Cir. 2005	11
Edward M. Goldberg, M.D. v. Medtronic, Inc., 26 IDEA 145, 145 (1985)	9
Gellman v. Telular Corp., No. 2011-1196 (Fed. Cir. Nov. 30, 2011)	14
Hobbs v. Atomic Energy Comm'n, 451 F.2d 849, 864 (5th Cir. 1971)	8
Jamesbury Corp. v. United States, 518 F.2d 1384, 1395 (Ct. Cl. 1975)	8
Mueller Brass Co. v. Reading Indus., Inc., 352 F. Supp. 1357, 1372 (E.D. Pa. 1972), afl'd, 487 F.2d 1395 (3d Cir. 1973)	8
Shatterproof Glass Corp. v. Libbey-Owens Ford Co., 758 F.2d 613, 624 (Fed. Cir	8
Wellcome Co. v. Barr Labs, Inc., 40 F.3d 1223, 1228-30 (Fed. Cir. 1994)	9

STATUTES

35 U.S.C. § 101	7
35 U.S.C. § 116	8
35 U.S.C. § 256	11
35 U.S.C. §102(f)	8
BCA	13
BCA of 1999	13
British Contracts Act ("BCA") of 1999	13
U.S. CONST. art. I, § 8, cl. 8.	7

TREATISES

1 J. THOMAS MCCARTHY, TRADEMARKS AND UNFAIR COMPETITION § 10:25, at 396 (2d ed. 984)[hereinafter MCCARTHY, TRADEMARKS]. 8

Edward G. Greive, Note, The Doctrine of Inventorship: Its Ramifications in Patent Law, 17 W. RES. L. REV. 1342, 1344 (1966) (addressing law of inventorship) 8

I. Background

Plaintiffs are Industry Experts in Digital Timestamping and US Evidence practices related to timestamping

PLAINTIFFS have standing as recognized Industry Experts in Digital Timestamping as Evidence. Plaintiff GLASSEY for instance is a co-author in the ABA "PKI Assessment Guidelines"(aka the PAG. An American Bar Association cryptography assessment from a legal perspective for managing digital evidence available at this hyperlink[1]). The ABA publication of this document certifies Plaintiffs as experts herein and defined the scope of their work.

A. The PAG and Glassey's company CertifiedTime.

As to the history of this work, Plaintiff Glassey and Ruven Schwartz Esq as the Vice president of Practices for Glassey's company CertifiedTime Inc. (created after GMT left working for Microsemi) Glassey and Schwartz wrote the digital-timestamping as evidence section of the PAG with help from Dr. Jon Graff, Mr. Steven Teppler Esq, Mr. John Stanley Esq, and Mr. Hoyt Kesterson. of the x509 Digital Certificate Consortia.

[1] American Bar Association "PKI Assessment Guidelines" aka the PAG ver 1.0 - http://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf

This material created and published in the PAG by Schwartz and Glassey was reviewed and commentary added from Chas Merrill Esq and a number of other ISC members meaning all of the key lawyers in Digital Evidence Standards were in fact involved in this and fully aware of Glassey's creativity and designs for digital evidence systems as key parts of the PAG.

B. Plaintiffs and Not Microsemi created the TRUSTED TIMING INFRASTRUCTURE

Plaintiffs are the creators, first instance implementers and the parties responsible for the Glassey TRUSTED TIMING INFRASTUCTURE in its genesis was conceived by PLAINTIFFS and disclosed under NDA with several members of the ABA "ISC" (aka American Bar Association's Information Security Committee) in the 1996 to 1998 time frame and those parties are available for direct testimony. PLAINTIFFS have submitted specific evidence showing they took the GMT TTI to Datum to get Datum to bid on building it. Instead Datum wound up licensing use of three sub-components and the name of the program for its marketing effort. As such all work done on any Datum technology is a derivative of PLAINTIFFS original Genesis and PLAINTIFFS as such are the true INVENTORS for US6393126.

C. The existence of the TTI Document itself invalidates the Patents Named Inventors

Plaintiff's assert the existence of the TTI Settlement at the very least disproves the named parties as the ONLY INVENTORS and that filing as a fraud in its entirety and entitles the Plaintiffs to demand either Removal of the incorrect names and replacement with the correct INVENTORS or under Walker Process invalidating the entire US63903126 family of filings thus enabling PLAINTIFFS to further file for a Summary Judgment there against Defendant Microsemi and their partners, resellers and specifically the THALES GROUP, who plaintiffs alleged became Microsemi's partner "in bringing . the Plaintiff's TTI based IP back into the US through a European 'washing' of the IP" in question to get it out from under US law, a clear SHERMAN ACT Section 2 violation.

D. In closing

At the time of the motion, Plaintiffs will move the Trial Court for a finding that Plaintiffs are the True Inventors of the Trusted Timing Infrastructure and order Plaintiff Glassey's name at least added to the Inventors of US6393126 or to actually replace all of the Inventors name therein and properly reassign US6393126 (and its foreign instances as necessary as well) to PLAINTIFSS.

This motion will have no effect on the CMC or any other case scheduled proceedings and will enable fast tracking of various settlements Plaintiffs believe and ask the Court to consider this PRE-CMC Motion in that light.

MEMORANDUM OF POINTS AND AUTHORITIES

I. Background

This motion stems from an unauthorized patent filing from Defendant Microsemi on intellectual properties they licensed for their limited use based on a settlement agreement. Instead Defendants Microsemi (Datum) represented the TRUSTED TIMING INFRASTRUCTURE as their original work[2] to the Patent Offices in four nations in violation of 35 U.S.C. § 116 (2008) and the Sherman Act.

[2] 2See U.S. CONST. art. I, § 8, cl. 8. The patent laws and the strict inventorship requirements therein are founded upon article I of the Constitution, which provides that "[t]he Congress shall have the Power... [t]o promote the Progress of ... useful Arts, by securing for limited Times to... Inventors the exclusive Right to their ... Discoveries." Id. Section 101 of the patent law gives effect to this constitutional patent grant by providing that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor." 35 U.S.C. § 101 (1988) (emphasis added); see also 35 U.S.C. § 102(f) (1988) (stating that person entitled to patent unless "he did not himself invent the subject matter sought to be patented"); ROBERT L. HARMON, PATENTS AND

The resulting application for US Patent issued as US6393126[3] and named DOE Van Der Kaay as the principal Inventor[4], which Plaintiffs assert is actually a violation of the law[5]. In fact none of the parties named on the filing are Core Inventors on the TRUSTED TIMING INFRASTRUCTURE but rather Engineers working on implementing a Program Code-Based System that implements the protocol and the "API" - the application programming interfaces to the TLC and TMC modules as described in the TTI Settlement and not inventors[6] of the Trusted Timing Infrastructure itself that the patent protects. This is all the Settlement provides for, it licensees only a limited use of three of the thirty-two TTI components created originally by Plaintiff Glassey and which were taken to Microsemi under NDA to propose they build them for Plaintiffs.

> The legislative history accompanying the 1984 amendment to 35 U.S.C. § 116 confirms that the amendment was not "intended to permit anyone other than the inventor to be named in a patent application or patent. Also, the amendment is not intended to enable appropriation of the invention of another." SECTION-BY-SECTION ANALYSIS: PATENT LAW AMENDMENTS OF 1984 (1984), 138 CONG. REc. 7, reprinted in 1984 U.S.C.C.A.N. 5827, 5834. See generally 1 J. THOMAS MCCARTHY, TRADEMARKS AND UNFAIR COMPETITION § 10:25, at 396 (2d ed. 984)[hereinafter MCCARTHY, TRADEMARKS]. Misappropriation is a common law action providing relief where a misappropriator has copied or appropriated an item or creation of the plaintiff that is not protected intellectual property. See

THE FEDERAL CIRCUIT § 3.3, at 51 (2d ed. 1991) (noting "fundamental principle" of American patent law that "you cannot patent another's invention").

[3] 35 U.S.C. §102(f); see also Jamesbury Corp. v. United States, 518 F.2d 1384, 1395 (Ct. Cl. 1975) (inclusion of more or less than the true inventors renders patent void and invalid); C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1353 (Fed. Cir. 1998) ("To invalidate a patent based on incorrect inventorship it must be shown not only that the inventorship was incorrect, but that correction is unavailable under section 256").

[4] To be considered an "inventor" under the patent laws, a party must be responsible for a development that falls within the scope of the statutory definition of invention, i.e., the inventor must have discovered something new, useful and unobvious. See, e.g., Edward G. Greive, Note, The Doctrine of Inventorship: Its Ramifications in Patent Law, 17 W. RES. L. REV. 1342, 1344 (1966) (addressing law of inventorship)

[5] services, ideas, and aid of others in the process of perfecting his invention.'" Shatterproof Glass Corp. v. Libbey-Owens Ford Co., 758 F.2d 613, 624 (Fed. Cir.) (quoting Hobbs v. Atomic Energy Comm'n, 451 F.2d 849, 864 (5th Cir. 1971)), cert. denied, 474 U.S. 976 (1985)

[6] The threshold inquiry to be addressed in naming the inventors of a patent is who "conceived" the invention. See Mueller Brass Co. v. Reading Indus., Inc., 352 F. Supp. 1357, 1372 (E.D. Pa. 1972), afl'd, 487 F.2d 1395 (3d Cir. 1973)

> McCARTHY, ENCYCLOPEDIA, supra note 4, at 206; see also Roy E. Hofer & John M. Wagner, Anatomy of a Misappropriation: Edward M. Goldberg, M.D. v. Medtronic, Inc., 26 IDEA 145, 145 (1985) (acknowledging rise of misappropriation of ideas and analyzing case of misappropriation of pacemaker technology)

Plaintiffs assert as well that their claims in this matter fully pass the tests of Burroughs Wellcome Co. v. Barr Labs, Inc., 40 F.3d 1223, 1228-30 (Fed. Cir. 1994) standards;

A. Plaintiffs believe that this Patent's Inventor's Can be Corrected with a 35 USC 256 Process

This patented Intellectual Property was originally invented solely by Plaintiff Glassey and he holds sole rights to it with the limited licensing of the IP to Microsemi for its use. As such Microsemi cannot file patents against IP it was not the inventor of. Since Microsemi would have to agree to this, we feel their refusal to return this property documents the claim of their conversions and tortuous interference with Plaintiffs economic advantage.

Under 35 USC 256 the USPTO has a process for correcting patent inventorship without needing to invalidate the patent. If the patent is invalidated its full loss will need to be filed as an IRC 165 Fraud Loss as well.

B. The settlement creates three mandatory components which cannot be unbundled or sold apart from each other.

Per the terms of the TTI Settlement Agreement (See Docket #6 Exhibits/Contracts/TTI Settlement) Datum (Microsemi today) licensed "a limited use of three specific components of the Trusted Timing Infrastructure Library of Technology".

Those three components must be used in concert with each other and cannot be unbundled. The settlement pertains to a specific derivatives from the main TTI library using their specific GPS and Timing Chips in the TRUSTED LOCAL CLOCK module.

C. All original aspects of the TTI Settlement were scrapped and the SW components sold off in violation of the three-component settlement

Microsemi no longer builds any components of this derivative TTI system and reduced the Trusted Local Clock hardware system to a Software Driver in violation of the Settlement Agreement to take the Hardware Costs for Microsemi out of the equation.

Plaintiffs allege that Microsemi then sold the product to themselves outside of the settlement agreement and setup a joint venture with British Company nCipher in direct violation of the Acceptance Clause and reporting clauses in section 8 of the contract.

D. The limitations of the TTI Settlement and its licensing

The TTI settlement is very specific as to which components were licensed of the larger TTI Library of Technologies. In the Settlement Datum (now Microsemi) only licensed the use of the TRADEMARKABLE TERM "Trusted Timing Infrastructure", the Timestamping protocol for use between the TRUSTED MASTER CLOCK and the TRUSTED LOCAL CLOCK. No software services without the Trusted Local and Trusted Master Clock may be sold.

These three components are the only elements of the larger Trusted Timing Infrastructure system developed in the mid 1990's when Plaintiff Glassey was a member of the American Bar Associations Information Security Committee.

As such not only did Datum not have authority to file the patent originally, because the Settlement was protected by an NDA which prevented their filing that patent application itself without Plaintiffs approval, but in addition they misrepresented themselves as the TTI creator rather than a simple Licensor and they placed their employees names on this "Core-Genesis[7]" type patent that Plaintiff Glassey is the creator of;

In filing their patent application they also in addition to the three limited components they licensed they included the other remaining twenty-nine (29) unlicensed elements of the original Trusted Timing Infrastructure Glassey presented to Microsemi for them to build for him, apparently we theorize to prevent Glassey from filing his own patent on the larger Trusted Timing Infrastructure.

As such the existence of the patent and the Settlement Agreement itself constitutes a documenting evidence of the alleged theft and conversion of intellectual property rights against the Trusted Timing Infrastructure design itself.

E. The existence of the Settlement Document also meets the Corroboration rule Requirement

Plaintiffs assert the mere existence of the settlement with its time line and description when compared to the affidavits on the beginning of the relationship between Datum and Plaintiff's fully meets the corroboration rule[8]. That further this document was sent to the USPTO with the attached complaint pertaining to the filing and issuance of a patent the Plaintiffs should own.

[7] A patent which can be leveraged against others and be used in a standards environment to enable larger capabilities.

[8] Checkpoint Sys., Inc. v. All-Tag Sec. S.A., 412 F.3d 1331, 1338-40 (Fed. Cir. 2005) (requiring claims of coinventorship by unnamed inventors to be corroborated by physical, documentary or circumstantial evidence or testimony from individuals other than the alleged inventors); see also 35 U.S.C. § 256

The settlement proves Microsemi licensed the use of the Term TTI and the three components they had GMT help them build specific derivatives of Glassey's TTI using their proprietary chips and hardware to enhance Microsemi (Datum) sales of these devices.

F. Microsemi is Successor to the last Fiduciary, Symmetricom

Microsemi is the Successor to both Symmetricom (the previous Fiduciary) and a new corporation called Microsemi. Symmetricom is successor to Datum through the same Merger type process.

II. Conclusion

Microsemi through the years clearly registered multiple international patents on technology it bought from Plaintiffs and only held a limited license to use; Further it registered the patent both in its name and named Microsemi employees as the inventors of the Trusted Timing Infrastructure, technology against which only Plaintiffs should have been able to file patent applications because of the NDA in place between the parties. As such any patent filings would need to be noticed through the section 8.7 messaging provisions John Cannon created when he designed the two contract-settlements.

Microsemi has to date also refused to discuss or acknowledge they had no right to file this patent under the limited use license in the settlement agreement. As such the Patent should have the other four names

(stating a patent may be corrected if there is proof that a named inventor was incorrectly listed or a true inventor was not named) removed from it and Plaintiff Glassey added as sole inventor therein and the assignment reassigned to Plaintiffs.

A. British Contracts Act ("BCA") of 1999 prevented laundering this IP through Britain

Microsemi used the core IP underneath the patent to increase the number of components from the larger Trusted Timing Infrastructure Technologies which it did not license. These became the core of its efforts with nCipher Corp. This was done Plaintiffs assert to push the controlled IP outside the US Jurisdiction so the contracts would become moot. The BCA of 1999 however had been put into play to stop this type of fraud from happening and so even today the California Law section and the Transcendental Rights sections persist.

1. Plaintiffs assert that the totality of its actions indicate that the intent of this off-shoring sale we believe was to move the US-based IP to Britain and then bring it back into the US under the British IP Laws, but the British Contracts Act ("BCA") of 1999 made that pointless unless Microsemi lawyers missed that any contract valid here in the US would be valid under the BCA as well in Britain as a fix for the loophole used up until the BCA was put in place to 'launder IP' so prosecution would be impossible on the return. Under the BCA of 1999 all of the previous contracts remain enforceable, even in British Courts.

III. Relief Sought

A. Correct Inventorship

B. Correct Inventorship on US6393126

Plaintiffs seek the correction of the INENTORS named in US6393126 to either have PLAINTIFFS added to the existing Inventors and as full joint-assignees of the Patent or the Plaintiffs names added to the Patent as replacements for the existing named Inventors

,

C. Correct Assignment as a separate relief from Inventorship Correction

Further as a second step, we seek formal reassignment of US6393126 and all published instances of it to Plaintiffs as not being authorized under the TTI Settlement[9]. Under Gellman[10] and other precedent rulings without specific enumeration on each authorized patent filing or a blanket release for global patent filings, no such release exists and so the Assignment of this IP in the context of patent filing was never contemplated or authorized.

DATED: November 30, 2014

Respectfully submitted,
Todd S. Glassey and Michael E McNeil, as in Pro Se litigants.

/s/ Todd S. Glassey
TODD S. GLASSEY, in pro se

/s/ Michael E.. McNeil
MICHAEL E. McNeil, in pro se

Todd S. Glassey, In Pro Se
Todd S., Glassey
305 McGaffigan Mill Road
Boulder Creek CA, 95006
408-890-7321
tglassey@earthlink.net

Michael E. McNeil, In Pro Se
Michael E. McNeil
PO Box 640
Felton CA, 95018
831-246-0998
memcneil@juno.com

[9] In GELLMAN - The court reiterated that present assignments of future rights must expressly set forth the assignment when the agreement is signed. As an example, the court highlighted its decision in *Board of Trustees of the Leland Stanford Junior Univ. v. Roche Molecular Systems, Inc*., 583 F.3d 832, 841–42 (Fed. Cir. 2009), which held that the phrase "I will assign and do hereby assign" created a *present* assignment of a future right. Because "agrees to execute" imposed a future rather than a present obligation on Seivert, Gellman established only an equitable claim to ownership.

[10] *Gellman v. Telular Corp.,* No. 2011-1196 (Fed. Cir. Nov. 30, 2011)

IV. ECF Service Declaration

I Todd S. Glassey swear under the penalty of perjury that this motion and its exhibits was electronically filed with the Courts ECF system on my account and for those two individuals not registered for ECF service of documents that they will be served by a third party to their respective addresses. - Sunday, November 30, 2014 /s/. Todd S. Glassey

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

[PROPOSED] ORDER CORRECTING INVENTORSHIP ON US6393126

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: December 26th, 8AM
Date: 9th December 2014

For good cause the motion is hereby granted. USPTO is ordered to under 35 USC 256 correct the Inventorship of US6393126 to read as follows

_____ Inventor: Remove existing INVENTORS and replace with Todd S. Glassey and Michael E McNeil ; or

_____ Inventor: Add Todd S. Glassey and Michael E. McNeil as named INVENTORS to existing INVENTORS

USPTO is also ordered to under this same ruling to correct the assignment to read as follows: ______ Assigned to: Todd S. Glassey and Michael E McNeil

Defendants are also assessed damages of ____________________ as well as all legal fees in this matter to date.

Witness my hand, Judge WH Alsup, __________________, Dated ________ 2014

Declaration in support of Production of Documents, Motion and Rescission Motions I and II

Failures under the first Settlement aka "The Trusted Timing Infrastructure" Agreement

Contents

oi

Declaration in support of Production of Documents, Motion and Rescission Motions I and II

Introduction

I Todd S. Glassey am one of the principal plaintiffs herein and this declaration and reference content is supplied under my perjury declaration in full, To that end under the laws of the State of California, I declare these statements to be true and accurate to the best of knowledge and to those things I rely on belief and faith in, that they also are true and accurate.

/TSG/ - Todd S. Glassey In Pro Se
9/18/2010

I also submit the following declaration in support of the motions to force the production of documents, rescission demands and in the "cease and desis"t their operations of the Global Time Service Business order the October 14th 2010 C&D Motion asks for.

The following document provides reference to the agreements now in dispute between the parties in the matter herein. This declaration references where possible established concepts and precedents in US and State law.

This Declaration

In addition to the attached motion, this declaration also pertains to the existing rescission motion for the GeoSpatial Controls Assignment, and the motions to produce documents.

This specific declaration documents the failures to meet the terms of the existing contract they created with Glassey to license the Trusted Timing Infrastructure technology as well.

Declaration in support of Production of Documents, Motion and Rescission Motions I and II

Summary

The assertions in this declaration state the following:

1) That this document pertains to motions calendared for October 24th 2010 in Department 5 of the Superior Court of the State of California in and for the County of Santa Cruz, and that it is properly served on defendants and the Court in a timely matter.

2) That DATUM and later Symmetricom and its Officers continued the breech that DATUM had started.

3) That based in these actions they have taken the properties licensed in the Courts of California to Europe and thus violated the license agreement.

4) That DATUM and Symmetricom have refused to provide any of the market development services that were the justification for sections 8.1 and 8.4 of the contract and its status under sale orders per 8.3 and in the process violated this agreement.

Original Settlement History

In February of 1998 a formal agreement between Glassey and Datum was reached which pertained to Datum's retaining Glassey to research the market-potentials of a product which Glassey had asked Datum to build so that he could produce his secured email gateway. That product was a secured time infrastructure which was intended for a reference time service in a watermarking system which applied provable time-data to a piece of email (or other document for that matter contained within that email as an attachment).

Glassey had designed a set of systems and components which provided actual evidentiary controls on digital content so that it could be proven in any step of the chain-of-custody for that data, something now critical in ensuring transparency in digital systems. These are of tremendous value in selling capability to an end-user who is building secure financial systems or other's which contain key controlled data. Secure Time has emerged as the leading issue in securities and financial trading and make up the bulk of the trading fraud complaints. In addition time, something now akin to everyone in the form of TOU (Time of Use) Billing for the Smart Grid operations is something that everyone is about to become keenly aware of.

The TTI or Trusted Timing Infrastructure is ONLY a single component of a larger set of Glassey Intellectual Properties that DATUM licensed only limited components use and not blanket use of all of the Glassey IP's. Those being the TLC/TMC Vendor Business, the Global Time Service Business, and the Foundation Business Model to operate the National Timebase. In its settlement with Glassey they ONLY licensed the use of the Trusted Time Infrastructure in their specific limited form.

Why this is so important is that most evidence processes in computers are tied to first-person attestation models and Glassey's vision is to build evidence systems so strong the people operating the systems become irrelevant to the integrity of the transactions represented. This for Glassey is a personal crusade and has caused him to build the other two businesses that DATUM refused to license or operate himself.

Background Info: The Trusted Timing Infrastructure – what is it?

The TTI is a framework-system which actually proves the distribution of time from one machine to another. Depending which TTI is used a provable service of synchronization can be documented to meet even the new emerging digital evidence mandates so this technology is now more than ever valuable in systems which need digital trust.

Time movement in the instantaneous is pretty simple. Proving it after the fact is much harder and that is what the TTI is for. The ultimate goals of the TTI are to provide a positive set of evidence of the movement of time in networks and that time-tokens induction and use in the receiving systems.

To accomplish this the TTI is composed of a Trusted Local Clock (TLC) which runs as an agent or external peripheral to a computer and a Trusted Master Clock (TMC) system which then deploys and logs that time data. The TLC and TMC are Hardware Modules or in the TMC's case an Appliance-type devices so this would be of particular interest to a company who built Time-Keeping Equipment like DATUM for instance.

There are also a set of propriety but well known network and transaction protocols for how the TLC talks to the TMC meaning there are a whole suite of functions it can perform with regard to trusted time deployment in a computing environment.[1]

[1] See NIST SP800-52 and SP800-53 for US Government Standards on Trusted Computing. See also the NORAMET Treaty for a minimum standard for interoperability in US, Canadian and Mexican computer-clocks to implement a uniform time-service for North America.

It is important to note that there is probably no need to protect this data it's been in public view for years and that since this software was published as part of an RFC3161 compliance for operations of secure information timestamp services in the EU, any claims of trade-secret disclosure would be moot. In this instance we also must note that the specifications for the TTI were published a decade ago and given without controls to thousands to review and then later published as 'confidential' after all efforts to maintain that confidentiality had been previously ignored.

Once the publication to the userbase was done all claims of confidentiality were lost since the software and API's became published in user forum posts accessible to the general public. That of course doesn't affect the proprietary license requirements just whether there is any reason to redact these documents from the records of the court or any manuals for the Trusted Timing Infrastructure itself..

Datum's license was for the time-keeping services of the TTI only.

In the final settlement with Glassey over the use of the TTI Version 2C, DATUM did not license the use of the Global Time Service (GTS) provide and its business operations. They opted to not pay the several million dollars Glassey asked for that license and only focused on the portions of the TTI which would allow them to build a time-keeping module as the TLC and an appliance system as the TMC.

A GTS provides a set of practices and services for use of a National Timebase as a private trust service. This means much more than just the movement of time in one direction which is what most anonymous time settings are but a full-relationship based time services model to insure that the client gets everything that they are needing as part of their audit.

GTS's are a separate business Intellectual Property from the TIME KEEPING COMPONENT provider business that the TTI enables and provide an independent and reliable source of time to anchor the operation of those self operated time services for any and al users not just TTI users.

The functional benefit of this physical "arms length" to the source of time is to ensure integiry in its operations. We think of it as the conceptual "Bank of Switzerland" in the form of a clock. As such GTS's operate as independent trust service providers and offer sources of time provided by the Government itself.

There are many Trusted Timing Infrastructures… Datum only licensed one of them from Glassey

It is important to understand that "there are any number of ways to accomplish this specific goal of secure time movement" but that Glassey's methods were leading-edge and unique in that time.

Datum retained Glassey (and through Glassey McNeil) to understand the scope of the market Glassey proposed was available to a first-mover. Direct testimony as to this relationship and its 'meltdown' can be provided by Mitch Stone the specific Officer of Datum at the time of hearings into this matter to corroborate this testimony. His NDA's have long since expired making his testimony directly admissible as first hand.

Through the relationship Datum continued to violate the terms of the consulting relationship by starting to use and claim rights to intellectual properties Glassey had designed for his specific solution and finally when they acquired Digital Delivery Corp which Glassey was working with on the GeoSpatial Controls patent (US 6370629) they wound up owning claims to IP which they by their actions apparently wanted 100% control of[2].

The Settlement process degrades

The matter then degraded into infringement litigation and a spurious litigation Datum filed against Glassey and McNeil to further tap-out their financial status so they could drive GMT into financial receivership.

CANNON was the sole keeper and principal architect of the Settlements

The Settlement Documents were both issued by DATUM's attorney's who agreed to produce the master signed copies and to hold them for independent verification, something that Datum agreed to pay for as part of the Settlement and which has been denied.

At all times they were required to serve Glassey and McNeil with actual wet-signed agreements to properly document the execution of the contract which they have refused to do to date.

In the Final Document - Settlement Section 8 Controls

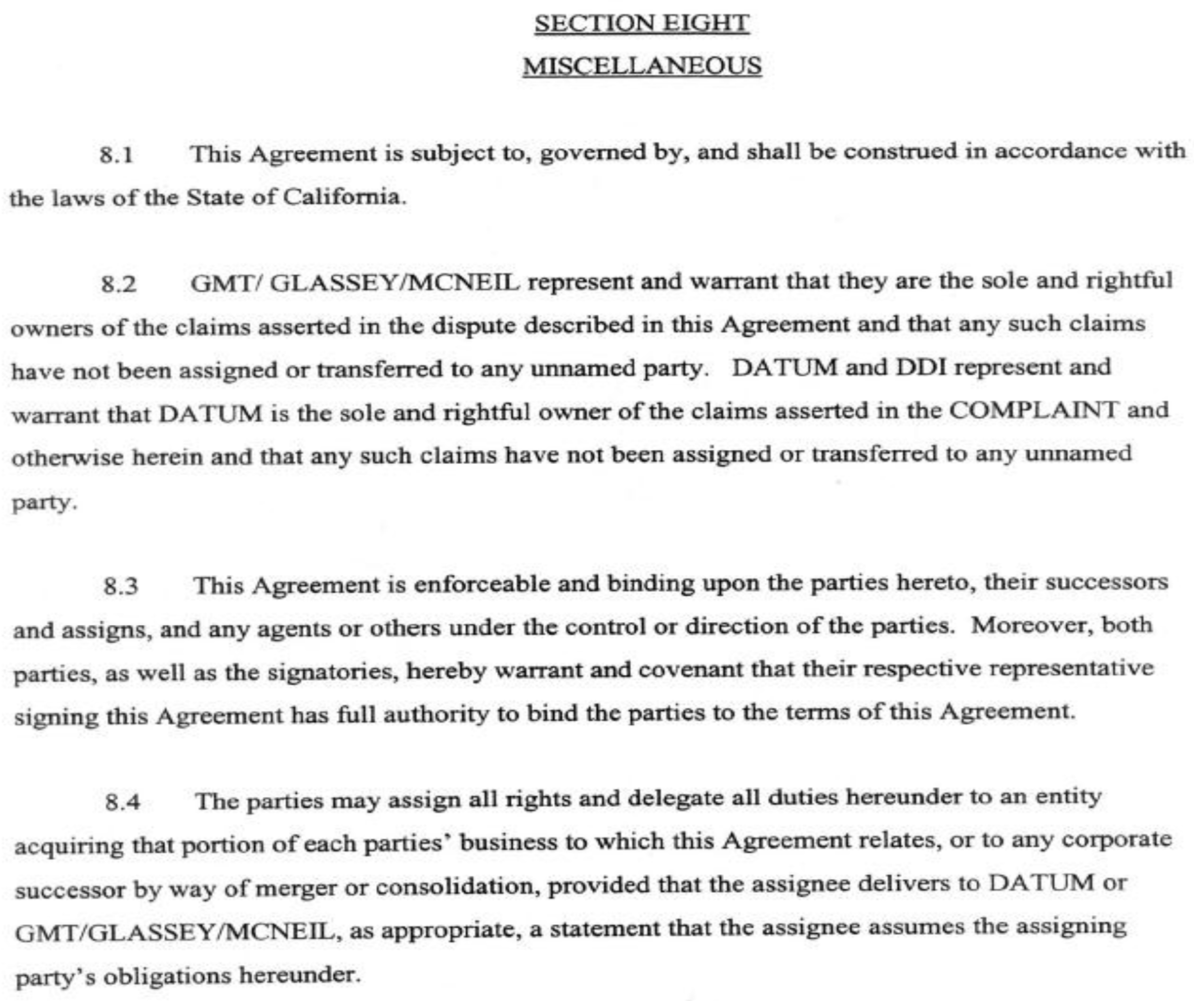
The Settlement went on and on as values for services were weighed against cash payments to Glassey (and McNeil) and it was finally agreed that the services DATUM

[2] The GeoSpatial control license (aka the Co-Inventor's Agreement) violations are addressed in the DDI Settlement matter being resolved as part of this litigation as well but are not germane to this matter except to support DATUM and later Symmetricom's actions in being adversarial to Glassey in their breach of the settlement agreement to license his Trusted Timing Infrastructure technologies.

would have to put in place to comply with 8.1 through 8.4 of the settlement would be valued at several million yearly for the life of the license.

As such the advancing and marketing of Glassey Technology had significant value in this as well. That would take a documentation and certification program to provide the reports from. The costs of those programs were to be absorbed by DATUM in its actions of paying reduced fees for the cash component of their license of the Trusted Timing Infrastructure.

In the following page’s scan from the Trusted Timing Infrastructure Settlement Agreement (Settlement Agreement #1 we see the following four control 8.1 which set the jurisdiction and choice of courts, something which was set in perpetuity through 8.3 and the final section 8.4 which mandates all of the compliance requirements for the use of the IP.



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.

Figure 1 – Section VIII Scan

Under California Law Ideas and Intellectual Property is protectable

I declare in the matter herein we see the licensing of the complex set of technologies called the Trusted Timing Infrastructure as documented in the already submitted "Trusted Timing Infrastructure™" documents which are evidence to the RESCISSION MOTIONS already on file.

Benefits provided included much more than the trivial license fee payment

I declare the settlement agreement's license provides for many benefits for Glassey (and McNeil) which are specifically part of the payment in addition to the limited amounts of actual cash payments. These other services including legal services which CANNON assured everyone that DATUM was including in these settlements were enforceable. As such the failure to provide those would have dramatic and significant and permanent damage for which this relief is warranted.

California Courts must maintain jurisdiction over this IP

I declare under Control #8.1 in the Settlement Agreement the laws (and through them the Courts of the State of California) in all instances will control and enforce this contract. That means at all times the Courts of the State of California are the controlling adjudication forum for resolving any and all disputes arising from the sale or use of products derived from this Intellectual Property and there is a constructive and potentially fraud-based requirement to inform any part this IP is licensed to or sold to of those requirements since they must accept them as well as enforce them on anyone this IP is transferred to in perpetuity.

I declare that this specific reporting control is the single most valuable consideration of the settlement since it controls the IP in perpetuity and establishes a mandatory compliance and reporting program of which the costs of operating are to be borne by the receiving party (Datum or its Successor Symmetricom) and anyone they sell, provide access to, or license the usage of these Intellectual Properties to. This compliance program is estimated to cost in the several million dollar area to operate and continue on a yearly basis and this is the reason for the cash figures in the actual settlement. The requirement to provide this was seen as a significant ongoing component of the settlement and so cash values were adjusted downward to keep the initial cash settlement cap in a specific area. The failing to provide that would open Symmetricom for a claim against that portion of the moneys and any legal fees necessary to reproduce and enforce those licenses.

Since we assert that the property is now in the possession of a French company it literally may not be possible to put this control back into effect and as such Glassey and McNeil would have suffered a significant permanent damage from the fraudulent sale of the IP to a foreign nation.

That is a critical control section because it means that at all times the IP this license pertains to 'must remain within the control of the Court's of the State of California and that would mean it could not be transferred without amending this agreement to a party outside the jurisdiction of this court. Any action which transferred this IP outside the California Court would breach this clause. The same is true for all derivatives built from this IP.

As such we reiterate again that under Control Section number 8.4 here that DATUM and Symmetricom had a formal duty to inform Glassey and McNiel of the sale or transfer of the IP to a third party and their agreement to be bound by this agreement (see control 8.3 above) would need to be delivered to Glassey and McNeil in a form which continued the continuity of their rights to seek redress in the California Courts.

The scope of the IP is defined in that agreement as well in section 2.1 and the following definitions as well as the Trusted Timing Infrastructure exhibits already on-file in the Rescission Motions now calendared.

IP Theft includes the movement of that property outside of the US

I declare the movement of the shared IP and licensed IP outside of the jurisdiction of the court constitutes a functional and actual theft of Intellectual Property as licensed and the transmission of that further by other acts outside this Court's jurisdiction.

> In documenting a theft of idea claim to prevail, a plaintiff must establish that: "the plaintiff prepared the work, disclosed the work to the offeree for sale, and did so under circumstances from which it could be concluded that the offeree voluntarily accepted the disclosure knowing the conditions on which it was tendered and the reasonable value of the work." Grosso v. Miramax Film, 383 F.3d 965, 967 (9th Cir. 2004) (citing Desny v. Wilder, 46 Cal.2d 715 (1956).

The settlement agreement and the supporting technical descriptions of the Trusted Timing Infrastructure provide this 'documentation' of the claim therein.

> There must be a reasonable expectation of payment, which can be inferred from the circumstances; however, the "idea man" who "blurts out his idea without having first made his bargain ... has no one but himself to blame for the loss of his bargaining power." Gunther-Wal Productions v. Mattel, Inc., 104 Cal.App.4th 27, 39 (2002); Desny, 46 Cal.2d 715.

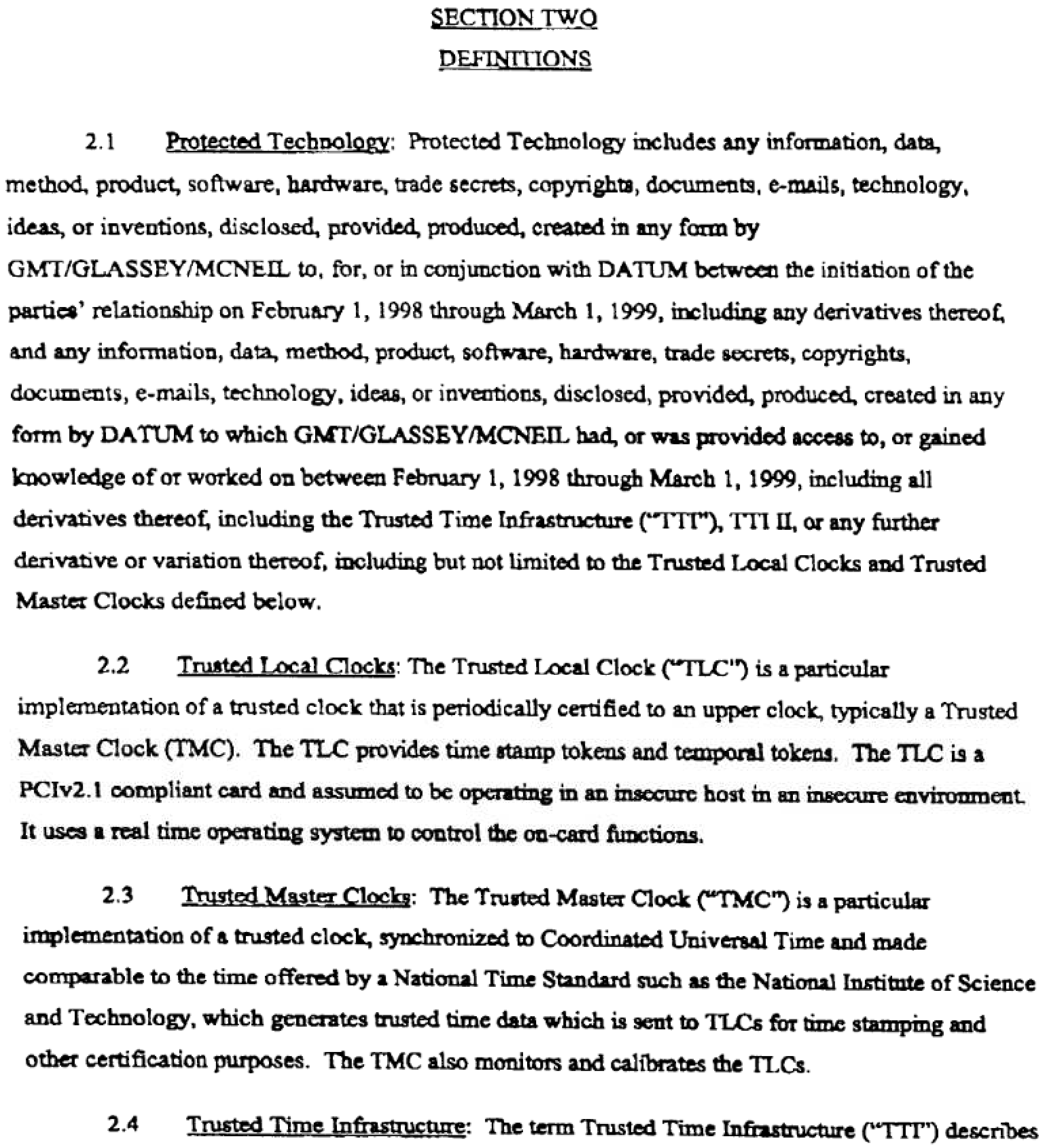
I declare in this case there were numerous pre-existing Non-Disclosure Agreements protecting the Intellectual Properties so all issues with those controls were properly met. As such Glassey's payment for the use of his Trusted Timing Infrastructure requires all of the terms be met by initially DATUM and its Successor Symmetricom, but also by anyone purchasing or being given access to the tools by DATUM, Symmetricom or anyone they would transfer this Intellectual Property as a product to for any reasons.

The specific trustable time service infrastructure licensed herein

This next figure, a scan of Section II of the agreement documents the definition of the Trusted Timing Infrastructure (TTI) per section 2.4, and further that DATUM only licensed the right to produce a derivative of GLASSEY's original evidentiary grade time service infrastructure designed after February 1st 1998.

No claim to any of the previous Intellectual Property is made or implied. The same is true of later IP's which were not designed from or as derivatives of any of the Trusted Timing Infrastructure license herein.

Because of this limitation all Glassey Secure Time Service Intellectual Property developed prior to February 1st 1998 or derived GLASSEY IP developed after the terminus of this agreement from those original IP's would still remain GLASSEY's property alone. The protected technology is defined as follows:



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.

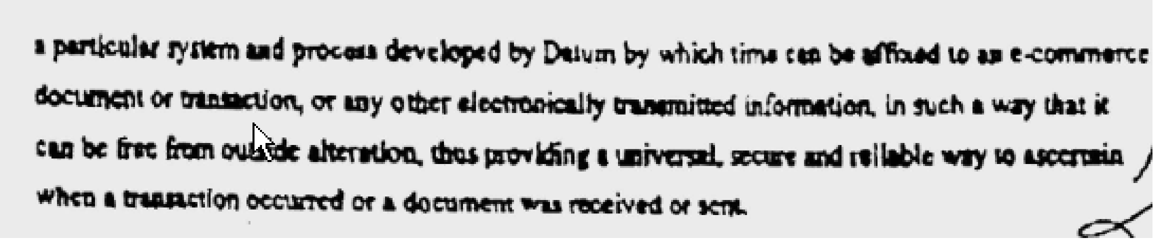
2.2 Trusted Local Clocks: The Trusted Local Clock ("TLC") is a particular implementation of a trusted clock that is periodically certified to an upper clock, typically a Trusted Master Clock (TMC). The TLC provides time stamp tokens and temporal tokens. The TLC is a PCIv2.1 compliant card and assumed 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

Figure 2 - Section II Scan

As such GLASSEY would retain any and all rights to those as well and this is why the transparency in the follow-on and client-users was so important. DATUM could not sell this product to people who would use it to infringe on GLASSEY IP rights in any manner. This next section below continues that SCAN on the next page of the Settlement Agreement for the TTI Use License Section 2.4.



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.

Figure 3 – Section 2.4 continued from previous page

The use of the Term Of Art "Trusted Timing Infrastructure"

The term of art called the "Trusted Timing Infrastructure" and its use specific to the IP defined in section 2.4 of this agreement is all that is being licensed. As such the TTI term can be trademarked by DATUM but it must be noted that because DATUM has not asserted public control and that the term has become common in talking about time in trusted computing infrastructure, we assert they have also lost this control as well by abandoning any claim to the term.

This Trusted Timing Infrastructure as licensed was a very specific Trutsed Timing Infrastructure and that it does not apply to any Glassey IP developed before February 1st 1998 or to any after the terminus of the working relationship either.

As such this IP which was licensed to DATUM in this agreement pertains to "a component time-stamping service particular to DATUM's use of DATUM clock modules and particular cryptographic math services to authenticate them". There are much other possible architecture's for building precision timing systems from, which are also secure like the IEEE 1588 Precision Timing Service and the IETF Network Time Protocol service or their predecessors which have existed for years. The point is that DATUM licensed a very specific technology package which is defined in a set of documents on file with the Court and nothing more.

No authorization to merge GeoSpatial Controls into TTI

Further there are other disputed technologies under other claims with DATUM which seem to at one level or another merged with the Trusted Timing Infrastructure who is not authorized to use any of the Glassey GeoSpatial controls under either settlement with Glassey. In fact it was specifically agreed that there would be no use of GeoSpatial Controls in any product outside of the Confidential Courier product as it was at the time of the signing of the agreement.

Specific Declarations

The following declaration is based on the above exhibits and points and authorities cited. To that end under the laws of the State of California, I declare these statements to be true and accurate to the best of knowledge and to those things I rely on belief and faith in, that they also are true and accurate.

I declare the following are requirements for any products built with the Trusted Timing Infrastructure technology licensed in this settlement to which I am a principal party.

Removing licensed IP from the jurisdiction of the court intentionally constitutes theft of the IP.

1 That this settlement agreement was intended to split Glassey's compensation to a smaller amount of cash because of the reporting and IP management requirements and the costs associated with those. That it was further agreed and represented by both CANNON and BOOK to Glassey and McNeil that per CANNON's agreements that any and all products are controlled through that this license and that it requires any and all sublicensed products to require legal resolution pertaining to this product or its services remain in the California Court. Any derivative products built from it are as such constrained by this same control mandate.

As such it was my understanding that all products including Software Developer Kits and Startup Licenses built by DATUM its successors or its customers must as such be so constrained.

The justification is simply that because no court has the jurisdiction other than California Courts herein, any and all derivative products created with this intellectual property are constrained as such and proper notice of the GLASSEY LICENSE MANDATES included with any products sold with or developed from these licensed IP's.

Declaration in support of Production of Documents, Motion and Rescission Motions I and II

TTI properties should require approval of the BIS to export

2 I declare that because this product contained controlled cryptographic technology that any and all Bureau of Export Affairs[3] legislation regarding Munitions Controls any parties purchasing or developing products based on this technology. As such any sales to entities outside the US must be properly noted with the US Department Of Commerce's export authorizations agency known as the Bureau of Industry and Security. [4]

a. **DATUM has violated this specific requirement previously in shipping atomic clocks, the key component in the development of the timing-control for the core of a thermo-nuclear weapon to Hostile Nations and the cover-up of those shipments with fraudulent shipping records. The existing settlement in this matter shows DATUM's integrity at the "top" and their willingness to violate US Law and clearly contracts with its suppliers by shipping controlled products anywhere they wanted 'for a buck'.**

TTI Settlement's compensation was mostly legal and not financial

3 I declare that a large portion of the compensation I was to receive from the Trusted Timing Infrastructure license to DATUM was in the form of use

[3] The Bureau of Export Affairs – now called the Bureau of Industry and Science is setup to control the export of technology developed here in the US to foreign countries. The GLASSEY digital position evidence systems are all controlled under such constraints and require formal notice to the US Government for the export of such technology as well as the approval of the Bureau's export administrations office.

[4] Specifically see http://www.access.gpo.gov/bis/ear/pdf/743.pdf PARAGRAPH (c)(1)(ii) which constrains positioning ("a process requiring precision timekeeping capabilities") as technology for which export licensing is required. As such the precision time-stamping service using PTP type timekeeping equipment would require this as well. As such any export with this system and its controls would also require reporting. This reporting was to be turned over to GLASSEY and MCNEIL to document the use of their product technologies and as such properly value other IP's still not included in these DATUM settlements. As such the refusal or failure to provide that information is a breach of the four reporting section requirements.

information they were to supply. This was contemplated and agreed upon as part of the agreement per section 8.1 and 8.4 and done so in perpetuity in 8.3. Based on this I declare that based on the license I signed it was my understanding that DATUM would notify each client they sold the use of the IP to that there was a formal requirement that the sale or transfer of control required that this IP cannot be sold, licensed or given to a third party without reporting its sale and possession or use by that third party. To date, although demanded numerous times no such notice has ever been served on GLASSEY or McNEIL that I am aware of.

DATUM-SYMMETRCIOM FAILURE

4 I declare that DATUM and SYMMETRICOM have failed in their re-licensing and through the subsequent illegal sale of that property to a Ireland-based Company in direct violation of the Settlement's requirements to stay within California's Jurisdiction with that property, and that entities further subsequent insolvency and that failed company's acquisition by another company, THALES GROUP , of France, which further violated the original use license since at all times the IP must remain within the jurisdiction of the Courts of the State of California.

The value of the settlement points – money was the smallest one!

The value considerations paid to GLASSEY for this were subsidize GLASSEY's creating of a global legal-template for time-stamping and providing proof in digital content. To do this DATUM was to provide the data specified for users and their acceptance of the license terms for each unit sold.

They also had the same requirement if they sold or transferred the IP rights to any other party in any form.

This was important to GLASSEY because the TTI DATUM licensed was a single TTI, one of thirty-two system designs GLASSEY had in place when he approached DATUM in the fall of 1997, and which finally concluded in the contract between the parties from February 1st 1998.

Datum's TTI license is as such a small portion of the IP Glassey entered into the agreement with and which he left with based on the particular language of the Settlement. As such it was important in valuing the entire Glassey portfolio to understand and know all of the end uses of all instances of all Glassey TTI's no matter who they were licensed to. That was the understood agreement between Glassey and DATUM on their use of his "type-2c" version of the TTI.

No reporting of sales of products made – no license acceptance proof provided

5 I declare that neither of those sales was reported to us under the TTI Settlement section 8 requirements nor in reviewing what information is available about those sales now, were they notified of the California Courts or California Law requirements for any matters pertaining to those IP's for them or any products built from them[5].

[5] It is worth noting that under this license model requirements, to receive that property that party which was using any product built with that Intellectual

/TSG/ - Witness my eHand, 9/18/2010
Todd S. Glassey, In Pro Per
Plaintiff
50 W. San Fernando St, Suite 320
San Jose CA 95113
800-511-2301

Property would also have to agree to be bound by the same controls (1) and (2) above as well since no derivative license can exceed the scope of the original license. The failure to require this would cause Glassey and McNeil tremendous damage and invalidate all of this agreement since it would enable anyone anywhere to reproduce the full scope of the GLASSEY DIGITAL EVIDENCE system these components are a part of.

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

Abstract

This document contains a detailed narrative on the five key claims which facilitate the State-level EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES complaint and a subsidiary set of Federal PRO-IP and EEA - Economic Espionage Act complaints also being filed by Todd S. Glassey (and Michael E. McNeil) against Symmetricom Inc. as well as its successors in this matter.

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

1. This document – THEFT BY FALSE PRETENSE/EMBEZZLEMENT BY AGENT Complaint Support

The specific claims herein pertain to CALIFORNIA PENAL CODE STATUTES 487 AND 503. Additionally they are also mapped to the Federal Economic Espionage Act 1831 and 1832 charging models per the USAA Handbook are included as section six in this document.

1.1. DIRTY HANDS: BENINSIG Prosecution Similarities

The claim-set is very similar to the claims by the State of California in the State v Franklin M. Beninsig prosecution.

1.1.1. DIRTY HANDS: "Patent Agent Representation Frauds" across six Jurisdictions!

Our case, like Beninsig pertains to IP Representation and follow-on Licensing Frauds alleged by Glassey (and McNeil) as well as both California and Foreign Patent Fraud through the EMBEZZLEMENT BY AGENT claim.

Patents derived from US6370629 – controlling access to stored information, are on file and in force in five jurisdictions today (US [US6370629], Canada [CA2287596], Brazil [BR9904979], Japan [JP2000163379] and South Africa. The EU Patent EP997808 was abandoned and its recovery blocked by Symmetricom and its Successors creating one of the fraud damage claims).

1.1.2. DIRTY HANDS: Intellectual Property Laundering

We also coin a new term for the State and Federal Authorities in this matter which we call INTELLECTUAL PROPERTY LAUNDERING, that being "the unlawful export and re-importation of said IP to attempt to set aside specific licensing terms and agreements" something that International IP Law like the British Contracts Act of 1999 pertain to.

1.1.3. DIRTY HANDS: WIPO and Lanham Act issues as well?

This also ties in the US to Lanham Act violations as well and a number of WIPO treaty violations. All in all the case is very strong in the sense of what happened, what property was stolen from us and how that was managed.

1.2. This Document – A Running Narrative

This document is intended to outline the specific areas of alleged California Penal Code, US Export/Import Act Frauds, and Federal EEA complaints which exist in the existing McNeil and Glassey v Symmetricom complaint.

These pertain to alleged international frauds and frauds instituted by Symmetricom and its precursor Datum INC to allegedly prevent Glassey from enforcing his rights in what was to be the shared-resource patent they convinced him to assign to them so that they could act as his agent. A patent they took payment for PRE-PAID LEGAL SERVICES as Glassey's Patent Agent in this matter. An act they demanded and then abused an assignment of patent rights here both in the US and abroad.

The frauds further are extended from IP frauds into property frauds allegedly extended by direct action of Symmetricom to prevent the enforcement of US Bankruptcy Court Sale orders to Glassey and to allow Symmetricom to 'continue to use other unlicensed IP which became Glassey's SOLE PROPERTY" per that same Bankruptcy Sale Order.

Also acts in this document are reviewed from several perspectives and so are repeated. Our apologies if this seemed repetitive but the intent was to keep the related evidence of the various claims together.

1.3. History Summary – the players and their interactions

1.3.1. DDI – Digital Delivery Inc

Digital Delivery Inc (DDI) is a Massachusetts based company who Glassey discovered in 1995 and who he worked with on their adding his GeoSpatial Controls to their Confidential Courier Product as an additional set of controls.

DDI's president Mark Hastings was the signatory to the Glassey CO-INVENTOR agreement which is the basis of DDI's use of the Glassey IP.

1.3.2. The Co-Inventor Agreement is a LEGAL SERVICES RETAINER – This created the AGENCY STATUS which is the basis of the EMBEZZLEMENT BY AGENT claim

The CO-INVENTOR AGREEMENT supplied in section 8 (aka "the PATENT SERVICES AGRREEMENT") is a LEGAL SERVICES RETAINER and was signed in 1998. It's retainer period opens a 1 year time clock for a complete set of terms and conditions to consummate the licensing of the Glassey Intellectual Properties to be produced or it rescinded the assignment of those rights fully.

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

The sole purpose of the CO-INVENTOR AGREEMENT is to BIND DIGITAL DELIVERY TO GLASSEY TO PROVIDE LEGAL SERVICES BEFORE USPTO AND OTHER PATENT AGENCIES GLOBALLY IN THE PROTECTION OF THE GLASSEY GEOSPATIAL CONTROLS.

The CO-INVENTORY AGREEMENT (Aka the CIA) also has a 1-year bomb clause and rescission language in it to cause the failure to provide the key supporting documents as the act which triggered rescission of the assignment. Datum is fully aware of the rescission clause as well.

1.3.3. DDI Agrees to provide these PRE-PAID LEGAL SERVICES to a LEGAL SERVICES AGENT in return for limited use of the IP the services were to be for.

In executing this agreement, DDI agreed to provide "Pre-paid Legal Services" for PATENT FILING and the prosecution of the original patent and any follow-on requirements therein.

It, these pre-paid legal services are the sole reason the patent was assigned to DDI without payment and for this service it would obtain very limited use of the IP as an extension of its pre-existing product, ConfidentialCourier™ and no other.

This requirement to provide these legal services and the limitations of the patent use survive the acquisition of DDI by DATUM and its sale to nCipher as well as the Thales group both under the CONTRACTS ACT of 1999 of the UK as well as US law.

Apparently the DDI product (the ConfidentialCourier product) and the '629 patent as well as other aspects of a intellectual property suite called the Trusted Timing Infrastructure or TTI have been sold to what is now the "Thales Group" and for which they are selling tens of thousands of the devices quarterly or more.

1.3.4. Datum

Datum Corporation is the Datum Corp late of Irvine California and now ½ of the merged entity called Symmetricom. The Symmetricom headquarters took over what was the San Jose California office of Datum's BANCOM DIVISION which was the division of Datum Glassey (and McNeil) wound up working with after the ATOMIC CLOCK division of Datum in Beverly Massachusetts declined to build the Glassey AUTONOMOUS TIME SERVERS or ATS systems.

[NOTE: ***The same ATS systems by the way which we assert now grace the Symmetricom product sheet as TimeCesium 4400 and 4500 devices].***

1.3.5. Relevant History: Fraud Claim with DoC

Additionally it's worth noting that Datum settled a fraud claim with the US Department of Commerce Bureau of Industry and Security (the BIS) which stemmed from another 1999 event where Datum apparently shipped atomic clocks to a part in a controlled country, one who was on the prohibited access list.

Symmetricom settled the matter by paying the fine without challenging the allegation of the underlying charge.

1.4. Datum's Alleged Frauds: ONGOING FRAUDS – including GRAND THEFT, THEFT BY FALSE PRETENSES, EMBEZZLEMENT BY AGENT

The currently alleged frauds span a decade and start with that Datum dealt in bad faith and had its attorney's create fraudulent documents it never intended to execute or be tied to as a strategy in wasting Glassey and McNeil's legal budget.

As such their (Datum's) offering to settle these claims through numerous meetings, and the production of two separate contracts at its expense, which contradict each other in places, is a clear statement documenting their fraudulent actions and underlying intentions.

We believe now that this was done as a legal strategy and consists of intentional busywork not for legal means but to expend valuable and key resources. As such it's a supporting effort to a formal act of fraud, that being the creation of a contract intentionally with no intent to execute it.

Further, after the signing of the first document (The TTI Settlement) that Datum asserted it had executed both of the settlement contracts and that Glassey and McNeil's Attorney Jason Book "Lost the executed copy" also supports these questions of intent. Especially since with the new law firm representing Symmetricom is now admitting Datum when the contracts were executed never executed the second contract nor did it (Symmetricom) intent to.

1.4.1. Datum's actions allegedly "involved their Lawyers in the Fraud to make it look legit"

As such it is our belief today that Datum functionally had its lawyers create as settlements, the TTI and DDI settlements as a smoke screen. This because of the newly admitted statements about Datum's "having never executed the second DDI Settlement document in regard to the Patent".

The problem they face is that while they can hide behind the assertion that the execution of the first TTI Settlement agreement ended all hostilities and legal actions between the parties the ownership of the Patent materials is still tied to the Co-Inventor's agreement since there is no follow-on contract defining individuals rights or the prosecution & enforcement practices which shared patents must by their very definition contain or they are not shared.

1.4.2. Intellectual Property Laundering: Symmetricom's actions in furthering those frauds.

This matter is an Intellectual Property Laundering offense. It is tied to the unlawful export of Intellectual Property which has now been returned to the US under licenses having no ties to the original IP licenses and copyrights.

1.4.3. Abandonment of EU Patent Filing EP997808

As part of its frauds against Glassey Symmetricom after the Datum fiasco actively was involved in the filing of the EPO Patent Filing (997808A2) which they later abandoned.

The abandonment was done after it was realized that GLASSEY would ultimatrely recover the patent ownership which would in the EU control key areas like RFC3161 timestamping and to prevent application to Time Of Use billing in the SmartGrid in the EU as well. This claim constitutes a formal fraud claim of the highest order based on DDI's agreement to provide the legal services and then their intentionally abandoning a patent after they became its steward.

1.4.4. Symmetricom Asserts it is sole owner and yet refuses to enforce these patents

Likewise Symmetricom through counsel to the various patent agencies asserts it is the sole owner of the US 6370629 Patent something it refuses to also serve Glassey notice with as well.

We feel this tends to support the assertion that Datum and its successor Symmetricom have waged a war of deceit from both Glassey and McNeil and their own Shareholders. A war which was facilitated to allow them to pick up all of the missing pieces of Glassey's TIME-AS-EVIDENCE and Systems Design library which they refused to pay him for in 1999.

This in fact we assert is what happened when Datum 'acquired pieces of the Intellectual Property (IP) which were only in Glassey's CertifiedTime Inc Japan Operations Center' something also documenting their actions in the IP theft with all parties cited herein.

Those CertifiedTime Inc IP's could not get to Symmetricom except as a submission from Amano who admits it stole them from CertifiedTime and refuted the US Bankruptcy Courts authority over them in Japan.

As such the importation of stolen IP is also a BIS matter for the Department of Commerce.

2. Claims 1 & 2 – THEFT and EMBEZZLEMENT: Patent Assignment Frauds

2.1. The '629 patent was assigned as part of a PRE-PAID LEGAL SERVICE AGREEMENT.

In 1999 I purchased pre-paid legal services before the USPTO (and other Patent Agencies) from a technology provider for limited use of the IP being patented. In that I agreed to share a Patent I was in the process of working on with Mark Hastings of Digital Delivery Inc. Mark offered to aid us in that process by amending a patent he already had issued which we would share in the ownership and licensing of. For this he and his company were to provide legal services to protect the shared IP as well as to file the IP before the USPTO and other Patent Agencies. As such it was clearly understood by all parties that this was to constitute "a pre-paid legal services agreement" and that the pre-payment was the limited use of the GeoSpatial Keying and Location Controls for Confidential Courier, the DDI product as it existed at the time of the signing. The Co-Inventor Agreement is formally then a LEGAL SERVICES RETAINER.

His patent, US 5646992 was the basis of a cryptographic envelope system called "ConfidentialCourier" which his company Digital Delivery sold. The envelope allowed for its content to be accessed under different rules and roles so that it could be used with internal access controls to manage large data distributions and was being used in real-estate services.

Hastings represented that by adding the Glassey GeoSpatial Controls you would be able to add "embargo and access-controls" so that a MLS listing for instance only was accessible from certain machines or at a specific time, as you could for sub-elements of those listings.

The value of such a system is substantial and so Hastings represented that what he got out of the fast-tracking the filing and covering all the legal and support fees was the use of the Glassey IP on the ConfidentialCourier product, and with that limitation the Co-Inventor's Agreement was crafted and executed as a first-document. One which by the way required other documents to be created with a 1 year time frame or they would become void for failure to perform.

2.1.1. Claim 1 – EMBEZZLEMENT BY AGENT through Pre-paid legal service fraud

CLAIM 1: EMBEZZLEMENT BY AGENT – CC Penal Code §503: Pre-paid legal services were purchased from DDI and Mark Hastings - In 1999 as part of a settlement into another IP area disputed with the defendant, Datum represented it would uphold the original contract from Digital Delivery Corp with the Plaintiffs (Glassey). That contract called for Digital Delivery Inc be a Patent Agent for GMT's use of it in creating GMT's initial first patent.

It (DDI and later Datum) would register the patent in numerous countries and then they (the inventors) would split the rights into areas of licensing so that Glassey could enforce his rights to the core IP. Additionally it would cover all of the costs therein unilaterally including the infringement prosecution's which was a key reason for licensing these IP's to DDI in the first place. All the time representing it was GLASSEY's PATENT AGENT through this CO-INVENTOR Agreement and the supporting PATENT ASSIGNMENT DOCUMENTS for the US and South African Patent filings.

The patent controls the use of LOCATION and TIME information as keys or controls to open and close (or lookup) other information or to trigger other digital events in a cohesive digital process.

This is now ubiquitous: With the expansion of GPS chips into everything these controls are now a sweet-spot which provide key value in a number of end-user and information control systems now especially those including location based networking services. As such this patent is arguably one of the single most valuable patents in the history of the planet Earth and its rights are specifically set up to be shared with Glassey as its principal inventor.

2.1.2. Hastings (Acting as GLASSEY's AGENT) expanded the filing by adding more GLASSEY IP to the Shared Patent Filings achieve the necessary NOVELTY to re-issue his original patent as the new Shared-Interest Patent:

This claim is further supported in that the Assignment Statement did not represent the last 3 Independent claims in US6370629 patent or any of the additions which HASTINGS and COUNSEL added to their original filing covertly.

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

These extra claims not licensed to DDI were in fact the core of Glassey's patent to be filed were added without approval or license to the DDI patent by Hastings in response to the Office Actions that demanded more novelty. As such Hastings added significant and key claims which he was not authorized to and it was the addition of those IP components which finally got the patent issued. As such what was supposed to be an amendment to US 5646992 was in fact a whole new patent, one which issued as US 6370629.

This LEGAL SERVICE RETAINER agreement is codified in a document called the CO-INVENTOR'S AGREEMENT (aka the CIA) and creates a set of shared rights and legal representation responsibilities for DDI or its successor regarding the creation of the remaining parts of the licensing agreement.

Without which per the Co-Inventor Agreement (CIA) the formal transfer of any IP rights becomes void 365 days after the signing of the CIA document.

In Summary:

- **LIMITED and SHARED RIGHTS:** The joint DDI/GMT patent was to be a shared-rights instance of the existing Confidential Courier Patent ( ), instead Datum acted in an ultra-vires manner and 'committed fraud' with the patent in its filing fraudulent assignment documents and then in later refuting that we had any rights to our shared IP.

- **SIX JURISDICTIONS:** That US patent was ultimately filed in six jurisdictions and abandoned in one prior to issuance of the patent, a further act of damage under the EEA complaint since no notice was sent to GMT members Glassey or McNeil in this and the matter is still sealed inside the EPO to prevent Glassey from recovering his rights therein.

  - The Jurisdictions are as follows: (US, Canada, Brazil, Japan, South Africa – where patents did issue) and the EU where patent filing 997808A2 was formally abandoned by Symmetricom without warning.

- It is interesting enough the only one instance of the patent Symmetricom have abandoned is the EU filing, but since the patent will control where a number of military technologies are built and who gets paid for them this makes total sense.

  - **SYMMETRICOM ABANDONS PATENT WHICH CONTROLS ITS OWN PRODUCT:** This patent would (does) control every IETF RFC3161 timestamping system in use on the planet earth today.
    - This technology component of new financial systems especially in the EU and constrains most all timestamping services in the GPS

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

Ground Segment as well. RFC3161 time stamping engines (now the rage in the EU) like the Thales Group Timestamp Server are the specific extension of the GLASSEY IP's herein and are fully controlled by the '629 patent and all of its other filings.

- What this means is "that Symmetricom abandoned the patent which would have protected their own product" were it not for the disputed ownership therein.
- ***Again another act by their management against their own shareholders.***

- This patent (had it issued in the EU) would have also controlled the German and British Braveheart 155mm Ballistic Sensor Fused Munitions for their Self-Propelled Howitzer technologies as of late. ***That alone brings BAE, the British Ministry of Defense and a number of others into this complaint and enables the use of the FOREIGN CORRUPT PRACTICES ACT complaint here.***
- Seimens and their Landys and Gyr division's infringement are significant with regard to the Time-Of-Use (TOU) billing in the SmartGrid as well.

- Further, because of these natural infringements which are being committed by parties in industries where Symmetricom sells the largest portion of its timing wares, is it our belief that SYMMETICOM abandoned this patent as part of a formal negotiation with nCipher and the British Government both of who it is formally tied to as well as to protect its ability to bid on and capture BAE and Home Office contracts for its timing gear.

- As well then, this action probably also constitutes or has criminal standing under the bribery and is ripe for a Serious Frauds Office prosecution in the UK if it occurred as it appears to have herein.

2.1.3. THEFT BY FALSE PRETENSES: Grand Theft and Embezzlement Complaints therein

Unlawful Licensing of a Patent is considered Grand Theft before the State of California (ss 487 [Theft by False Pretenses] and ss 503 [Embezzlement by Agent] of the California State penal code) and similar sections of the US Code as well.

2.1.4. Tolling the Statute of Limitations

Formal actions in discovering the key aspects of this fraud are currently before the California Superior Court where they have been since 2009 and were based on enforcement actions started in 2005-2007.

Attorney's became co-defendants to the Frauds
Because of actions of the Defendant's Counsel in this matter in 'hiding evidence of these grand thefts of Intellectual Property when documents were demanded' the law-firms used to 'dance this matter around to expire the Statute Of Limitations' for these grand-thefts also constitute participants in the fraud and have performed direct acts on behalf of those Symmetricom employees who committed the original frauds, and in doing so bring themselves into this matter as well beyond their role as Legal Advisers an act which made them direct participants in the continuing frauds.

As such the Statute of Limitations is proper and timely and since these are ongoing frauds – i.e. Symmetricom actively represents it is the sole owner of these Intellectual Properties the actual acts of fraud persist even to today.

2.2. Claim 2: Symmetricom is preventing Glassey and McNeil from enforcing Infringement Claims as a matter of Tortuous Interference and Patent Fraud

CLAIM 2: SYMMETRICOM is representing that it and only it owns all six patents and there is no shared access agreement in place. This constitutes a second claim in its violation of its role as the GMT Patent Agent.

How this happened is that Datum (now Symmetricom) acquired DDI and apparently covertly decided to not meet the terms of the contracts it was then tied to. In its actions SYMMETRICOM is representing that it alone owns all of this Intellectual Property. This means it is denying that the CO-INVENTOR AGREEMENT (CIA) terms are the controlling one only they cannot show any documents which set the CIA aside.

2.3. Scope of infringement claims

To understand the damage claims against Symemtricom [for its actions in fraudulently denying us access to the patent is held in trust for us] one has to look at their actions as a whole.

2.3.1. Intentionally preventing the proper valuation of the IP is a starting place

We will come back to this complaint later, but we need to bring up here in this complaint that the first one starts in refusing to allow proper external review of the patent for an establishment of value and their refusal to allow the enforcement for the infringers (who for the most part happen to be smaller customers of SYMMETRICOM who also have told SYMMETRICOM if the patent is enforced they will lose their business).

That said this claim is simple – our allegation herein is that Symmetricom has covered up the value of the patent to protect them from fraud and criminal prosecution before the SEC and their Shareholders. Symmetricom abandoned the EU patent filing as part of this cover-up to continue to be able to sell timing equipment to those infringers. That in and of itself is a staggering loss to the shareholders if Symmetricom owns the IP and a fraud which any reasonable damage claim would destroy the company over. In both instances there is a serious issue for the shareholders here.

2.3.2. Our Estimated Scope of Damages

The scope of the damages based in that statement are staggering. The Infringement claims against this patent cover-up should at the very least include the following market segments and providers.

- **<u>Location Based Services across a secure transport (network)</u>** – this will include all location based services in ***Search Engine Providers and in Social Networking Operations*** as well as portable computing platforms like cellphones.
    - **<u>Yearly damages here are conservatively estimated in the tens of Billions of USD based on the NTP v RIM court award alone.</u>**
    - Package and Freight Tracking is also included here
    - Google Street View is included here as well
    - Google and the other Click-Through Advertising services also fit directly under this USE INFRINGEMENT CLAIM to totally cement the value perspective of this filing.

- **<u>Time of Use Billing in the SmartGrid is another key area</u>**, and since SIEMENS (Landys and Gyr) has been aware of this patent and its implications on their ability to sell their own meters into Time of Use billing scenarios in Europe this is another key damage claim. It also may involve Seimens directly who also is a Symmetricom Customer at this time as well in a Balance-Of-Trade agreement between them and Symmetricom for its actions in blocking our enforcement against Seimens. Estimated royalties from this area are about 5B to 9B yearly.

- **<u>Time of Use Digital-Rights-Management on streaming or media content is also huge.</u>** It controls most streaming media and on-demand systems since they tag those to both a location where the media is to be delivered but also a time-of-use window to constrain that further. This particular use may also expand to control most on-demand media controls in all US and International Cable systems making it the first trillion-dollar area of infringement on the global use of the Glassey GeoSpatial Controls.

3. Claims 3 & 4: LAUNDERING THE IP: PRO-IP/2008 and the Trusted Timing Infrastructure Settlement Breaches

This next section talks to the next two claims, claims 3 and 4 which both pertain to the only valid Settlement License Symmetricom holds with Glassey and McNeil and its noticing that there is another Settlment or there is the Co-Inventor Agreement, one or the other of these two documents is in control of the Patent IP…

These are very important per the PRO-IP act of 2008 and its protections for licensed and trade-secret protected Intellectual Properties, a subject focused on in the Federal Offenses section of this paper.

3.1. THEFT BY FALSE PRETENSE: Theft of other controlled Glassey IP which was merged with the TTI architecture license (settlement 1)

<u>CLAIM 3:</u> THEFT BY FALSE PRETENSE: That outside of the DDI PATENT, Datum licensed a very specific set of Intellectual Property which it then violated both the use terms and the scope terms for that IP by selling it to a third party outside the license terms (See TTI Settlement Agreement as attached). Further that it exported that property outside the Jurisdiction of the US and failed to inform the party it sold the IP to that there were other constraints pertaining to that property.

ADDITION OF OTHER UNLICENSED IP: We further claim that in the fraudulent transfer of licensed proper to a third party outside of the license contract itself, that SYMMETRICOM also expanded the scope of that IP it sold to include numerous components of the Glassey TRUSTED TIMING infrastructure technology beyond the two-board solution defined in section 2 of the TRUSTED TIMING INFRASTRUCTURE Settlement which it had licensed a narrow use of.

SUCCESSORS ACTIONS: In doing so DATUM and its successors expanded the TTI to include "Any and All Software Clients" and integrated aspects of the DDI Patent Controlled IP into the TTI system it apparently sold to nCipher as part of a Joint Venture with them to off-shore this key Glassey time-as-evidence technology.

DATUM's LIMITED USE: Why this is important is that the TTI (per the Settlement Agreement description in Section 2) is constrained in the form of the TTI Settlement and the NDA Agreements under which Glassey submitted the original TTI suite of IP to Datum to build for him. Datum decided to 'go cheap' and only licensed 1 of a number of TTI forms which were shown to Datum because its goal was to expand the sales of its BOARD LEVEL TIMING PRODUCTS as described in the section 2 of the TTI Settlement and License Agreement.

3.2. All TTI users are tied to California Law and Courts

To reduce their licensing costs Datum agreed that a key portion of its licensing royalties would come in the form of on-going reports and market development efforts.

The requirement for this act and term to be propagated through the settlement to any subsidiary licenses or sales is a key part of the settlement itself.

This claim is/was codified in the contract per Datum's Attorney John Cannon Esq's who wrote this settlement "by leveraging the effects of sections 8.1, 8.3, 8.4, and 8.7 collectively" and that this requirement existed separately from any royalties which were limited to the first three years of the license.

SYMMETRICOM now refuses to comment either way on whether this was part of the agreement it created and it's attorney's produced. It was always agreed that Datum could come back and pay the marketing development moneys and extended licensing which would remove those requirements from the contract.

3.2.1. EXPORT and IMPORT FRAUDS: INTELLECTUAL PROPERTY LAUNDERING: The Unlawful Export and Re-importation of the "washed" IP

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

<u>CLAIM 4</u>: EXPORT and IMPORT FRAUDS: That SYMMETRICOM did combine unlicensed ’62 Patent IP with Trusted Timing Infrastructure technology to create the nCiper/DATUM Timestamp Server and that in doing so it exported that IP to England and then re-imported it back into the US under new and favorable license. As such this constitutes the “Laundering of Intellectual Property” and is a criminal as well as civil fraud against Glassey and McNeil.

The TTI contract has specific provisions that any and all parties assuming ownership of the IP must meet the requirements specified in sections 8 dot 1, 3, 4, 5, ad 7. And as part of Claim 4 Datum/SYMMETRICOM engineered the sale of this IP to a JV it and nCipher were undertaking together. As such this created a new owner for the IP and that owner was constrained by the original contract.

This action was used by SYMMETRICOM to ‘Wash the Intellectual Property’ to get it out from under the TTI License Limitations specifying the scope of the IP, its limited uses, and what HW components it must contain. Further when leveraged against the IP Abandonment of the EP997808 Patent Filing in the EU, to make that Intellectual Property which they used without license unprotectable by Glassey and his successors.

Without these constraints attached to the limited use license larger portions of the IP Portfolio SYMMETRICOM and DATUM refused to license as part of the Settlements would have factually been implemented by DATUM and its successors in violation of those limited use agreements.

As part of Claim 4 we assert that Symmetricom sold the TTI system to its new partner nCipher as part of a JV between the parties, and did so without bringing the key controls of the TTI license which must be propagated into this contract into place. This triggers the EEA in both 1831 and 1832 statutes and is fully qualified in 1831 by all four (4) constraints and in 1832’s case, by all six (6) constraints.

The claim is then that SYMMTRICOM entered into a contract with nCipher which specifically set aside the controls of the pre-existing licensing agreement and caused tremendous damage to Glassey in their theft of his intellectual properties which were later sold to THALES GROUP for an amount of $100M Euros.

How this is tied to this complaint - British Contract Act of 1999: Further while we assert that this sale was performed outside the legal controls of the US to enable these matters to be nearly impossible to control or exert damage claims to after the fact, what neither Symmetricom nor nCipher factored into this was the British Contracts Act and its effect on the sale.

3.3. For STATE EMBEZZLEMENT and THEFT claims this compliant is timely

In supporting the "Timeliness Aspect" of this all Statute of Limitations (SoL) in criminal prosecutions, the tolling of the SoL provides proper coverage for this complaint.

Further this is an ongoing fraud in which misrepresentations to third parties as to the ownership of the IP rights has happened within a clear window of that SoL such that this complaint is timely.

Finally, that the egregiousness of these acts both in the US and abroad broach the public interest in this tolling of the SoL as well to protect this US based resource and its global rights.

3.3.1. TTI Damages

The TTI Damages are simply that the system built exceeded the license and that the licenses were not enforced through to the new Successor, the Thales Group.

Further that the key hardware-based clock components of the license are no longer being built and have been replaced in violation of section 2 of the TTI Settlement with another unlicensed TTI-component, a general purpose software interface which was deployed to make it possible "to use the time-stamping features without the trusted local and trusted master clock systems" which directly violates the limited use licenses. All TTI Systems as sold by DATUM and its successors are limited to a TTI which uses the hardware based clock modules per section 2 of the settlement agreement. Any other implementation is forbidden in the license.

Further as part of the laundering of the IP, Symmetricom has apparently passed the product to a third party with no adherence to the transfer rules and requirements for this IP per section 8 of the TTI Settlement, especially sections 8.[2, 3, 4, 5, and 7] with especial notice to the refusal to provide the key documents contemplated under section 8.7 of the contract or its mandatory promulgation through to end users through section 8.3 and 8.4 of the TTI settlement agreement.

Since the Intellectual Property is in use in Foreign Governments for things like counting votes in elections in South America or other used in Britain and France, including military ones, this warrants a significant review of the licensing scope and the terms of the contract itself.

3.3.2. TTI Conclusion

We are asserting here that intent of this sale was to create a license for the TTI technologies which was far more than Symmetricom licensed and yet was impossible for

Glassey and McNeil to control because it was setup outside and intentionally apart from the laws of the State of California's Courts, an act which was intentional on all parties parts.

4. Claim 5: CONTINUING TORTUOUS INTERFERRANCE: SYMMETRICOM's Blocking the Enforcement of the US Bankruptcy Court's Sale Order

In 1999 when he started the Global Time Service provider company CertifiedTime Glassey cut a deal with the Japanese Reseller of Datum clocks. They were Amano Cincinnati Inc and built all types of systems including ones for digital timestamping of stock trades. Glassey was one of the global clock designers who was there when NASD and other Trading Frameworks went paperless and this created a hole in Amano's business such that they needed a new line of business.

Glassey approached them to work as his Japanese distributor and after contracting NIST to design an extension of the US Internet Time Server system which could be used to install a clone of the US National Timebase into a parties network as a trust-resource, they agreed.

Ultimately they (Amano) wound up 'stealing Glassey's customized IP and the computers in Japan while in the process driving the company, CertifiedTime into bankruptcy', or so we allege and assert here. They in the process worked with Datum then to package up the time service center which was apparently returned to Datum and which parts of are now seen in designs like the Symmetricom Time Scale Server and the like. Amano freely admitted they took the property and refused to return it. We are still trying to force Symmetricom to reveal the location of the two stolen atomic clocks so we may properly obtain warrants to recover them, something Symmetricom is also blocking with all means possible.

4.1. *Property Withheld: Atomic Clocks*

In 2002 the Global Time Service (GTS) provider CertifiedTIme Inc was sold to Glassey. A GTS which is a company which serves certified time to the systems that Glassey designed as trustable evidence sources, and which Datum and later SYMMETRICOM used extensively. The Debtor, CertifiedTime Inc was sold to Glassey through an order of the US Bankruptcy Court in BK #01-54207-MM in San Jose California.

This sale order included all of the Intellectual Properties including all products and the like. Datum had been in possession of all of this key materials through a NDA it signed with the DEBTOR when it made an effort to buy the DEBTOR, CertifiedTime Inc. Rather than selling the company to Datum the Bankruptcy Court chose to settle Glassey's 5.2M USD claim against CertifiedTime by transferring all of its assets to him including full title to those properties which CertifiedTime purchased from Glassey and then failed to pay for based on being driven into Bankruptcy.

This included a set of Atomic Clocks which are a US Only Controlled Resource since they are a key component of Crystron Triggers, the devices used in detonating thermo-nuclear devices.

In this instance this set of Atomic Clocks was stolen by Mr. Takamitsu Naito of Amano Corporation on June 21st 2001, and then turned over to the Government of Japan to operate a service Amano signed a contract with the Government to provide which is interesting because they were my (as in my personal selection) for our partners in Tokyo and it was CertifiedTime who in fact was installing a NIST UTC time service based around the operations of these clocks in Tokyo.

Why this is important is that Symmetricom has direct knowledge or should have knowledge of where those clocks are.

The reason is that when they acquired the product line from HP/Agilent Instruments in 2005 and 2006 they changed the serial numbers and re-certified all of the devices on HP Support Contracts so that their Serial Numbers were compliant to Symmetricom ones.

This action took physical access to the devices and an ongoing partnership with the people who stole them in the first place or the parties who have them today.

4.2. UNLAWFUL DETAINER: Symmetricom was in possession of key IP

4.2.1. Glassey IP

When I approached Symmetricom (Datum) in 1997 to build my Trusted Timing Infrastructure boards and my Master Timing Service system we signed an NDA so I could reveal the scope of the IP and its forms.

At that time the Trusted Timing Infrastructure was a collection of 8 key system architectures with 4 (four) variants each and they formed a matrix of 32 different methods of delivering and logging secure timestamps for evidence.

The argument here is that Datum only licensed one of these models and then took key factors of others and implemented them as its Trusted Timing Infrastructure – a system which ultimately discarded the Trusted Local Clock and Trusted Master Clock and became a pure-software timestamping solution in direct violation of the license.

This allegedly stolen IP also included the design of a device called an Autonomous Time Server, which is a Stratum-1 Time Server which can turn it self on and calibrate to a national time standard through some process. Symmetricom now offers this device family as a product without paying for that license and has for several years now.

4.2.2. CertifiedTime IP

As part of Symemtricom's diligence on Glassey's Global Time Service (GTS) provider business model Symmetricom *(and Datum) signed NDA's with CertifiedTime's executives to enable them to review all of the IP developed for the operations of the International Timing Center (a GTS system) in Tokyo with AMANO.

Much of that IP has magically appeared in a Symmetricom Product Offering called A Time Scale Server which is a repackaged version of the Timing Center on a Skid deployed with CertifiedTime's partnership with AMANO corp in Japan.

Amano Cincinnati is one of Datum's platinum resellers so anything that expanded the ability of both parties to sell Datum (now Symmetricom's) Timekeeping Equipment was considered a win.

5. VALUING THE IP: Why figuring out what the actual value of the damage claim is key to other potential claims from the State pertaining to an ongoing tax fraud

One of the key things Symmetricom (and everyone else along the line) have blocked is a proper review of

- What the TTI license provided for and what was ultimately implemented by it. Further what residual or follow-on license controls are tied to it

- What the value and scope of the Patent was – both as to what it covered and whether those matters provided extra potential revenue for the patent's owners or license holders.
  - Especially as to the predicted loss in the intentional abandonment of the EU Patent Filing.

5.1. The importance of Valuing the IP

Why this is important is that if the value of the corporation is tied to its intellectual properties and their licensing potentials then the failing to report that to the shareholders and to the State in their Tax and Corporations yearly filings would constitute a further criminal action, and in a world where transparency is key this hiding of an assets value is a serious fraud against the State and the Shareholders of the Corporation both one would think.

5.2. The Legal Logic in Valuing the IP

Corporation's do not have a legal right to 'hide' assets as offbook, or to mis-state their value to the auditors for both the State and the Shareholders. We assert both have been done in this instance.
The legal logic is simply that ***in an instance where an IP was worth billions of dollars this could change the minimum reporting and many other regulatory requirements for that entities operations as well within the State of California.***

This section talks to those claims then.

5.2.1. AMPLIFICATION: SYMMTRICOM's FRAUD IN PREVENTING PROPER VALUATION OF THE IP!

What's amusing about that claim is that it (SYMMTERICOM) has worked to prevent a proper valuation on that IP from ever being made.

The only possible reason for that is because it already knows what the IP is worth and if there is a third-party attestation to that there will be a serious cause for a fraud investigation of the Board and "C" level officers for their cover-up and withholding of this asset information from both their Shareholders and the SEC through their corporate asset disclosure in their 8K and 10K filings.

5.2.2. Scope of the Fraud relative to Symmetricom's total MarCap

As to why, it is our feeling that if Symmetricom had to disclose this single asset's value to the Shareholders as a real corporate asset this would change their MarCap from the

208M it sat at on Friday of last week to several hundred billion dollars based solely on the licensing revenue it would generate.

5.2.3. A third party's attestation makes it impossible to continue hiding the asset

It (the impending "finding of substantial value") will also directly change their filing status and corporate size statement with SEC and their tax rates as well documenting why its so important to keep the actual asset value off-book while still trying to gain control of all aspects therein.

As such whether GMT founders own this IP or Symmetricom owns the IP a serious fraud has occurred here.

5.2.4. The third party's attestation also will force the Government's hands

Further why this is equally important is that a key aspect of whether the British Government or the US DoJ will prosecute these formal complaints is clearly tied to the scope of damages and its dollar amount.

5.3. The implication and reasoning for Symmetricom's acting to block valuation of the IP

Why this is important is that one of the important things Symmetricom has been preventing is the proper valuation of the IP. With a world-class IP management firms attestation they would formally have to place the asset on their balance sheets and show its net value as an enforcement-revenue source, something that they are desperately trying to prevent.

5.3.1. Potential Criminal Implications of this action

The key concept in this is that we assert Symmetricom is blocking the valuation of the IP both because they don't own it and because the scope of the damage claim is many times their Market-Cap *(MarCap) of 232M as of the market close on Friday of last week.

That makes the minimum scope of the damages at the NTP v RIM award from several years ago as much as ten times their MarCap for cellular phones alone, not counting any other area of infringement.

Any single area of damage claims will drive the company directly into bankruptcy and as such their alleged actions in blocking or refusing to properly value the IP are understandable.

The problem is that this is an act then against the Shareholders of their company in doing one of two things – either intentionally preventing a legitimate damage claim which could destroy the company from being enforced, or in preventing their shareholders from enforcing their rights as the owners of the IP in question.

Either way, the officers of the company have committed an apparent fraud if this allegation is supportable and as such SEC and PCAOB should investigate Symmetricom as well.

5.4. IP Valuation is under-way and when completed will be supplied to the SEC as a source of fraud claim against Symmetricom itself

That failing by Symmetricom is being remedied here by the retention of a world-class IP management firm who will be submitting a formal statement as to the value of the IP.

This same document and its attestation will be filed in a formal complaint to the SEC alleging fraud in reporting of corporate assets and the failing of the PCAOB installed SOX controls against the management team at Symmetricom.

Since the firm in question who is evaluating the IP value are generally considered the #1 of these around today, their estimation should give all both the existing Shareholders and the SEC the fire-power needed to document the assertion of this specific fraud in their own actions.

5.5. EMBEZZLEMENT BY AGENT: The EU Patent Fraud and its Beneficiaries

The next question to answer is who would benefit from these alleged frauds? That as it happens is very simple to answer.

5.5.1. British Government and the British Contracts Act of 1999

The key beneficiaries of these two key frauds (the Patent abandonment in the EU and the alleged TTI frauds) are the British and German Governments and their Ministries of Defense as well as the British National Library and its Home Office as well creating yet another claim under a Foreign Corrupt Practice Act.

In this instance the British Government has acted in a unethical manner since it has refused to take notice of this ongoing fraud or its actions therein. Formal complaints have been filed with the Serious Frauds Office and MP Harman's office as the AG for the Shadow Parliament. Neither have picked up this case and have forced an instance where formal infringement claims will be filed against the British Government in an effort to seize assets of the Government itself to settle these issues – specifically its consulate.

Luckily the British Government and all parties through the sale of the IP to first nCipher and to their successor, there is the British Contracts Act of 1999 (the Act) which provides for the maintaining of the original license rights and mandates against the successors whether they are aware or willing to allow those to be enforced as we have here in. As such under the Act this matter (the EMBEZZLEMENT BY AGENT) and its unlawful sale of the IP without enforcing the licensing is correctable.

5.5.2. IETF LTANS document and RFC3161 time service providers

The violation of the protections of the patent would fall true for nCipher/THALES and several other entities including any number of parties in providing IETF RFC3161 solutions in Europe or those fielding Long Term Archival Storage protocol solutions (also called LTANS within the IETF).

This is actually a significant number of EU and British Banks who use this technology to meet their long term document/receipt storage requirements and their use is expanding now that transparency based on timestamping is becoming accepted.

5.5.3. BAE Systems

Additionally BAE systems and its handling of the Braveheart Programme aspects of this also opens them to scrutiny in this matter as well.

This would pertain to the use of all Location Based Services in any military operations by BAE an not just in Bravehearte Programme but in all of its operations. Battlefield Accounting, PNT Ground Segment, they are all covered under the applications based on location based services IP.

5.5.4. nCipher/Thales

Thales liability here is substantial – it has a direct responsibility in the UK to validate this, review the contracts and then "do the right thing" – something they are avoiding and which should have criminal repercussions for them if a parliamentary investigation supports this assertion of fraud on their part.

5.5.5. Cellular Providers – NOKIA, Vodaphone/Virgin Mobile and others

Finally we get to the Streaming Content Provides and Cellular Phone Manufacturers in Europe.

The last class if infringers is that of the mobile device providers, including but not limited to VIRGIN MOBILE, VODAPHONE, and NOKIA to name a few of the many which are tied to this. Likewise the content delivery providers and GeoTagging operations also infringe directly as does the GPS navigator applications as defined in the INFRINGEMENT ANALYSIS DOCUMENTS.

6. Federal Complaint: Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act of 2008)

Under the PRO-IP act the IP Laundering and re-entry into the US and into countries with IP Treaties with the US creates a new claim as well.

Section 506 (a)(1) of Title 17 states that "any person who willfully infringes a copyright shall be punished...if the infringement was committed—(A) for purposes of commercial advantage or private financial gain; (B) by the reproduction or distribution, including by electronic means...copyrighted works, which have a total retail value of more than $1,000; or (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public..."

The removal of the Intellectual Property which was controlled both under Copyright and numerous Patents from the US, combining it with other controlled IP under the two disputed settlements and then re-entering that as a commercial new product for sale in the US by the Thales Group constitutes a PRO-IP violation by the Thales Group themselves as well as Symmetricom Inc.

7. Federal Complaint: EEA Requirements

In setting up this complaint we want to aid the FBI in documenting the procedural and event-qualifications which make this a true EEA matter and provide a 'hook to hang your coat on' with regard to a complaint before the US Courts.

7.1. The parties maligned have made full efforts to protect the IP in question

Per the 18 U.S.C. 1839(3)(A) requirements, Glassey and McNeil have taken all necessary steps to protect their rights in comparison to SYMMETICOM who has formally abandoned one of the patent filings and has also not filed any notices of any infringement or notices of the patents existence or coverage area with the key Standards Committees as Glassey has, and as such this documents the assertion that Glassey and McNeil have fully meet the key standard of proof for "the owner…[of the trade secrets] has taken reasonable measures to keep such information secret." requirement under 18 U.S.C. 1839(3)(A).

7.2. For EEA consideration this compliant is timely

In supporting the "Timeliness Aspect" of this EEA complaint we assert that until this year and the last two months we were prevented from obtaining factual information around the abandonment of the EU Patent Filing such that this complaint could be made and that it is timely in its filing since this is an ongoing fraud.

As such since we have just formally obtained these key Datum this August 19th 2011 filing of this complaint is timely and meets the filing deadlines for the Statute of Limitations in this matter fully.

7.3. EEA Elements

This is a unique case since it qualifies for EEA prosecution under both the 1831 and 1832 statutes as follows.

7.3.1. 18 U.S.C. § 1831/1832: Element One – The Defendant Stole or, Without Authorization of the Owner, Obtained, Destroyed, or Conveyed Information

The Defendant acted as a Patent Registration Agent for a shared patent as well as a recipient of a specific set of IP called the Trusted Timing Infrastructure which are key properties and per attempts of the Defendant's counsel to protect that information from review of the courts based in its confidentiality and trade-secret value this documents full compliance with Section One – the information in question was taken by the defendant herein and made public to destroy its "protectability" as an Intellectual Property and Trade Secret while in their possession to prevent the plaintiffs from being able to exercise their rights herein.

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

7.3.2. 18 U.S.C. § 1831/1832: Element Two – The Defendant Knew the Information Was Proprietary

The Defendant in this matter, Symmetricom (nee Datum) was specifically retained to protect certain proprietary information which was the basis of this filing. As such as the Plaintiff's Hired-Agent they knew their role and the commitment. As such it clearly knew what was and was not proprietary information to the plaintiffs.

7.3.3. 18 U.S.C. § 1831/1832: Element Three – *The Defendant knew the information was trade secrets*

The defendant was retained to protect the Plaintiffs trade secrets by converting them to patents. The intentional adding of more and more protected and unlicensed IP from the Plaintiff to the US Patent it filed on both parties benefit was a key point in getting the US Patent issued. The additional trade secret material that was added in US 6370629's nine office actions came from protected and unlicensed IP which was controlled between the plaintiff and the defendant here by a non-disclosure agreement which fully documents that the defendant knew of the trade-secret status of all of this information.

7.3.4. 18 U.S.C. § 1831/1832: Element Four – *The Defendant Acted With the Intent to Benefit a Foreign Government, Foreign Instrumentality, or Foreign Agent*

The abandonment of the EP patent filing by the filing Agent, was clearly done to make the IP the patent would have enforced controls against wide open. Specifically those of Ballistic Sensor Fused Munitions *(smart bombs) and other services offered to the British Public through the Home Office and other verticals like the British National Library system.

7.3.5. 18 U.S.C. § 1832: Element Five – *Intent to injure the owner of the trade secret*

The Agent status of Symmetricom in this matter is key to understanding its responsibilities. In this matter the executives of the company have clearly expropriated property from both Glassey and from CertifiedTime inc (which was sold to Glassey under Sale Order from US BK 01-54207-MM exclusively). This was done to prevent Glassey from deploying his Smart Weapon Systems controls and his TIME AS EVIDENCE service technology for digital networking, both key assets in US and Global Security.

7.3.6. 18 U.S.C. § 1832: Element Six – Interstate or Foreign Commerce

Like Element 5 the Agent Status is key to understanding Symmetricom's responsibilities and intent. They (Symmetricom) apparently "Abandoned the EU Patent Filing to prevent Glassey from being able to assert the claims he would ultimately recover through the California Courts who would undo the Assignment for breech and fraud and in doing so this act clearly satisfied the requirement of 'an act perpetrated to prevent a US Citizen from being able to perform certain commerce in foreign countries'.

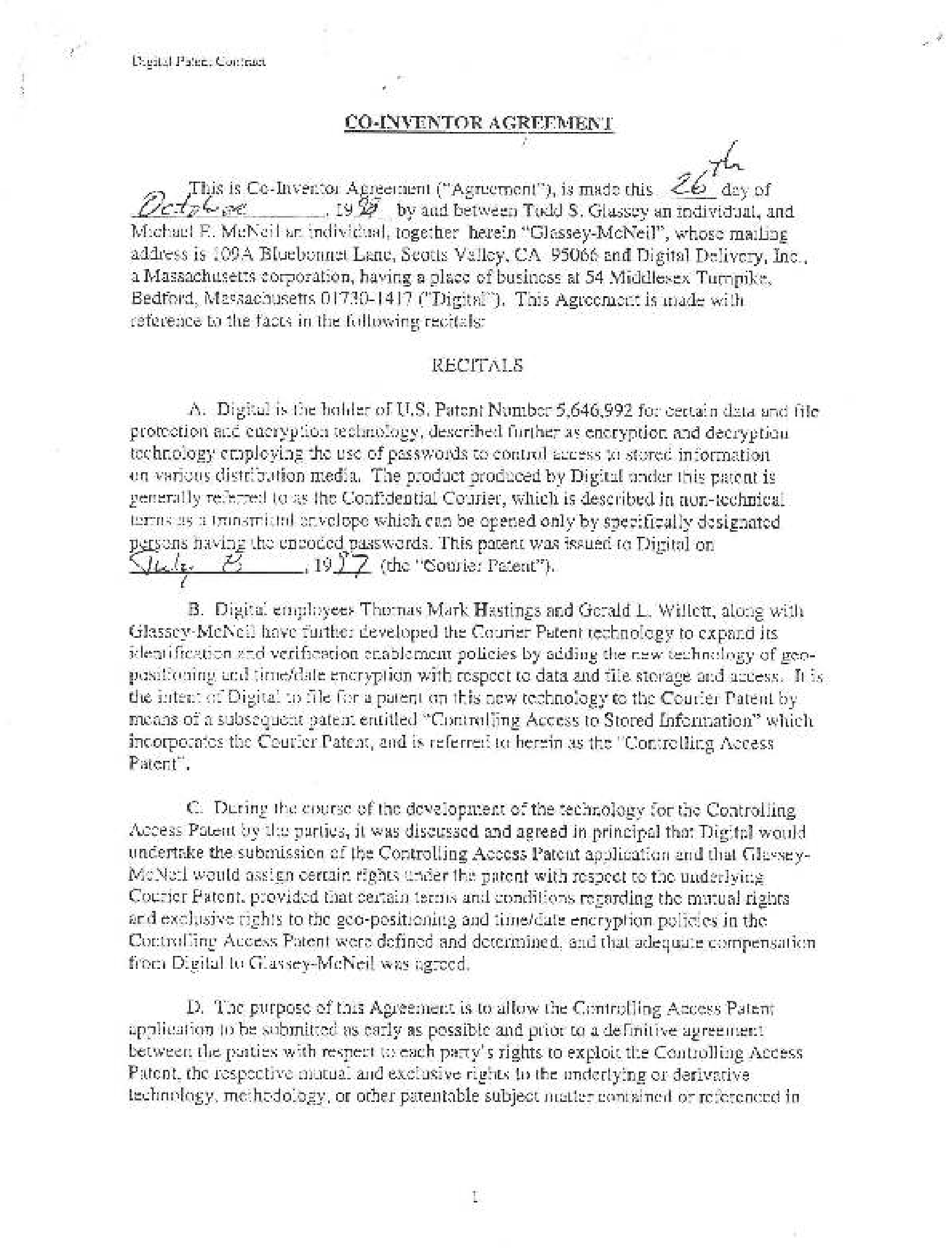
8. Perjury Declaration and Signature Block

Witness my hand in this declaration, it is made under the perjury laws of the United States of America and to that I declare that all statements herein for which I have knowledge directly are true and correct and to those I rely on information and belief, they also are true and correct, and that attestation is made so under the US Perjury Laws and its control.

Further that I have both existing PACER and ECF accounts and file electronic documents with the US Courts which are like constrained by the same laws and as such am recognized by the US Court System as an electronic document filer meaning that we apply that same level of credibility to this filing as well.

Witness my e-hand
Todd S. Glassey, 3/25/2012, California
//Todd S Glasssey - esign- enabled

9. Supporting Documentation: CO-INVENTOR AGREEMENT for LEGAL REPRESENTATION SERVICES BEFORE US and GLOBAL PATENT AUTHORITIES



Digital Patent Contract

CO-INVENTOR AGREEMENT

This is Co-Inventor Agreement ("Agreement"), is made this 26th day of October, 1997 by and between Todd S. Glassey an individual, and Michael F. 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".

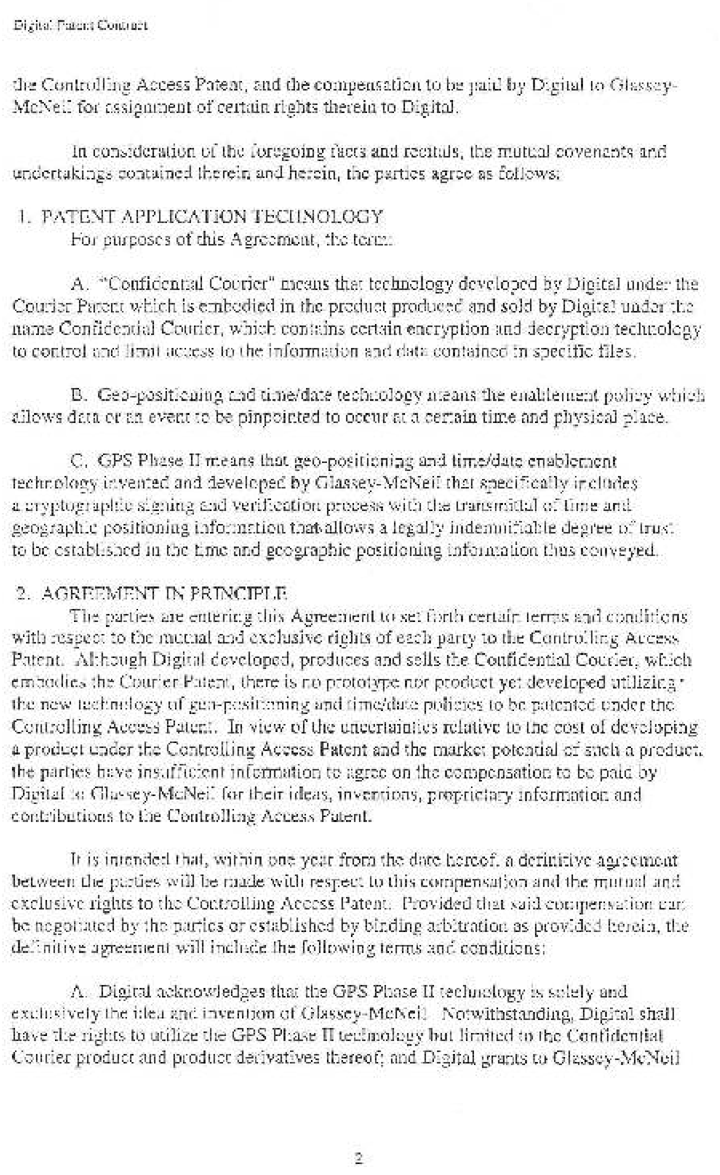
C. During the course of the development of the technology for the Controlling Access Patent by the parties, it was discussed and agreed in principal that Digital would undertake the submission of the Controlling Access Patent application and that Glassey-McNeil would assign certain rights under the patent 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

1

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court



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. "Conficential 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 thatallows a legally indemnifiable degree of trust to be established in the time and geographic positioning information thus conveyed.

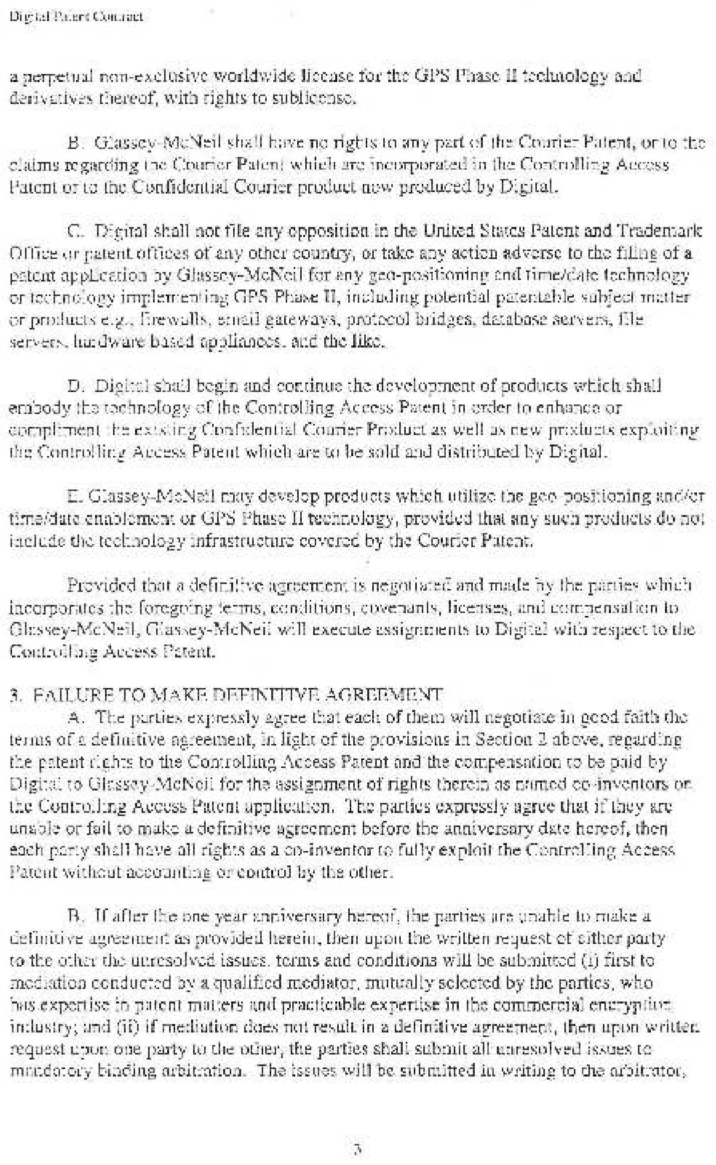
2. AGREEMENT IN PRINCIPLE
The parties are entering this Agreement to set forth certain terms and conditions with respect to the mutual and exclusive rights of each party to the Controlling Access Patent. Although Digital developed, produces and sells the Confidential Courier, which embodies the Courier 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

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court



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.

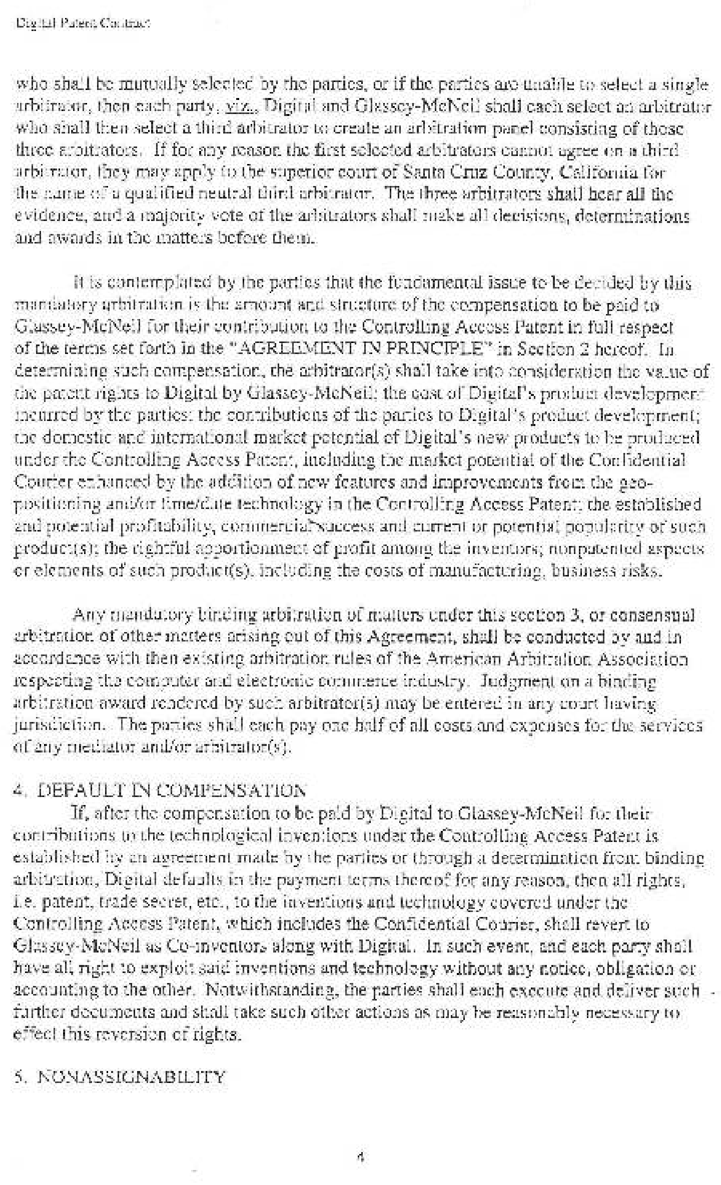
3. FAILURE TO MAKE DEFINITIVE AGREEMENT

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,

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court



Digital Patent Contract

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

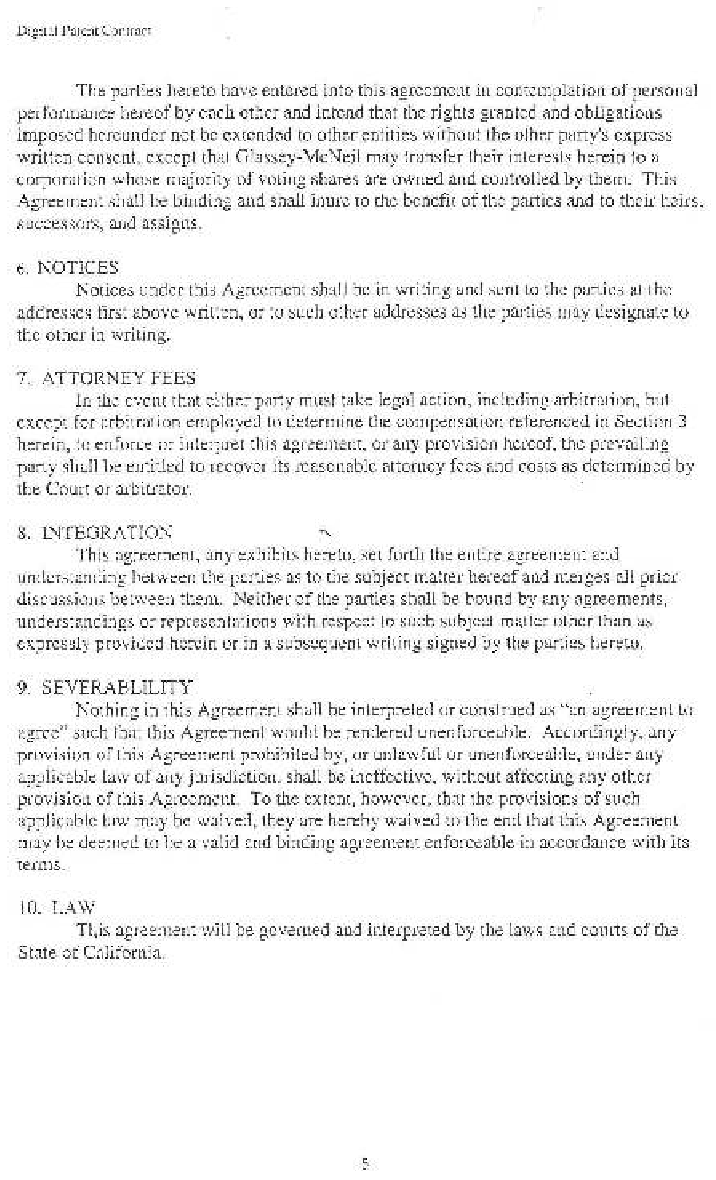
If, after the compensation to be paid by Digital to Glassey-McNeil for their contributions to the technological inventions under the Controlling Access Patent is established by an agreement made by the parties or through a determination from binding arbitration, Digital defaults in the payment terms 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

4

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court



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. SEVERABLILITY

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.

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court

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

DIGITAL DELIVERY

[Signature]

Tmack Hastings President
[Please Print Name/Title]

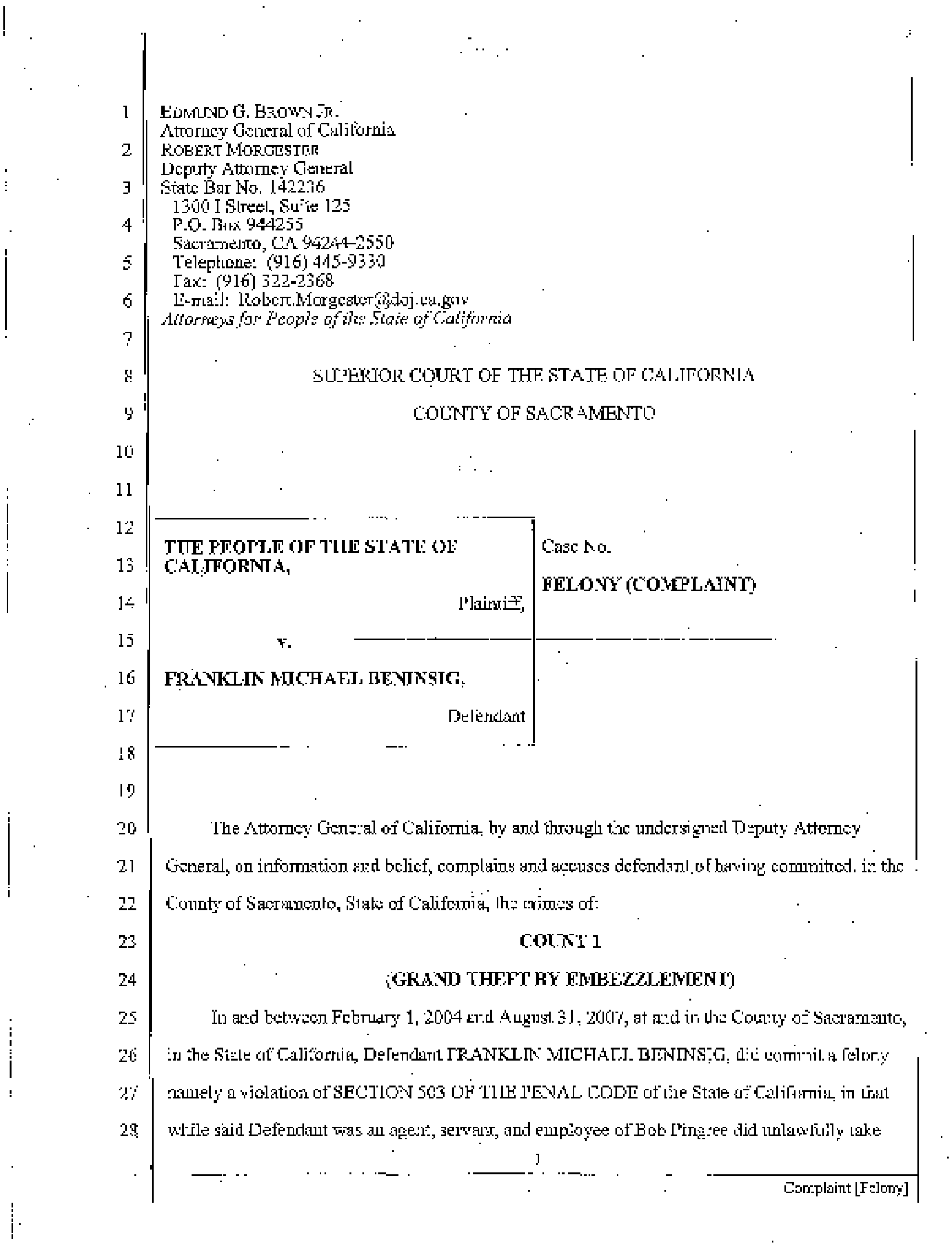
GLASSEY-McNEIL

TODD S. GLASSEY

Michael McNeil
MICHAEL E. McNEIL

10. Supporting Documentation: BENINSIG FELONY COMPLAINT

The following document is the State of California's Felony Complaint in the Prosecution of the BENINSIG matter.



EDMUND G. BROWN JR.
Attorney General of California
ROBERT MORGESTER
Deputy Attorney General
State Bar No. 142236
1300 I Street, Suite 125
P.O. Box 944255
Sacramento, CA 94244-2550
Telephone: (916) 445-9330
Fax: (916) 322-2368
E-mail: Robert.Morgester@doj.ca.gov
Attorneys for People of the State of California

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SACRAMENTO

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, **v.** **FRANKLIN MICHAEL BENINSIG,** Defendant	Case No. **FELONY (COMPLAINT)**

The Attorney General of California, by and through the undersigned Deputy Attorney General, on information and belief, complains and accuses defendant of having committed, in the County of Sacramento, State of California, the crimes of:

COUNT 1

(GRAND THEFT BY EMBEZZLEMENT)

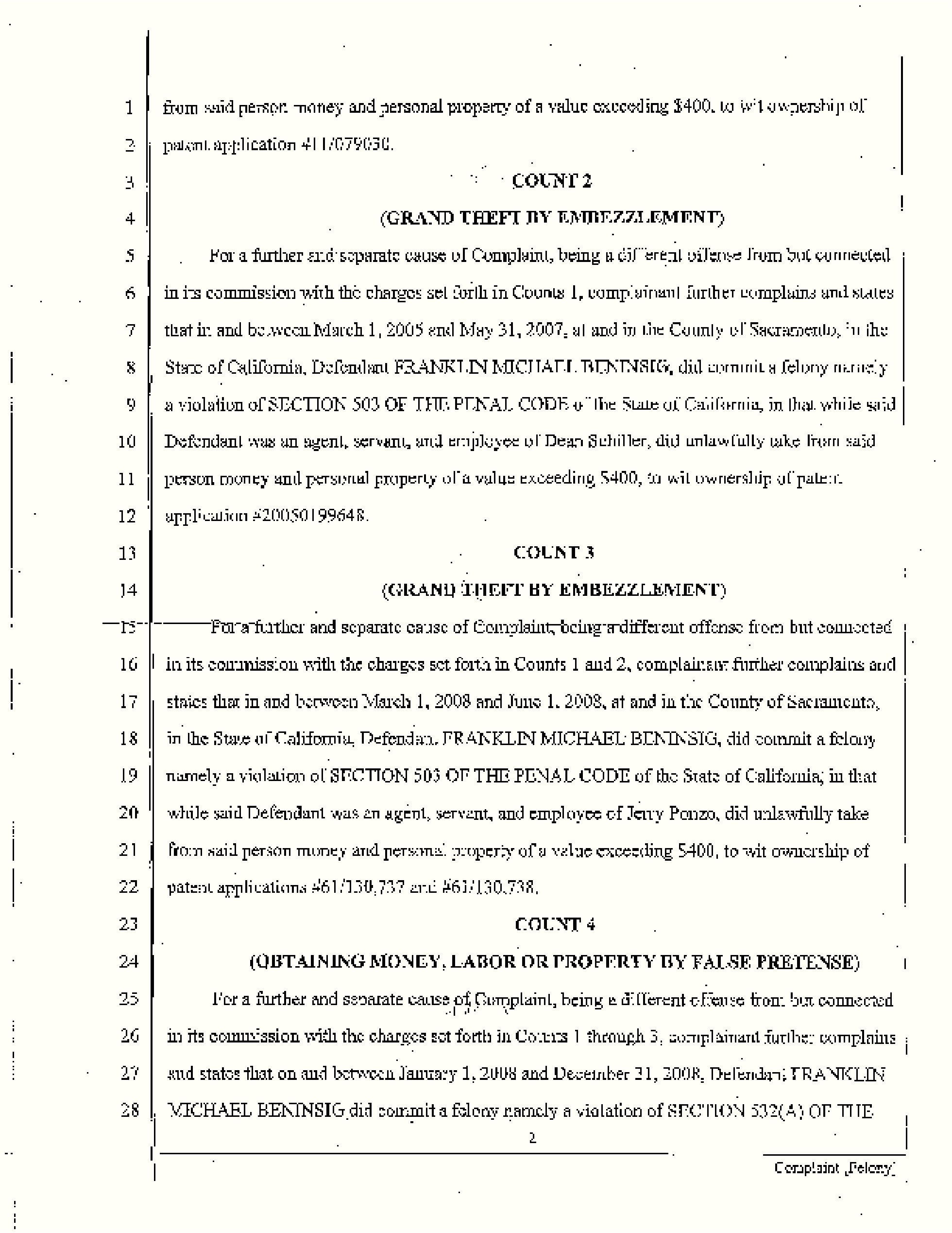
In and between February 1, 2004 and August 31, 2007, at and in the County of Sacramento, in the State of California, Defendant FRANKLIN MICHAEL BENINSIG, did commit a felony namely a violation of SECTION 503 OF THE PENAL CODE of the State of California, in that while said Defendant was an agent, servant, and employee of Bob Pingree did unlawfully take

1

Complaint [Felony]

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court



from said person money and personal property of a value exceeding $400, to wit ownership of patent application #11/079030.

COUNT 2

(GRAND THEFT BY EMBEZZLEMENT)

For a further and separate cause of Complaint, being a different offense from but connected in its commission with the charges set forth in Counts 1, complainant further complains and states that in and between March 1, 2005 and May 31, 2007, at and in the County of Sacramento, in the State of California, Defendant FRANKLIN MICHAEL BENINSIG, did commit a felony namely a violation of SECTION 503 OF THE PENAL CODE of The State of California, in that while said Defendant was an agent, servant, and employee of Dean Schiller, did unlawfully take from said person money and personal property of a value exceeding $400, to wit ownership of patent application #20050199648.

COUNT 3

(GRAND THEFT BY EMBEZZLEMENT)

For a further and separate cause of Complaint, being a different offense from but connected in its commission with the charges set forth in Counts 1 and 2, complainant further complains and states that in and between March 1, 2008 and June 1, 2008, at and in the County of Sacramento, in the State of California, Defendant FRANKLIN MICHAEL BENINSIG, did commit a felony namely a violation of SECTION 503 OF THE PENAL CODE of the State of California, in that while said Defendant was an agent, servant, and employee of Jerry Ponzo, did unlawfully take from said person money and personal property of a value exceeding $400, to wit ownership of patent applications #61/130,737 and #61/130,738.

COUNT 4

(OBTAINING MONEY, LABOR OR PROPERTY BY FALSE PRETENSE)

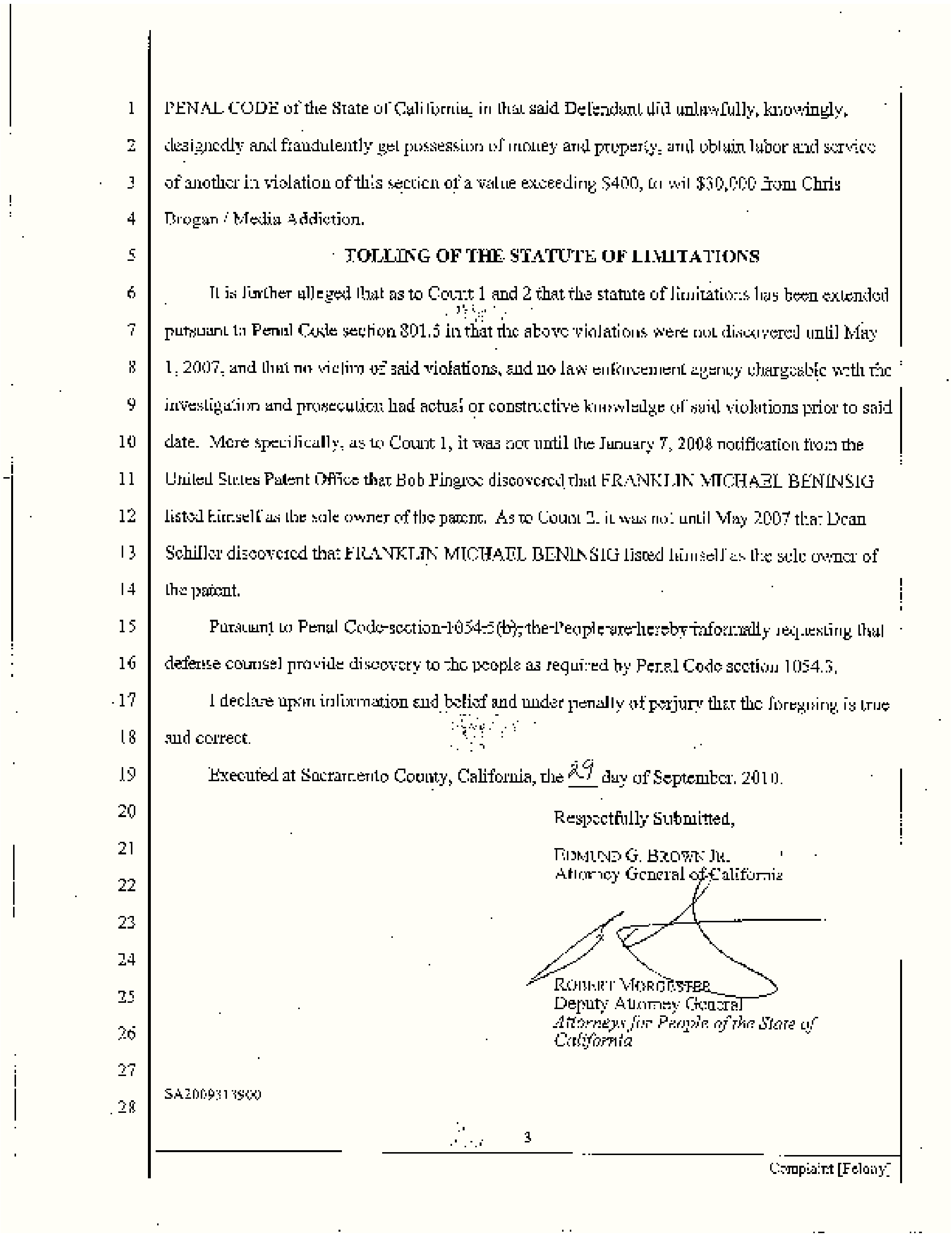
For a further and separate cause of Complaint, being a different offense from but connected in its commission with the charges set forth in Counts 1 through 3, complainant further complains and states that on and between January 1, 2008 and December 31, 2008, Defendant FRANKLIN MICHAEL BENINSIG did commit a felony namely a violation of SECTION 532(A) OF THE

2

Complaint (Felony)

EMBEZZLEMENT BY AGENT, THEFT BY FALSE PRETENSES
An State and Federal Damage Claim

(*in re:* McNeil and Glassey v Symmetricom, et Al)
CV165643 – Santa Cruz Superior Court



PENAL CODE of the State of California, in that said Defendant did unlawfully, knowingly, designedly and fraudulently get possession of money and property, and obtain labor and service of another in violation of this section of a value exceeding $400, to wit $30,000 from Chris Drogan / Media Addiction.

TOLLING OF THE STATUTE OF LIMITATIONS

It is further alleged that as to Count 1 and 2 that the statute of limitations has been extended pursuant to Penal Code section 801.5 in that the above violations were not discovered until May 1, 2007, and that no victim of said violations, and no law enforcement agency chargeable with the investigation and prosecution had actual or constructive knowledge of said violations prior to said date. More specifically, as to Count 1, it was not until the January 7, 2008 notification from the United States Patent Office that Bob Pingree discovered that FRANKLIN MICHAEL BENINSIG listed himself as the sole owner of the patent. As to Count 2, it was not until May 2007 that Dean Schiller discovered that FRANKLIN MICHAEL BENINSIG listed himself as the sole owner of the patent.

Pursuant to Penal Code section 1054.5 (b), the People are hereby informally requesting that defense counsel provide discovery to the people as required by Penal Code section 1054.3.

I declare upon information and belief and under penalty of perjury that the foregoing is true and correct.

Executed at Sacramento County, California, the 29 day of September, 2010.

Respectfully Submitted,

EDMUND G. BROWN JR.
Attorney General of California

ROBERT MORGESTER
Deputy Attorney General
Attorneys for People of the State of California

SA2009313900

3

Complaint [Felony]

Counterfeiting/Patent Fraud claims

The Counterfeiting and Patent Fraud claims are based on the following points

1) There are two specific contracts affecting this Device and the technology underneath it.
   a. In the first instance the Responsible Party (DATUM and later Symmetricom Inc) – licensed the use of this IP to a third party (nCipher) outside the US in violation of the terms in the US Only License Agreement (per Section 8.6 of the DATUM GLASSEY Settlement (settlement #1)).
   b. In the second instance DATUM after acquiring Digital Delivery Inc took the IP they held in Trust as a Patent Filing Agent and 'ran off with it' and in one instance abandoned the patent they (DDI) had filed on our behalf to prevent it in the EU of being applied to this box below and its market. They have sold somewhere between 20,000 and 50,000 of these units making them one of the most popular information security tools in the world.

<u>What is the infringing/counterfeit product?</u>
The Thales Timestamp Server product is the Datum Trusted Timing Infrastructure expanded to use portions of the TTI which Datum did not license from GMT Inc in the TTI Settlement. It was built using the GLASSEY TTI Intellectual Properties licensed by DATUM and nCipher (of Cambridge) who was later acquired by the Thales Group.

http://www.thales-esecurity.com/Products/Time%20Stamping/Time%20Stamp%20Server.aspx

The Thales TTI based timestamp server is now a very popular product in Europe and in the US as well.

<u>Contract Acts of 1999 implications</u>

The transfer of the license from DATUM to nCipher, and later from nCipher to Thales Group is controlled under the terms of the Contracts Act of 1999 and the TTI License Settlement.

The Timestamp Server has other technology added to it

Claims (These claims pertain to Symmetricom Inc, the merged successor to DATUM) and through the Contracts Act of 1999 they also pertain to the Thales Group and the Timestamp Server as well as its software and hardware components.

We assert the following:

1) **In Re TTI License Frauds:** Datum (now Symmetricom and later nCihpher Inc and finally the Thales Group – both UK Companies) took Intellectual Properties it was licensed to use called the TTI inside the US and under California Law and transferred them to a party outside the US without any controls for the original license.

2) **In Re TTI License Frauds:** The license limited the use the US per section 8.6 of the TTI Settlement Agreement. Under this agreement the product was only licensed for use "in the Counties and States in the United States where Datum did business at that time". No other licenses beyond the use of the IP in this limited geographic region was contemplated or authorized. ***Symmetricom's sale and transfer of the TTI IP to nCipher in the UK violated this US Limitation by placing this product outside the US.***

3) **In Re TTI License Frauds:** The TTI license limited the use to certain HW systems which were implemented as software and then sold on open systems in violation of the terms of the IP licensed. ***The claim here is that Symmetricom and nCipher expanded the use of the TTI to include a key component DATUM had refused to license from GLASSEY and McNEIL – that being a SOFTWARE ONLY CLOCK and TIMESTAMPING SYSTEM. DATUM's sole version of the TTI was the card-set TTI that it purchased from GLASSEY per sections 2.1, 2.2, and 2.3 of theTTI Settlement Agreement. No other product versions are authorized and all timestamping systems must use this service model as part of the TTI Settlement (including PTP – precision time protocol cards designed years later).***

4) **In Re TTI License Frauds:** The license does not allow for any other IP to be merged with the licensed IP because of the limited scope of use of the type of systems licensed (those being PCI 2.1 based computer cards and the software to use those cards). ***The claim here is that first Datum and later Symmetricom and nCipher merged IP it held in trust for GLASSEY per the co-inventor agreement (a separate agreement***

from the TTI Settlement) and merged that IP without license and authorization with the TTI technology the Time Stamp Server was built on top of to add more unique functionality designed by GLASSEY to the product. No license for this was contemplated or authorized. Finally that nCipher was acquired by THALES GROUP with all of its licensing issues to address which THALES GROUP has ignored in total to this date.

TTI License Agreement Fraud Summary:

As such, per the claims above Symmetricom sold the property to a party outside of the license agreement outside of the Jurisdiction of the US and California Courts (nCipher who was later acquired by the Thales Group).

We believe this is counterfeiting matter in that they "illegally transferred IP outside the US to serve the government of another country through the party they sold the IP to. Those IP's are in use in the Japanese, British, South African, and three other South American Governments in the form of voting and digital record keeping systems called Timestamping Systems. The timestamp server is a key part of many of the British Government's control processes making it a recipient and beneficiary of that fraud as well.

Because of the TTI Settlement's language of Sections 8.1 selecting California Law, and Section 8.3 which states that these requirements are transcendental – i.e. that they apply to licensee's of the products and that the licensee *** MUST *** agree to this set of terms. DATUM and its Successor Symmetricom sold this IP to nCipher who was later acquired by the French Aerospace/Military Systems Corp Thales Group without either of them agreeing or being willing to be tied to those terms. Both entities have refused to comment and continue to sell those systems including the Thales Timestamp Server in the US and Globally in direct violation of the license agreement from myself to Datum.

5) GLASSEY assigned a set of intellectual properties to a third party (Digital Delivery Inc) for their role as a patent agent. This is a LEGAL SERVICES AGREEMENT and was to provide PRE-PAID LEGAL SERVICES to GLASSEY in the form of PATENT FILING and PROSECUTION SERVICES.

a. ***The payment for those services was the pre-contemplated use of the IP protected in the PATENTS in a limited manner described in the CO-INVENTOR AGREEMENT in the Jurisdictions where the various patents were filed.***

b. ***Under the CO-INVENTOR Agreement (the limited use agreement to provide legal services) GLASSEY Patents were filed for in the US, Canada, EU, South Africa, Japan and Brazil. All issued except the EU***

patent which Symmetricom and nCipher (the successor to DATUM) later abandoned without notice.

6) **PATENT AGENT FRAUDS:** As to how DATUM and its successor Synmmetricom got into this patent complaint, this PATENT AGENT relationship was functional until DIGITAL DELIVERY INC was acquired by DATUM corporation who GLASSEY had an ongoing IP dispute with based on a contracting agreement in market-development which turned into a 'relationship where Datum was allegedly stealing Glassey's IP'.

a. **In valuing the Patents IP:** Since the patent in the US was used 'covertly to collareralize a loan for millions of dollars shortly after its issuance without authorization from GLASSEY' a basic multi-million dollar valuation at that time was placed on the patent.

7) **PATENT AGENT FRAUDS:** Some years later after GLASSEY formally as part of a global standards group IP Rights Discussion formally posted a "We Will Not License this IP to the IETF (the Internet Engineering Task Force – the keepers of all Internet Standards) the patent filing was 'quietly and with no notice' formally abandoned by the filing agent (now Symmetricom/nCipher) in what we believe was an attempt to make the patent non-enforceable against nCipher and its successors in its native country for this fraud. As such, as our PATENT AGENT entity, this is a clear representational fraud and one done to provide significant revenue in the sales of the nCipher Entity to THALES GROUP.

a. **PATENT AGENT FRAUDS:** Further that in its representation of GLASSEY and MCNEIL IP Rights per the TTI and DDI Co-Inventor Agreements, that Datum and later Symmetricom 'abandoned the filing of a European Patent it contractually was filing for GLASSEY under section 2C of the CO-INVENTOR Agreement (between Glassey and Datum). As noted above the patent (US6370629) was filed in five other jurisdictions in which it all issued except for the abandonment of the EP997808 filing.

b. We believe that this action was done to prevent GLASSEY from being able to assert that patent against the THALES TIMESTAMP SERVER since it uses a considerable amount of the patent's controlled IP therein.

Dealing in bad faith: *DATUM AND THE TWO SETTLEMENT PROGRAM THEY CREATED…* As its solution to the dispute DATUM Attorney JOHN CANNON proposed a two contract settlement – one for the TTI and the second for the Digital Delivery Patent because the two sets of intellectual properties were not being licensed for use in the same system – something we assert DATUM, SYMMETRICOM and its successors nCipher and THALES GROUP all intentionally violated.

The Two Contract Settlement turned out to be smoke and mirrors when DATUM refused to execute the extended DDI Patent IP Licensing Agreement:

Oddly enough DATUM performed a fraud at the signing time saying they had properly executed both documents, something they have retreated from since denying that the second agreement – the DDI Patent License Agreement was ever executed. This made the only controlling document the CO-INVENTOR AGREEMENT per section 3.5 of the TTI Settlement.

8) **PATENT AGENT FRAUDS:** Under Either Contract – the DDI Patent Assignment and Co-Inventor Agreement or the CANNON unexecuted license for the use of the DDI IP, DATUM and its successors hold only very limited rights in the DDI Patent IP. They may only use it in the manners contemplated in the actual CO-INVENTOR AGREEMENT and as such Datum SOLD ILLEGALLY WITHOUT LICENSES technology, the DDI materials represented myself and my partner in its Patent Application in a number of foreign jurisdictions to parties as part of the Time Stamping system as described above.

NOTE: California State is criminally prosecuting another PATENT AGENT FRAUD matter.

a. A very similar case (California v Franklin Michael Benensig) is being prosecuted as a Theft By Agent matter before the State of California as a criminal prosecution as well, further demonstrating the scope and breadth of this heinous act. Our assertion is that 'being a patent agent is a fiduciary role and that as such there is no difference in this matter than the one in Benensig herein'.

As such we assert that we are victims of frauds and that the THALES DEVICE called the TIME STAMP SERVER (see attached collateral) is being sold illegally without license and we are applying from protection from US Customs and Border Patrol in this matter for IP Rights Violations.

Witness my hand, and this declaration made under the perjury statutes of the United States of America from my office in San Jose California.

//TSG – Todd S. Glassey
e-Sign Authorization 4/3/2012

TODD GLASSEY

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321
tglassey@earthlink.net

Michael E McNeil In Pro Se
Michael E McNeil In Pro Se
PO Box 640
Felton CA, 95018-0640
831-246-0998
memcneil@juno.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

Todd S. Glassey In Pro Se and Michael E. McNeil In Pro Se, Plaintiffs, vs. Microsemi, et Al., Defendants	**Case No.: 3:14-CV-03629-WHA** **PARTIAL SUMMARY JUDGEMENT - Count-8 IETF PERFORMANCE RIGHTS AWARD** **Date: January 29th 2015** **Time: 8 AM** **Courtroom 8** **Judge W.H. Alsup**

PARTIAL SUMMARY JUDGEMENT - Count-8 IETF PERFORMANCE RIGHTS AWARD

1. May it please the Court, on January 29th 2015 at 8AM or as soon as may be considered, Plaintiffs in the above captioned action hereby move, pursuant to Fed. R. Civ. P. 56(b), for Partial Summary Judgment in their favor, and against DEFENDANT IETF, issuing Plaintiffs a PERFORMANCE RIGHTS STANDING against any IETF protocol Plaintiffs can demonstrate contains their protected PHASE-II IPs.
2. This motion is made up of this Notice of Motion and Motion, Declarations, Memorandum of Points and Authorities, and Exhibits, with Testimony to be given at the time of the hearing into this matter.

BACKGROUND

3. This Motion is a precursory motion for a set of secondary set of summary judgment motions 35 USC 271 and 17 USC Infringement claims pertaining to PERFORMANCE RIGHTS in programs which contain Plaintiffs' PHASE-II IPs and which are controlled under the IETF's Copyright and Performance Licensing control therein.
4. QUESTION - what happens to the IP rights for a Derivative Program created from a Standard which contains PATENT PROTECTED Intellectual Properties. How do those Patented Computer Program Rights translate into Programs which are written and infringe and republished under a separate copyright cover?
5. Plaintiffs have documented 20 notices over 2006-2008 of Infringement on Plaintiffs' PHASE-II IP enforcement rights which IETF refuses to recognize, and have stopped noticing the IETF after filing a Blanket Denial of Rights to use any PHASE-II IP in any Standards Documents; Plaintiffs have identified 64 other key Internet Backbone protocols which in today's versions from the IETF infringe US6370629's Claims 19-32 Controls in one or more areas.
6. For the CORE PROTOCOLS they also have no no-infringing methods of operation. As such these infringements pertain to critical Internet Protocols which today control all key Internet Operations.

Summary Relief Statement

7. Plaintiffs seek a summary order against IETF, and its sub-licensees (by their reliance on the IETF's Master License), granting Plaintiffs full PERFORMANCE RIGHTS STANDING against the execution of any program derived from an IETF Standard containing Plaintiffs' PHASE-II IPs.
8. That this is a full Performance Rights Standing against the entire Publication Length of that Document and Plaintiffs enjoy all protections

and privileges against the Copyright controlled performance rights for the execution of those programs.

9. This is appropriate for all IETF Standards after being served with the Master Cease and Desist any and all uses including in systems IETF operates upon in 2005, 2006, 2007, 2008 and 2010.

Table of Contents

Cases

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

The Court must accept all well plead complaints as factual and accurate

10. Under precedent, the court must accept as true all of the well-pleaded facts alleged in the complaint, and may not dismiss the action unless it is convinced that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief. *Bloor v. Carro, Spanbock, Londin, Rodman & Fass, 754 F.2d 57 (2d Cir.1985)*; *Austad v. United States,* 386 F.2d 147 (9th Cir.1967).

IETF, the keeper of the Worlds LAN and Internet Networking Standards

11. The IETF, the folks who publish all of the STANDARDS globally for LAN and Internet Applications, is an organization which is run by the Internet Society and functionally operated by ISOC with hand-in-hand help from the Industry Members and the US Government; all of the key parties who use its practices as a way of creating network and Internetworking which talks to each other.

12. Without the Standards the Internet would not be possible, but these same standards also control all local area networking outside of the

Ethernet Standard itself, so all switches and routers speak IETF Protocols meaning the IETF protocols run the world as well.

IETF Protocols Specifications called RFC's create a Software Program...

13. The RFC is a cookbook for how to build a network-practice or process, i.e it is a specific statement of method, and that means a Standard can in fact be based on processes and practices which are part of a method patent, especially true in the new world of patenting programs.

14. Because a network standard is a process-specification for the implementation of a computer networking program and its licensing provides either a blanket or, for "SYSTEMS AND PROGRAMS BUILT FROM ITS USE, A PER-USE PERFORMANCE RIGHT type license.

The IETF is a Rogue State

15. The IETF has become somewhat of a rogue state which has allowed the Corporate Sponsors to create and manage their own camps.

16. Most independent parties have no real chance unless they are backed by a University of getting an IETF Working Group setup or actually undertaking a protocol standardization effort (a two year minimum financial commitment to the IETF and the underlying engineering costs).

17. Inside the IETF process (see Exhibits BCP78 and BCP79 for the complete framework today) the workgroups churn away compromised documents between the engineering partnerships. Generally this is two or more companies or universities and often a government or two as well. That has an implied cost of several million dollars today as well placing a statement of worth on an IETF Standard as being somewhere between two million and four million to considerably more in some programs.

18. Once prototypes are built and the functionality taken to the next step, the IETF publishes all documents under a basic research exemption under

section 107 of the Copyright Code even though they are not a research entity (they maintain that as the IRTF) and refuse to create a licensing model with meets DMCA or create a takedown policy for any documents which contain unauthorized, stolen or already copyrighted IP from another source not authorizing its inclusion in the IETF document copyright protection.

19. Copyright protection extends to the particular form in which an idea is expressed. In the case of software, copyright law would protect the source and object code, as well as certain unique original elements of the user interface.

Defendants CISCO, JUNIPER, Apple, Google, Microsoft, and Oracle all implement their own IETF Licensed Products for resale

20. CISCO and JUNIPER sell Network Infrastructure Equipment. These are specialized computers with programs which implement the processes standardized in the IETF PROTOCOL SPECIFICATIONS. So if there are infringing designs, i.e. Patent Protected IP in those Standards it will be mirrored into every device Cisco and Juniper make which runs that protocol module. Apple, Google, Microsoft and Oracle all implement pure software, and in all but Oracle's case also implement cellular and mobile (pad) systems. As such they also create and reproduce IETF Protocols as does Oracle in its Sun OS network computer service infrastructure and products. As such all six of these defendants are directly tied to the IETF license and its Licensing Policies under BCP78 and BCP79 (both exhibits on this filing).

21. Copyright Section 102 and the associate sections provide that no copyright release can be asserted on an un-released Intellectual Property component of a Copyrighted Work, specifically Computer Programs which Implement the IETF Protocol Standards with Plaintiffs' PHASE-II IP so heavily integrated that they cannot function without it.

22. Copyright 102 also provides a relief as well in a reverse of the ***Apple Computer, Inc. vs. Microsoft Corporation***, 35 F.3d 1435 ruling. In this case Patent Protected Programs were copied into the Standards Documents which were then relicensed by the IETF for millions to use for their own network developments.

23. This buries the Plaintiffs' Protected PHASE-II IP into a computer which is programmed by each of the Defendants implementing the IETF protocols.

24. Those programs infringe when they are executed. The runtime licensing against the Use of the Programs is controlled under "performance rights" i.e. the ability to execute or "perform the work" as in to run the program.

A. Mazer and the Supreme Court's view on Patents with associated Copyrights

25. Plaintiffs assert that they as the actual owners of PHASE-II Rights do, and that this precedent is based on common sense, reinforced by the Nimmer on Copyrights commentary on Mazer[1] from the US Supreme Court, affirming that while Copyrights Cannot have Associated Patents per the USDC, the reverse can and is in fact true and that according to the Mazer ruling from the Supreme Court a Patent may in fact if it qualifies have Copyright Protections available for it in very specialized ways. In the case of Computer Programs those constrain PERFORMANCE RIGHTS.

26. In the context of the Copyright Act those Programs are controlled either by an open license or a closed one. Closed licenses can, and many do, operate based on a PERFORMANCE based Use and in fact most commercial software is "Entitled on a PER EXECUTION BASIS" at startup.

[1] *Mazer v. Stein,* 347 U.S. 201, 219, 74 S.Ct. 460, 471, 98 L.Ed. 630 (1954).

Named Defendants all have other Infringements, this pertains to IETF derived products they build and sell or give away.

27. Additionally most of the Named Defendants have Software Clients and Server Systems which serve them with infringing services, and those both constitute direct infringements as well, together with inducements to infringe when they are executed by third parties with the server systems in the Defendants' Operations - but those are addressed in other motions.

28. Microsoft as just one example brands its Operating System images based on both location and time of activation and cryptographically signs their control-blocks to create the tokens used to re-compute the Entitlement at Startup time.

29. This practice is a direct infringement of Claims 19-32 of the US6370629 Patent, making each startup action - i.e., simply turning on a Microsoft Operating System on any of the Computers it is sold for or run atop in the United States and arguably the rest of the World as well.

30. Apple, Google, Oracle as well as the commercial operators Ebay (and through this unnamed DOE AliBaba) and Ebay's Bank PayPal Inc, have the same issues. Each of their transactions in one or more ways infringe on US6370629's Claims 19-32 as well.

31. As another example, YouTube - the Ad which pops up and says "After N Seconds You can skip this" - that whole process as well as AdWords and their control practices are an infringement of Claims 19-32 as well. The secured transport handles the data signing and verification as a part of the appliance-like functionality in the Infringement Model.

32. This makes each and every video or image viewed through YouTube an infringement.

Xerox v. Apple commentary

33. The court framed the use of copyright in regard to everything pursuant to a design but stopped short of a performance rights statement against the execution of the code which contains infringing materials.

> The signers of our Constitution were as experienced in practical endeavors as they were in political activities. From an appreciation of both, the signers determined to permit the establishment of property rights in the realm of ideas. Hence, Article I, Section 8 of the Constitution provides that Congress shall have the power:
>
> > To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to Their respective Writings and Discoveries.
>
> Under the laws enacted pursuant to this clause, copyright protection is not available for many useful ideas (e.g., supermarkets, self-service gasoline stations, discount retailing, theories about historical facts). *See* A. Alchian & W. Allen, *Exchange and Production* 292-293 (3d ed. 1983); M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 2.11[A], at 2-157 to 2-159, § 2.18[H], at 2-213 (1989). Originators of such nonprotected ideas must derive their profits ("Ricardian rents") by being the first or most innovative to produce or deliver goods and services embodying nonprotected ideas (*see* A. Alchian and W. Allen, *supra,* at 189-191). But for creators of protected ideas, copyrights offer an additional reward by legally sanctioning a monopoly in accordance with the terms set by Congress. As a monopolist, a copyright holder will charge more and produce less than the price or output which would obtain under competitive conditions, but the resulting monopoly rent from copyright affords an incentive for socially beneficial creative activity:

34. The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is a most productive way to advance public welfare through the talents of authors and inventors in "Science and useful Arts." Sacrificial time and efforts devoted to such creative activities deserve rewards commensurate with the value of the innovative services rendered.

CONCLUSION AND RELIEF

35. As noted from the Ninth Circuit ruling in Xerox v. Apple, because the Copyright Act doesn't allow the Court to unpublish or delicense a

copyright as issued. The IETF is fully aware of this and its licensing program has been mentored under the watchful eye of Professor Jorge Contares Esq, a Rhodes Scholar and key Internet Advocate. One who in this instance apparently covered up this key flaw in the legal framework he as the IETF's counsel was personally responsible for over a decade with his Firm Wilmer Hale.

36. Because of the problems in pulling a fraudulently published document under US Copyright, which does not have a DMCA compliance practice because of both MAZER and the Ninth Circuit ruling on de-registering Copyrights being not an available form of relief under the law, Plaintiffs assert there is only one possible relief for their infringement. Granting Plaintiffs standing as a co-copyright holder specifically for PERFORMANCE RIGHTS from derivative Computer Programs crafted to implement parts of or all of the IETF Standards which infringe.

37. From Xerox v. Apple:

> The Copyright Act does not provide that a court may order the cancellation of a copyright. Of course, the inquiry does not end there. In determining whether a private right of action can be implied from a regulatory statute, the court must look to the Mazer Ruling for authorization and then the *Cort v. Ash* for the controlling factors:
>
> - Is the plaintiff a member of a class for whose *especial* benefit the statute was enacted?
> - Is there any indication of legislative intent, explicit or implicit, either to create such a remedy or to deny one?
> - Is it consistent with the underlying purposes of the legislative scheme to imply such a remedy for the plaintiff?
> - Is the cause of action one traditionally relegated to state law, so that it would be inappropriate to infer a cause of action based solely on federal law?
>
> *Cort v. Ash,* 422 U.S. 66, 78, 95 S.Ct. 2080, 2088, 45 L.Ed.2d 26 (1975) (citations omitted).

38. As noted from the Ninth Circuit ruling in Xerox v. Apple, because the Copyright Act doesn't allow the Court to unpublish or delicense the copyright as issued, in order that a Copyright may not be used to unilaterally invalidate a US Software Patent, Plaintiffs should be granted Performance Rights against Any Programs or like which are derived from IETF Protocol Specifications which contain PHASE-II IP. Likewise Plaintiffs are a unique subcategory holder of enforcement rights against a set of Intellectual Properties which are Patent Protected and which are today in use in millions of networking systems globally with no compensation to Plaintiffs whatsoever.

39. As such the Trial Court should issue this in a ruling granting Plaintiffs' Motion.

40. And finally we see from the Xerox v. Apple " In copyright law, remedies not provided are remedies not intended.[2]" Which is why the Supreme Court Ruling in Mazer stating that certain patents could in fact have copyright protection added to them; certainly Software Patents are exactly that animal.

41. That being the point - that Copyright Protections are available for Run Time Control against the execution of the binary or digital program are in fact Performance Rights in their purest definition and clearly anyone with Intellectual Property contained within those Programs would have Copyright Protection under the law automatically as an un-released participant in

[2] There is no indication in the legislative history that additional remedies are implicit in any other sections of the Act. *See generally* S.Rep. 94-473 (Nov. 20, 1975), H.R.Rep. 94-1476 (Sept. 3, 1976), and H.R.Con.Rep. 94-1733 (Sept. 29, 1976), *reprinted in* 5 U.S.Code, Cong. and Admin.News, 94th Cong., 2d Sess. 5659 (1976). The fact that a plaintiff's ideal relief is not specified in §§ 501 *et seq.* does not give the courts license to grant such relief simply upon application by the plaintiff. Except in this case MAZER in fact does allow the awarding of a recognition of the addition of PHASE-II IP to IETF standards in a performance right against the execution of those derivative programs from those standards.

the publication of that program earning that IP own full rights in that system as any other co-copyright holder has.

Closing

42. As such Plaintiffs move this Motion be granted and they be awarded a full and formal co-copyright owner standing in the copyright over the actual Standard Document; and/or

43. At the very least be awarded PERFORMANCE RIGHTS STANDING in the execution of any Programs implemented to those "infringing standards" which are the product of the IETF it relicenses use of. That this be made inclusive of any and all IETF protocols created or issued since the Patent issued in 2002 through the terminus of the US Patent.

44. That this include any and all IETF protocols shunted into the IETF TRUST created recently to isolate certain Intellectual Property issued from the main body of the IETF as well.

45. That this be set for any protocol or other process which Plaintiffs can demonstrate "contains an infringing or inducement to infringe component" (aka embedded PHASE-II technologies) as part of any program or other 'thing' which would be capable of using the IETF protocol standards.

x // Todd S. Glassey, In Pro Se 11/29/2014
Todd S. Glassey In Pro Se
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321

x // Michael E. McNeil In Pro Se, 11/29/2014
Michael E. McNeil In Pro Se
PO Box 640
Felton CA 95018-0640

ECF FILING DECLARATION

This filing was made on this day from my ECF account and as such was properly served on all parties with the exception of the State of California who still refuses to answer the complaint. The State is as such being mailed a paper-copy for their review.

Dated this 29th day of November, 2014

Todd S. Glassey, In Pro Se
Todd S. Glassey In Pro Se,
305 McGaffigan Mill Rd.
Boulder Creek CA 95006
408-890-7321

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

PLAINTIFFS,

vs.

Microsemi Inc; US Government - POTUS, the State of California, Governor Brown, The IETF and the Internet Society, Apple Inc, Cisco Inc, eBay Inc. Paypal Inc, Google Inc, Juniper Networks, Microsoft Corp, NetFlix Inc, Oracle Inc, Mark Hastings, Erik Van Der Kaay, and Thales Group as UNSERVED DOES

Defendants.

Case No. 14-CV-03629-WHA

[PROPOSED] ORDER

PARTIAL SUMMARY JUDGEMENT - Count-8 IETF PERFORMANCE RIGHTS AWARD

Judge: His Honor, Judge ALSUP
Where: Court Room 8
When: December 19th, 8AM

For good cause the Plaintiffs Motion to confirm PERFORMANCE RIGHTS for all IETF Standards defined and identified properly as containing Infringing PHASE-II Technologies with all standing as a co-copyright holder for the overall Copyright and sole owner under the Patent for the use of the IP through the Performance Rights created by IETF's unauthorized inclusion of those IP's in its Standards..

Witness my hand, Judge WH Alsup, ___________________, Dated ________ 2014

Subject: Library Question - Answer [Question #9755163]
From: law@loc.gov
Date: 8/8/2014 11:10 AM
To: tglassey@earthlink.net
X-Account-Key: account4
X-UIDL: 11e4-1f27-5bdbc4e6-9361-0021281794ea
X-Mozilla-Status: 1003
X-Mozilla-Status2: 00000000
Status: U
Return-Path: <law@loc.gov>
Received: from mx-stork.atl.sa.earthlink.net ([207.69.195.24]) by mdl-harvest.atl.sa.earthlink.net (EarthLink SMTP Server) with SMTP id 1xfOD41PI3Nl36V2; Fri, 8 Aug 2014 14:11:02 -0400 (EDT)
Received: from mshieldserver1.oclc.org ([132.174.29.209]) by mx-stork.atl.sa.earthlink.net (EarthLink SMTP Server) with SMTP id 1xfOD12ko3Nl34c0 for <tglassey@earthlink.net>; Fri, 8 Aug 2014 14:10:59 -0400 (EDT)
Received: From qpap02pxdu.prod.oclc.org ([132.174.4.254]) by mshieldserver1.oclc.org (WebShield SMTP v4.5 MR3) id 140752100748; Fri, 8 Aug 2014 14:03:27 -0400
Message-ID: <1052376894.1407521007137.JavaMail.prodcon@qpap02pxdu.prod.oclc.org>
Reply-To: "law@loc.gov" <questionpoint@oclc.org>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_Part_3740_201944222.1407521007136"
X-ELNK-Received-Info: spv=0;
X-ELNK-AV: 0
X-ELNK-Info: sbv=0; sbrc=.0; sbf=bb; sbw=000;
X-Antivirus: AVG for E-mail 2014.0.4744 [4007/8003]
X-AVG-ID: ID5F5F96FA-1F2ACA24

##- Please reply above this line. Anything below this line will not be sent in your reply. We do not accept attachments via this reply method -##

Thank you for your question regarding patent and copyright law. Legal advice, interpretation, or analysis (which could be considered the practice of law) are outside of the scope of services provided by the Law Library of Congress; however, we are happy to offer you guidance on how you might go about conducting your own research. You can also get in touch with the Copyright Office at http://copyright.gov/help/, or with the United States Patent and Trademark Office (PTO) at http://www.uspto.gov/about/contacts/index.jsp.

General information about researching patent law can be found on our blog at http://blogs.loc.gov/law/2013/03/patent-law-a-beginners-guide/.   Major legal treatises for matters of copyright and patent law include:

- Chisum on Patents (in our catalog at http://lccn.loc.gov/78070641)

- Moy's Walker on Patents (in our catalog at http://lccn.loc.gov/2004616151)
- Nimmer on Copyright (in our catalog at http://lccn.loc.gov/78109488)
- Patry on Copyright (in our catalog at http://lccn.loc.gov/2007618471)

As a courtesy, we have reviewed *Nimmer on Copyright* and have attached a copy of §2.19, entitled "Copyrightability for Patented Works," which might be useful to your research.

You can locate the above titles (or similar resources) in a library near you using the WorldCat catalog at http://www.worldcat.org. After searching for an item in WorldCat, open the resource's entry, scroll down to the "Find a copy in my library" section, and enter in your zip code. WorldCat will list the closest libraries to you that own that resource. You can then click on the library's name to be taken to the resource's entry in that library's catalog.

You may also be able to find these or other useful resources at a local law library. Law libraries local to your area include the Santa Cruz County Law Library (located in the basement of the County Government Building at 701 Ocean Street, Rm. 070 in Santa Cruz, CA; (831) 420-2205; http://www.lawlibrary.org/) and the Santa Clara County Law Library (located at 360 North First Street in San Jose, CA; (408)299-567; (408)299-3568, http://www.sccll.org/).

Finally, if you would like to learn more about how certain laws have been interpreted and applied by the courts, you could also consult case law on your topic. We recommend conducting this sort of research using the resources available at your local public law library; however, for information on finding case law online, you may want to consult our blog entry at http://blogs.loc.gov/law/2013/02/how-to-locate-free-case-law-on-the-internet/, which includes a video tutorial demonstrating the use of Google Scholar.

We hope this information has been useful and wish you luck with your research.

****

Public Services Division
Law Library of Congress
Library of Congress
101 Independence Ave., SE
Washington, D.C. 20540-3120
Telephone: 202-707-5079
URL: http://www.loc.gov/law

Please take a moment to fill out a survey at: http://www.questionpoint.org/crs/servlet/org.oclc.ask.PatronSurveyForm?&language=1&type=ask&qid=9755163

Question History:

Patron: To Law Library Reading Room:
When the US Government publishes a patent - that creates a set of claims which it assigns control of to a third party - either an individual or group of individuals or other entity under the law.

Does the issueance of this create an implicit copyright against the claims in that patent? This is a VERY important question about Copyright Law and how Patents tie into them.

If not how would a Copyright be issued against a registered patent and its content?

Librarian 1: Thank you for your question regarding patent and copyright law. Legal advice, interpretation, or analysis (which could be considered the practice of law) are outside of the scope of services provided by the Law Library of Congress; however, we are happy to offer you guidance on how you might go about conducting your own research. You can also get in touch with the Copyright Office at http://copyright.gov/help/ [http://copyright.gov/help/] , or with the United States Patent and Trademark Office (PTO) at http://www.uspto.gov/about/contacts/index.jsp [http://www.uspto.gov/about/contacts/index.jsp] .

General information about researching patent law can be found on our blog at http://blogs.loc.gov/law/2013/03/patent-law-a-beginners-guide/ [http://blogs.loc.gov/law/2013/03/patent-law-a-beginners-guide/] . Major legal treatises for matters of copyright and patent law include:

Chisum on Patents (in our catalog at http://lccn.loc.gov/78070641 [http://lccn.loc.gov/78070641])

Moy's Walker on Patents (in our catalog at http://lccn.loc.gov/2004616151 [http://lccn.loc.gov/2004616151])

Nimmer on Copyright (in our catalog at http://lccn.loc.gov/78109488 [http://lccn.loc.gov/78109488])

Patry on Copyright (in our catalog at http://lccn.loc.gov/2007618471 [http://lccn.loc.gov/2007618471])

As a courtesy, we have reviewed Nimmer on Copyright and have attached a copy of §2.19, entitled "Copyrightability for Patented Works," which might be useful to your research.

You can locate the above titles (or similar resources) in a library near you using the WorldCat catalog at http://www.worldcat.org [http://www.worldcat.org] . After searching for an item in WorldCat, open the resource's entry, scroll down to the "Find a copy in my library" section, and enter in your zip code. WorldCat will list the closest libraries to you that own that resource. You can then click on the library's name to be taken to the resource's entry in that library's catalog.

You may also be able to find these or other useful resources at a local law library. Law libraries local to your area include the Santa Cruz County Law Library (located in the basement of the County Government Building at 701 Ocean Street, Rm. 070 in Santa Cruz, CA; (831) 420-2205;

http://www.lawlibrary.org/ [http://www.lawlibrary.org/]) and the Santa Clara County Law Library (located at 360 North First Street in San Jose, CA; (408)299-567; (408)299-3568, http://www.sccll.org/ [http://www.sccll.org/]). Finally, if you would like to learn more about how certain laws have been interpreted and applied by the courts, you could also consult case law on your topic. We recommend conducting this sort of research using the resources available at your local public law library; however, for information on finding case law online, you may want to consult our blog entry at http://blogs.loc.gov/law/2013/02/how-to-locate-free-case-law-on-the-internet/ [http://blogs.loc.gov/law/2013/02/how-to-locate-free-case-law-on-the-internet/] , which includes a video tutorial demonstrating the use of Google Scholar.

We hope this information has been useful and wish you luck with your research.

****

Public Services Division
Law Library of Congress
Library of Congress
101 Independence Ave., SE
Washington, D.C. 20540-3120
Telephone: 202-707-5079
URL: http://www.loc.gov/law

Thank you for contacting the Law Library of Congress. If you wish to send another question to us, please visit our question form at http://www.loc.gov/rr/askalib/ask-law.html.

No virus found in this message.
Checked by AVG - www.avg.com
Version: 2014.0.4744 / Virus Database: 4007/8003 - Release Date: 08/08/14

Attachments:

9755163 - Nimmer - Copyrightability for Patentable Works.pdf	224 KB

§ 2.19 Copyrightability for Patentable Works

There is an overlapping area wherein certain works may claim either copyright or patent protection. This is most apparent with respect to a design that may qualify for copyright as a work of art[1] or as a print or label used for articles of merchandise,[2] or may claim patent protection as a design patent.[3] This may also be true as to scientific or technical drawings.[4] The Supreme Court has held that a work, such as a work of art, may be eligible for either copyright or patent protection.[5] Other courts, both prior[6] and subsequent[7] to the Supreme Court's decision, have similarly held, although one older decision is to the contrary.[8]

The more difficult question is whether a work remains eligible for copyright if a patent has in fact been obtained for the work. In *Mazer v. Stein*,[9] the Supreme Court expressly declined to decide whether an election to obtain a patent bars the subsequent right to obtain copyright, or *vice versa*. However, one court had previously held that filing for a patent constitutes a publication that divests the claimant of copyright protection.[10] This holding was not followed in a more recent case[10.1] and is questionable in light of the now prevailing view that placing a work in a public file does not *per se* constitute a publication.[11] Further, it would seem that, in any event, such a result might be avoided simply by placing a copyright notice on the copy of the work that is filed with the Patent and Trademark Office.[11.1]

[1] See § 2.08[B] *supra.*

[2] See § 2.08[G] *supra.*

[3] 35 U.S.C. § 171 *et. seq.*

[4] See § 2.08[D] *supra.*

[5] Mazer v. Stein, 347 U.S. 201 (1954).

[6] William A. Meier Glass Co. v. Anchor Hocking Glass Corp., 95 F. Supp. 264 (W.D. Pa. 1951); Jones Bros Co. v. Underkoffler, 16 F. Supp. 729 (M.D. Pa. 1936).

[7] Vacheron & Constantin-Le Coultre Watches, Inc. v. Benrus Watch Co., 260 F.2d 637 (2d Cir. 1958); *In re* Deister Co., 289 F.2d 496 (C.C.P.A. 1961). Cf. Midway Mfg. Co. v. Artic Int'l, Inc, 704 F.2d 1009 (7th Cir. 1983), *cert. denied,* 464 U.S. 823 (1983).

[8] Taylor Instrument Co. v. Fawley-Brost Co., 139 F.2d 98 (7th Cir. 1943).

[9] 347 U.S. 201 (1954).

[10] Korzybski v. Underwood & Underwood, 36 F.2d 727 (2d Cir. 1929).

[10.1] Zachary v. Western Publishing Co., 75 Cal. App. 3d 911, 143 Cal. Rptr. 34 (1977), relying in part upon that portion of § 8 of the 1909 Act, which provides that "publication . . . by the Government . . . shall not be taken to cause any abridgement or annulment of the copyright . . ." *Zachary* holds that a common law copyright is not lost by reason of a public filing that occurs as a part of the procedure for obtaining a design patent.

[11] See § 4.10 *infra.* Vacheron & Constantin-Le Coultre Watches, Inc. v. Benrus Watch Co., 260 F.2d 637 (2d Cir. 1958), suggests (although it does not so hold) that the doctrine of the *Korzybski* case cited in N. 10 *supra* may no longer be valid law.

[11.1] Even voluntarily omitting a copyright notice from a patent application has been held to have essentially no impact on an infringement claim. See Kohus v. Mariol, 328 F.3d 848, 859 (6th Cir. 2003) (construing 37 C.F.R. § 171.1(d) as making such notices permissive).

Moreover, it is now clear that if a copyright is first obtained, the claimant is not thereby barred from subsequently also obtaining a design patent in the same work.[12] Thus, in the context of obtaining a design patent, it has been held that the doctrine requiring an election between patent and copyright protection "is in direct conflict with the clear intent of Congress manifested in the two [patent and copyright] statutory provisions. . . ."[13] A more limited approach has been suggested in one copyright case,[14] which case indicates that, even if a patent has been issued, if such patent is subsequently found to be invalid, then copyright protection should be available.

Without offering the rationale of publication or any other basis, Copyright Office Regulations, under the 1909 Act, simply provided that once a patent has been issued, copyright registration would be denied to a work of art[15] and to a scientific or technical drawing.[16] There appears to be no statutory or other justification for this position, It would seem, on principle, that if a work otherwise meets the requirements of copyrightability, it should not be denied such simply because the claimant happens to be entitled to supplementary protection under other legislation.[17]

Notwithstanding that logic, the same regulation continued under the 1976 Act following its enactment. But in 1995, the Register of Copyrights looked at the issue afresh. Quoting in full the preceding paragraph, the Copyright Office concluded: "We agree."[18] Accordingly, the Office rescinded the election doctrine, and now allows copyright registration of matter over which patent

[12] Application of Yardley, 493 F.2d 1389 (C.C.P.A. 1974).

[13] *Id.* See also Application of Penthouse Int'l, Ltd., 565 F.2d 679 (C.C.P.A. 1977) (copyright, patent and trademark laws are not mutually exclusive); Schnadig Corp. v. Gaines Mfg. Co., 620 F.2d 1166 (6th Cir. 1980) ("Both copyright and design patents can be used in some circumstances to protect the design of useful articles.") It is not entirely clear from the context of the foregoing statement in *Schnadig* whether "both" was intended cumulatively or in the alternative.

[14] See Vacheron & Constantin-Le Coultre Watches, Inc. v. Benrus Watch Co., 260 F.2d 637 (2d Cir. 1958) (the precise holding involved the reverse situation of an unenforcible copyright and a consequently valid patent).

[15] 37 C.F.R. § 202.10(b) (1959). Clarke v. G.A. Kayser & Sons, Inc., 472 F. Supp. 481 (W.D. Pa. 1979), *aff'd mem.*, 631 F.2d 725 (3d Cir. 1980), questioned whether § 202.10(b) is limited in its application to design patents, or also includes utility patents. The court ignored the regulation cited in the next footnote.

[16] 37 C.F.R. § 202.12(c) (1959).

[17] 17 U.S.C. § 301(d). See § 1.01[D] *supra.* Barton Candy Corp. v. Tell Chocolate Novelties Corp., 178 F. Supp. 577 (E.D.N.Y. 1959), suggests that a copyright may be claimed on a work for which a patent has theretofore expired. See Knickerbocker Toy Co. v. Winterbrook Corp., 554 F. Supp. 1309 (D.N.H. 1982).

[18] 60 Fed. Reg. 15,605 (March 14, 1995) (Treatise quoted).

protection may be simultaneously claimed.[19] One court expresses doubt whether the election doctrine ever represented good law.[20]

§ 2.20 Berne-Era Architectural Works

[A] Architectural Features

We have already seen in a previous section that United States copyright law prior to the Berne era did not accord protection to structures, except those few that served no utilitarian purpose.[1] With United States' accession to the Berne Convention, the question arose whether that exclusion of useful structures from copyright protection complied with Berne strictures. The "literary and artistic works" for which Berne commands protection include "three-dimensional works relative to . . . architecture,"[2] separate and distinct from the requirement, also contained in the same paragraph of the Convention, that protection extend to "illustrations, maps, plans, sketches and three-dimensional works relative to . . . architecture."[3] On that basis, pre-BCIA law on the subject was incompatible with Berne.[4] Aware of the discrepancy, Congress chose, nonetheless, to leave existing United States law on the subject unaltered when it enacted the BCIA.[5] However, in connection with passage of the BCIA, the Senate Judiciary Committee asked the Copyright Office to undertake an in-depth study by January 2, 1989, evaluating whether the level of protection for architectural works should be increased.[6] When that report recommended redress of this continuing

[19] "The availability of protection or grant of protection under the law for a utility or design patent will not affect the registrability of a claim in an original work of pictorial, graphic, or sculptural authorship." 37 C.F.R. § 202.10(a) (1995). Note that the 1995 recension eliminates former paragraphs (a) and (b) from this regulation.

[20] Dam Things from Denmark v. Russ Berrie & Co., 173 F. Supp. 2d 277, 283–284 (D.N.J. 2001) *rev'd on other grounds*, 290 F.3d 548 (3rd Cir. 2002). In that case, plaintiff attempted to restore copyright protection in a work adjudicated in 1965 to be in the public domain due to a notice defect. See § 9A.04[A][2] *infra*. Defendant ingeniously argued the work was previously ineligible for copyright protection not based on the absence of copyright notice, but because it held a 1961 design patent. *Id.* at 283. The court's rejection of that argument arguably requires the construction that the election doctrine was inapplicable not only in 1995 when the Copyright Office so declared, but in 1961 as well.

[1] See § 2.08[D][2][b] *supra*.

[2] Berne Convention (Paris text), art. 2(1).

[3] *Id.* See H.R. Rep. No. 101-735, 101st Cong., 2d Sess. 11 (1990). The two forms of protection are cumulative, and can form the basis for separate causes of action (albeit not cumulative damages) if appropriate. See § 2.08[D][2][a] N. 163.4 *supra*.

[4] *Final Report of Ad Hoc Working Group on U.S. Adherence to the Berne Convention*, 10 Colum.-VLA J. L. & Arts 513, 603, 607–609 (1986).

[5] See H. Rep. (BCIA), pp. 49–51 & ns.117–118 (Treatise cited); S. Rep. (BCIA), p. 39. The Copyright Office's solution to this discrepancy was, simultaneous with Berne adherence, to add a new paragraph to 17 U.S.C. § 102(a) to accord explicit protection to architectural works. *Copyright Office Draft Discussion Bill*, 10 Colum.-VLA J. L. & Arts 621, 629 (1986). That approach was not adopted when the United States joined the Berne Union in 1989.

[6] S. Rep. (BCIA) at 9.